MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó
Korlátolt Felelosségu Társaság

Szolgáltatási Szabályzat
Titkosítás Hitelesítés-szolgáltatáshoz
(HSZSZ-T)

Verziószám	**3.0**
Objektum azonosító (OID)	**1.3.6.1.4.1.14868.1.3.3**
Hatálybalépés dátuma	**2005. augusztus 18.**

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

Változáskezelés

Verzió	Dátum	A változás leírása	Készítette
1.0	2004. 08. 25.	Szolgáltatás megindításához elokészített változat	Néder Ferenc
2.0	2004. 11. 29.	Felülvizsgált, javított változat	Néder Ferenc
3.0	2005. 08. 18.	Felülvizsgált, javított változat	Néder Ferenc

Tartalom

1. Bevezetés

E dokumentum a MÁV INFORMATIKA Kft. (továbbiakban Szolgáltató) titkosító tanúsítvány hitelesítés-szolgáltatás ára vonatkozó muködési szabályokat és eljárásrendet tartalmazza.

A Szolgáltató a titkosító tanúsítvány hitelesítés-szolgáltatást a vele elofizetoi szerzodéses viszonyban álló igénybevevok részére szolgáltatja. A Szolgáltató a következo szolgáltatásokat nyújtja:

a. Titkosító kulcspár eloállítás,

b. Titkosító tanúsítvány hitelesítés,

c. Titkosító kulcspár és tanúsítvány adathordozóra történo elhelyezése,

d. Titkosító kulcspár és tanúsítvány érvényesség kezelés,

e. Titkosító kulcspár és tanúsítvány biztonságos megorzése hosszabb távra,

f. Titkosító kulcspár visszaállítás a kulcshordozó eszköz elvesztése vagy illetéktelen kezekbe kerülése esetén.

A jelen Szolgáltatási Szabályzat (továbbiakban: HSZSZ-T) további fejezeteiben a „*szolgáltatások*” kifejezés alatt a fenti részszolgáltatások bármelyike értendo.

A fenti szolgáltatásokat a Szolgáltató fokozott biztonságú szinten szolgáltatja.

1.1 Szolgáltató adatai

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

Cégjegyzék szám: 01-09-563711

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

Telefonszám: (36-1) 457-9300

Telefax szám: (36-1) 457-9500

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

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

Illetékes fogyasztóvédelmi felügyeloség:

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

Kapcsolat az ügyfelekkel:

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

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

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

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

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

Panaszok bejelentésének helye:

a. személyesen az Ügyfélkapcsolati Irodákban

b. írásban a Szolgáltató székhelyére címezve

c. telefonon az Ügyfélkapcsolati Irodákban vagy az Ügyfélszolgálatnál

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

1.2 Alapok

1.2.1. Szabályzat célja

Jelen HSZSZ-T célja, hogy összefogja azokat az eloírásokat, adatokat és információkat, melyeket a Szolgáltató titkosítás-hitelesítés szolgáltatásával valamilyen módon kapcsolatba kerülo feleknek tudni kell. A szabályzat biztosítja a Szolgáltató muködésének átláthatóságát, s lehetové teszi a felhasználók és az érintett felek számára, hogy megállapítsák azt, hogy az ismertetett szolgáltatási gyakorlat, valamint a kibocsátott titkosító tanúsítványok menynyiben felelnek meg az elvárásaiknak. A HSZSZ-T és egyéb, a HSZSZ-T-ben hivatkozott dokumentumok, ajánlások, szabványok tartalmának megismerése után a titkosító tanúsítvány elfogadóinak egyértelmuen meg kell tudni állapítani a titkosító tanúsítványkezelésének módját, az általa garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelosség vállalásokat.

1.2.2. Jogszabályok, szabványok

A Szolgáltató által nyújtott szolgáltatásokra elsosorban a következo 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 követelményekrol

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

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

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

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

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

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

1.3 HSZSZ-T azonosítás

A Szolgáltató az ISO/IEC és az ITU szabványok által eloírt regisztrációs eljárásnak megfeleloen eljárva regisztrálja a jelen HSZSZ-T-t.

A jelen HSZSZ-T a Szolgáltató ügyfélkapcsolati irodáiban és az Interneten a szolgáltatás honlapján érheto el. Jelen HSZSZ-T-nek csak a Szolgáltató aláírásával ellátott változata tekintheto hitelesnek.

1.4 A szolgáltató és felhasználó közösség, alkalmazhatóság

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösség a következo:

a. a Szolgáltató elektronikus aláírásra és titkosításra feljogosított munkatársai,

b. a Szolgáltatóval kapcsolatban álló hitelesíto és regisztráló szervezetek,

c. a szerzodéses elofizetok titkosításra feljogosított munkatársai,

d. a szerzodéses elofizetok informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.),

e. az érintett felek.

1.4.1. A Szolgáltató egységei

1.4.1.1 Ügyfélkapcsolati Irodák ("ÜKI")

Az Ügyfélkapcsolati Irodák (rövidítve: ÜKI) a Szolgáltató és a vele szerzodéses alapon együttmuködo Társas ágok (mint szerzodött közremuködok) azon szervezeti egységei, amelyek az elofizetoi tanúsítvány kérelmek összeállítását és az elkészült tanúsítványok átadását végzik, valamint az adminisztrációs feladatokat látják el.

1.4.1.2 Regisztrációs Iroda ("RA")

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

1.4.1.3 Hitelesíto Központ ("CA")

A Hitelesíto Központ (rövidítve: CA) a szolgáltatás-támogató informatikai rendszer központi eroforrásaiból, az ezt körül vevo biztonságos fizikai környezetbol, valamint az üzemelteto és szolgáltatást ellátó személyzetbol áll. Feladata az aláírás létrehozó adatok és tanúsítványok eloállítása, a tanúsítványok közzététele.

1.4.2. Felhasználók

1.4.2.1 Elofizeto

Az Elofizeto a Szolgáltatóval szerzodéses viszonyban álló Felhasználó, aki számára a Szolgáltató Tanúsítványt bocsát ki. Elofizeto lehet természetes vagy jogi személy. A szerzodési feltételeket az Általános Szolgáltatási Feltételek Titkosítás Hitelesítés Szolgáltatáshoz (továbbiakban: ÁSZF-T) tartalmazza.
Az Elofizeto egyben titkosító magánkulcs felhasználó is, amennyiben birtokolja és használja a titkosító magánkulcsot.
Az Elofizeto lehet jogi személy (szervezet) is. Ebben az esetben a szervezet cégjegyzésre jogosult vezetoje képviseloként egy természetes személyt bíz meg, akit felruház hagyományos, illetve elektronikus aláírási jogosultsággal, valamint rendelkezik a 6.1.2 pontban meghatározott transzport magánkulccsal. Ez a személy a jogi személyt (szervezetet) képviselve ír alá hagyományos papíralapú, illetve elektronikus dokumentumokat.

1.4.2.2 Titkosító magánkulcs felhasználó

Titkosító magánkulcs felhasználó lehet:

a. bármely természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítvány osztálynak megfeleloen, a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSZSZ-F 3.1.8 pontjában eloírtak szerint igazolta.

b. bármely természetes személy, aki részére a titkosító tanúsítvány azzal a céllal kerül kibocsátásra, hogy jogi személy (szervezet) képviseletében legyen jogosult titkosított adatállomány visszaállítására. Ebben az esetben a titkosító magánkulcs felhasználó személyazonosságának ellenorzése mellett a regisztráció során a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSZSZ-F 3.1.9 pontjában meghatározott módon a képviseleti jogosultságot is ellenorizni kell.

