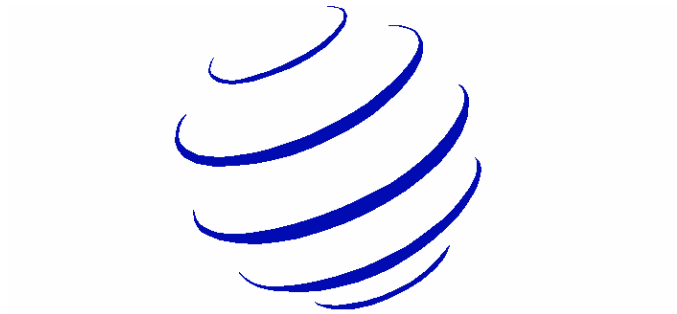

MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó
Korlátolt Felelősségű Társaság

Szolgáltatási Szabályzat
Fokozott Biztonságú Elektronikus Aláírás Hitelesítés-szolgáltatáshoz
(HSZSZ-F)

Verziószám	**2.0**
Objektum azonosító (OID)	**1.3.6.1.4.1.14868.1.1.2**
Hatósági nyilvántartásba vétel napja	**2005. október 26.**
Hatósági nyilvántartásba vétel száma	**HL-15400-3/2005.**
Hatálybalépés dátuma	**2005. október 26.**

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 verziók

Verzió	Dátum	A változás leírása	Készítette
1.0	2002.09.30	A fokozott biztonságú szolgáltatói regisztrálásra előkészített változat	Bodlaki Ákos
1.1	2002.11.29	A HIF észrevételeivel javított változat	Bodlaki Ákos
1.2	2003.03.31.	A fokozott biztonságú szolgáltatás kezdeti gyakorlata alapján javított változat	Bodlaki Ákos
1.3	2003.07.30	Formai és sajtóhibák javításával, szakértői észrevételek alapján felülvizsgált és javított változat	Néder Ferenc
2.0	2005. 08. 19.	Felülvizsgált, átdolgozott változat	Néder Ferenc

TARTALOMJEGYZÉK

1. Bevezetés 6
1.1 Szolgáltató adatai 6
1.2 Alapok 6
1.2.1 Szabályzat célja 6
1.2.2 Jogszabályok, szabványok, ajánlások 7
1.3 HSZSZ-F azonosítás 7
1.4 Hitelesítés szolgáltató és felhasználó közösség, alkalmazhatóság 7
1.4.1 A Szolgáltató egységei 8
1.4.2 Felhasználók 8
1.4.3 Alkalmazhatóság 8
1.5 Tanúsítványok jellemzői 9
1.5.1 Tanúsítványok fajtái és tulajdonságaik 9
1.5.2 Tanúsítványtípusok 9
2. Általános rendelkezések 11
2.1 Kötelezettségek 11
2.1.1 A Szolgáltató kötelezettségei 11
2.1.2 Az Előfizető és az Aláíró feladatai és hatásköre 12
2.1.3 Az Érintett félre vonatkozó ajánlások 12
2.2 Felelősségek 12
2.2.1 A Szolgáltató felelőssége 12
2.2.2 Az Előfizető és az Aláíró felelőssége 13
2.2.3 Az Érintett fél felelőssége 13
2.2.4 Az anyagi felelősség korlátai 13
2.3 Értelmezés és alkalmazás 13
2.3.1 Irányadó jog 13
2.3.2 Érvénytelenség, hatályosság, megszűnés, értesítések 14
2.3.3 Vitás kérdések kezelése 14
2.4 Díjak 14
2.4.1 Tanúsítvány kibocsátás és megújítás 14
2.4.2 Tanúsítvány hozzáférés 14
2.4.3 Visszavonás és állapot információ hozzáférés 14
2.4.4 Egyéb szolgáltatásokra vonatkozó díjak 14
2.4.5 Visszatérítési elvek 15
2.5 Közzététel 15
2.5.1 Szolgáltatói információk közzététele 15
2.5.2 A közzététel gyakorisága 15
2.5.3 Tanúsítványtár 15
2.5.4 Elérési szabályok 15
2.6 A megfelelőség vizsgálata 15
2.7 Bizalmasság – adatkezelési szabályok 16
2.7.1 Bizalmas adatok, információk 16
2.7.2 Nem bizalmas információk 16
2.7.3 Tanúsítvány visszavonási és felfüggesztési okok felfedése 16
2.7.4 Feltárás törvényi meghatalmazással rendelkezők részére 16
2.7.5 Feltárás bírósági meghatalmazással rendelkezők részére 16
2.7.6 Feltárás tulajdonos kérésére 16
2.7.7 Feltárás más esetekben 17
2.8 Szellemi tulajdonhoz fűződő jogok 17
3. Azonosítás és hitelesítési eljárások 18
3.1 Regisztráció 18
3.1.1 Nevek típusa 18
3.1.2 Nevek szemantikája 18
3.1.3 Nevek egyedisége 18

3.1.4 Név igénylési viták feloldása 18
3.1.5 Védjegyek elismerésének és hitelesítésének módszere 18
3.1.6 Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere 18
3.1.7 Regisztráció „Személyes" típusú tanúsítvány igénylése esetén 18
3.1.8 Regisztráció „Szervezeti" típusú tanúsítvány igénylése esetén 19
3.1.9 Regisztráció „Eszköz" tanúsítvány igénylése esetén 19
3.2 Érvényes tanúsítvány megújítása (tanúsítvány frissítése) 20
3.3 Érvénytelen tanúsítvány megújítása 20
3.4 Felfüggesztés és visszavonási kérés 20
4. A működésre vonatkozó követelmények 20
4.1 Tanúsítványigénylés 20
4.2 Tanúsítvány kibocsátás 21
4.3 Tanúsítvány elfogadás 21
4.4 Tanúsítvány visszavonás és felfüggesztés 21
4.4.1 Visszavonáshoz/felfüggesztéshez vezető körülmények 21
4.4.2 Visszavonás/felfüggesztés kérelmezése 22
4.4.3 Visszavonási eljárás 22
4.4.4 Visszavonási kérelemre vonatkozó türelmi idő 22
4.4.5 Felfüggesztési eljárás 22
4.4.6 Felfüggesztett állapotra vonatkozó korlátozások 23
4.4.7 Visszavont tanúsítványok Listája (CRL) és kibocsátásának gyakorisága 23
4.4.8 Visszavont Tanúsítványok Listája ellenőrzési követelmények 23
4.4.9 Visszavonási állapot közlés más formái 23
4.4.10 Magánkulcs kompromittálódás speciális követelményei 23
4.5 Biztonsági naplózások, archívum 23
4.5.1 Naplózott esemény típusok 23
4.5.2 Napló adatok tárolása 24
4.5.3 Adatarchiválás 24
4.5.4 Az archívum megőrzési időtartama 24
4.5.5 Az archívum védelme 24
4.6 Katasztrófa elhárítás 24
4.6.1 A hitelesítés-szolgáltatás azonnali felfüggesztése 24
4.6.2 Üzletmenet-folytonossági Terv 24
4.7 A hitelesítés-szolgáltatási tevékenység megszüntetése 24
5. Fizikai, eljárásrendi és humán biztonsági szabályozások 25
5.1 Fizikai biztonsági szabályozások 25
5.1.1 Hitelesítő Központok 25
5.2 Eljárásrendi szabályozások 25
5.3 Humán szabályozások 25
6. Műszaki biztonsági óvintézkedések 26
6.1 Kulcspár előállítás és telepítés 26
6.1.1 Kulcspár előállítás 26
6.1.2 Az aláírás-létrehozó adat eljuttatása az Aláíróhoz (Előfizetőhöz) 26
6.1.3 Az Aláírók aláírás-ellenőrző adatának eljuttatása az érintett felekhez 26
6.1.4 A Szolgáltató aláírás-ellenőrző adatainak eljuttatása a felhasználói közösséghez 26
6.1.5 Kulcsméretek, használt algoritmusok 26
6.1.6 Kulcs felhasználási célok 26
6.2 Aláírás-létrehozó adat védelme 27
6.2.1 Kriptográfiai modulra vonatkozó szabványok 27
6.2.2 A többszereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése 27
6.2.3 Aláírás-létrehozó adat letét, mentés, archiválás 27
6.2.4 Aláírás-létrehozó adat aktiválása 27
6.2.5 Aláírás-létrehozó adat deaktiválása 27
6.2.6 Aláírás-létrehozó adat megsemmisítése 27
6.3 Az előfizetői tanúsítványok megőrzése 27

6.4 Aktiválási adatok (PIN kódok) 27
6.5 Számítógép biztonsági szabályok 27
6.6 Életciklus technikai szabályok 28
6.6.1 Rendszerfejlesztési szabályok 28
6.6.2 Biztonságkezelési szabályok 28
6.7 Hálózati biztonsági szabályok 28
6.8 Kriptográfiai modul ellenőrzése 28
7. Tanúsítvány és tanúsítvány-visszavonási profil 29
7.1 Tanúsítvány profil 29
7.1.1 Alap mezők 29
7.2 Tanúsítvány kiterjesztések 29
7.3 Tanúsítvány-visszavonási profil 29
8. A szolgáltatási szabályzat adminisztrációja 30
8.1 Változáskezelés 30
8.1.1 Változtatási eljárások 30
8.1.2 Észrevételek kezelése 30
8.2 Közzétételi és tájékoztatási elvek 30
8.2.1 A HSZSZ-F-ben nem tárgyalt elemek 30
8.2.2 A HSZSZ-F közzététele 30
8.3 Elfogadási eljárások 30
9. Hivatkozások és fogalom-meghatározások 31
9.1 Hivatkozások 31
9.2 Fogalom-meghatározások 32

1. Bevezetés

A jelen Szolgáltatási Szabályzat (továbbiakban: HSZSZ-F) a MÁV INFORMATIKA Kft. (továbbiakban Szolgáltató) fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatására vonatkozó működési szabályokat és eljárásrendet tartalmazza.

