Kereskedelmi, Szolgáltató és Tanácsadó
Zártkörűen Működő Részvénytársaság

Szolgáltatási szabályzat titkosító tanúsítvány szolgáltatáshoz (HSZSZ-T)

Verziószám	**4.0**
Objektum azonosító (OID)	**1.3.6.1.4.1.14868.1.4.4**
Hatálybalépés dátuma	**2008. október 1.**

Változáskezelés

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2005. 04. 15.	Szolgáltatás megindításához előkészített változat	Néder Ferenc		
2.0	2005. 06. 15.	Felülvizsgált, módosított változat	Néder Ferenc		
3.0	2005. 08. 16.	Felülvizsgált, módosított változat	Néder Ferenc		
4.0	2008. 10. 01.	Szervezeti változás kapcsán módosított változat	Néder Ferenc	Juhász György HBSZE vezető	Hosszú Sándor István vezérigazgató

Tartalom

1. Bevezetés

A MÁV INFORMATIKA Zrt. mint kereskedelmi hitelesítés-szolgáltató 2002. novemberétől nyújt az elektronikus aláírási törvény (Eat.) hatálya alá tartozó elektronikus aláíráshoz hitelesítés-szolgáltatást.

E dokumentum a MÁV INFORMATIKA Zrt. (továbbiakban Szolgáltató) **az elektronikus aláírási törvény (Eat.) hatálya alá nem tartozó titkosító tanúsítvány szolgáltatására** vonatkozó részletes eljárási és működési szabályokat tartalmazza.

A Szolgáltató a titkosító tanúsítvány szolgáltatást a vele előfizetői szerződéses viszonyban álló *Előfizetők* és az *érintett felek* részére nyújtja. A Szolgáltató titkosító tanúsítvány szolgáltatás címszó alatt a következő szolgáltatásokat nyújtja:

a. titkosító kulcspár előállítás és hitelesítés

b. titkosító tanúsítvány előállítás és kibocsátás

c. titkosító kulcspár és tanúsítvány adathordozóra helyezés

d. titkosító kulcspár és tanúsítvány érvényesség kezelés

e. titkosító magánkulcs letét

f. titkosító magánkulcs visszaállítás

A jelen szolgáltatási szabályzat (továbbiakban: szabályzat) további fejezeteiben a „*szolgáltatások*” kifejezés alatt a fenti részszolgáltatások bármelyike vagy tetszőleges csoportosítása értendő.

A fenti szolgáltatásokat a Szolgáltató fokozott biztonságú szinten szolgáltatja.

1.1 Áttekintés

Jelen szabályzat célja, hogy összefogja azokat az előírásokat, adatokat és információkat, melyeket a Szolgáltató titkosító tanúsítvány szolgáltatásával valamilyen módon kapcsolatba kerülő feleknek tudni kell. A szabályzat biztosítja a Szolgáltató működésének átláthatóságát, s lehetővé teszi a felhasználók és az érintett felek számára, hogy megállapítsák azt, hogy az ismertetett szolgáltatási gyakorlat, valamint a kibocsátott titkosító tanúsítványok menynyiben felelnek meg az elvárásaiknak. A szabályzatban hivatkozott dokumentumok, ajánlások, szabványok tartalmának megismerése után a tanúsítvány elfogadóinak egyértelműen meg kell tudni állapítani a tanúsítvány kezelésének módját, az általa garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelősség vállalásokat.

1.2 A dokumentum neve és azonosítója

A Szolgáltató jelen dokumentumot az ISO/IEC és az ITU szabványok által előírt regisztrációs eljárásnak megfelelően eljárva regisztrálja.

A jelen dokumentum teljes neve: Szolgáltatási szabályzat titkosító tanúsítvány szolgáltatáshoz

Azonosítója: HSZSZ-T

Első hatálybalépés időpontja 2005. 04. 15.

A HSZSZ-T megtekinthető a Szolgáltató ügyfélkapcsolati irodáiban, elektronikus változata a szolgáltatás internetes honlapján érhető el. A szabályzatnak csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

1.3 A szolgáltató és a felhasználói közösség

1.3.1. Szolgáltató adatai

Név: MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Zártkörűen Működő Részvénytársaság

Cégjegyzék szám: 01-10-045838

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

Levélcím: 1253 Budapest Pf. 28

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:

Nemzeti Fogyasztóvédelmi Hatóság Közép-magyarországi Regionális Felügyelősége

1052 Budapest, Városház u. 7.

Telefon: 318-2681, telefax: 318-1639, Email: *fogyasztovedelem@pest.b-m.hu*

Fogyasztókapcsolati Iroda

1088 Budapest, József krt. 6.

Telefonszám: + 36 1 459 4999, +36 1 459 4836

Ingyenes zöldszám: +36 80 201 205, Telefax: +36 1 303 9075

Kapcsolat az ügyfelekkel:

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

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

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

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

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

Panaszok bejelentésének helye:

a. személyesen az Ügyfélkapcsolati Irodákban
b. írásban a Szolgáltató székhelyére címezve
c. telefonon az Ügyfélkapcsolati Irodákban vagy az Ügyfélszolgálatnál
d. elektronikus levélben a mavinformatika@mavinformatika.hu és a hiteles@mavinformatika.hu címeken

1.3.2. A Szolgáltató regisztráló és hitelesítő egységei

1.3.2.1 Ügyfélkapcsolati Irodák ("ÜKI")

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 és eszközök átadását végzik, valamint az adminisztrációs feladatokat látják el.

1.3.2.2 Regisztrációs Iroda ("RA")

A Regisztrációs Iroda (rövidítve: RA) a szolgáltatás keretein belül biztosítja az előfizetők technikai regisztrációját, a tanúsítványok felfüggesztés és visszavonás kezelését és a titkosító kulcspár és tanúsítvány adathordozó eszközre helyezését.

1.3.2.3 Hitelesítő Központ ("CA")

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 a kulcspárok és tanúsítványok előállítása, a tanúsítványok közzététele.

1.3.3. Felhasználói közösség

A Szolgáltató által kibocsátott előfizetői titkosító tanúsítványokat felhasználó közösség a következő:

a. az Előfizetők és az Előfizetők feljogosított munkatársai,

b. az Előfizetők informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.),

c. az érintett felek.

1.3.3.1 Előfizető

Az Előfizető a Szolgáltatóval szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató titkosító tanúsítványt bocsát ki. Előfizető lehet természetes vagy jogi személy. A szerződési feltételeket a [30] Általános Szerződési Feltételek PKI szolgáltatásokhoz (továbbiakban: ÁSZF-PKI) tartalmazza.
Az Előfizető illetve az Előfizető feljogosított munkatársa egyben titkosító magánkulcs felhasználó is, amennyiben birtokolja és használja a titkosító magánkulcsot.
Az Előfizető lehet jogi személy (szervezet) is. Ebben az esetben a szervezet cégjegyzésre jogosult vezetője képviselőként egy természetes személyt bíz meg, akit felruház hagyományos, és/vagy elektronikus aláírási jogosultsággal, valamint rendelkezik az Előfizető feljogosított munkatársai titkosító magánkulcsainak titkosítására szolgáló ún. transzport magánkulccsal. Ez a személy a jogi személyt (szervezetet) képviselve ír alá hagyományos papíralapú, illetve elektronikus dokumentumokat.