1.4.2.3 Érintett fél

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

b. Érintett fél lehet titkosító szerver is.

Az Érintett fél ezen muveletnél a titkosító magánkulcs felhasználó Nyilvános kulcsához tartozó tanúsítvány érvényességi ellenorzésére hagyatkozva jár el.

1.4.3. Alkalmazhatóság

1.4.3.1 Szabályzat hatálya

A HSZSZ-T idobeli hatálya a hatálybalépés dátumával kezdodik és határozatlan idore szól. Idobeli hatálya megszunik egy újabb szabályzat verzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor.
A HSZSZ-T személyi hatálya a felhasználó közösségre terjed ki.

A HSZSZ-T tárgyi hatálya a következokre 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 a jelen szabályozás keretében az Eat. szerinti fokozott biztonságúval azonos szintu szolgáltatást nyújt.

1.4.3.3 Titkosító tanúsítványok alkalmazhatósága

A titkosító tanúsítványok alkalmazhatóságára a következo alapszabályok érvényesek:

Engedélyezett alkalmazási lehetoségek

> **A kibocsátott titkosító nyilvános kulcs csak elektronikus állományok titkosítására, a titkosító magánkulcs pedig csak a titkosított elektronikus állományok visszaállítására használható fel, a titkosító tanúsítványba foglaltaknak megfeleloen.**

Korlátozott alkalmazási lehetoségek

> Szolgáltató az elofizetoi szerzodésben felhasználási, területi, pénzügyi, stb. korlátozásokat szabhat. A korlátozásokat a kibocsátott elofizetoi tanúsítványban is megadja.

Tiltott alkalmazási lehetoségek

> Tilos az elofizetoi titkosító tanúsítványok felhasználása más nyilvános kulcsú tanúsítványok aláírására, vagy alkalmazása bármilyen hitelesítés szolgáltatás nyújtásához.

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

A Szolgáltató nem vállal felelosséget a titkosításra kibocsátott tanúsítvány, illetve az ehhez kapcsolódó titkosító kulcspárok titkosítástól eltéro felhasználásáért.

Jelen HSZSZ-T hatálya alatt kibocsátott titkosító tanúsítványok csak az 1.4 fejezetben meghatározott hitelesítés-szolgáltató és felhasználó közösség körében használhatók az Általános Szerzodési Feltételek Titkosítás Hitelesítés Szolgáltatáshoz c. dokumentumban (ÁSZF-T), illetve az Elofizetoi Szerzodésben meghatározott összeghatárok szerinti korlátokkal.

A titkosító tanúsítvány használati lehetoségére vonatkozó fenti információk a titkosító tanúsítványban is rögzítésre kerülnek. A titkosító tanúsítvány elfogadása, a feltüntetett használati információktól eltéro bármely módú használata a titkosító magánkulcs felhasználó és az Érintett fél egyéni felelossége és kockázata.

Összefoglalva:

A titkosításra kibocsátott kulcsok és tanúsítványok kizárólag titkosított állományok létrehozására, illetve azok visszaállítására használhatók. A Szolgáltató nem vállal felelosséget a titkosításra kibocsátott kulcsok és tanúsítványok titkosítástól eltéro célú használatáért.

A Szolgáltató a jelen HSZSZ-T által meghatározott szolgáltatási körében csak titkosító tanúsítványokat bocsát ki.

2. Általános rendelkezések

2.1 Feladatok és hatáskörök

2.1.1. A Szolgáltató feladatai és hatásköre

1. A Szolgáltató gondoskodik a szolgáltatásra vonatkozó valamennyi, a jelen HSZSZ-T-ben részletezett feltétel teljesüléséről, amennyiben azok az adott tanúsítványtípusra alkalmazhatók.
2. A Szolgáltató szolgáltatásait nyilvánosan elérhetové teszi.
3. A Szolgáltató jogi személy.
4. A Szolgáltató HSZSZ-T-ét rendszeresen felülvizsgálja.
5. A Szolgáltató mindenkor az Elofizeto által megadott és az Ügyfélkapcsolati Irodák által ellenorzött adatok alapján bocsátja ki a tanúsítványokat.
6. A Szolgáltató a tanúsítvány kibocsátását követoen a tanúsítvány adataiban nem változtathat.
7. A Szolgáltató kötelezettséget vállal arra, hogy az elofizeto regisztrációját követoen a tanúsítvány kiadása ára intézkedik és errol az Elofizetot értesíti. Tanúsítvány kiállítására ezt követoen legkésobb 30 naptári napon belül kerül sor.
8. A Szolgáltató a szolgáltatások muködtetése 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 elérhetové teszi a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó saját szabályzatait.
11. A Szolgáltató az érvényes tanúsítványok tekintetében a lejárat elotti 30 napban értesítést küld a lejáró tanúsítványokról az Elofizeto részére.
12. Szolgáltató a tanúsítványban feltünteti az Elofizetoi Szerzodésben 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 megorzi a titkosító tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetoleg – amennyiben ezen idoszakban a titkosító tanúsítvánnyal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogeros lezárásáig. Ugyanezen határidoig olyan eszközt is biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.
15. Ha a Szolgáltató be kívánja fejezni tevékenységét, errol legalább hatvan nappal korábban értesíti az Elofizetoket.
16. A Szolgáltató intézkedik az iránt, hogy legkésobb a tevékenysége befejezésekor más - vele legalább azonos besorolású - szolgáltató átvegye nyilvántartásait, így különösen a visszavont tanúsítványok nyilvántartását, valamint ellássa a hatályos jogszabályokban foglalt feladatokat. A Szolgáltató a visszavont tanúsítványokkal kapcsolatos minden adatot - beleértve a személyes adatokat is – átadja ezen szolgáltatónak.

2.1.1.1 Az Ügyfélkapcsolati Iroda feladatai és hatásköre

1. Felveszi a regisztráció során az elofizeto adatait és elkészíti az elofizetoi szerzodést,
2. összegyujti, illetve meghatározza a tanúsítványba kerülo adatokat,
3. megorzi a nyilvántartásokat,
4. bizalmas információként kezeli az Elofizeto és a titkosító magánkulcs felhasználó minden adatát, kivéve azokat, amelyeket a tanúsítványba kerülnek,
5. gondoskodik a titkosító magánkulcs hordozó eszköz és a PIN kód biztonságos kezeléséről és az Elofizetonek történo biztonságos átadásáról,
6. korlátozás nélkül biztosítja a titkosító magánkulcs felhasználó számára a rá vonatkozó regisztrációs és egyéb adatokhoz történo 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 a titkosító magánkulcs felhasználó adatainak változására vonatkozó kérelmeket.