A Szolgáltató szolgáltatásait a vele előfizetői szerződéses viszonyban álló Előfizetők részére szolgáltatja.

A hitelesítés-szolgáltatás keretében a Szolgáltató a 2001. évi XXXV. törvényben (a továbbiakban: Eat.) meghatározott szolgáltatások közül a következőket nyújtja:

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

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

A HSZSZ-F további fejezeteiben a „*szolgáltatások*” kifejezés alatt a fenti részszolgáltatások közül bármelyik vagy mindkettő együtt értendő.

1.1 Szolgáltató adatai

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

Cégjegyzék szám: 01-09-563711

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

Telefonszám: (36-1) 457-9300

Telefax szám: (36-1) 457-9500

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

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

Illetékes fogyasztóvédelmi felügyelőség:

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

Kapcsolat az ügyfelekkel:

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

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

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

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

A tanúsítványok felfüggesztésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) ad. Az Ügyfélszolgálat elérhető a +36 80 39-93-93-as zöldszámon, a +36-1-457-93-93 közvetlen számon, a +36-1-457-93-00 központi számon, valamint elektronikus levélben a *helpdesk@mavinformatika.hu* címen.

Panaszok bejelentésének helye:

a. személyesen az Ügyfélkapcsolati Irodákban

b. írásban a Szolgáltató székhelyére címezve

c. telefonon az Ügyfélkapcsolati Irodákban vagy az Ügyfélszolgálatnál

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

1.2 Alapok

1.2.1 Szabályzat célja

Jelen HSZSZ-F célja, hogy összefogja azokat a szabályokat, adatokat és információkat, melyeket a Szolgáltató hitelesítés szolgáltatásával valamilyen módon kapcsolatba kerülő feleknek ismerni kell vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát, és lehetővé teszi a szolgáltatást igénybe vevők számára, hogy megállapítsák azt, hogy az ismertetett szolgáltatási gyakorlat, valamint a kibocsátott tanúsítványok mennyiben felelnek meg az elvárásaiknak. A HSZSZ-F és egyéb, a HSZSZ-F-ben hivatkozott dokumentumok, ajánlások, szabványok tartalmának megismerése után, a tanúsítvány elfogadóinak egyértelműen meg kell tudni állapítani a tanúsítvány kezelésének módját, az általa garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelősségvállalásokat.

1.2.2 Jogszabályok, szabványok, ajánlások

A Szolgáltató által nyújtott szolgáltatásokra elsősorban a következő jogszabályok mérvadók:

2001. évi XXXV. törvény az elektronikus aláírásról (Eat.)

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

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

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

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

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

Hivatkozott ajánlások, szabványok:

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

Internet Közösség RFC 2459, RFC 2527 és RFC 3039 ajánlásai

Európai Unió ETSI TS 101 456 és ETSI TS 101 862 szabványok

NIST FIPS 140-1 Level 1-3

American Bar Association (ABA) PKI Assessment Guidelines (PAG)

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

MeH ITB 12. ajánlás, ITSEC, Common Criteria

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

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

1.3 HSZSZ-F azonosítás

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

A dokumentum neve:	Szolgáltatási Szabályzat Fokozott Biztonságú Elektronikus Aláírás Hitelesítés-szolgáltatáshoz. A jelen dokumentumban és a kapcsolódó szabályzatokban HSZSZ-F-ként történik rá hivatkozás.
PKI szoftver technikai azonosító:	T&S PCAV1.0
Első hatálybalépés időpontja	2002. november 18.

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

A jelen szabályzat a következő tanúsítványok kezelését írja le:

Nyilvános körben kibocsátott nem minősített tanúsítvány (NMT)

OID: 1.3.6.1.4.1.14868.2.1.0

A HSZSZ-F a Szolgáltató ügyfélkapcsolati irodáiban és a Szolgáltató Internetes honlapján érhető el. Jelen HSZSZ-F-nek csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

1.4 Hitelesítés szolgáltató és felhasználó közösség, alkalmazhatóság

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösséget a következők alkotják:

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

1.4.1 A Szolgáltató egységei

1.4.1.1 Ügyfélkapcsolati Irodák

Az Ügyfélkapcsolati Irodák (rövidítve: ÜKI) a Szolgáltató és a vele szerződéses alapon együttműködő Társaságok (mint szerződött közreműködők) azon szervezeti egységei, amelyek az előfizetői tanúsítvány kérelmek összeállítását és az elkészült tanúsítványok átadását végzik, valamint az adminisztrációs feladatokat látják el.

1.4.1.2 Regisztrációs Iroda

A Regisztrációs Iroda (rövidítve: RA) a szolgáltatás keretein belül biztosítja az előfizetők technikai regisztrációját, a tanúsítványok felfüggesztés és visszavonás kezelését és az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezését.

1.4.1.3 Hitelesítő Központ

A Hitelesítő Központ (rövidítve: CA) a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata az aláírás létrehozó adatok és tanúsítványok előállítása, a tanúsítványok közzététele.

1.4.2 Felhasználók

1.4.2.1 Előfizető, Aláíró

Előfizető a Szolgáltatóval, az Általános Szerződési Feltételekben (továbbiakban: ÁSZF-F) és az Előfizetői Szerződésben foglaltak szerint szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató tanúsítványt bocsát ki.

Az Előfizető mint természetes személy egyben Aláíró is, amennyiben saját maga birtokolja és használja az aláírás-létrehozó adatot.

Az Előfizető lehet jogi személy vagy jogi személyiség nélküli szervezet is. Az Aláíró(k) ebben az esetben a szervezet munkatársa(i) vagy informatikai eszköze(i).

1.4.2.2 Érintett fél

Az Érintett fél (Aláírás Ellenőrző) olyan természetes vagy jogi személy, aki az elektronikus dokumentum fogadója, és egy tanúsítvánnyal hitelesített elektronikus aláírásra hagyatkozva jár el.

1.4.3 Alkalmazhatóság

1.4.3.1 Szabályzat hatálya

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

A HSZSZ-F személyi hatálya a felhasználó közösségre terjed ki.

A HSZSZ-F tárgyi hatálya a következőkre terjed ki:

a. az 1. pontban meghatározott szolgáltatásokra,

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

1.4.3.2 Szolgáltatás szintje

A Szolgáltató szolgáltatásait jelen szabályozás keretében az Eat. 2.§. 15. pontjában meghatározott **fokozott biztonságú elektronikus aláírás** hitelesítéséhez nyújtja.

1.4.3.3 Tanúsítványok alkalmazhatósága

A tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

Engedélyezett alkalmazási lehetőségek:

- **A kibocsátott magánkulcsok az elektronikus aláírások megtételére használhatók fel.**
- **A nyilvános kulcsok a tanúsítványok aláírásának ellenőrzésére használhatók fel.**

Korlátozott alkalmazási lehetőségek:

- Szolgáltató az előfizetői szerződésben felhasználási, területi, pénzügyi, stb. korlátozásokat szabhat. A korlátozásokat a kibocsátott előfizetői tanúsítványban is megadja.
- Az Előfizető szervezet élhet korlátozásokkal Aláíró és érintett felek tanúsítvány felhasználási tevékenységével kapcsolatosan.

Tiltott alkalmazási lehetőségek:

- **A Szolgáltató és az Előfizető eltérő megállapodásának hiányában tilos az előfizetői magánkulcs felhasználása más nyilvános kulcsú tanúsítványok aláírására, vagy az előfizetői tanúsítványok alkalmazása bármilyen hitelesítés szolgáltatás nyújtásához.**

A fentiek alapján a kibocsátott tanúsítványok (illetve az ezekhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, amelyek támogatják a PKI technológián alapuló elektronikus aláírási, azonosítás-

hitelesítési és letagadhatatlansági funkciókat. Az elektronikus aláírás-hitelesítés céljából kibocsátott tanúsítványt és a tanúsítványhoz kapcsolódó kulcspárt kizárólag aláírás létrehozására, illetve annak ellenőrzésére lehet felhasználni az Eat. értelmében, betartva a tanúsítványokban található esetleges egyéb korlátozásokat is.

A Szolgáltató nem vállal felelősséget az elektronikus aláírásra kibocsátott tanúsítványok és kulcspárok titkosításra történő, vagy más, az elektronikus aláírástól eltérő felhasználásáért.

A tanúsítvány használati információk a tanúsítványban is rögzítésre kerülnek. Az eltérő használat az Aláíró egyéni felelőssége és kockázata, ahogy az ilyen módon felhasznált tanúsítvány elfogadása az érintett fél (Aláírás Ellenőrző) felelőssége és kockázata.

1.5 Tanúsítványok jellemzői

A jelen HSZSZ-F a fokozott biztonságú elektronikus aláíráshoz nyilvános körben kibocsátott - nem minősített - tanúsítványokat (NMT) és az ezekkel kapcsolatos szabályokat írja le.

A tanúsítványok felhasználási területe és célja szerint megkülönböztetünk:

- Előfizetői,
- szolgáltatói és
- teszt tanúsítványokat.