1.3.3.2 Előfizetők informatikai eszközei

Az Előfizetők informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.) rendelkezhetnek titkosító kulcspáron alapuló titkosító tanúsítvánnyal. Az informatikai eszköz ebben az esetben titkosító magánkulcs felhasználó. Eszközök estében a regisztráció során meg kell nevezni az eszköz üzemeltetéséért felelős személyt (rendszerint a rendszergazdát) is.

1.3.3.3 Titkosító magánkulcs felhasználó (alany)

Titkosító magánkulcs felhasználó lehet:

a. bármely természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítványnak megfelelően, a jelen szabályzat 3.2 pontjában előírtak 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 ellenőrzése mellett a regisztráció során a 3.2.3 pontban meghatározott módon a képviseleti jogosultságot is ellenőrizni kell.

c. tetszőleges, titkosított állomány visszaállítására feljogosított informatikai eszköz,

1.3.3.4 Érintett fél

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

b. érintett fél lehet tetszőleges, titkosításra feljogosított informatikai eszköz is

Az Érintett fél a titkosító műveletnél a titkosító magánkulcs felhasználó nyilvános kulcsához tartozó tanúsítvány érvényességi ellenőrzésére hagyatkozva jár el.

1.4 Tanúsítványhasználat

1.4.1. A szolgáltatás szintje

A Szolgáltató a jelen szabályozás keretében a fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatásával azonos szintű és rendelkezésre állású szolgáltatást nyújt.

1.4.2. A titkosítással elérhető bizalmasság szintje

A Szolgáltató által generált titkosító kulcs hossza legalább 1024 bit. Az 1024 bites titkosító kulccsal védett adatok feltörése a szakirodalom szerint a jelenleg rendelkezésre álló eszközökkel nem lehetséges. A Szolgáltató figyelemmel kíséri a technikai fejlődést és ennek függvényében indokolt esetben gondoskodik a kulcsméret növeléséről.

Az aszimmetrikus kulcsú titkosítás a gyakorlatban lassú, ezért csak rövid állományok titkosítására alkalmas. Ezért a Szolgáltató által kibocsátott titkosító kulcspár általában a szimmetrikus titkosító kulccsal tikosított terjedelmes állományok szimmetrikus titkosító kulcsainak titkosítására hivatott. Ebből eredően a titkosított állományok bizalmassága elsősorban az alkalmazott szimmetrikus titkosító kulcs hosszától és az alkalmazott titkosító algoritmustól, valamint a titkosítást végző számítógép biztonsági rendszerétől függ.

1.4.3. Titkosító tanúsítványok alkalmazhatósága

Az előfizetői titkosító tanúsítványok alkalmazhatóságára a következő szabályok érvényesek:

A Szolgáltató által kibocsátott titkosító tanúsítványok **nem alkalmazhatók** az 1995. évi LXV. törvény az államtitokról és a szolgálati titokról, valamint a minősített adat kezelésének rendjéről szóló 179/2003. (XI. 5.) Korm. rendelet hatálya alá tartozó adatok kezelésére.

A Szolgáltató által kibocsátott titkosító tanúsítványok a magánkulcs hordozó eszköz biztonságának függvényében **alkalmazhatók** üzleti titkok és bizalmas üzleti információk védelmére. Az általánosan használt kulcshordozó eszközök (ALE) alkalmazása közepes biztonságú titkosítási szintet biztosít, míg „Biztonságos Aláírás Létrehozó Eszköz” (BALE) alkalmazása esetén magas biztonsági szintű titkosítás érhető el.

1.4.3.1 Megfelelő tanúsítványhasználat

A kibocsátott titkosító tanúsítványokhoz tartozó nyilvános kulcs csak elektronikus állományok titkosítására, a titkosító magánkulcs pedig csak a titkosított elektronikus állományok visszaállítására használható fel, a titkosító tanúsítványba foglaltaknak megfelelően.

1.4.3.2 Korlátozott alkalmazási lehetőségek

Szolgáltató az előfizetői szerződésben felhasználási, területi, pénzügyi, stb. korlátozásokat szabhat. A korlátozásokat a kibocsátott előfizetői tanúsítványban is megadja.

1.4.3.3 Tiltott tanúsítványhasználat

Tilos az előfizetői 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. A titkosító tanúsítványhoz kapcsolódó titkosító magán-, illetve nyilvános kulcsot kizárólag titkosításra lehet felhasználni.

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

Jelen szabályzat hatálya alatt kibocsátott titkosító tanúsítványok csak az 1.3 fejezetben meghatározott szolgáltató és felhasználó közösség körében használhatók az előfizetői szerződésben rögzített összeghatárok szerinti korlátokkal.

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

Összefoglalva:

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

1.5 A szolgáltatási szabályzat adminisztrációja

1.5.1. Szabályzat hatálya

A HSZSZ-T 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-T személyi hatálya a Szolgáltatónak a titkosító tanúsítvány szolgáltatással kapcsolatban álló munkatársaira és a felhasználói közösségre terjed ki.
A HSZSZ-T tárgyi hatálya a következőkre terjed ki:

a. az 1. pontban meghatározott szolgáltatásokra

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

1.5.2. Kapcsolattartó személy

A Szolgáltató részéről a kapcsolattartó személy a Hálózati és biztonsági szolgáltató egység vezetője. Elérhetősége az ügyfélkapcsolati irodákon keresztül biztosított.

1.5.3. Változáskezelés

1.5.3.1 Változtatási eljárások

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoport működik, amely a HSZSZ-T karbantartásáért felelős. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a változtatásokat életbe lépteti, az új szabályzat verziókat elektronikus aláírással hitelesíti.
A szabályzatot a Szolgáltató vezetése hagyja jóvá és lépteti hatályba.
A szolgáltatási szabályzat módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

1.5.3.2 Kapcsolattartás, észrevételek kezelése

A szabályzattal, illetve a szolgáltatással kapcsolatos észrevételeket a Szolgáltató vezetésének kell címezni.
A HSZSZ-T-vel kapcsolatos észrevételeket Szolgáltató az Ügyfélkapcsolati Iroda útján fogadja.

1.5.4. Közzétételi és tájékoztatási elvek

1.5.4.1 A HSZSZ-T-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyeztetik [29], [30]. A Szolgáltató több belső biztonsági és egyéb szabályzattal [24] – [28], operatív szintű előírással rendelkezik [31], [32], melyeket bizalmasan, üzleti titokként kezel.

1.5.5. A HSZSZ-T közzététele

A Szolgáltató az érvényben lévő HSZSZ-T-t a szolgáltatás internetes honlapján teszi közzé.

1.5.6. Elfogadási eljárások

A jelen HSZSZ-T szerkezetében és tartalmában követi az RFC 3647 szabványt azzal az eltéréssel, hogy a szabályzat nem tartalmazza a nem értelmezhető vagy lényegi előírásokat nem tartalmazó fejezeteket, illetve tartalmaz az RFC-ben nem tárgyalt fejezeteket is.

A Szolgáltató a jelen HSZSZ-T-t indokolt esetben, de legalább évente felülvizsgálja.

1.6 Meghatározások

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 adat: olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.

Aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön (eszközellátás): az aláírás-létrehozó eszközök elkészítése és az előfizetők részére történő átadása.

Aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

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

Alany: egy tanúsítványban azonosított egyed, aki/amely a tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

Biztonságos aláírás-létrehozó eszköz: az [Eat] - Elektronikus aláírás törvény 1. számú mellékletében foglalt követelményeknek eleget tevő, illetve e törvény 7. § (5) illetve (6) bekezdése szerinti tanúsítással rendelkező aláírás-létrehozó eszköz.

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

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

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

Elektronikus aláírás: elektronikus adat, amely egy elektronikus dokumentumhoz azonosítási célból logikailag hozzárendelt, vagy ahhoz elválaszthatatlanul kapcsolódik.

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.

Egyed (entitás): a nyilvános kulcsú infrastruktúra (PKI) autonóm eleme, pl. egy tanúsítványkiadó, regisztrációs szervezet, végfelhasználó vagy eszköz.

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

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

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

Érintett fél: Az elektronikus állomány tikosítását végző entitás (személy/eszköz), aki/amely a titkosító magánkulcs felhasználó nyilvános kulcsához tartozó tanúsítvány ellenőrzése alapján kezdeményezi az elektronikus állomány titkosítását; olyan egyed, aki egy adott tanúsítványon alapuló nyilvános kulcsú technikára (elektronikus aláírásra, titkosításra vagy hitelesítésre) hagyatkozva jár el..

Felhasználó (végfelhasználó): olyan egyed, aki/amely a szolgáltatás keretében előállított kulcsokat és tanúsítványokat rendeltetésüknek megfelelően használja. Felhasználó lehet előfizető, alany (aláíró) vagy érintett fél. Eszköz vagy alkalmazás is lehet felhasználó.

Fokozott biztonságú szolgáltató: a Nemzeti Hírközlési Hatóságnál bejelentett és nyilvántartási számmal rendelkező (regisztrált) elektronikus aláírás-hitelesítés szolgáltató, amely a 2001. évi XXXV. törvényben és a 3/2005. (III. 18.) IHM rendeletben foglaltaknak megfelel és az elektronikus aláírás-hitelesítés szolgáltatás mellett fokozott biztonságú titkosító kulcspárt és ehhez tartozó tanúsítványt bocsát ki.

Hitelesítési rend (HR): olyan szabálygyűjtemény, amely bizonyos tanúsítványok alkalmazhatóságát határozza meg egy meghatározott - közös biztonsági követelményeknek eleget tevő - közösség és/vagy alkalmazás-osztálya számára.

Hitelesítés-szolgáltató (HSz): a tanúsítványon lévő nyilvános kulcs és a tulajdonos azonosító adatainak hiteles összekapcsolásáért felelős, a kommunikációban résztvevő felek mindegyike által hitelesnek tartott szervezet. (A szolgáltató ezt a kapcsolatot a tanúsítvány elektronikus aláírásával igazolja.) A HSz személy vagy szervezet lehet, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványokhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány visszavonási listát.

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

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

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

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

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

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

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

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

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

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

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

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

Regisztráló szervezet: A regisztráló szervezetek a Szolgáltató és a vele szerződése alapon együtt működő Társaságok azon szervezeti egységei, amelyek az előfizetők adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a hitelesítő szervezethez történő továbbítását, és egyéb azonosítási, Tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

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

Szolgáltatás: Elektronikus titkosító tanúsítvány szolgáltatás. Titkosító magánkulcs előállítása és elhelyezése a titkosító magánkulcsot tároló eszközön. Titkosító tanúsítvány kibocsátás és publikálás. Tanúsítványkezelés (megújítás, visszavonás, felfüggesztés stb.)

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

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

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

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

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

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

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

Tanúsítványtár: lásd: címtár

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

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

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

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

Titkosító tanúsítvány: olyan, az RFC 2459 szabványban leírt X.509 3-as verziójú tanúsítvány, amelyben a kulcshasználat titkosításra van beállítva.

Transzport kulcspár: A transzport kulcspár a titkosító magánkulcs védelmét szolgálja a kulcs előállításától a kulcs felhasználója (alanya) által történő birtokba vételig. A Szolgáltató a felhasználó titkosító magánkulcsát a kulcspár generálás befejező fázisaként a publikus transzport kulccsal titkosítja.

a. a transzport kulcspár titkos (privát) kulcsa a felhasználó (alany) birtokában van, így a titkosító magánkulcsának visszaállítását maga végezheti el.

b. a transzport kulcspár titkos (privát) kulcsa a szervezet felhatalmazott megbízottjának a birtokában van, így a felhasználó titkosító magánkulcsának visszaállítását a megbízott végzi el felhasználó (alany) jelenlétében.

Transzport tanúsítvány: A transzport kulcspárhoz tartozó tanúsítvány.

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

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

1.7 Hivatkozások

A Szolgáltató által nyújtott szolgáltatásokra elsősorban a következő jogszabályok és szabványok mérvadók:

[1] 2001. évi XXXV. törvény az elektronikus aláírásról (a továbbiakban: Eat.)

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

[4] 194/2005. (IX. 22.) Korm. rendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről

[5] 15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

[6] 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

[9] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára

Hivatkozott ajánlások, szabványok:

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

[18] Internet Közösség RFC 2459, RFC 2527, RFC 3039, RFC 3280 és RFC 3647 ajánlásai

[19] Európai Unió ETSI TS 101456, ETSI TS 101862 és ETSI TS 102042 szabványok

[20] NIST FIPS 140-1 Level 1-3

[21] American Bar Association (ABA) PKI Assessment Guidelines (PAG)

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

A Szolgáltató hivatkozott dokumentumai:

[24] A MÁV INFORMAIKA Zrt. Szervezeti és Működési Szabályzata

[25] A MÁV INFORMAIKA Zrt. Iratkezelési szabályzata

[26] A MÁV INFORMAIKA Zrt. Titokvédelmi szabályzata

[27] A MÁV INFORMAIKA Zrt. Információbiztonsági politikája

[28] A MÁV INFORMAIKA Zrt. Információbiztonsági szabályzata

[29] Szolgáltatási Szabályzat a fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatásokhoz és nem-minősített időbélyegzés szolgáltatáshoz (HSZSZ-F)

[30] Általános Szerződési Feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI)

[31] A PKI Szolgáltatások biztonsági szabályzata

[32] A PKI Szolgáltatások üzletmenet-folytonossági terve

[33] A MÁV INFORMAIKA Zrt. Kulcs-visszaállítási szabályzata

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 szerint jár el.

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

2. 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 elérhetővé teszi.
3. A Szolgáltató jogi személy.
4. A Szolgáltató a HSZSZ-T-t rendszeresen felülvizsgálja.
5. A Szolgáltató mindenkor az Előfizető által megadott és az Ügyfélkapcsolati Irodák által ellenőrzött adatok alapján bocsátja ki a tanúsítványokat. A Szolgáltató a tanúsítvány kibocsátását követően a tanúsítvány adataiban nem változtathat.
6. A Szolgáltató a Tanúsítványtárában teszi közzé az általa kibocsátott, a visszavonási listájában a felfüggesztett és visszavont előfizetői tanúsítványokat. A Tanúsítványtár és a visszavonási listák elérhetőségét a Szolgáltató 99%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 24 órás időtartamot.
7. A Szolgáltató kötelezettséget vállal arra, hogy az előfizető regisztrációját követően a tanúsítvány kiadásáról 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 küldhet 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 titkosító tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetőleg – amennyiben ezen időszakban a titkosító tanúsítvánnyal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.
15. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről legalább hatvan nappal korábban értesíti az Előfizetőket.
16. A Szolgáltató intézkedik az iránt, hogy legkésőbb a tevékenysége befejezésekor más - vele legalább azonos besorolású - szolgáltató átvegye nyilvántartásait, így különösen a visszavont tanúsítványok nyilvántartását, valamint ellássa a hatályos jogszabályokban foglalt feladatokat. A Szolgáltató a visszavont tanúsítványokkal kapcsolatos minden adatot - beleértve a személyes adatokat is – átadja ezen szolgáltatónak.