2.1.2. Az Elofizeto és a titkosító magánkulcs felhasználó feladatai és hatásköre

Az Elofizeto és a titkosító magánkulcs felhasználó kötelessége a Szolgáltató szerzodéses feltételeinek és szabályzatainak megfeleloen eljárni a szolgáltatás igénybevétele során, ezen belül köteles:

1. a tanúsítvány igénylését és a kulcspár felhasználását úgy végezni, hogy a z harmadik fél jogait ne sértse,
2. az Elofizeto a tanúsítvány kiadásához szükséges, a titkosító magánkulcs felhasználókra vonatkozó adatokat ellenorizni,
3. az Elofizeto és a titkosító magánkulcs felhasználó megismerni a magánkulcsának átvétele és felhasználása elott a magánkulcs tárolásával, az állományok titkosításával, illetve visszaállításával kapcsolatos technikai, jogi, biztonsági követelményeket és feltételeket,
4. a titkosító magánkulcs felhasználó biztosítani a kulcshordozó eszközének és adatának, valamint a kulcshordozó eszköz és a transzport kulcs PIN kódjának védelmét,
5. az Elofizeto, illetve a titkosító magánkulcs felhasználó 3 (három) munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történo változásokat, különös tekintettel a titkosító tanúsítványba foglalt adatokra,
6. a jogi személy Elofizeto a titkosító magánkulcs felhasználóinak figyelmét külön felhívni arra, ha az Elofizetoi Szerzodés a tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat tartalmaz
7. a titkosító magánkulcs felhasználó tudomásul venni, hogy magánkulcsának használata és védelme kizárólag a saját felelossége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelosség nem terheli,
8. a jogi személy Elofizeto megbízott kapcsolattartója tudomásul venni, hogy transzport magánkulcsának használata és védelme kizárólag a saját felelossége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelosség nem terheli,
9. a titkosító magánkulcs felhasználó azonnal intézkedni Tanúsítványának visszavonása, illetve felfüggesztése végett, ha
   9.1. tudomására jut, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, tartalmában, a regisztrációs adatokban pontatlanság van, illetve azokban változás következett be,
   9.2. a titkosító magánkulcs és/vagy a PIN kód nem a titkosító magánkulcs felhasználó kizárólagos birtokában van (elveszett, ellopták, esetleg kompromittálták), vagy ennek alapos gyanúja áll fenn;
10. a titkosító magánkulcs felhasználó vagy az Elofizeto a titkosítási eljárással vagy a titkosított állománnyal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót.
11. a titkosító magánkulcs felhasználó jogosult arra, hogy a magánkulcsot birtokolja, és azt titkosított állományok visszaállítására (a Tanúsítványban is feltüntetett névmegadás szerint) saját, illetve szervezete nevében felhasználja,

2.1.3. Érintett fél feladatai és hatásköre

A titkosítás elott az Érintett fél kötelessége a Szolgáltató szabályzatainak megfeleloen a legnagyobb gondossággal eljárni a titkosító magánkulcs felhasználó Nyilvános kulcsához tartozó tanúsítvány elbírálásakor, ezen belül:

1. A tanúsítvány elfogadása elott meg kell értenie a titkosítással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat.
2. Meg kell ismernie Szolgáltató nyilvánosan elérheto szabályzatait (a jelen HSZSZ-T-t és a hozzá tartozó ÁSZF-T-t). A titkosítási eljárásnak a titkosítandó állományon történo alkalmazása a Szolgáltató ezen szabályzatainak elfogadását jelenti.
3. A tanúsítvány érvényességét és hatályosságát ellenoriznie kell a nyilvánosan elérheto Tanúsítványban. Az Érintett fél köteles tudomásul venni, hogy a titkosító nyilvános kulcshoz tartozó tanúsítvány ellenorzésének elmulasztásából eredo következményekért az Érintett fél felel
4. A titkosítási akciót az Érintett fél nem indíthatja el, ha a titkosító magánkulcs felhasználó Nyilvános kulcsának Tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata annak érvénytelenségére utal,
5. az Érintett fél tudomásul veszi, hogy a titkosító magánkulcs felhasználó Nyilvános kulcsával titkosított állományt saját felelosségére készíti, és viseli ennek esetleges jogkövetkezményeit;
6. az Érintett fél a Tanúsítványt csak a jelen HSZSZ-T-nek megfeleloen használhatja; titkosított állományt csak a tanúsítvány érvényességi ideje alatt készíthet.

2.2 A szolgáltató és a felhasználó közösség tagjainak felelossége

2.2.1. A Szolgáltató felelossége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-T 1.4.3.3 pontja szerint meghatározott titkosító tanúsítványt – és ezzel jelzi a felhasználói közösség és az érintett felek felé ezen HSZSZ-T használatát –, csak azért vállalja a felelosséget, hogy a titkosító tanúsítvány eloállítása, kibocsátása, közzététele, visszavonása és a Visszavonási Lista közzététele a jelen HSZSZ-T-ben eloírtaknak teljes mértékben megfelel, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy maga és az elofizetok is a jelen HSZSZ-T eloírásainak megfeleloen járjanak el.

A Szolgáltató köteles a tanúsítvány megfelelo mezojében feltüntetni, ha az Elofizetoi Szerzodésben a tanúsítvány felhasználhatóságával kapcsolatban összegszeru, területi vagy egyéb korlátozásokat köt ki. Ezen korlátokat meghaladó ügyletekben felvetett követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.

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

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

2.2.2. Az Elofizeto és a titkosító magánkulcs felhasználó felelossége

Az Elofizetonek felelossége áll fenn a Szolgáltatóval szemben a regisztráció során megadott adatainak valódiságával kapcsolatban.

Az Elofizetonek kártérítési felelossége áll fenn Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket a regisztráció során megadott helytelen adataival, vagy az azokban bekövetkezett változások be nem jelentésével, vagy egyéb kötelezettségeinek be nem tartásával számára okoz.

A titkosító magánkulcs felhasználó felelos azért, ha magánkulcsát nem a HSZSZ-T-ben, az ÁSZF-T-ben és a vonatkozó jogszabályokban meghatározott módon és célra használta.

Az Elofizeto és a titkosító magánkulcs felhasználó felelos a magánkulcs biztonságos megorzéséért, a kulcs tartalom és a PIN kód illetéktelenek tudomására jutásának megakadályozásáért.

2.2.3. Érintett fél felelossége

Érintett fél felelossége fennáll a titkosító tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a titkosító tanúsítvány érvényességének és hatályosságának ellenorzése során nem a jelen HSZSZ-T szerint jár el.

Az Érintett fél felelos a Szolgáltató által kibocsátott titkosító tanúsítványok elfogadása során tanúsított körültekinto magatartásért, a tanúsítványlánc ellenorzéséért, valamint a Szolgáltató nyilvánosan elérheto szabályzatai rá vonatkozó részeinek megismerésért, a szabályzatokban meghatározott kötelezettségeinek betartásáért.

2.2.4. Az anyagi felelosség korlátai

A Szolgáltató anyagi felelosségérol és annak korlátairól az ÁSZF-T rendelkezik.

2.3 Értelmezés és alkalmazás

2.3.1. Alkalmazott jogszabályok

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

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

2.3.2. Érvénytelenség, hatályosság, megszunés, értesítések

2.3.2.1 Érvénytelenség

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

2.3.2.2 Hatályosság

A HSZSZ-T, az ÁSZF-T és az elofizetoi szerzodés a közösség résztvevoinek valamennyi kötelezettségét, felelosségét és jogát tartalmazza.