A felhasználási területen belül a következő tanúsítványokat különböztetjük meg:

- „személyes” tanúsítványokat
- „szervezeti” vagy „Munkatársi” tanúsítványokat
- „eszköz” tanúsítványokat.

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

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

1.5.1 Tanúsítványok fajtái és tulajdonságaik

Szolgáltató a jelen HSZSZ-F szabályozása keretében Nem Minősített Tanúsítványokat kezel. A Nem Minősített Tanúsítvány a CWA 14167-1:2001 szerint az Európai Unió 1999/93. direktívájának (a továbbiakban: Direktíva) 5.2 cikkelyével összhangban levő elektronikus aláírást tanúsítja. A direktíva 5.2 cikkelye kimondja, hogy a Tagállamoknak biztosítani kell, hogy egy elektronikus aláírás jogi eljárásban nem utasítható vissza, mint törvényesen hatályos és elfogadható bizonyíték csupán azon az alapon, mert az

a. elektronikus formában létezik, vagy mert az
b. nem minősített tanúsítványra alapozott, vagy mert az
c. nem egy akkreditált hitelesítés-szolgáltató által kibocsátott minősített tanúsítványra alapozott, vagy mert azt
d. nem biztonságos aláírás-létrehozó eszközzel (BALE) hozták létre.

1.5.1.1 Előfizetői tanúsítvány

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

Az Előfizetői tanúsítványok objektum-azonosítója (OID): 1.3.6.1.4.1.14868.2.1.0

1.5.1.2 Szolgáltatói tanúsítvány

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

A Szolgáltatói tanúsítványok objektum-azonosítója (OID): 1.3.6.1.4.1.14868.2.1.1

1.5.1.3 Teszt tanúsítvány

A Szolgáltató teszt tanúsítványokat kizárólag tesztelési célokból ad ki.

A teszt aláírást létrehozó adatok az Aláírók által semmilyen olyan célra nem használhatók, amelynél az átvitt adatok hitelességének vagy sértetlenségének sérüléséből vagy elvesztéséből, az aláírás-létrehozó adat vagy eszköz illetéktelen kezekbe történő jutásából az Aláírónak bármilyen kára származna. Teszt tanúsítványok használatából eredő károkért a Szolgáltató semmilyen felelősséget nem vállal.

A Teszt tanúsítványok azonosíthatók az alapján, hogy a tanúsítványok „Common Name” (CN) és „Title” mezőjében megtalálható a ’teszt’ vagy ’Teszt’ szövegrészlet.

A Teszt tanúsítványok objektum-azonosítója (OID): 1.3.6.1.4.1.14868.2.1.2

1.5.2 Tanúsítványtípusok

A Szolgáltató a Szolgáltatói és Teszt tanúsítványok tekintetében nem alkalmaz típus-megkötést.

A Szolgáltató a következőkben meghatározott Előfizetői tanúsítványokat adhatja ki:

1.5.2.1 „Személyes" tanúsítvány

Személyes tanúsítványokat természetes személy igényelhet a saját nevében. A személyes tanúsítvány esetében az Előfizető és az Aláíró jellemzően ugyanaz a személy.

A tanúsítvány „Country" és „Locality" mezőjében az Előfizető lakóhelyének országkódja és helységneve, az „E" mezőben az Előfizető e-mail címe, a „Common Name" (CN) mezőben az igénylő neve vagy álneve szerepel. A tanúsítvány „Organization" és „Organization Unit" mezői üresen maradnak.

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

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

1.5.2.2 „Szervezeti" vagy „Munkatársi" tanúsítvány

„Szervezeti" vagy „Munkatársi" tanúsítványokat jogi személy vagy jogi személyiség nélküli szervezet igényelhet munkatársai, tisztségviselői vagy a szervezet illetve annak alszervezetei számára. A szervezet - egyebek mellett - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány, stb. Az Előfizető ebben az esetben a szervezet, az Aláíró pedig a szervezet munkatársa.

A tanúsítvány „Country" és „Locality" mezőjében az igénylő szervezete telephelyének országkódja és városa, az „Organization" mezőben a szervezetének neve, az „Organizational Unit" mezőben az igényt támasztó szervezeti egység neve, az „E" mezőben a szervezet, alszervezet vagy szervezeti személy e-mail címe, a „Common Name" (CN) mezőjében az aláíró személy, szervezet vagy alszervezet neve szerepel.

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

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

1.5.2.3 Eszköz tanúsítvány

Eszköz tanúsítványt természetes személy vagy szervezet igényelhet az általa működtetett informatikai eszköz részére. Tipikus eszközök: web szerver, WAP szerver, VPN, stb.

A tanúsítvány „Country" és „Locality" mezőjében a szervezet telephelyének országkódja és városa, az „Organization" mezőben a szervezet neve (ha van ilyen), az „Organizational Unit" mezőben a szervezeti egység neve (ha van ilyen), az „E" mezőben az Előfizető e-mail címe, a „Common Name" mezőjében az eszköz neve szerepel.

Szerver tanúsítványok esetében a tanúsítvány Title mezője a 'szerver' vagy 'Szerver' szöveget tartalmazza.

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

2. Általános rendelkezések

2.1 Kötelezettségek

2.1.1 A Szolgáltató kötelezettségei

1. A Szolgáltató gondoskodik a szolgáltatásra vonatkozó valamennyi, a jelen HSZSZ-F-ben részletezett feltétel teljesüléséről, amennyiben azok az adott tanúsítványtípusra alkalmazhatók.
2. A Szolgáltató szolgáltatásait nyilvánosan elérhetővé teszi.
3. A Szolgáltató jogi személy.
4. A Szolgáltató HSZSZ-F-ét rendszeresen felülvizsgálja.
5. A Szolgáltató mindenkor az Előfizető által átadott és az Ügyfélkapcsolati Irodák által ellenőrzött adatok alapján bocsátja ki a tanúsítványokat.
6. A Szolgáltató a tanúsítvány kibocsátását követően a tanúsítvány adataiban nem változtathat.
7. A Szolgáltató kötelezettséget vállal arra, hogy az előfizető regisztrációját követően a tanúsítvány kiadására intézkedik és erről az Előfizetőt értesíti. Tanúsítvány kiállítására ezt követően legkésőbb 30 naptári napon belül kerül sor.
8. A Szolgáltató a szolgáltatások működtetése és menedzselése során az ügyfélkapcsolati tevékenységet Ügyfélkapcsolati Irodák által biztosítja.
9. A Szolgáltató Ügyfélszolgálata folyamatos felügyeletet biztosít a tanúsítvány visszavonási és felfüggesztési igények kezelésére.
10. A Szolgáltató vezeti és az Internetes honlapján keresztül bárki számára folyamatosan elérhetővé teszi a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó saját szabályzatait.
11. A Szolgáltató az érvényes tanúsítványok tekintetében a lejárat előtti 30 napban értesítést küld a lejáró tanúsítványokról az Előfizető részére.
12. Szolgáltató a tanúsítványban feltünteti az Előfizetői Szerződésben vagy más szabályozásban rögzített, a tanúsítvány felhasználhatóságával kapcsolatos korlátozásokat.
13. A Szolgáltató indokolt esetben felfüggeszti vagy visszavonja a tanúsítvány érvényességét és ezt a szolgáltatás honlapján közzéteszi.
14. Szolgáltató megőrzi a tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetőleg – amennyiben ezen időszakban az elektronikus aláírással vagy az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.
15. A Szolgáltató tevékenységi köréből csak az új tanúsítvány kibocsátást szüneteltetheti. A tanúsítvány megújítás technikai okokból ebben az értelemben szintén új tanúsítvány kibocsátásnak minősül.
16. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről legalább hatvan nappal korábban értesíti az Előfizetőket és a Nemzeti Hírközlési Hatóságot.
17. A Szolgáltató intézkedik az iránt, hogy legkésőbb a tevékenysége befejezésekor más - vele legalább azonos besorolású - szolgáltató átvegye nyilvántartásait, így különösen a visszavont tanúsítványok nyilvántartását, valamint ellássa a hatályos jogszabályokban foglalt feladatokat. A Szolgáltató a visszavont tanúsítványokkal kapcsolatos minden adatot - beleértve a személyes adatokat is – átadja ezen szolgáltatónak.

2.1.1.1 Az Ügyfélkapcsolati Iroda feladatai és hatásköre

1. Felveszi a regisztráció során az előfizető adatait és elkészíti az előfizetői szerződést,
2. összegyűjti, illetve meghatározza a tanúsítványba kerülő adatokat,
3. megőrzi a nyilvántartásokat,
4. bizalmas információként kezeli az Előfizető és az Aláíró minden adatát, kivéve azokat, amelyeket a tanúsítványba kerülnek,
5. gondoskodik az aláírás-létrehozó eszköz és a PIN kód biztonságos kezeléséről és az Előfizetőnek történő biztonságos átadásáról,
6. a tanúsítvány kezelési eljárások során korlátozás nélkül biztosítja az Aláíró számára a rá vonatkozó regisztrációs és egyéb adatokhoz történő hozzáférést,
7. fogadja a tanúsítvány visszavonásra, felfüggesztésre, vagy a felfüggesztés megszüntetésére vonatkozó kérelmeket,
8. felfüggesztési/visszavonási kérelem elfogadása után intézkedik a tanúsítvány felfüggesztéséről/visszavonásáról,
9. tájékoztatja a visszavont, illetve felfüggesztett tanúsítvány tulajdonosát tanúsítványa állapotának változásáról.
10. fogadja az Aláíró adatainak változására vonatkozó kérelmeket.