2.1.1.1 Az Ügyfélkapcsolati Iroda feladatai és hatásköre

A ügyfélkapcsolati iroda:

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 a titkosító magánkulcs felhasználó minden adatát, kivéve azokat, amelyek a tanúsítványba kerülnek,
5. gondoskodik a titkosító magánkulcs hordozó eszköz és a PIN kód biztonságos kezeléséről és az Előfizetőnek történő biztonságos átadásáról,

6. korlátozás nélkül biztosítja a titkosító magánkulcs felhasználó 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 a titkosító magánkulcs felhasználó adatainak változására vonatkozó bejelentéseket.

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

Az Előfizető és a titkosító magánkulcs felhasználó kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során, ezen belül köteles:

1. a tanúsítvány igénylését és a kulcspár felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse,
2. az Előfizető a tanúsítvány kiadásához szükséges, a titkosító magánkulcs felhasználókra vonatkozó adatokat ellenőrizni,
3. az Előfizető és a titkosító magánkulcs felhasználó megismerni a magánkulcsának átvétele és felhasználása előtt a magánkulcs tárolásával, az állományok titkosításával, illetve visszaállításával kapcsolatos technikai, jogi, biztonsági követelményeket és feltételeket,
4. a titkosító magánkulcs felhasználó biztosítani a kulcshordozó eszközének, valamint a kulcshordozó eszköz és PIN kódjának védelmét,
5. az Előfizető, illetve a titkosító magánkulcs felhasználó 3 (három) munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a titkosító tanúsítványba foglalt adatokra,
6. a jogi személy Előfizető a titkosító magánkulcs felhasználóinak figyelmét külön felhívni arra, ha az Előfizetői Szerződés 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 felelőssége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
8. a jogi személy Előfizető megbízott kapcsolattartója tudomásul venni, hogy transzport magánkulcsának használata és védelme kizárólag a saját felelőssége, ezért ezzel - így különösen a transzport magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
9. a titkosító magánkulcs felhasználó azonnal intézkedni Tanúsítványának visszavonása, illetve felfüggesztése végett, ha

   tudomására jut, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, tartalmában, a regisztrációs adatokban pontatlanság van, illetve azokban változás következett be,

   a titkosító magánkulcs és/vagy a PIN kód nem a titkosító magánkulcs felhasználó kizárólagos birtokában van (elveszett, ellopták, esetleg kompromittálták), vagy ennek alapos gyanúja áll fenn;
10. a titkosító magánkulcs felhasználó vagy az Előfizető 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 félre vonatkozó ajánlások

A titkosítási eljárás alkalmazása előtt az Érintett fél részére ajánlott a legnagyobb gondossággal eljárni a titkosító nyilvános kulcshoz tartozó tanúsítvány elbírálásakor, ezen belül:

1. a tanúsítvány elfogadása előtt ajánlott megértenie a titkosítással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat,
2. ajánlott ellenőriznie a tanúsítvány érvényességét és hatályosságát, ezzel tudomásul venni, hogy a titkosító nyilvános kulcshoz tartozó tanúsítvány ellenőrzésének elmulasztásából eredő következményekért az Érintett

fél felel, valamint tudomásul venni, hogy a titkosító magánkulcs felhasználó nyilvános kulcsával titkosított állományt saját felelősségére készíti, és viseli ennek esetleges jogkövetkezményeit,

3. ajánlott megismernie Szolgáltató nyilvánosan elérhető szolgáltatási szabályzatát (a jelen HSZSZ-T-t), mert a titkosító tanúsítvány elfogadása és a titkosítási eljárás alkalmazása a Szolgáltató ezen szabályzatának elfogadását jelenti.

2.2 A szolgáltató és a felhasználó közösség tagjainak felelőssége

2.2.1. A Szolgáltató felelőssége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-T szerint meghatározott titkosító tanúsítványt – és ezzel jelzi a felhasználói közösség és az érintett felek felé ezen HSZSZ-T használatát –, csak azért vállalja a felelősséget, hogy a titkosító tanúsítvány előállítása, kibocsátása, közzététele, visszavonása és a visszavonási lista közzététele a jelen szabályzatban előírtaknak teljes mértékben megfelel, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy maga és az előfizetők is a jelen HSZSZ-T előírásainak megfelelően járjanak el.

A Szolgáltató köteles a tanúsítvány megfelelő mezőjében feltüntetni, ha az Előfizetői Szerződésben a tanúsítvány felhasználhatóságával kapcsolatban összegszerű, területi vagy egyéb korlátozásokat köt ki. Ezen korlátokat meghaladó ügyletekben felvetett követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.

A Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott tanúsítvány a jelen szabályzatban 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 szabályzatai szerint járt el vagy nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató nem vállal felelősséget a magánkulcs hordozó elvesztéséből, vagy a kulcs biztonságának egyéb módon történő sérüléséből (ide értve a chipkártya megrongálódását is), elvesztéséből, illetve a PIN kód illetéktelen tudomásra jutásból származó károkért.

2.2.2. Az Előfizető és a titkosító magánkulcs felhasználó felelőssége

Az Előfizető felelős a regisztráció során megadott adatok valódiságáért.

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

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

A titkosító magánkulcs felhasználó felelős a magánkulcs biztonságos megőrzéséért, a kulcs tartalom és a PIN kód illetéktelenek tudomására jutásának megakadályozásáért.

2.2.3. Érintett fél felelőssége

Érintett fél felelőssége fennáll a titkosító tanúsítvány használatából fakadó bármely következményért és kárért, ha a titkosító tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a jelen HSZSZ-T szerint jár el, valamint ha nem tikosításhoz használható kulccsal titkosítja az adatokat a felhasználó számára.

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

2.3 Értelmezés és alkalmazás

2.3.1. Alkalmazott jogszabályok

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

A Szolgáltató tevékenységére vonatkozó fő jogszabályok felsorolását az 1.7 fejezet tartalmazza.

2.3.2. Hatályosság, megszűnés, értesítések

2.3.2.1 Hatályosság

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

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

2.3.2.2 Megszűnés

A HSZSZ-T a Szolgáltató titkosító tanúsítvány szolgáltatásának befejezésével tekintendő megszűntnek.

2.3.2.3 Értesítések

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.

Az Előfizetők 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.

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 20 munkanapon belül kivizsgálja és ennek eredményéről a panaszost írásban tájékoztatja.

A jogvitáik rendezésére vonatkozó szabályokat az ÁSZF-PKI tartalmazza.

2.4 Közzététel

2.4.1. Adatbázisok

2.4.1.1 Tanúsítványtár

A Szolgáltató az általa kibocsátott tanúsítványokat Tanúsítványtárában helyezi el.

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

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

2.4.1.2 Titkosító kulcspárok adatbázisa

A Szolgáltató a titkosító kulcspárokat az archiválásig kiemelten biztonságos környezetben tárolja. A titkosító kulcspárok adatbázisának kezelési eljárásait a [31] PKI szolgáltatások biztonsági szabályzata tartalmazza.