A HSZSZ-T csak a Szolgáltató részérol, írott és aláírással hitelesített formában módosítható.

2.3.2.3 Megszunés

A HSZSZ-T a Szolgáltató titkosítás hitelesítés-szolgáltatásának befejezésével tekintendo megszuntnek.

2.3.2.4 Értesítések

Az Elofizetok és az Érintett felek vagy bármely harmadik fél az Ügyfélkapcsolati Irodát megkeresheti ügyfélfogadási idoben 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 Elofizetoket és Érintett feleket tipikusan a szolgáltatás Internetes honlapján történo közzététellel, illetve az ügyfélkapcsolati irodákban elérheto dokumentumokkal tájékoztatja. Az ügyfélkapcsolati irodák az Elofizetoket esetenként írásban vagy elektronikus úton is értesíthetik.

2.3.3. Vitás kérdések kezelése

Bármely vitás kérdés felmerülése esetén az Elofizetonek, az Érintett félnek, vagy bármely harmadik félnek kötelessége a Szolgáltató haladéktalan értesítése és teljes köru tájékoztatása a kérdés minden vonatkozását érintoen, a vita jogi útra terelése elott.

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

A jogvitáik rendezésére vonatkozó szabályokat az ÁSZF-T 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 elofizetokre vonatkozó hatályos szolgáltatási díjak az Elofizetoi Szerzodésben kerülnek rögzítésre.

A Szolgáltató a következo pontokban ismertetett díjtípusokat alkalmazza a szolgáltatások nyújtásakor.

2.4.1. Tanúsítványok kibocsátása

Szolgáltató a kibocsátott titkosító tanúsítványokért a tanúsítványok érvényességének idotartamára éves fenntartási díjat számol fel az Elofizeto felé. Az éves fenntartási díj tartalmazza

a. a titkosító tanúsítványok kibocsátásának és a titkosító kulcspárok eloállításának díját,

b. a titkosító tanúsítványoknak a Szolgáltató Tanúsítványtárában történo közzétételének díját,

c. a titkosító tanúsítványok és kulcspárok biztonságos megorzésének a díját.

Visszavont tanúsítványok esetén minden megkezdett év teljes évnek számít.

A Szolgáltató külön díjfizetés ellenében vállalja a titkosító tanúsítványok érvényességi idejének lejárta, illetve esetleges visszavonása után is a tanúsítványok és a titkosító kulcspárok biztonságos megorzését és tárolását, továbbá szükség esetén, - a korábbi titkosított állományok visszaállítása érdekében - a tanúsítványok és a titkosító kulcspárok kiadását az Elofizetonek.

A tanúsítvány újbóli kiadásáért a Szolgáltató minden esetben díjat számol fel.

2.4.2. Tanúsítvány hozzáférés

Szolgáltató a tanúsítványok közzétételéért, valamint 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 a kibocsátott tanúsítványok újraérvényesítéséért eljárási díjat számol fel az Elofizeto felé, mely tartalmazza a tanúsítvány megváltozott állapota közzétételének díját is.

2.4.5. Visszatérítési elvek

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

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

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

c. a kibocsátott kulcshordozó eszközön szereplo adatok a Szolgáltató hibájából fakadóan nem megfelelok,[1]

d. a kibocsátott kulcshordozó eszköz, az aktivizáló kód és a kulcsok nem összetartozók,

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

A díj visszatérítésére vonatkozó igényt elofizetonek a tanúsítvány kibocsátását, illetve megújítását követo 30 naptári napon belül a regisztrációt végzo Ügyfélkapcsolati Irodánál kell 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 Elofizeto által megjelölt bankszámlaszámra 20 naptári napon belül átutalja, vagy részére új tanúsítványt bocsát ki.

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

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 elofizetok és az érintett felek rendelkezésére álljanak. Ezek közé tartozik különösképpen:

a. tanúsítványok használatára vonatkozó ismertetok, szabályzatok, nyomtatványok

b. a kibocsátott elofizetoi és szolgáltatói tanúsítványok

c. a felfüggesztett és visszavont elofizetoi és szolgáltatói tanúsítványok

d. szolgáltatói közlemények

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

a. A Szolgáltató az elofizetoi tanúsítványokat a kibocsátást követoen, a regisztrációs eljárás részeként, az Elofizetonek átadja,

b. A Szolgáltató az elofizetoi tanúsítványokat a kibocsátást követo 24 órán belül Tanúsítványtárában közzéteszi.

2.5.2. Elérési szabályok

A Szolgáltató minden Elofizeto és Érintett fél számára elérhetové teszi a szolgáltatás Internetes honlapját, azon keresztül Tanúsítványtárát és Visszavonási Tanúsítványok Listáját olvasás céljából. A Tanúsítványtárban keresési lehetoséget biztosít a tanúsítványokban tárolt adatok alapján.

A Szolgáltató belso adatbázisait és egyéb adatállományait a jogszabályokban meghatározott kötelezettségeken túl csak és kizárólag a Szolgáltató biztonsági szabályzatai által meghatározott szerepkörü és jogosultságú munkatársai érhetik el.

2.5.3. Tanúsítványtár

A Szolgáltató a tanúsítványokat, a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, valamint a visszavont tanúsítványok listáját Tanúsítványtárán keresztül teszi hozzáférhetové.

2.6 Bizalmasság – Adatkezelési szabályzat

2.6.1. Bizalmas információk

Szolgáltató az elofizetok és a titkosító magánkulcs felhasználók adatait kizárólag csak a titkosítás hitelesítési-szolgáltatással összefüggésben használhatja fel.

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

1. A titkosító magánkulcs tárolt példányát és a fontos bejegyzéseket védi az elveszéstol, tönkretételtol és hamisítástól,
2. megfelelo technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénysérto kezelése ellen,
3. nyilvántartásba veszi az elofizetovel aláírt szerzodést, beleértve az elofizeto és a titkosító magánkulcs felhasználó hozzájárulását az alábbiakhoz:

[1] Pl. a kártya fizikai megszemélyesítése nem megfelelo

3.1. hozzájárulás a szolgáltatások során felhasznált adatok hitelesítés-szolgáltató által történo nyilvántartásba vételéhez,

3.2. hozzájárulás a nyilvántartásba vett adatok harmadik félhez történo 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 Elofizetore és a titkosító magánkulcs felhasználóra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz o maga hozzájárul, vagy ha bíróság, illetve egyéb jogi követelmény ezt eloírja,

6. védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az elofizetovel folytatott adatcsere során is.

A Szolgáltató az Elofizetok és a titkosító magánkulcs felhasználók személyes adatait csak a közöttük fennálló Elofizetoi Szerzodéssel összhangban levo célokra használhatja fel, harmadik félnek azokat az Elofizetok és az Aláírók írásos hozzájárulása nélkül nem adhatja át, kivéve a 2.6.4 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 Elofizeto és a titkosító magánkulcs felhasználó azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

2.6.2. Nem bizalmas információk

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

2.6.3. 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.

2.6.4. Feltárás törvényi meghatalmazással rendelkezok részére

A Szolgáltató a titkosítás felhasználásával elkövetett buncselekmények felderítése vagy megelozése céljából, illetoleg nemzetbiztonsági érdekbol – az érintett személyazonosságát igazoló adatok tekintetében a 2001. évi XXXV. törvény 11.§ paragrafusa alapján – adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató a titkosító magánkulcs felhasználót nem tájékoztathatja.