2.1.2 Az Előfizető és az Aláíró feladatai és hatásköre

Az Előfizető és az Aláíró kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybe vétele során. Ennek során az Előfizető és az Aláíró köteles:

1. a tanúsítvány igénylését és az aláíró eszközének felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse,
2. az Előfizető a regisztráció során a tanúsítvány kiadásához szükséges adatokat ellenőrizni,
3. az Aláíró saját érdekében biztosítani az aláírás-létrehozó eszközének és PIN kódjának védelmét,
4. az Előfizető, illetve az Aláíró 3 (három) munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a tanúsítványba foglalt adatokra,
5. az Előfizető az Aláíró figyelmét külön felhívni arra, ha az Előfizetői Szerződés a tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat tartalmaz,
6. az Aláíró tudomásul venni, hogy magánkulcsának védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
7. az Aláíró azonnal intézkedni tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben
   7.1. tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, tartalmában, a regisztrációs adatokban pontatlanság van, illetve azokban változás következett be,
   7.2. 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,
8. az Aláíró vagy az Előfizető az elektronikus aláírással ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót.

Ezeken kívül:

9. az Aláíró jogosult arra, hogy a magánkulcsot birtokolja és a jogszabályokban meghatározott módon elektronikus aláíráshoz saját, illetve szervezete nevében felhasználja,
10. az Aláíró tudomásul veszi, hogy a magánkulcsával készített elektronikus aláírás a saját elektronikus aláírásának minősül, és viseli ennek jogkövetkezményeit,
11. az Aláíró a tanúsítványt csak a HSZSZ-F-nek, valamint a hatályos jogszabályi rendelkezéseknek megfelelően használhatja.

2.1.3 Az Érintett félre vonatkozó ajánlások

2.1.3.1 Az Érintett fél számára ajánlott az aláírás ellenőrzése során

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

1. ajánlott elvégeznie az Elektronikus aláírás ellenőrzését, az ún. tanúsítási lánc vizsgálatával az alábbiak szerint:
   1.1. az Aláíró tanúsítványának segítségével meggyőződni az Aláíró tanúsítványt kibocsátó (hitelesítés Szolgáltató) kilétéről;
   1.2. a hitelesítés Szolgáltató tanúsítványának segítségével meggyőződni az Aláíró tanúsítványának integritásáról;
   1.3. az Aláíró tanúsítványának állapotát (érvényességét) ellenőrizni a tanúsítvány visszavonási listák (CRL) áttanulmányozásával;
   1.4. áttanulmányozni az Aláíró tanúsítványának összes attribútumát, és az adott tranzakcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni az aláírás elfogadásáról vagy elutasításáról,
2. nem szabad elfogadni az Elektronikus aláírást, ha az Elektronikus aláírás, az aláíró tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata, annak érvénytelenségére utal; az aláírás elfogadása nem jelenti az aláírt üzenet tartalmának tudomásul vételét vagy elfogadását.

2.1.3.2 Az Érintett fél számára ajánlott az időbélyeg ellenőrzése során

Időbélyeg ellenőrzése során ajánlott meggyőződni arról, hogy az időbélyeg valóban a lebélyegzett dokumentumhoz tartozik-e és az időbélyeg aláírása érvényes-e.

2.2 Felelősségek

2.2.1 A Szolgáltató felelőssége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-F szerint meghatározott tanúsítványt, illetve időbélyeget – és ezzel jelzi a felhasználó közösség és az érintett felek felé ezen HSZSZ-F használatát – azért vállalja a felelősséget, hogy a tanúsítvány előállítása, kibocsátása, közzététele, visszavonása, a Visszavonási Lista közzététele és az időbélyegzés tevékenységek a jelen HSZSZ-F-ben előírtaknak teljes mértékben megfelelnek, és a Szolgáltató megteszi a szükséges

intézkedéseket ahhoz, hogy a Szolgáltató maga és az előfizetők is a jelen HSZSZ-F előírásainak megfelelően járjanak el.

Az Eat. 15. § (1) értelmében a hitelesítés-szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a Magyar Köztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény 339. §-a szerint, az Előfizetővel szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért. A szabályok megtartását kétség esetén a Szolgáltatónak kell bizonyítania.

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

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

2.2.2 Az Előfizető és az Aláíró felelőssége

Az Előfizetőnek felelőssége áll fenn Szolgáltatóval szemben, a regisztráció során megadott adatainak valódiságával kapcsolatban.

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

Az Előfizető vagy az Aláíró köteles haladéktalanul tájékoztatni a hitelesítés-szolgáltatót, ha:

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

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

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

d. a tanúsítvánnyal ellátott elektronikusan aláírt elektronikus dokumentummal kapcsolatos jogvita megindulásáról.

Ha az aláíró elmulasztotta teljesíteni tájékoztatási kötelezettségét, az ebből eredő kárért felel.

Az Előfizető, az Aláíró, vagy az Eat. 10. § szerinti képviselt személy (szervezet) kérheti a tanúsítvány felfüggesztését vagy visszavonását.

Az aláíró az aláírás-létrehozó adatot kizárólag az aláírás létrehozására használhatja, betartva a tanúsítványban jelzett esetleges egyéb korlátozásokat is.

Az Aláíró jogosult az aláírás-létrehozó adatot birtokolni.

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

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

2.2.3 Az Érintett fél felelőssége

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

Az Érintett fél felelős az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok elfogadása során tanúsított körültekintő magatartásért és a tanúsítványlánc ellenőrzéséért.

2.2.4 Az anyagi felelősség korlátai

A Szolgáltató anyagi felelősségéről és annak korlátairól az ÁSZF-F rendelkezik.

2.3 Értelmezés és alkalmazás

2.3.1 Irányadó jog

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

A Szolgáltató tevékenységére vonatkozó fő jogszabályok felsorolását az 1.2.2 fejezet tartalmazza.

2.3.2 Érvénytelenség, hatályosság, megszűnés, értesítések

2.3.2.1 Érvénytelenség

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

2.3.2.2 Hatályosság

A HSZSZ-F, az ÁSZF-F és az előfizetői szerződés a felhasználói közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza.

A HSZSZ-F csak a Szolgáltató részéről, írott és aláírással hitelesített formában módosítható.

2.3.2.3 Megszűnés

A HSZSZ-F a Szolgáltató fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatásának befejezésével tekintendő megszűntnek.

2.3.2.4 Értesítések

Az Előfizetők, az Aláírók és az Érintett felek vagy bármely harmadik fél az Ügyfélkapcsolati Irodát megkeresheti ügyfélfogadási időben személyesen vagy telefonon, postai úton írásban, e-mail-ben vagy faxon. A Szolgáltató Ügyfélszolgálata folyamatos szolgálattal áll rendelkezésre telefonos vagy e-mail megkeresés esetén.

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

2.3.3 Vitás kérdések kezelése

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

Panaszt az Előfizetőt nyilvántartó Ügyfélkapcsolati Irodán vagy az Ügyfélszolgálatnál lehet írásban vagy szóban előterjeszteni. A panaszt a Szolgáltató az előterjesztéstől számított 10 munkanapon belül kivizsgálja.

A jogvitáik rendezésére vonatkozó szabályokat az ÁSZF-F tartalmazza.

2.4 Díjak

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

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

A Szolgáltató a következő pontokban ismertetett díjtípusokat alkalmazza a Szolgáltatások nyújtásakor.

2.4.1 Tanúsítvány kibocsátás és megújítás

Szolgáltató a kibocsátott illetőleg megújított tanúsítványokért éves fenntartási díjat számol fel az Előfizető felé, amely tartalmazza:

a. a tanúsítványok kibocsátásának illetőleg megújításának díját,
b. a tanúsítványtárban történő közzététel díját az érvényesség időtartamára,
c. a tanúsítvány felfüggesztésének illetve visszavonásának díját (amennyiben ilyen tevékenységre sor kerül),
d. a tanúsítványok lejárat utáni archiválásának a díját.

2.4.2 Tanúsítvány hozzáférés

Szolgáltató a tanúsítványok közzétételéért, a közzétett tanúsítványok eléréséért nem számol fel díjat.

2.4.3 Visszavonás és állapot információ hozzáférés

Szolgáltató a közzétett visszavonási információ eléréséért nem számol fel díjat.

2.4.4 Egyéb szolgáltatásokra vonatkozó díjak

Szolgáltató – ha a felfüggesztést az Aláíró vagy az Előfizető kérte – a kibocsátott tanúsítványok újraérvényesítéséért eljárási díjat számol fel az Előfizető felé. Az eljárási díj tartalmazza a tanúsítvány megváltozott állapotának a tanúsítványtárban visszavonási lista formájában történő közzétételének díját is.

Szolgáltató az időbélyegzés és az OCSP szolgáltatásért az erre vonatkozó Előfizetői Szerződésben rögzített díjat számolja fel.

2.4.5 Visszatérítési elvek

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

a. a kibocsátott tanúsítvány valamely adata a Szolgáltató hibájából fakadóan nem megfelelő,
b. a kibocsátott tanúsítvány, magánkulcs és aktivizáló adat nem összetartozó,
c. a kibocsátott aláírás-létrehozó eszközön szereplő adatok a Szolgáltató hibájából fakadóan nem megfelelők,[1]
d. a kibocsátott aláírás-létrehozó eszköz, az aktivizáló kód és a kulcsok nem összetartozók,
e. a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét Előfizető tanúsítványának kezelésekor.