2.4.1.3 Naplók, regisztrációs adatok

A Szolgáltató a működése során keletkező naplófájlokat, regisztrációs adatokat belső adatbázisokban, fokozottan védett körülmények között tárolja.

2.4.1.4 Az adatbázisok elérésének szabályozása

A Szolgáltató minden Előfizető és érintett fél számára elérhetővé teszi a szolgáltatás Internetes honlapját, azon keresztül Tanúsítványtárát és visszavonási listáit 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.

2.4.2. A tanúsítványokra vonatkozó 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 elektronikus formában Internetes honlapján keresztül teszi elérhetővé. Szolgáltatónak csak saját, legalább fokozott biztonságú elektronikus aláírásával ellátott dokumentumai tekinthetők eredetinek. Az elektronikus dokumentumok nyomtatott változatai nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

A Szolgáltató hiteles nyomtatott dokumentumai az Ügyfélkapcsolati Irodán férhetők hozzá.

2.4.3. A közzététel gyakorisága

Tanúsítványok, kikötések és feltételek nyilvánosságra hozatala:

A Szolgáltató a kibocsátott előfizetői tanúsítványokat - az érintett alany, illetve előfizető hozzájárulása esetén - a Tanúsítványtárban 24 órán belül közzéteszi és azok elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.1.1 pont szerinti rendelkezésre állással biztosítja.

A Szolgáltató általa működtetett hitelesítő központok szolgáltatói tanúsítványait a Tanúsítványtárában 24 órán belül közzéteszi és azok elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.1.1 pont szerinti rendelkezésre állással biztosítja.

Visszavonási állapot információk nyilvánosságra hozatala:

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

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

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

A Szolgáltató a visszavonási listák elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.1.1 pont szerinti rendelkezésre állással biztosítja.

3. Azonosítási és hitelesítési eljárások

3.1 Megnevezési konvenciók

3.1.1. Nevek típusa

A tanúsítványokban szereplő névmegadás az ITU-T[1] X.500 ajánlásának felel meg.

Nem természetes személy alany esetén: a tanúsítványban szereplő név az automatizmus (szerver) DNS szerinti, vagy egyéb módon hitelesített elnevezése, szóköz elválasztójel(eke)t és az UTF-8 kódolást használva.

3.1.2. Nevek szemantikája

Megnevezési konvenciók:

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

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

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

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

3.1.3. Nevek egyedisége

A Szolgáltató biztosítja tanúsítványtárában a tulajdonosazonosítók egyediségét, azaz gondoskodik arról, hogy az általa kiadott tanúsítványokban használt megkülönböztetett nevet (DN) sohasem fogja egy másik entitáshoz rendelni. Erről elsődlegesen a titkosító magánkulcs felhasználó e-mail címének a névmegadásban való szerepeltetése gondoskodik. A Szolgáltató a név azonosító kiosztásakor ellenőrzi, hogy az adott e-mail cím nem szerepel-e egy más titkosító magánkulcs felhasználó 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 a titkosító magánkulcs felhasználóra, de biztosítja a megkülönböztethetőséget.

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

3.1.4. Név igénylési viták feloldása

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

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

3.1.5. Álnevek használata

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

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.

3.1.6. 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

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

közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában. Szolgáltató nem garantálja Előfizetők számára védjegyeik feltüntetését a tanúsítványban.

3.2 Regisztráció

A regisztrálás során:

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

b. a regisztrációs űrlap elfogadásával Szolgáltató gondoskodik az Előfizetői Szerződés előkészítéséről és intézkedik a kulcspár és az előfizetői tanúsítvány elkészítésére,

c. 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.

3.2.1. A titkosító magánkulcs birtoklás ellenőrzésének módszere

A tanúsítványhoz tartozó kulcspár előállítása és elhelyezése a kulcshordozó eszközre a Szolgáltató Hitelesítő Központjában történik fokozottan védett, biztonságos körülmények között. A nyilvános- és magánkulcs egymáshoz tartozásának, valamint a magánkulcs birtoklásának ellenőrzésére ebben az esetben nincs szükség, csupán a kulcshordozó eszköz és a PIN kód átadásának-átvételének igazolása szükséges. Az átadási eljárás során az Előfizető írásban igazolja a kulcshordozó eszköz és a PIN kódot tartalmazó boríték átvételét. Az átvétel után az Előfizető és a magánkulcs felhasználó teljes felelősséget visel a kulcshordozó eszköz és a PIN kód biztonságos használatáért és megőrzésért.

3.2.2. Regisztráció „Személyes" tanúsítvány igénylése esetén

Természetes személy, mint Előfizető a regisztrációs űrlap kitöltésével igényelhet tanúsítványt. A Szolgáltató az űrlapon a következő Előfizetői adatokat kéri megadni:

1. név,
2. álnév, ha annak megjelölésére az Előfizető igényt tart
3. személyazonosításra alkalmas okmány száma (személyi igazolvány, útlevél, stb.),
4. lakcím,
5. anyja neve,
6. születési hely és idő,
7. e-mail cím,

A regisztrációs űrlapot a Szolgáltató biztosítja; azon további adatok megadására vonatkozó mezők is rendszeresíthetők.
Természetes személyt az Ügyfélkapcsolati Iroda személy azonosítására alkalmas igazolvány személyes bemutatásával azonosít.
A Szolgáltató megtagadhatja a tanúsítvány igénylést, ha az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.
A Szolgáltató eltekint a személyes megjelenéstől, ha az Előfizető az elektronikusan kitöltött regisztrációs űrlapot minősített elektronikus aláírással látja el.

3.2.3. Regisztráció „Munkatársi" tanúsítvány igénylése esetén

Jogi személy vagy jogi személyiség nélküli szervezet, mint Előfizető a regisztrációs űrlap kitöltésével igényelhet tanúsítványt. A Szolgáltató az űrlapon a következő Előfizetői adatokat kéri megadni:

1. Az Előfizető tekintetében:
   - 1.1. az Előfizető szervezet neve, székhelye
   - 1.2. a titkosító magánkulcs felhasználó(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. A titkosító magánkulcs felhasználó(k) tekintetében:
   - 3.1. annak a szervezeti egységnek a megnevezése, ahol a titkosító magánkulcs felhasználó dolgozik,
   - 3.2. annak a szervezeti egységnek a telephelye, ahol a titkosító magánkulcs felhasználó dolgozik
   - 3.3. titkosító magánkulcs felhasználó neve

3.4. titkosító magánkulcs felhasználó álneve, amennyiben annak megjelölésére a titkosító magánkulcs felhasználó igényt tart és azt számára az Előfizető engedélyezte,

3.5. a titkosító magánkulcs felhasználó beosztása

3.6. a titkosító magánkulcs felhasználó azonosítására használt igazolvány száma (ha a tanúsítvány személyhez köthető)

3.7. a titkosító magánkulcs felhasználó e-mail címe

A regisztrációs űrlapot a Szolgáltató biztosítja; azon további adatok megadására vonatkozó mezők is rendszeresíthetők.
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.
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 Szolgáltató megtagadhatja a tanúsítvány kibocsátását, ha a bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.
A Szolgáltató a regisztrációs űrlapot legalább fokozott biztonságú elektronikus aláírással ellátott elektronikus dokumentumként is elfogadja abban az esetben, ha az Előfizetővel erről előzetesen megegyezett.