2.6.5. Információszolgáltatás polgári eljárás keretében

A Szolgáltató a tanúsítvány érvényességét érinto polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - a titkosító magánkulcs felhasználó személyazonosságát igazoló adatokat átadhatja az ellenérdeku peres félnek vagy képviselojének feltárhat bizalmas felhasználói információkat, illetoleg azt közölheti a megkereso bírósággal. A Szolgáltató rögzíti az információszolgáltatás tényét, és arról tájékoztatja az Elofizetot és a titkosító magánkulcs felhasználót.

2.6.6. Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezok részére történo adatszolgáltatáson túl más Társaság üzleti titkát, az Elofizetok és a titkosító magánkulcs felhasználók nem nyilvános személyes adatait csak az illeto Társaság, illetve Elofizeto írásos (hagyományos vagy minosített elektronikus aláírással ellátott) meghatalmazása alapján tárhatja fel hamadik fél részére.

2.7 Szellemi tulajdonhoz fuzodo jogok

A Szolgáltató által elofizetoi részére kibocsátott tanúsítványok és az azokhoz tartozó kulcspárok tulajdonosa az Elofizeto, teljes jogú használója pedig a titkosító magánkulcs felhasználó, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

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

A Szolgáltató tulajdonát képezik:

a. a titkosító magánkulcs felhasználó részére kibocsátott egyedi azonosító

b. a visszavonási információk

c. a Szolgáltató szabályzatai, szerzodéses feltételei

d. a Tanúsítványban szereplo hitelesíto azonosító.

3. Azonosítási és hitelesítési eljárások

3.1 Regisztráció

A regisztrálás során:

a. Az Elofizeto kitölti vagy kitölteti a regisztrációs urlapot és az Ügyfélkapcsolati Iroda részére átadja személyesen vagy megküldi (elektronikus) levélben,

b. a regisztrációs urlap elfogadásával Szolgáltató gondoskodik az Elofizetoi Szerzodés elokészítéséról és intézkedik a kulcspár és az elofizetoi tanúsítvány elkészítésére,

c. Az elofizetoi tanúsítvány elkészültével értesíti az elofizetot és egyezteti vele a tanúsítvány és az Elofizetoi Szerzodés átvételének módját.

A regisztrációs urlap egyúttal az Elofizetoi Szerzodés szerepét is betöltheti.

Nevek típusa

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

Nevek szemantikája

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

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

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

Nevek egyedisége

A Szolgáltató biztosítja tanúsítványtárában a tulajdonosazonosítók egyediségét. Errol elsodlegesen a titkosító magánkulcs felhasználó e-mail címének a névmegadásban való szerepeltetése gondoskodik. A Szolgáltató a név azonosító kiosztásakor ellenorzi, hogy az adott e-mail cím nem szerepel-e egy más titkosító magánkulcs felhasználó részére korábban kibocsátott tanúsítványban. Ha szerepel, és a tanúsítvány egyéb mezoi sem biztosítják az egyediséget, akkor a Szolgáltató fenntartja magának a jogot a név olyan megváltoztatására, amely továbbra is jellemzo a titkosító magánkulcs felhasználóra, de biztosítja a megkülönböztethetoséget.

Név igénylési viták feloldása

A titkosító magánkulcs felhasználót a tanúsítványban megadott név és a tanúsítvány sorozat száma különbözteti meg egyértelmuen a többi a titkosító magánkulcs felhasználótól.

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

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

Védjegyek elismerésének és hitelesítésének módszere

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

3.1.1. A titkosító magánkulcs birtoklás ellenorzésének módszere

A titkosító tanúsítványhoz tartozó titkosító kulcspár generálása a Szolgáltató Hitelesíto Központjában történik. Központi kulcspár generálás esetén a titkosító nyilvános és magánkulcs egymáshoz tartozásának, valamint a titkosító magánkulcs birtoklásának ellenorzésére nincs szükség, csupán a titkosító magánkulcs felhasználóhoz eljutatott kulcshordozó eszköz, illetve magánkulcs átvételének igazolására van szükség. A kulcshordozó eszköz személyes átvételénél az Elofizeto írásban igazolja a kulcshordozó eszköz és a PIN kód átvételét. Az átvétel után az

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

Elofizeto és a titkosító magánkulcs felhasználó teljes felelosséget visel a kulcshordozó eszköz és a PIN kód biztonságos használatáért és megorzésért.

Az Elofizeto és a titkosító magánkulcs felhasználó azonosság hitelesítése

Titkosító tanúsítvány igénylése esetén a Szolgáltató az Elofizeto és a titkosító magánkulcs felhasználó azonosság hitelesítés ét a fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatásra érvényes szolgáltatási szabályzat (HSZSZ-F) aktuális változata 3.1.7. - 3.1.9 fejezetei szerint végzi el.

3.2 Tanúsítványok érvényessége

A Szolgáltató által kibocsátott elofizetoi titkosító tanúsítványok érvényességi ideje 5 év.

3.3 Érvénytelen tanúsítványok megorzése

A Szolgáltató a visszavont és a lejárt elofizetoi titkosító tanúsítványokat a visszavonástól, illetve a lejárattól számított öt évig megorzi, igény esetén újra kiadja.

3.4 Felfüggesztés és visszavonási kérés

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványok érvényességét az elofizeto vagy a titkosító magánkulcs felhasználó kérésére felfüggessze vagy a tanúsítványt visszavonja. Ennek érdekében a Szolgáltató a 4.4 pontban rögzíti a tanúsítványok visszavonásának és felfüggesztésének eljárásai.

4. A muködésre vonatkozó követelmények

4.1 Tanúsítványigénylés

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

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

a. vállalja a kulcshordozó eszköz has ználatát, védelmét
b. garantálja feltüntetett adatainak valódis ágát
c. megfizeti a szolgáltatások díját
d. az adatok késobbi változásairól a Szolgáltatót értesíti

A regisztráció során az Ügyfélkapcsolati Iroda nyilvántartásba veszi a titkosító magánkulcs felhas ználó azonosítására használt adatokat, beleértve az igazoláshoz használt dokumentumok regisztrációs számát és az azok érvényességével kapcsolatos esetleges korlátozásokat. Az Elofizeto aláírásával tudomásul veszi és elfogadja, hogy a dokumentációkról az Ügyfélkapcsolati Iroda másolatot készíthet.

A Tájékoztató a szolgáltató internetes honlapján bárki számára elérheto.

4.2 Tanúsítvány kibocsátás

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

Az elkészült Tanúsítványt a Szolgáltató a következo módon juttatja el az Elofizetohöz:

a. az Elofizeto, a titkosító magánkulcs felhasználó vagy azok képviseloje személyesen átveheti az Ügyfélkapcsolati Irodán, vagy
b. postai úton eljuttatja az Elofizeto által megadott címre, vagy
c. az Elofizeto utólagosan letöltheti a nyilvános Tanúsítványtárból

4.3 Tanúsítvány elfogadás

A tanúsítvány elfogadása az Elofizeto részérol az átvétellel történik meg.