A díj visszatérítésére vonatkozó igényt előfizetőnek a tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon belül a regisztrációt végző Ügyfélkapcsolati Irodánál kell írásban jeleznie a Szolgáltató részére. Az igényt a Szolgáltató 15 naptári napon belül köteles elbírálni. Az igény pozitív elbírálása esetén a Szolgáltató a tanúsítványt díjmentesen visszavonja és a fenntartási díjat az Előfizető által megjelölt bankszámlaszámra 20 naptári napon belül átutalja, vagy részére új tanúsítványt bocsát ki.

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

Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

2.5 Közzététel

2.5.1 Szolgáltatói információk közzététele

A Szolgáltató gondoskodik arról, hogy a tanúsítványok és az azokhoz kapcsolódó kikötései és egyéb feltételei az előfizetők és az érintett felek rendelkezésére álljanak. Ezek közé tartozik különösképpen:

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

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

2.5.2 A közzététel gyakorisága

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

A Szolgáltató általa működtetett hitelesítő központok szolgáltatói tanúsítványait a Tanúsítványtárában 24 órán belül közzéteszi.

A Szolgáltató a Visszavont Tanúsítványok Listáját a 4.4.7 pontban részletezett gyakorisággal frissíti.

A Szolgáltató a HSZSZ-F-ben és az ÁSZF-F-ben tervezett változásokról a hatályba lépést megelőzően tájékoztatja a Nemzeti Hírközlési Hatóságot.

2.5.3 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.

2.5.4 Elérési szabályok

A Szolgáltató minden Előfizető és Érintett fél számára elérhetővé teszi a Szolgáltatás Internetes honlapját, Tanúsítványtárát és Tanúsítvány Visszavonási Listáját olvasás céljából. A Tanúsítványtárban keresési lehetőséget biztosít a tanúsítványokban tárolt adatok alapján.

A Szolgáltató belső adatbázisait és egyéb adatállományait a jogszabályokban meghatározott kötelezettségeken túl csak és kizárólag a Szolgáltató biztonsági szabályzatai által meghatározott szerepkörű és jogosultságú munkatársai érhetik el, egyénileg differenciált azonosítás-hitelesítési és feljogosítási eljárás után.

2.6 A megfelelőség vizsgálata

A Szolgáltatót a Nemzeti Hírközlési Hatóság jogelődje, a Hírközlési Felügyelet fokozott biztonságú szolgáltatóként 2002. november 06-án nyilvántartásba vette.

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

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

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

2.7 Bizalmasság – adatkezelési szabályok

2.7.1 Bizalmas adatok, információk

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

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

1. A fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól,
2. megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénysértő kezelése ellen,
3. nyilvántartásba veszi az előfizetővel aláírt szerződést, beleértve az előfizető hozzájárulását az alábbiakhoz:
   3.1. hozzájárulás a szolgáltatások során felhasznált adatok hitelesítés-szolgáltató által történő nyilvántartásba vételéhez,
   3.2. hozzájárulás a nyilvántartásba vett adatok harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén,
   3.3. a tanúsítvány közzétételéhez,
4. csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához,
5. gondoskodik az Előfizetőre és az Aláíróra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,
6. védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az előfizetővel folytatott adatcsere során is.

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

A Szolgáltató az Előfizetők és az Aláírók személyes adatait csak a közöttük fennálló Előfizetői Szerződéssel összhangban levő célokra használhatja fel, harmadik félnek azokat az Előfizetők és az Aláírók írásos hozzájárulása nélkül nem adhatja át, kivéve a 2.7.4 pontban meghatározott eseteket.

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

2.7.2 Nem bizalmas információk

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

2.7.3 Tanúsítvány visszavonási és felfüggesztési okok felfedése

A Szolgáltató az általa kibocsátott tanúsítványok felfüggesztését és visszavonását tanúsítvány-visszavonási listákban teszi közzé.

A Szolgáltató a tanúsítvány visszavonás okát a vonatkozó szabványok által támogatott módon feltünteti a visszavonási listában. Ezen kívül a visszavonással kapcsolatos minden egyéb adatot bizalmasan kezel.

2.7.4 Feltárás törvényi meghatalmazással rendelkezők részére

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

2.7.5 Feltárás bírósági meghatalmazással rendelkezők részére

A Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az aláíró személy-azonosságát igazoló adatokat átadhatja az ellenérdekű peres félnek vagy képviselőjének feltárhat bizalmas felhasználói információkat, illetőleg azt közölheti a megkereső bírósággal az Eat. 11.§ paragrafusa alapján.

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

2.7.6 Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson és adategyeztetésen túl az Előfizetők és az Aláírók nem nyilvános személyes adatait csak az Előfizető írásos meghatalmazása alapján tárhatja fel harmadik fél részére.

2.7.7 Feltárás más esetekben

Szolgáltatónak tevékenysége befejezésekor az Eat. 16. § (2.) bek. szerint nyilvántartásait, a bizalmas adatokkal együtt, át kell adnia másik szolgáltató részére.

2.8 Szellemi tulajdonhoz fűződő jogok

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

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

A Szolgáltató tulajdonát képezi(k):

a. a visszavonási információ(k)
b. a Szolgáltató által az Aláíró részére kibocsátott egyedi azonosító
c. a Szolgáltató szabályzatai, szerződéses feltételei
d. a tanúsítványban szereplő hitelesítő azonosító

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

A tanúsítványban szereplő megkülönböztető név használatára az Előfizető jogosult.

3. Azonosítás és hitelesítési eljárások

3.1 Regisztráció

A regisztrálás során:

1. Az Előfizető kitölti vagy kitölteti a regisztrációs űrlapot és az Ügyfélkapcsolati Iroda részére átadja személyesen vagy megküldi (elektronikus) levélben,
2. a regisztrációs űrlap elfogadásával Szolgáltató gondoskodik az Előfizetői Szerződés előkészítéséről és intézkedik az előfizetői kulcspár és tanúsítvány elkészítésére,
3. Az előfizetői tanúsítvány elkészültével értesíti az előfizetőt és egyezteti vele a tanúsítvány és az Előfizetői Szerződés átvételének módját.

A regisztrációs űrlap egyúttal az Előfizetői Szerződés szerepét is betöltheti.

3.1.1 Nevek típusa

A tanúsítványokban szereplő névmegadás az ITU-T[2] X.500 ajánlásának felel meg.

3.1.2 Nevek szemantikája

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

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

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

3.1.3 Nevek egyedisége

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

3.1.4 Név igénylési viták feloldása

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

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

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

3.1.5 Védjegyek elismerésének és hitelesítésének módszere

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

3.1.6 Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere

Ha az Aláíró számára az aláírás-létrehozó és -ellenőrző adat előállítása a Szolgáltatás keretében a Szolgáltató által történik, akkor a kulcspár generálása a Szolgáltató Hitelesítő Központjában, fokozott biztonságú környezetben történik.

Előfizető vagy Aláíró által készített kulcspár használta esetén az Előfizető köteles az aláírás-ellenőrző adathoz tartozó aláírás-létrehozó adat birtoklását a regisztráció során a Szolgáltató számára hitelt érdemlően bizonyítani. Ennek hiányában a Szolgáltató a kért tanúsítvány kiállítását megtagadhatja.

3.1.7 Regisztráció „Személyes" típusú tanúsítvány igénylése esetén

Természetes személy, mint Előfizető a regisztrációs űrlap kitöltésével igényelhet tanúsítványt. Az űrlapon a következő Előfizetői adatokat lehet, illetve kell megadni:

1. név,

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

2. álneve, amennyiben annak megjelölésére az Előfizető igényt tart,
3. azonosítására használt okmány száma (személyi igazolvány vagy útlevél szám),
4. lakcím,
5. anyja neve,
6. születési hely és idő,
7. e-mail cím,
8. amennyiben az aláírás-létrehozó adatot az Előfizető hozta létre, úgy az ahhoz tartozó aláírás-ellenőrző adat azonosítója vagy lenyomata.

A regisztrációs űrlapot a Szolgáltató biztosítja; azon további adatok megadására vonatkozó mezők is rendszeresíthetők.

Természetes személyt az Ügyfélkapcsolati Iroda személyi igazolvány vagy útlevél, illetőleg lakcímigazolvány személyes bemutatásával azonosít. A személyes megjelenést helyettesítheti az űrlap adatait megerősítő hiteles közjegyzői okirat.

A Szolgáltató megtagadhatja a tanúsítvány igénylést, ha az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.