3.2.4. Regisztráció „Szervezeti" tanúsítvány igénylése esetén

Jogi személy vagy jogi személyiség nélküli szervezet, mint Előfizető a regisztrációs űrlap kitöltésével igényelhet Szervezeti tanúsítványt. A Szolgáltató az űrlapon a következő Előfizetői adatokat kéri megadni:

1. Az Előfizető tekintetében:
   1.1. az Előfizető szervezet neve, székhelye
   1.2. a titkosító magánkulcs felhasználó(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. A titkosító magánkulcs felhasználó(k) tekintetében:
   3.1. annak a szervezeti egységnek a megnevezése, ahol a titkosító magánkulcs felhasználó dolgozik,
   3.2. annak a szervezeti egységnek a telephelye, ahol a titkosító magánkulcs felhasználó dolgozik
   3.3. a titkosító magánkulcs felhasználó neve, és/vagy célja (pl.: xy szervezeti egység xxyy adatfeldolgozás)
   3.4. a titkosító magánkulcs felhasználó azonosítására használt regisztrációs szám (pl. cégjegyzékszám)
   3.5. a titkosító magánkulcs felhasználó e-mail címe

A regisztrációs űrlapot a Szolgáltató biztosítja; azon további adatok megadására vonatkozó mezők is rendszeresíthetők.
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.
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 Szolgáltató megtagadhatja a tanúsítvány kibocsátását, ha a bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.
A Szolgáltató a regisztrációs űrlapot legalább fokozott biztonságú elektronikus aláírással ellátott elektronikus dokumentumként is elfogadja abban az esetben, ha az Előfizetővel erről előzetesen megegyezett.

3.2.5. Regisztráció „Eszköz" tanúsítvány igénylése esetén

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

Természetes személy által igényelt eszköz-tanúsítvány esetén:

1. az Előfizető személyes adatai a 3.2.2 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 3.2.4 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 rendje a 3.2.2 illetve 3.2.4pontokban 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.

A Szolgáltató a regisztrációs űrlapot legalább fokozott biztonságú elektronikus aláírással ellátott elektronikus dokumentumként is elfogadja abban az esetben, ha az Előfizetővel erről előzetesen megegyezett.

4. Tanúsítvány-életciklusra vonatkozó szabályok

4.1 Tanúsítványigénylés

4.1.1. Ki nyújthat be tanúsítványkérelmet

Tanúsítványkérelmet azok az előfizetők nyújthatnak be, akik előzetesen a Szolgáltatóval szerződéses kapcsolatot létesítettek. A kérelmező lehet magánszemély vagy egy jogi szervezet képviselő személy, aki személyazonosságát a regisztráció során hitelt érdemlően igazolta (lásd: 3.2.1.-3.2.7 pontok)

4.1.2. A tanúsítványigénylés folyamata és a résztvevők felelőssége

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

Az Előfizetői Szerződés aláírásával Előfizető egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, valamint saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Ha a titkosító magánkulcs felhasználó (alany) nem azonos az Előfizetővel, úgy őt az Előfizető tájékoztatja kötelességeiről. 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 információ harmadik félhez történő továbbításához a Szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb jogszabályok által meghatározott esetekben. Az Előfizető aláírása igazolja azt is, hogy:

a. vállalja a kulcshordozó 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 a titkosító magánkulcs felhasználó azonosítására használt adatokat, beleértve az igazoláshoz használt dokumentumok regisztrációs számát és az azok érvényességével kapcsolatos esetleges korlátozásokat.

Az előfizetői Tájékoztató a szolgáltató internetes honlapján bárki számára elérhető.

4.2 A tanúsítványkérelem feldolgozása

4.2.1. Azonosítási és hitelesítési funkciók megvalósítása

A Szolgáltató a regisztráció során az ott leírt módon ellenőrzi a tanúsítványkérelem érvényességét.

4.2.2. A tanúsítványkérelem jóváhagyása vagy visszautasítása

A Szolgáltató az előfizetői szerződés aláírásával hagyja jóvá a tanúsítványkérelmet. A tanúsítványkérelem visszautasítása esetén a Szolgáltató az igénylővel előfizetői szerződést nem köt.

4.2.3. A tanúsítványigénylések feldolgozásának időtartama

A tanúsítványigénylések feldolgozásának időtartama legfeljebb 30 nap, amennyiben a szükséges adatok hiánytalanul és helyesen lettek megadva.

4.3 Tanúsítvány kibocsátás

Sikeres regisztráció után az Ügyfélkapcsolati Iroda a tanúsítvány igényt a Regisztrációs Iroda felé továbbítja. A Regisztrációs Iroda a szolgáltatást támogató informatikai rendszerben elindítja a tanúsítvány kibocsátást.
Az elkészült Tanúsítványt a Szolgáltató a következő módon juttatja el az Előfizetőhöz:

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

4.4 Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető részéről az átvétellel történik meg.

A titkosító kulcspár használatba vétele előtt az Előfizető (alany) kötelessége ellenőrizni a tanúsítványban feltüntetett adatainak helyességét és visszaigazolni a tanúsítvány átvételét. Amennyiben bármilyen rendellenességet talál, a titkosító kulcspárt nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonására.
A visszaigazolás egyben a hitelesítési rendek, a szolgáltatási szabályzat és az általános szerződési feltételek elfogadását is jelenti.

4.4.1. Tanúsítvány közzététele a szolgáltató által

A Szolgáltató a kibocsátott tanúsítványokat Tanúsítványtárában teszi közzé.

4.4.2. A további szereplők értesítése a tanúsítvány kibocsátásáról

További szereplőket a Szolgáltató a kibocsátott tanúsítványokról nem értesít.

4.5 Kulcspár és tanúsítvány használat

4.5.1. Az alany magánkulcs- és tanúsítvány használata

a) Az alany magánkulcsát és tanúsítványát csak az előfizetői szerződésben rögzített korlátozásnak megfelelően használhatja.

b) Az alany csak a megfelelő tanúsítvány elfogadása után (lásd 4.4.) használhatja magánkulcsát.

c) Az alany a megfelelő tanúsítvány lejárta után nem használhatja tovább magánkulcsát.

d) Az alanynak az adott helyzetben általában elvárható gondosságot kell tanúsítania annak érdekében, hogy megelőzze magánkulcsának illetéktelen felhasználását.

e) Az alany magánkulcsait csak olyan célokra és olyan alkalmazásokkal használhatja, melyek összhangban vannak a tanúsítványok „kulcshasználat" és „kiterjesztett kulcshasználat" mezőinek tartalmával (lásd még 6.1.5 és 7.1.2).

4.5.2. Az érintett felek nyilvános kulcs- és tanúsítvány használata

Annak érdekében, hogy az érintett fél megalapozottan hagyatkozhasson a tanúsítvánnyal igazolt kriptográfiai kulcspár használatával működő alkalmazásra, a kulcspár megfelelő használatát és a hozzá tartozó tanúsítványt az adott helyzetben tőle általában elvárható gondossággal ellenőriznie kell. Ennek során többek között az alábbiakra kell figyelemmel lennie:

a) Az érintett fél csak olyan célokra és olyan alkalmazásokkal fogadhat el nyilvános kulcsokat, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat" és „kiterjesztett kulcshasználat" mezőinek tartalmával.

b) Mielőtt egy tanúsítványba foglalt nyilvános kulcsot felhasználna, az érintett félnek ellenőriznie kell a tanúsítvány érvényességét, valamint azt, hogy a tanúsítvány nincs felfüggesztve, illetve visszavonva az érvényes visszavonási állapot információ alapján.

c) Amennyiben ésszerű módon egy tanúsítványra kíván hagyatkozni, az érintett félnek figyelembe kell vennie a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban szerepel.