4.4 Tanúsítványok visszavonása

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatásokat nyújt.

A visszavonási/felfüggesztési kérelmeket a Szolgáltató folyamatosan (mindennap 24 órában) fogadja úgy, hogy esetenként a visszavonási/felfüggesztési kérelem végrehajtásának ideje nem lehet több, mint 24 óra.

4.4.1. Visszavonáshoz/felfüggesztéshez vezeto körülmények

Az Elofizeto vagy a titkosító magánkulcs felhasználó a következo körülmények fennállása esetén kezdeményezheti a visszavonást/felfüggesztést:

1. a magánkulcs kompromittálódása, vagy annak gyanúja,
2. a kulcshordozó eszköz elvesztése, eltulajdonítása, megrongálódása,
3. a kulcshordozó eszközt védo aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja,
4. a magánkulcs átvételének visszautasítása,
5. a Tanúsítványban feltuntetett hibás adatok,
6. az Elofizetonek a Tanúsítványban feltuntetett adatainak megváltozása,
7. a titkosító magánkulcs felhasználónak a Tanúsítványban feltuntetett adatainak megváltozása,
8. a Tanúsítványban feltuntetett szervezet adatainak megváltozása,
9. a Tanúsítványban feltuntetett titkosító magánkulcs felhasználó és szervezet kapcsolatának megváltozása vagy megszunése miatt.

Szolgáltató a visszavonási kérelmet mérlegelés nélkül teljesíti, ha azt a titkosító magánkulcs felhasználó vagy az Elofizeto kéri.

A tanúsítvány a Szolgáltató kezdeményezése alapján kerül visszavonásra, ha:

1. a tanúsítvány felfüggesztési ideje lejárt,
2. az Elofizeto és/vagy a titkosító magánkulcs felhasználó az ÁSZF-T-et vagy az Elofizetoi Szerzodést megszegi,
3. az Elofizeto és/vagy a titkosító magánkulcs felhasználó kötelezettségeiket nem tartják be,
4. az Elofizetoi szerzodés megszunik,
5. a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról,
6. a Tanúsítványban feltuntetett kibocsátó adatok megváltoznak,
7. a hitelesítési szolgáltatás megszunik,
8. a Regisztrációs Iroda megszunik,
9. a Szolgáltató valamely magánkulcsa kompromittálódik.

4.4.2. Visszavonás/felfüggesztés kérelmezése

A visszavonási/felfüggesztési kérelmet be lehet nyújtani személyesen vagy írásban a Szolgáltató Ügyfélkapcsolati Irodájánál. Ha a bejelento akadályoztatása miatt a visszavonási igényét személyesen nem tudja bejelenteni vagy azonnali intézkedés szükséges, akkor a tanúsítvány felfüggesztése telefonon vagy elektronikusan aláírt e-mailben is kérheto az Ügyfélszolgálaton. A tanúsítvány visszavonására vagy visszaállítására az ettol számított 30 napon belül lehet intézkedni.

A visszavonási/felfüggesztési kérelem teljesítéséhez a következo adatok szükségesek:

a. a tanúsítvány sorszáma

b. a visszavonást/felfüggesztést kéro azonosító adatai

c. a visszavonást/felfüggesztést kéro e-mail címe

d. a visszavonáshoz/felfüggesztéshez vezeto körülmények

4.4.3. Visszavonási listák (CRL) kibocsátási gyakorisága

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

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

4.4.4. Visszavont Tanúsítványok Listája (CRL) ellenorzési követelmények

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

A tanúsítvány visszavonási listában a Szolgáltató által közzétett érvénytelen, vagy felfüggesztett tanúsítvány elfogadásából keletkezo bárminemu kár Érintett felet terheli. (Lásd még a 2.2.3 pontot.)

4.4.5. Speciális követelmények magánkulcs kompromittálódás esetére

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

A kompromittálódott titkosító magánkulcsot a megsemmisítésig ugyanolyan felügyeletben kell részesíteni, mint egy érvényes titkosító magánkulcsot.

Az Elofizetonek kötelessége a kompromittálódott titkosító magánkulcs által esetlegesen érintett felek értesítése, és minden intézkedés megtétele az esetleges károk megelozése és enyhítése érdekében.

4.5 Biztonsági naplózások, archívum

4.5.1. Naplózott esemény típusok

A Szolgáltató által végzett muveletek naplózásra kerülnek. A naplóbejegyzések a regisztráció, a titkosító kulcs-pár generálása, a kulcshordozó eszköz megszemélyesítése, a tanúsítvány létrehozása, kibocsátása és kezelése, valamin egyéb Szolgáltatói tevékenységek során készülnek.

4.5.2. Napló adatok tárolása

A napló adatok rendszeresen archiválásra kerülnek ellenorzés, 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 megorzésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

4.5.4. Az archívum megorzési idotartama

A Szolgáltató a titkosító kulcspárt és tanúsítványokra vonatkozó archív adatokat a lejáratuktól számított 5 évig, illetve jogi eljárásban a tanúsítványokon keresztül történo bizonyításhoz szükséges ideig megorzi.

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. Errol az eseményrol Szolgáltató lehetoségei szerint értesíti 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.

5. Fizikai, eljárásrendi, és humán biztonsági szabályozások

A fizikai, eljárásrendi, és humán biztonsági szabályozásokra a HSZSZ-F aktuális változata 5. fejezetének tartalma irányadó, azzal a megjegyzéssel, hogy az ott néhány helyen eloforduló, az elektronikus aláírással kapcsolatos kifejezések helyett a megfelelo titkosítási kifejezéseket kell használni.

6. Muszaki biztonsági óvintézkedések

A Szolgáltató megbízható, biztonságtechnikailag értékelt és minosített termékekbol álló, egységes inform atikai rendszert használ szolgáltatásai nyújtásához.

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

6.1 Kulcs-pár eloállítás és telepítés

6.1.1. Kulcs-pár eloállítás

A Szolgáltató maga generálja a kulcspárt biztonságos hardver (HSM) modulban[3], vagy magán a kulcshordozó eszközön (kártyán). Nem fogad el az Elofizeto által generált titkosító magánkulcsot, illetve kulcshordozó eszközt.

A Szolgáltatónál a kulcseloállítást fizikailag védett környezetben, bizalmi munkakört betölto személyzet végzi. A kulcspár eloállítási funkció végrehajtására felhatalmazott személyzet körét a Szolgáltató a leheto legkisebbre korlátozza. A Szolgáltató a kulcs eloállítását a fokozott biztonsági szintnek megfelelo módon állítja elo.

A titkosító magánkulcs kulcshordozó eszközön történo elhelyezésére a Szolgáltató csak a titkosító kulcspárhoz tartozó tanúsítvány kulcshordozó eszközön történo elhelyezésével együtt vállalkozik.

A Szolgáltató személyes típusú tanúsítványokhoz kulcshordozó eszközként általában csipkártyát alkalmaz. A csipkártya megszemélyesítés szolgáltatáshoz vizuális – egy oldali nyomással történo – grafikus megszemélyesítés is kapcsolódik az Elofizetoi Szerzodésben meghatározott adattartalommal. A kulcshordozó eszköz megszemélyesítése a Szolgáltatónál – fokozott biztonságú környezetben – üzemelo megszemélyesíto rendszeren történik.