3.1.8 Regisztráció „Szervezeti" típusú tanúsítvány igénylése esetén

Jogi személy vagy jogi személyiség nélküli szervezet, mint Előfizető a regisztrációs űrlap kitöltésével igényelhet tanúsítványt. A regisztrációs űrlapon a következő adatokat lehet, illetve kell megadni:

1. Az Előfizető tekintetében:
   1.1. az Előfizető szervezet neve, székhelye
   1.2. az Aláíró(k) kijelölését engedélyező, a cég- vagy szervezet képviseletére jogosult személy neve, beosztása, munkahelyi telefonszáma, fax-száma, e-mail címe
2. A Kapcsolattartó tekintetében:
   2.1. Kapcsolattartó neve, beosztása, telefonszáma és e-mail címe
3. Az Aláíró(k) tekintetében:
   3.1. annak a szervezeti egységnek a megnevezése, ahol az Aláíró dolgozik,
   3.2. annak a szervezeti egységnek a telephelye, ahol az Aláíró dolgozik
   3.3. Aláíró neve
   3.4. Aláíró álneve, amennyiben annak megjelölésére az Aláíró igényt tart és azt számára az Előfizető engedélyezte
   3.5. az Aláíró beosztása
   3.6. az Aláíró azonosítására használt személyi igazolvány vagy útlevél száma (ha a tanúsítvány személyhez köthető)
   3.7. Az Aláíró anyja neve, születési helye és ideje (ha a tanúsítvány személyhez köthető),
   3.8. az Aláíró telefonszáma (ha a tanúsítvány személyhez köthető),
   3.9. az Aláíró e-mail címe
   3.10. amennyiben az aláírás-létrehozó adatot az Aláíró hozta létre, úgy az ahhoz tartozó aláírás-ellenőrző adat azonosítója vagy lenyomata

A regisztrációs űrlapot a Szolgáltató biztosítja; azon további adatok megadására vonatkozó mezők is rendszeresíthetők.

Az Előfizető nevében eljáró, a cég- vagy szervezet képviseletére jogosult személy képviseleti jogát az Előfizetőnek a regisztráció során igazolnia kell.

A szolgáltatási szerződés megkötése során az Előfizető szervezet kapcsolattartót nevezhet meg a Szolgáltató részére, aki aláírási joggal rendelkezik a tanúsítványok kibocsátását, illetve kezelését illetően; a Szolgáltató később e személynek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén. A Szolgáltató ez esetben jogosult a kapcsolattartó azonosítás-hitelesítését személyi igazolvány vagy útlevél személyes bemutatásával elvégezni.

Az Aláíró(k) azonosítása az Ügyfélkapcsolati Irodán a személyi igazolvány vagy útlevél, illetőleg lakcímigazolvány bemutatásával személyesen történik. A Szolgáltató eltekinthet az Aláíró(k) személyes azonosításától abban az esetben, ha ezt az Előfizető más hitelesnek tekinthető módon (pl. közjegyzői okiratban) igazolja.

A Szolgáltató megtagadhatja a tanúsítvány kibocsátását, ha a bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.

A Szolgáltató a regisztrációs űrlapot minősített aláírással ellátott elektronikus dokumentumként is elfogadja abban az esetben, ha az Előfizetővel erről előzetesen megegyezik.

3.1.9 Regisztráció „Eszköz" tanúsítvány igénylése esetén

Eszköz tanúsítvány regisztrációs űrlap kitöltésével igényelhető. Az eszköz azonosításához és hitelesítéséhez a következőben megadott adatokat kéri az Ügyfélkapcsolati Iroda.

Természetes személy által igényelt eszköz-tanúsítvány esetén:

1. az Előfizető személyes adatai a 3.1.7 pont szerint,
2. az eszköz tanúsítványban feltüntetendő neve,
3. az Előfizető írásos nyilatkozata az eszköz birtoklásáról.

Jogi személy vagy jogi személyiség nélküli szervezet által igényelt eszköz-tanúsítvány esetén:

1. az Előfizető szervezet hitelesítéséhez szükséges adatok a 3.1.8 pont szerint,
2. az eszköz tanúsítványban feltüntetendő neve,
3. az Előfizető szervezet írásos nyilatkozata az eszköz birtoklásáról.

A regisztrációs űrlapon szereplő adatok ellenőrzése, az azonosítás rendre a 3.1.7 illetve 3.1.8 pontokban feltüntetett módon történik.

A regisztrációs űrlapot a Szolgáltató biztosítja; azon további adatok megadására vonatkozó mezők is rendszeresíthetők.

A Szolgáltató megtagadhatja a tanúsítvány kibocsátását, ha a regisztráció során az eszköznek az Előfizetőhöz tartozásával, annak eredetiségével kapcsolatban kétség merül fel.

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 időtartamra.

Előfizetői tanúsítvány megújítása akkor lehetséges, ha:

1. a tanúsítvány nem szerepel a Visszavont Tanúsítványok Listájában
2. a regisztráció alkalmával rögzített összes adat még érvényességéről és változatlanságáról az Előfizető írásban nyilatkozik.

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

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 visszavonási kérés

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványok érvényességét az előfizető vagy az aláíró kérésére felfüggessze vagy a tanúsítványt visszavonja. Ennek érdekében a Szolgáltató a 4.4 pontban rögzíti a tanúsítványok visszavonásának és felfüggesztésének eljárásait.

4. A működésre vonatkozó követelmények

4.1 Tanúsítványigénylés

A Szolgáltató azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatja az Előfizetőt a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről.

Tanúsítvány igényléséhez ki kell tölteni a regisztrációs űrlapot és le kell folytatni a regisztrációs eljárást. Az űrlap igényelhető az Ügyfélkapcsolati Irodánál, vagy letölthető a Szolgáltatás Internetes honlapjáról.

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

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

A regisztráció során az Ügyfélkapcsolati Iroda nyilvántartásba veszi az Aláíró azonosítására használt adatokat, beleértve az igazoláshoz használt dokumentumok regisztrációs számát és az azok érvényességével kapcsolatos esetleges korlátozásokat. Az Előfizető aláírásával tudomásul veszi és elfogadja, hogy a dokumentumokról az Ügyfélkapcsolati Iroda másolatot készíthet.

A Tájékoztató a szolgáltató internetes honlapján bárki számára elérhető.

4.2 Tanúsítvány kibocsátás

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

Az elkészült tanúsítvány a következő módon jut el az Előfizetőhöz:

a. az Előfizető, az Aláíró vagy azok képviselője személyesen átveszi az Ügyfélkapcsolati Irodán, vagy

b. a Szolgáltató postai úton eljuttatja az Előfizető által megadott címre, vagy

c. az Előfizető letölti a Szolgáltató nyilvános Tanúsítványtárából

4.3 Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető részéről az átvétellel történik meg.

Az aláírás-létrehozó adat használatba vétele előtt az Előfizetőnek kötelessége ellenőrizni a tanúsítványban feltüntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál, az aláírás-létrehozó adatot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonására.

4.4 Tanúsítvány visszavonás és felfüggesztés

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatást nyújt. A tanúsítvány visszavonása a tanúsítvány állapotát végérvényesen érvénytelenre állítja. Felfüggesztés esetén a tanúsítvány csak rövid, átmeneti időszakra érvénytelen. A tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam (lásd 4.4.6 pont) után állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni.

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

4.4.1 Visszavonáshoz/felfüggesztéshez vezető körülmények

A Szolgáltató indokolt esetben felfüggeszti vagy visszavonja a tanúsítványt ha:

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

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

1. a magánkulcs kompromittálódása, vagy annak gyanúja,
2. az aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása,
3. az aláírás-létrehozó eszközt védő aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja,
4. a tanúsítványban feltűntetett hibás adatok,
5. az Előfizető tanúsítványban feltűntetett adatainak megváltozása,
6. az Aláíró tanúsítványban feltűntetett adatainak megváltozása,
7. a tanúsítványban feltűntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszűnése[3].

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

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

1. a tanúsítvány felfüggesztési idejének lejárata
2. amennyiben a törvény erre kötelezi,
3. az ÁSZF-F vagy az Előfizetői Szerződés megszegése az Előfizető és/vagy az Aláíró által,
4. az Előfizető és/vagy az Aláíró kötelezettségeinek be nem tartása,
5. az Előfizetői szerződés megszűnése,
6. a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról,
7. a tanúsítványban feltűntetett kibocsátó adatok megváltozása
8. a hitelesítési szolgáltatás megszűnése,
9. a Szolgáltató valamely magánkulcsának kompromittálódása miatt.

[3] Eat. 10. § (3)

4.4.2 Visszavonás/felfüggesztés kérelmezése

Tanúsítvány visszavonását/felfüggesztését az előző pontban feltüntetett körülmények alapján az Aláíró, az Előfizető vagy azok képviselője, a Szolgáltató, a Nemzeti Hírközlési Hatóság vagy más harmadik fél kezdeményezheti. Az Előfizetőnek és a Szolgáltatónak kötelessége, harmadik félnek joga az előző (4.4.1) pontban feltűntetett esetekben a visszavonás azonnali kezdeményezése.

A visszavonási/felfüggesztési kérelmet be lehet nyújtani személyesen vagy írásban a Szolgáltató Ügyfélkapcsolati Irodájánál. Ha a bejelentő akadályoztatása miatt a visszavonási igényét személyesen nem tudja bejelenteni vagy azonnali intézkedés szükséges, akkor a tanúsítvány felfüggesztése telefonon vagy elektronikusan aláírt e-mail-ben is kérhető az Ügyfélszolgálaton.

A visszavonási/felfüggesztési kérelem teljesítéséhez a következő adatok szükségesek:

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

b. a visszavonást/felfüggesztést kérő azonosító adatai

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

d. a visszavonáshoz/felfüggesztéshez vezető körülmények

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

4.4.3 Visszavonási eljárás

A visszavonási eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt:

a. E-mail-ben történt bejelentés esetén az Aláíró tanúsítványa alapján azonosítja és hitelesíti a visszavonás kérelmezőjét.

b. Személyesen az Ügyfélkapcsolati Irodánál az Iroda munkaidején belül lehet a visszavonási kérelmeket bejelenteni a bejelentő azonosítása-hitelesítése mellett.