4.6 Tanúsítványok érvényessége, megújítása

A Szolgáltató által kibocsátott titkosító tanúsítványok érvényességi ideje legfeljebb 5 év, mely az előfizető kérésére legfeljebb további 5 évre meghosszabbítható, a tanúsítvány megújítható.

Előfizetői tanúsítvány megújítása akkor lehetséges, ha:

1. a tanúsítvány nem szerepel a visszavonási listákban
2. a tanúsítványban rögzített adatok érvényességéről és változatlanságáról az Előfizető írásban nyilatkozik.

Ha a feltételek valamelyike nem teljesül, új tanúsítványt kell igényelni a regisztrációs eljárás újbóli végrehajtásával. A Szolgáltató a tanúsítvány megújítás szükségességéről a lejárat előtt értesítést küld az Előfizetőnek.

4.6.1. Érvénytelen tanúsítványok megőrzése

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

4.7 Kulcscsere

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

Kulcscserére a következő esetekben lehet szükség:

1. a tanúsítvány valamilyen okból visszavonásra került,
2. a tanúsítvány lejárt,
3. a magánkulcsot tartalmazó állomány megsérült

A kulcscserét az Előfizető kezdeményezheti. Kulcscsere esetén a Szolgáltató lefolytatja a 3.2 pontban rögzített regisztrációs eljárást. A megújított tanúsítvány kibocsátása és publikálása megegyezik az új tanúsítványra vonatkozó eljárásokkal.

4.8 Tanúsítvány-módosítás

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

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

A tanúsítvány-módosítást az Előfizető kezdeményezheti.

A kérelem benyújtásakor a Szolgáltató ellenőrzi a tanúsítvány létezését és érvényességét, valamint az alany azonosságának és jellemzőinek igazolására használt információk érvényességét a 3.2 pontban rögzített regisztrációs eljárás szerint.

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

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

4.9 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 lesz érvénytelen. A tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam 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.

4.9.1. Visszavonáshoz vezető körülmények

Az Előfizető vagy a titkosító magánkulcs felhasználó a következő körülmények fennállása esetén kezdeményezheti a visszavonást:

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

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

A tanúsítvány a Szolgáltató kezdeményezése alapján kerül visszavonásra, ha:

1. a tanúsítvány felfüggesztési ideje lejárt,

2. az Előfizető és/vagy a titkosító magánkulcs felhasználó az ÁSZF-PKI-t vagy az Előfizetői Szerződést megszegi,
3. az Előfizető és/vagy a titkosító magánkulcs felhasználó kötelezettségeiket nem tartják be,
4. az Előfizetői szerződés megszűnik,
5. a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról,
6. a Tanúsítványban feltűntetett kibocsátó adatok megváltoznak,
7. a hitelesítési szolgáltatás megszűnik,
8. a Regisztrációs Iroda megszűnik,
9. a Szolgáltató valamely magánkulcsa kompromittálódik.

4.9.2. Visszavonás/felfüggesztés kérelmezése

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-mailben is kérhető az Ügyfélszolgálaton. A tanúsítvány visszavonására vagy visszaállítására az ettől számított 5 napon belül lehet intézkedni.

A visszavonási/felfüggesztési kérelem teljesítéséhez a következő adatok szükségesek:

a. a tanúsítvány sorszáma

b. a visszavonást/felfüggesztést kérő azonosító adatai

c. a visszavonást/felfüggesztést kérő e-mail címe

d. a visszavonáshoz/felfüggesztéshez vezető körülmények

4.9.3. A visszavonási kérelemre vonatkozó eljárás

a. A visszavonási eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt, majd mérlegeli a visszavonási okokat. Ha a visszavonási okok megalapozottak és az ellenőrzések sikeresek, a Szolgáltató elvégzi a tanúsítvány visszavonását.

b. 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

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

d. A visszavont tanúsítvány a visszavonási eljárás befejezése után haladéktalanul bekerül a visszavont tanúsítványok listájába.

Visszavont tanúsítványt a Szolgáltató semmilyen körülmények között sem állít vissza érvényesre.

4.9.4. A felfüggesztési kérelemre vonatkozó eljárás

a. A felfüggesztési eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt, majd mérlegeli a felfüggesztési okokat. Ha a felfüggesztési okok megalapozottak és az ellenőrzések sikeresek, a Szolgáltató elvégzi a tanúsítvány felfüggesztését

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

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

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

e. A felfüggesztett tanúsítvány a felfüggesztési eljárás befejezése után azonnal bekerül a visszavont tanúsítványok listájába.

A felfüggesztett tanúsítványt a Szolgáltató az Előfizető vagy a titkosító magánkulcs tulajdonosának kérésére a felfüggesztési időn belül visszaállítja érvényesre.

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

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

A felfüggesztési idő lejárta után a Szolgáltató a tanúsítványt feltétel nélkül visszavonja.

4.9.5. A visszavonási/felfüggesztési kérelemre vonatkozó kivárási idő

A Szolgáltató akkor tekinti a visszavonási/felfüggesztési kérelmet elfogadottnak, ha annak jogosságáról meggyőződött.

a. A felfüggesztési kérelemre vonatkozó türelmi idő 3 óra. Ha a Szolgáltató a felfüggesztési kérelem érvényességéről 3 órán belül nem tud kétséget kizáróan meggyőződni, akkor a felfüggesztési kérelmet visszautasítja.

b. A visszavonási kérelemre vonatkozó türelmi idő 3 óra. Ha a Szolgáltató ezen időn belül sem tud a kérelem jogosságáról meggyőződni, akkor a visszavonási kérelmet visszautasítja.

c. A Szolgáltató a visszavonási (illetve felfüggesztési) kérelem szerint módosított visszavonási állapotot 1 órán belül közzéteszi.

4.9.6. Az érintett felek kötelezettsége a visszavonási információ ellenőrzésére

Ha az érintett felek kellő gondossággal kívánnak eljárni a tanúsítvány visszavonási állapotának ellenőrzésekor, akkor a tanúsítvány visszavonási információ hitelességéről is meg kell győződniük.

4.9.7. Visszavonási listák (CRL) kibocsátási gyakorisága

A visszavonási listában 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 visszavonási listák érvényességi ideje 24 óra. Szolgáltató legkésőbb a lista érvényességi idejének lejártakor új listát bocsát ki, új érvényességi idővel.

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

4.9.8. A visszavonási lista előállítása és közzététele közötti idő maximális hossza

A visszavonási lista előállítása és közzététele közötti idő maximális hossza 1 óra.

4.9.9. Visszavonási listák ellenőrzése

A visszavonási listák ellenőrzése az érintett felek kötelessége és 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 érvénytelen, vagy felfüggesztett tanúsítvány elfogadásából keletkező bárminemű kár Érintett felet terheli. (Lásd még a 2.2.3 pontot.)