A Szolgáltató a kulcshordozó eszközhöz PIN kódot biztosít.

A generált titkosító tanúsítvány és magánkulcs egy példányát a Szolgáltató fokozottan biztonságos körülmények között megorzi és tárolja (archiválja) a tanúsítvány érvényességi idejének lejárta, vagy visszavonása után szükségessé váló titkosított állományok visszaállíthatósága céljából.

6.1.2. A titkosító magánkulcs Felhasználóhoz történo eljuttatása

A Szolgáltató:

a. a kulcsokat az Elofizeto által történo átvételig biztonságos módon tárolja,

b. a magánkulcsot az Elofizetonek úgy adja át, hogy a magánkulcs titkossága ne sérüljön,

c. a kulcshordozó eszköz aktivizálási adatát (PIN kódját) biztonságosan készíti el és a kulcshordozó eszköztol elkülönítve tárolja.

Az Elofizetonek a kulcshordozó eszközt és a PIN kódot tartalmazó borítékot az átvétel írásos elismerésével kell átvennie.

A kulcshordozó eszköz átvételének megtagadása a titkosító tanúsítványra nézve visszavonási kérelemnek számít.

6.1.3. Nyilvános kulcs ellenorzo adat eljuttatása a Felhasználókhoz

A Szolgáltató a Hitelesíto Központok és az Elofizetok nyilvános kulcsait a kibocsátott tanúsítványokban helyezi el. A Hitelesíto Központok tanúsítványait a szolgáltatás honlapján, az Elofizetoi tanúsítványokat a Tanúsítványtárában teszi a felhasználói közösség számára elérhetové.

6.1.4. Kulcs méretek, használt algoritmusok

A Szolgáltató Hitelesíto Központja elektronikus aláírás létrehozására az RSA[4] algoritmust használja. Az Elofizetoi tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

A titkosító magánkulcs felhasználók (Elofizetok)
titkosító magánkulcsainak mérete: 1024 bit

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

6.1.5. Kulcs felhasználási célok

A Szolgáltató Elofizetoi részére kulcspárt a jelen HSZSZ-T hatókörében csak titkosítási céllal bocsát ki.

---

[3] HSM: Hardware Security Modul

4 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.

Ennek érdekében az Elofizetok részére kibocsátott titkosító tanúsítványok bovítmény (Extension) részében található „KeyUsage” mezoben a titkosítási célt megjelölo paramétert állít be.

6.2 Magánkulcsok védelme

6.2.1. Kriptográfiai modulra vonatkozó szabványok

Az Elofizetok titkosító magánkulcsának tárolására Szolgáltató olyan kulcshordozó eszközt bocsát ki, mely teljesíti a FIPS 140-1 Level 3 követelményeket

A titkosító magánkulcsot a Szolgáltató PIN kóddal védve bocsátja ki. A titkosító magánkulcs dokumentált átvétele után az Elofizeto felelos a kulcshordozó eszköz, a titkosító magánkulcs, valamint a PIN kód védelméért.

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

A Szolgáltató az elofizetoi titkosító magánkulcsokat a kulcshordozó eszközre a következo módokon viheti fel:

1. Egy olyan biztonságos kulcshordozó eszközben tárolja, amely nem kompromittálja a magánkulcs biztonságát, megfelel az ISO/IEC 15408 1999/1.,2.,3. szabvány szerint kidolgozott SSCD-PP[5] védelmi profil követelményeinek, és amely szerepel a Nemzeti Hírközlési Hatóság elektronikus aláírás termék listáján.
2. A titkosító magánkulcs a 6.1.2 pontban meghatározott módon a transzport nyilvános kulccsal titkosítva kerül a kulcshordozó eszközre, amelyet a megbízott kapcsolattartó a 6.1.2 pontban meghatározott módon állít vissza a titkosító magánkulcs felhasználó jelenlétében.

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

A Szolgáltatónál egyedül a Hiteles íto Központban alkalmazzák az „n-bol m” ellenorzést.

6.2.3. Titkosító magánkulcs letét

Az elofizetoi titkosító magánkulcsot a Szolgáltató letétbe nem helyezheti.

6.2.4. Titkosító magánkulcs biztonsági mentése

A Szolgáltató az elofizetok titkosító magánkulcs airól generálás után biztonsági másolatot (mentést) készít. A biztonsági másolatokat megbízható és biztonságos körülmények között tárolja (archiválja), annak érdekében, hogy szükség esetén a korábban titkosított állományok visszaállíthatók legyenek.

Szolgáltató az elofizetok titkosító magánkulcsait csak archiválási céllal menti.

6.2.5. Titkosító magánkulcs archiválása

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

6.2.6. Magánkulcsok aktiválása

Az elofizetoi titkosító magánkulcs aktiválása a Felhasználó által történik a jelszó vagy PIN kód megadás ával, azokban az esetekben, amikor a titkosító magánkulcs használatára szükség van.
A kulcshordozó eszközt a titkosító magánkulcs aktiváláskor sem hagyja el, azt az eszközrol leolvasni nem lehet.

6.2.7. Magánkulcsok deaktiválása

Az elofizetoi titkosító magánkulcsok deaktiválását a Felhasználó alkalmazása végzi a titkosító magánkulcs felhasználó kijelentkezésekor, vagy amikor a titkosító magánkulcs felhasználó a kulcshordozó eszközt eltávolítja az olvasóból.

6.2.8. Magánkulcsok megsemmisítése

Az elofizetoi titkosító magánkulcs lejárta után a kulcshordozó eszköz fizikai megsemmisítését az Elofizetonek saját felelosségi körében úgy kell elvégezni, hogy az semmilyen körülmények között ne legyen újra felhasználható.

A szolgáltatói titkosító magánkulcsok megsemmisítése a Szolgáltató kötelessége.

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

6.3 Aktivizáló adatok (PIN kódok)

6.3.1. Aktivizáló adatok generálása és installációja

A Szolgáltató a Felhasználó titkosító magánkulcsának védelme érdekében a kulcshordozó eszközök használatához aktivizáló adatot (PIN kódot) kapcsol. A Szolgáltató által kibocsátott titkosító magánkulcsok, illetve kulcshordozó eszközök PIN kódjait a Szolgáltató PKI alkalmazása állítja elo.

6.3.2. Aktivizáló adatok védelme

A Szolgáltató az általa kibocsátott kulcshordozó eszközök PIN kódjait muszaki[6] és szervezési[7] intézkedésekkel védi, majd a kulcshordozó eszköztol elkülönítve[8] tárolja és osztja szét.

A titkosított állományok bizalmassága megorzésének és visszaállításának alapveto feltétele, hogy a titkosító magánkulcsot, illetve a kulcshordozó eszközt és annak PIN kódját a Felhasználó kizárólagosan birtokolja, melyet a Felhasználónak saját felelosségi körében kell biztosítania. Ha ez sérül vagy a PIN kód elvész, illetve ennek alapos gyanúja fennáll, akkor a Felhasználónak (Elofizetonek) ezt haladéktalanul jeleznie kell az ot regisztráló Ügyfélkapcsolati Irodánál, vagy a Szolgáltató Ügyfélszolgálatánál és intézkedni kell a titkosító tanúsítvány felfüggesztésérol vagy visszavonásáról.