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

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

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

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

4.4.4 Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási/felfüggesztési kérelem esetén a bejelentési kötelezettség azonnali, a Szolgáltató ennek végrehajtását soron kívül végrehajtja a kérelem elfogadása után. A legnagyobb késedelem a visszavonási/felfüggesztési kérelem elfogadása és a visszavonási állapot közzététele között: 30 perc.

A Szolgáltató akkor tekinti a visszavonási/felfüggesztési kérelmet elfogadottnak, ha annak jogosságáról meggyőződött. A visszavonási/felfüggesztési kérelemre vonatkozó türelmi idő 5 munkanap. Ha a Szolgáltató ezen időn belül sem tud a kérelem jogosságáról meggyőződni, akkor a felfüggesztési/visszavonási kérelmet visszautasítja.

Visszavont/felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok:

a. A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig és elfogadásáig az ÁSZF-F-nek megfelelően az Előfizető felelős a felmerülő károkért.

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

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

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

4.4.5 Felfüggesztési eljárás

A felfüggesztési eljárás megegyezik a visszavonási eljárással (lásd 4.4.3 pont), az alábbi kiegészítésekkel:

a. A felfüggesztett tanúsítványok is a Visszavont Tanúsítványok Listájában kerülnek közzétételre,

b. Tanúsítvány felfüggesztési igény telefonon is bejelenthető a Szolgáltató Ügyfélszolgálatán. Telefonon történt bejelentés esetén a Szolgáltató a személyes adatok bemondása után felfüggesztési jelszóval azonosítja a

felfüggesztés kérelmezőjét, majd elvégzi a felfüggesztés kérelem formai és tartalmi ellenőrzését, illetve ezek sikeressége esetén a tanúsítvány felfüggesztését.

4.4.6 Felfüggesztett állapotra vonatkozó korlátozások

Tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig lehet.

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

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

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

Az újraérvényesítés feltételei a következők:

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

b. Az újraérvényesítést kérő személyt azonosítani és hitelesíteni kell.

Az újraérvényesítés kéréséhez a következő adatokat kell megadni:

a. a felfüggesztett tanúsítvány sorszáma,

b. a felfüggesztés megszüntetését kérő személy azonosító adatai,

c. a felfüggesztés megszüntetésének oka.

4.4.7 Visszavont tanúsítványok Listája (CRL) és kibocsátásának gyakorisága

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

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

4.4.8 Visszavont Tanúsítványok Listája ellenőrzési követelmények

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

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

4.4.9 Visszavonási állapot közlés más formái

A Szolgáltató nem alkalmaz a Visszavont Tanúsítványok Listájától különböző nyilvános visszavonási állapot közlő eljárást.

4.4.10 Magánkulcs kompromittálódás speciális követelményei

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

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

4.5 Biztonsági naplózások, archívum

4.5.1 Naplózott esemény típusok

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

A Szolgáltató által végzett műveletek naplózásra kerülnek. A naplóbejegyzések többek között a regisztráció, az aláírás-létrehozó és ellenőrző kulcs-pár generálása, az aláírás-létrehozó eszköz megszemélyesítése, a tanúsítvány létrehozása, kibocsátása és kezelése, valamin egyéb Szolgáltatói tevékenységek során készülnek.

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

4.5.2 Napló adatok tárolása

A napló adatok rendszeresen archiválásra kerülnek ellenőrzés, szükségessé váló visszakeresés és újbóli használat céljából.

4.5.3 Adatarchiválás

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

4.5.4 Az archívum megőrzési időtartama

A Szolgáltató a tanúsítványokra vonatkozó archív adatokat a 3/2005 (III. 18.) IHM rendelettel összhangban a keletkezésüktől számított 10 évig, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig megőrzi.

4.5.5 Az archívum védelme

A Szolgáltató archívumában olyan fizikai védelmet biztosít, amely fenntartja az archivált adatok bizalmasságát és sértetlenségét.

4.6 Katasztrófa elhárítás

4.6.1 A hitelesítés-szolgáltatás azonnali felfüggesztése

A katasztrófa esemény bekövetkezése a hitelesítés-szolgáltatás azonnali felfüggesztésével jár. Erről az eseményről Szolgáltató értesíti a Nemzeti Hírközlési Hatóságot és lehetőségei szerint a felhasználó Közösség tagjait .

4.6.2 Üzletmenet-folytonossági Terv

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

4.7 A hitelesítés-szolgáltatási tevékenység megszüntetése

A Szolgáltató a szolgáltatás megszűnése esetén késlekedés nélkül értesíti a Nemzeti Hírközlési Hatóságot és a felhasználó Közösség tagjait. .Ha a megszűnés tervezett, az értesítés legkevesebb 60 nappal megelőzi a szolgáltatás leállítását.

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más szolgáltatókkal a szolgáltatás átvételéről.

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

Ezzel egyidejűleg leállítja a visszavonás kezelési szolgáltatást.

5. Fizikai, eljárásrendi és humán biztonsági szabályozások

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

- A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására
- A Szolgáltató felelősséget vállal minden – jelen HSZSZ-F-ben tárgyalt – elektronikus aláírással kapcsolatos szolgáltatásért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki.
- A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja.
- A Szolgáltató a PKI Szolgáltatások Biztonsági Szabályzatában dokumentálja és folyamatosan fenntartja a hitelesítés-szolgáltatást nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait. A PKI Szolgáltatások Biztonsági Szabályzata biztonsági okokból nem nyilvános.
- A Szolgáltató gondoskodik az informatikai biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez kerülnek kiadásra.

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

5.1 Fizikai biztonsági szabályozások

5.1.1 Hitelesítő Központok

A hitelesítő központok legmagasabb védelmi szintet képező objektuma a Bizalmi Központ, amely a biztonsági szempontból legkritikusabb hardver/szoftver elemeket tartalmazza. A Bizalmi Központban történik a kulcspárok és a tanúsítványok előállítása, a kulcspárok elhelyezése az aláírás-létrehozó eszközre és az aláírás-létrehozó eszközök megszemélyesítése.

Az objektum védelme kielégíti a MeH ITB 12. ajánlása szerinti fokozott biztonsági osztály követelményeit.

5.2 Eljárásrendi szabályozások

A Szolgáltató eljárásrendi szabályait három szabályzat tartalmazza:

- a Szolgáltató Szervezeti és Működési Szabályzata, amely részletesen meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes munkaköröket és az azokhoz kapcsolt feladat-, felelősség és hatásköröket,
- a jelen Szolgáltatási Szabályzat,
- a PKI Szolgáltatások Biztonsági Szabályzata, amely részletesen szabályozza az adatokhoz és az informatikai rendszerekhez, valamint a személyi és a fizikai környezethez kapcsolódó biztonsági szabályokat.

5.3 Humán szabályozások

A Szolgáltató gondoskodik arról, hogy a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát. A Szolgáltató kellő számú, az elektronikus aláírás-hitelesítéssel kapcsolatos szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező munkatársakat alkalmazzon. A Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa független minden olyan ütköző érdektől, ami hátrányosan érinthetné a hitelesítés-szolgáltatási tevékenységek semlegességét.

Valamennyi bizalmi munkakört betöltő munkatárs a munkakörbe kinevezéskor a foglalkoztatási dokumentumok részeként:

- írásos tájékoztatást kap jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról,
- titoktartási nyilatkozatot ír alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is szerepelnek.

6. Műszaki biztonsági óvintézkedések

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

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

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

A Szolgáltató maga generálja a szolgáltatói kriptográfiai kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben, nagy biztonságú hardver modulban (HSM[4]), kettős ellenőrzés mellett. A nagy biztonságú hardver modul hazai tanúsítvánnyal rendelkezik és szerepel a Nemzeti Hírközlési Hatóság által jóváhagyott minősített elektronikus aláírási termékek listájában. A kulcspárok generálását olyan algoritmussal valósítja meg, melyet jogszabály ismer el erre a célra alkalmasnak.[5]

A kulcspár generálását és az aláírás-létrehozó eszköz (pl. csipkártya) megszemélyesítését a Bizalmi Központban bizalmi munkakört betöltő személy végzi.

Az aláírás-létrehozó adat elhelyezésére a Szolgáltató csak tanúsítvány kibocsátással együtt vállalkozik.

A csipkártya megszemélyesítés szolgáltatáshoz vizuális – egy oldali nyomással történő – grafikus megszemélyesítés is kapcsolódik az Előfizetői Szerződésben meghatározott adattartalommal. A Szolgáltató az aláírás-létrehozó adatot és a tanúsítványt tartalmazó csipkártyához PIN kódot biztosít.

6.1.2 Az aláírás-létrehozó adat eljuttatása az Aláíróhoz (Előfizetőhöz)

A Szolgáltató:

a. a kulcsokat az Előfizető vagy az Aláíró által történő átvételig biztonságos módon tárolja,

b. a magánkulcsot az Előfizetőnek vagy az Aláírónak úgy adja át, hogy a magánkulcs titkossága ne sérüljön,

c. az aláírás-létrehozó eszköz aktivizálási adatát (PIN kódját) biztonságosan készíti el és az aláírás-létrehozó eszköztől elkülönítve tárolja.

Az Előfizetőnek az aláírás-létrehozó eszközt és a PIN kódot tartalmazó borítékot az átvétel írásos elismerésével kell átvennie.

6.1.3 Az Aláírók aláírás-ellenőrző adatának eljuttatása az érintett felekhez

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

6.1.4 A Szolgáltató aláírás-ellenőrző adatainak eljuttatása a felhasználói közösséghez

A Szolgáltató a hitelesítő központok (Root CA, Produktív CA) tanúsítványait és ezen keresztül aláírás-ellenőrző adatait (nyilvános kulcsait) a szolgáltatás internetes honlapján keresztül teszi mindenki számára elérhetővé.

A szolgáltatói tanúsítványok letölthetők és a felhasználók kliens-alkalmazásaiba installálhatók.

6.1.5 Kulcsméretek, használt algoritmusok

A Szolgáltató Hitelesítő Központja elektronikus aláírás létrehozására az RSA[6] algoritmust használja. Az Előfizetői tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

A Hitelesítő Központ („Produktív CA") aláíró kulcsainak mérete: 2048 bit

Az Aláírók (Előfizetők) aláíró kulcsainak mérete: legalább 1024 bit

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

6.1.6 Kulcs felhasználási célok

A Szolgáltató Előfizetők részére tanúsítványt (és kulcspárt) elektronikus aláírási vagy azonosítás-hitelesítési célra bocsát ki.

Ennek érdekében a Szolgáltató az Előfizetői tanúsítványok egyes attribútumait a felhasználási területnek és célnak megfelelően állítja be.

---

[4] Hardware Security Module, IBM 4758-002 PCI (co-processzor) 2-es modell, hardver, Miniboot 1: A verzió

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

6 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.

A kulcspár kizárólag arra a célra használható, amelyre a Szolgáltató kibocsátotta, a HSZSZ-F-nek és az Előfizetői Szerződés feltételeinek megfelelően.

A tanúsítványok és a benne foglalt aláírás-ellenőrző adatok (nyilvános kulcsok) érvényességének kezdete a kibocsátás időpontjával (év, hónap, nap, óra, perc, másodperc) egyezik meg. Az előfizetői aláíró kulcsok és tanúsítványok érvényességi ideje 1 év.

6.2 Aláírás-létrehozó adat védelme

6.2.1 Kriptográfiai modulra vonatkozó szabványok

Az Előfizetők aláírás-létrehozó adatának tárolására Szolgáltató igény esetén olyan eszközt bocsát ki, mely teljesíti a FIPS 140-1 Level 3 követelményeket

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

A Szolgáltató saját kulcsainak tárolására hardveres biztonsági modult alkalmaz.

6.2.2 A többszereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése

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

6.2.3 Aláírás-létrehozó adat letét, mentés, archiválás

Szolgáltató nem nyújt aláírás-létrehozó adat letét szolgáltatást. Szolgáltató az Előfizető aláírás-létrehozó adatát semmilyen formában nem menti vagy archiválja; annak előállítására, visszafejtésére alkalmas programot, adatot nem tárol.

6.2.4 Aláírás-létrehozó adat aktiválása

Az előfizetői aláírás-létrehozó adat aktiválása a felhasználó által történik a jelszó vagy PIN kód megadásával, azokban az esetekben, amikor az aláírás-létrehozó adat használatára szükség van.

6.2.5 Aláírás-létrehozó adat deaktiválása

Az előfizetői aláírás-létrehozó adatok deaktiválását a felhasználó alkalmazása végzi az Aláíró kijelentkezésekor, vagy – pl. csipkártya esetén – amikor az Aláíró az aláírás-létrehozó eszközt eltávolítja az olvasóból.

6.2.6 Aláírás-létrehozó adat megsemmisítése

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

A szolgáltatói aláírás-létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3 Az előfizetői tanúsítványok megőrzése

Az előfizetői tanúsítványokat a Szolgáltató az érvényesség lejáratától számított 10 évig megőrzi.

6.4 Aktiválási adatok (PIN kódok)

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

A Szolgáltató a PIN kódokat műszaki és szervezési intézkedésekkel védi és az Előfizető részére az aláírás-létrehozó eszköztől elkülönítve adja át. Az átvételt követően az Előfizetőnek saját felelősségi körében kell biztosítania PIN kód kizárólagos birtoklását.

Az Előfizető bármikor megváltoztathatja PIN kódját.

A PIN kódot a Szolgáltató nem tárolja és nem állítja újra elő sem az Előfizető, sem harmadik fél vagy hatóság kifejezett kérése esetén sem.

Az aktiváló adat elvesztése, elfelejtése vagy illetéktelen kezekbe történő jutása esetén minden esetben új aktiválási adatot kell előállítani, amely esetenként új aláírás létrehozó adat illetve tanúsítvány előállítását is feltételezi.

6.5 Számítógép biztonsági szabályok

A Szolgáltató biztonságtechnikai követelményeit a MeH ITB 12. ajánlás szerinti fokozott biztonsági osztályba sorolás határozza meg.

Az alkalmazott informatikai rendszer követelményeit a Szolgáltató az alábbi termékeken alapulva elégíti ki:

- operációs rendszer,
- PKI alkalmazás,
- kriptográfiai hardver modulok,
- tűzfalak,
- behatolás detektorok.

6.6 Életciklus technikai szabályok

6.6.1 Rendszerfejlesztési szabályok

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

6.6.2 Biztonságkezelési szabályok

A biztonságkezelési szabályokat a Szolgáltató társasági szintű Informatikai Biztonságpolitikája és Informatikai Biztonsági Szabályzata tartalmazzák. A Szolgáltató hitelesítés-szolgáltatást támogató informatikai rendszere vonatkozásában a PKI szolgáltatások Biztonsági Szabályzata érvényesül.

6.7 Hálózati biztonsági szabályok

A Szolgáltató társasági szintű informatikai, valamint a hálózati biztonságpolitikájának és biztonsági architektúrájának megfelelően a rendszerelemek közötti belső hálózati kommunikáció védett módon történik.

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

A Hitelesítő Központ közvetlen külső kommunikációt nem folytat a végfelhasználókkal.

6.8 Kriptográfiai modul ellenőrzése

A Szolgáltató a fokozott biztonságú szolgáltatáshoz alkalmazott hardveres kriptográfiai modult rendszeresen ellenőrzi.

7. Tanúsítvány és tanúsítvány-visszavonási profil

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

7.1 Tanúsítvány profil

7.1.1 Alap mezők

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

7.2 Tanúsítvány kiterjesztések

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

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

7.3 Tanúsítvány-visszavonási profil

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

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

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

8. A szolgáltatási szabályzat adminisztrációja

8.1 Változáskezelés

8.1.1 Változtatási eljárások

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

A hitelesítési rend módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

8.1.2 Észrevételek kezelése

A HSZSZ-F-el kapcsolatos észrevételeket Szolgáltató az Ügyfélkapcsolati Iroda útján fogadja.

8.2 Közzétételi és tájékoztatási elvek

8.2.1 A HSZSZ-F-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyeztetik. A Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan, üzleti titokként kezel.

8.2.2 A HSZSZ-F közzététele

A Szolgáltató a HSZSZ-F-t a szolgáltatás internetes honlapján teszi közzé.

8.3 Elfogadási eljárások

A jelen HSZSZ-F az RFC 2527 szabványnak való megfelelőségét közzététel előtt a Szolgáltató megvizsgálta.

A szabályzat törvényeknek való megfelelőségét a Nemzeti Hírközlési Hatóság is vizsgálja.

A Szolgáltató alkalmanként konzultál a Nemzeti Hírközlési Hatósággal a tervezett változtatásairól. Módosítás esetén a Szolgáltató a HSZSZ-F-t, annak a változtatásokkal egybeszerkesztett új verzióját, hatósági felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Hírközlési Hatóságnak. A HSZSZ-F új változata hatályba léptetésének feltétele, hogy azt a Nemzeti Hírközlési Hatóság nyilvántartásba vette.

9. Hivatkozások és fogalom-meghatározások

9.1 Hivatkozások

A Szolgáltató hivatkozott dokumentumai:

A MÁV INFORMATIKA Kft. Szervezeti és Működési Szabályzata
A MÁV INFORMATIKA Kft. Iratkezelési Szabályzata
A MÁV INFORMATIKA Kft. Titokvédelmi Szabályzata
A MÁV INFORMATIKA Kft. Informatikai Biztonságpolitikája
A MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata
Hitelesítési Rend Nem Minősített Tanúsítványokra (HR-NMT)
Általános Szerződési Feltételek Fokozott Biztonságú Elektronikus Aláírás Hitelesítés-szolgáltatáshoz (ÁSZF-F)
A PKI Szolgáltatások Biztonsági Szabályzata
A PKI Szolgáltatások Üzletmenet-folytonossági Terve
A PKI Szolgáltatások Üzemeltetési Kézikönyve

9.2 Fogalom-meghatározások

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

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

Aláírás-létrehozó eszköz: olyan hardver 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

Biztonsági tisztviselő, biztonsági menedzser: a hitelesítés-szolgáltatás biztonságáért általánosan felelős személy

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

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

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

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

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

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

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

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes

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

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

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

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

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

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

a) alkalmas az aláíró azonosítására,

b) egyedülállóan az aláíróhoz köthető,

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

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

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

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

Igénylő: a minősített tanúsítvány iránti igényt benyújtó személy

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

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

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

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

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

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

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

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

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

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

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

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

Szolgáltatói kulcspár: a szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs

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

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

Tanúsítvány: hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot az Eat. 9. § (3), illetőleg (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 elérhetővé tétele az aláíró által meghatározott kör részére

Visszavonás kezelése: az Eat. 14. §-ban meghatározott esetekben a kibocsátott tanúsítványok visszavonására és felfüggesztésére vonatkozó eljárások lefolytatása

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