6.3.3. Aktivizáló adatok mentése

A Szolgáltató a Felhasználó PIN kódjáról az eloállítást követoen biztonsági másolatot (mentést) készít annak érdekében, hogy szükség esetén az archivált titkosító kulcsok újra aktivizálhatók legyenek.

A PIN kódok biztonsági másolatait a Szolgáltató megbízható és biztonságos körülmények között tárolja.

6.4 Kriptográfiai modul ellenorzése

A Szolgáltató a titkosítás hitelesítés-szolgáltatáshoz alkalmazott hardveres kriptográfiai modult rendszeresen ellenorzi.

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

[7] A címzettekhez történo továbbításig, a rendszerüzemeltetok gondoskodnak a beborítékolt PIN kódok biztonságos tárolásáról.

[8] Az elkülönítés úgy van biztosítva, hogy a kulcshordozó eszközök és a PIN kódok szétosztása, illetve átadása külön lezárt borítékokban történik.

7. A szolgáltatási szabályzat adminisztrációja

A jelen fejezetre a HSZSZ-F aktuális változata 7. fejezetének tartalma érvényes.

8. Hivatkozások és meghatározások

8.1 Hivatkozások

A hivatkozott törvényeket, rendeleteket, ajánlásokat és szabványokat az 1.2.2 fejezet tartalmazza.

A Szolgáltató hivatkozott dokumentumai:

A MÁV INFORMATIKA Kft. Szervezeti és Muködési Szabályzata,

A MÁV INFORMATIKA Kft. Iratkezelési Szabályzata

A MÁV INFORMATIKA Kft. Titokvédelmi Szabályzata

A MÁV INFORMATIKA Kft. Informatikai Biztonságpolitikája

A MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata

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

Általános Szerzodési Feltételek Titkosítás Hitelesítés-szolgáltatáshoz (ÁSZF-T)

Elofizetoi Szerzodés Minta

A PKI Szolgáltatások Biztonságpolitikája

A PKI Szolgáltatások Biztonsági Szabályzata

A PKI Szolgáltatások Üzletmenet-folytonossági Terve

8.2 Meghatározások

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

Biztonságos környezet: Olyan fizikai környezet, mely védett illetéktelen hozzáféréstol, és bizonyos mértékig tuz, víz és egyéb katasztrófaeseményektol, egyéb eroszakos behatásoktól.

Címtár (Tanúsítványtár): X. 500 szabvány alapú címtár, amelyben a tanúsítványok, az állapotuk, a visszavonási listák (CRL) rendszeresen frissülnek. Tartalma nyilvánosan elérheto LDAP-al vagy web lapról.

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

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

Elektronikus dokumentum: elektronikus eszköz útján értelmezheto adategyüttes.

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

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

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

Ellenorzési lépések: A titkosító nyilvános kulccsal történo titkosításkor a titkosító magánkulcs felhasználó Tanúsítványa ellenorzésekor kötelezoen elvégzendo muveletsor.

Elofizeto: Az a személy vagy szervezet, amely Szolgáltatóval érvényes elofizetoi szerzodéssel rendelkezik hitelesítés-szolgáltatás igénybe vételére, és így a Szolgáltató által kiadott tanúsítvány tulajdonosának tekintheto.

Érintett fél: Az elektronikus állomány tikosítását végzo entitás (személy/eszköz), aki/amely a titkosító magánkulcs felhasználó Nyilvános kulcsához tartozó tanúsítvány ellenorzése alapján kezdeményezi az elektronikus állomány titkosítását.

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

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

Elsodleges (root) hitelesíto szervezet: az elsonek létrehozott, fizikailag is muködo hitelesíto szervezet, amely az alája rendelt másodlagos hitelesíto központokat hitelesíti,

Produktív hitelesíto szervezet: az elsodleges hitelesíto szervezet által létrehozott logikailag vagy fizikailag létezo hitelesíto szervezet, amely egy adott alkalmazási, szervezeti, földrajzi stb. területre ad ki tanúsítványokat.

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

Igénylo: Az a személy vagy szervezet, amely Szolgáltatóhoz fordul a hitelesítés-szolgáltatás igénybe vétele céljából. Az Igénylo elofizetoi szerzodés megkötése után válik Elofizetové.

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

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

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

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

Magánkulcs aktiválása: A magánkulcs aktiválása az a folyamat, melynek során a jogosult – különbözo azonosító elemek pl. jelszó, PIN kód megadásával – engedélyezi, hogy a leolvasóba helyezett magánkulcs megkezdje üzemszeru muködését. Az aktiválás általában a magánkulcsot igénylo környezetben (dokumentum kezelo, levelezo rendszer) történik, és érvényes lehet a visszavonásig (deaktiválásig) illetve egyszeri használatra.

Magánkulcs deaktiválása: A magánkulcs deaktiválása az a folyamat, melynek során a magánkulcs üzemszeru muködése megszüntetésre kerül. Ez olyan kulcshordozó eszköz esetén, amikor a kulcs üzemszeru muködés során nem hagyja el a kulcshordozó eszközt, történhet a kulcshordozó eszköz olvasóból történo eltávolításával, más esetekben a kulcshordozó eszköznek a titkosító környezetbol való eltávolításával, vagy az alkalmazásból való kilépéssel.

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

Regisztráló szervezet: A regisztráló szervezetek a Szolgáltató és a vele szerzodése alapon együtt muködo Társaságok azon szervezeti egységei, amelyek az elofizetok adatainak regisztrációját, ellenorzését, az igénylo személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a hitelesíto szervezethez történo továbbítását, és egyéb azonosítási, Tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

Regisztrációs adatok: Azon információk, adatok összessége, amelyeket a Szolgáltató a Tanúsítványkiadás érdekében az Elofizetorol begyujt.

Szolgáltatás: Elektronikus titkosító tanúsítvány hitelesítés-szolgáltatás (röviden: hitelesítés-szolgáltatás) és titkosító magánkulcs eloállítása és elhelyezése a titkosító magánkulcsot tároló eszközön. titkosító tanúsítvány kibocsátás és publikálás. Tanúsítványkezelés (visszavonás, felfüggesztés stb.)

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

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

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

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

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

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

Tanúsítványok osztályai: A tanúsítványok megbízhatósága szerinti megkülönböztetés. A kibocsátást megelozo ellenorzo lépések biztonságosságának jelzésére is szolgál (a jelenleg létezo osztályok: minosített, fokozott biztonságú, szolgáltatói, teszt).

Tanúsítványtár: lásd: címtár

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

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

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

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

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

Transzport kulcspár: A transzport kulcspár azt a célt szolgálja, hogy a titkosító magánkulcs a hordozóra kerüléstol a megbízott kapcsolattartó által történo transzporton keresztül a titkosító magánkulcs felhasználó által tö rténo átvételig a transzport nyilvános kulccsal titkosítva kerüljön átvitelre úgy, hogy a transzportáló személy a m agánkulcshoz ne férhessen hozzá. A transzportáló személy a titkosító magánkulcs felhasználó által tö rténo PIN kód megadás után a transzport magánkulccsal állítja vissza a transzportált titkosító magánkulcsot.

Transzport tanúsítvány: A transzport kulcspárhoz tartozó tanúsítvány.

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

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