4.9.10. Valósidejű tanúsítványállapot-ellenőrzés

A Szolgáltató valósidejű tanúsítványállapot-ellenőrzést (OCSP szolgáltatást) nem szolgáltat.

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

4.9.12. A felfüggesztés körülményei

Az Előfizető vagy a titkosító magánkulcs felhasználó a következő körülmények fennállása esetén kezdeményezheti a felfüggesztést:

1. a magánkulcs kompromittálódásának gyanúja,

2. a kulcshordozó eszközt védő aktivizáló adat (PIN kód) kompromittálódásának gyanúja,

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

A Szolgáltató felfüggeszti a tanúsítványt, ha:

1. a Szolgáltató tudomására jutott alapos gyanú a regisztrációs adatok valótlanságáról,
2. az Előfizető vagy a titkosító magánkulcs felhasználó visszavonási kérelme kiegészítésre szorul.

4.9.13. Ki kérelmezheti a felfüggesztést

A felfüggesztést kérelmezheti a magánkulcs felhasználó vagy az Előfizető illetve annak képviselője.

4.9.14. A felfüggesztés maximális hossza, újraérvényesítés

Tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig lehet.
Ha a felfüggesztést az Előfizető vagy a magánkulcs tulajdonos kérte, akkor a kérelmezőnek ezen időszak alatt értesítenie kell a Szolgáltatót a tanúsítvány érvényesítése vagy visszavonása felől. Ha ilyen értesítés nem történik, akkor a 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. Amennyiben a körülmények kivizsgálásának elhúzódása a Szolgáltató hibája, akkor az Előfizető igénye estén részére térítésmentesen új Tanúsítványt bocsát ki.
A felfüggesztés megszüntetése a felfüggesztési időszak vége előtt is kérhető. A felfüggesztés megszűntetésének eredménye a tanúsítvány újraérvényesítése vagy visszavonása.
Az újraérvényesítés feltételei a következők:

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

b. az újraérvényesítést kérő személyt azonosítani kell.

Az újraérvényesítés kéréséhez a következő adatokat kell megadni:

a. a felfüggesztett tanúsítvány sorszáma

b. a felfüggesztés megszüntetést kérő személy azonosító adatai

c. a felfüggesztés megszüntetésének oka

4.10 Kulcs letétbe helyezése és visszaállítása

A Szolgáltató a titkosító tanúsítványok esetében az alany titkosító magánkulcsát az Előfizetői Szerződésben rögzített feltételekkel a [33] Kulcs-visszaállítási szabályzatban meghatározott módon letétbe helyezi, illetve az Előfizető kérésére visszaállítja.

5. Elhelyezési, irányítási és működtetési szabályozások

A Szolgáltató az elfogadott szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza. A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására. A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja.
A biztonságkezelési szabályokat a Szolgáltató társasági szintű informatikai biztonságpolitikája [27] és biztonsági szabályzata [28] tartalmazza. A Szolgáltató hitelesítés-szolgáltatást támogató informatikai rendszere vonatkozásában a PKI szolgáltatások biztonsági szabályzata [31] érvényesül. Ez a szabályzat szervezeti egység szinten és munkakörökre lebontva rögzíti a biztonságkezeléssel összefüggő feladatokat, felelősségeket és szabályokat, így többek között a bizalmi munkakörök felsorolását, a kinevezési feltételeket és az összeférhetetlenségi kritériumokat.
A MÁV INFORMATIKA Zrt. rendszeres belső és külső auditjai ezen dokumentumokat és a dokumentumokban a titkosító tanúsítvány szolgáltatásra vonatkozó előírások teljesülését az évente esedékes ellenőrzései során vizsgálja.
Szolgáltató gondoskodik az információbiztonság fenntartásáról azokban az esetekben is, amikor a titkosítással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősségek más szervezethez kerülnek kiadásra.
A Szolgáltató felelősséget vállal minden – jelen HSZSZ-T-ben tárgyalt – titkosítással kapcsolatos szolgáltatásért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki.

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 a kulcshordozó eszközre és a kulcshordozó eszközök megszemélyesítése.

5.2 Eljárásrendi szabályozások

A Szolgáltató eljárásrendi szabályait három szabályzat tartalmazza:

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

b. a jelen szolgáltatási szabályzat,

c. a [31] 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:

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

b. titoktartási nyilatkozatot ír alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is szerepelnek.

5.4 Naplózási eljárások

5.4.1. 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 a regisztráció, a kulcspár generálása, letétbe helyezése, visszaállítása, a kulcshordozó eszköz megszemélyesítése, a tanúsítvány létrehozása, kibocsátása és kezelése, valamint 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.

5.4.2. Napló adatok védelme

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

A Szolgáltató biztosítja naplóállományok bizalmasságát és sértetlenségét.

5.4.3. A naplók feldolgozásának gyakorisága

A Szolgáltató a hitelesítő központok (CA-k) naplóit naponta, az egyéb napló fájlokat a [31] biztonsági szabályzatában rögzített gyakorisággal dolgozza fel.

5.4.4. Napló adatok tárolása

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

5.4.5. A napló fájlok megőrzési időtartama

Lásd: 5.5 Adatok archiválása c. fejezetet.

5.5 Adatok archiválása

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

5.5.1. A tárolt adatok típusai

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

- *a.* az Előfizető által a regisztráció támogatása céljából benyújtott igazolványok és dokumentumok típusa, egyedi azonosító adatai (például a személyazonosító igazolvány száma)
- *b.* az Előfizetői Szerződés másolata
- *c.* a regisztrációs kérelmet elfogadó regisztrációs felügyelő (RO) azonosítója
- *d.* Az 5.4.1 pontban felsorolt összes esemény, illetve napló típus.

5.5.2. Az archívum megőrzési időtartama

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

5.5.3. Az archívum védelme

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

5.5.4. Az archívum hozzáférését és ellenőrzését végző eljárások

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

a. A Szolgáltató biztosítja, hogy mindaddig, amíg az archivált adatokat őrzi, az arra jogosult személyek számára hozzáférhetők és értelmezhetők lesznek.

b. A tanúsítványokra vonatkozó adatokat rendelkezésre bocsátja, ha azokra jogi eljárásokban bizonyíték nyújtása céljából szükség van.

c. Az alanynak, illetve az adatvédelmi követelmények korlátozásain belül az előfizetőnek hozzáférést biztosít az alanyra vonatkozó regisztrációs és egyéb információkhoz.

5.6 A Szolgáltató kulcscseréje

A Szolgáltató szolgáltatói kulcsának tervezett cseréje előtt fél évvel köteles tájékoztatni az MK-PKI Tanácsadó Testületet és vele egyeztetni a szükséges feladatokról.

A szolgáltatói kulcs kompromittálódása esetén az 5.8 pontban előírtak szerint kell eljárni.

5.7 Katasztrófa elhárítás

5.7.1. A szolgáltatás azonnali felfüggesztése

A katasztrófa esemény bekövetkezése a szolgáltatás azonnali felfüggesztésével jár. Erről az eseményről Szolgáltató lehetőségei szerint értesíti a felhasználó Közösség tagjait.

5.7.2. Minimális szolgáltatás rendkívüli üzemeltetési helyzetben

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

Rendkívüli üzemeltetési helyzetben a Szolgáltató minden egyéb szolgáltatást szüneteltet.

5.7.3. Rendkívüli eseményekről történő értesítés

A hitelesítés-szolgáltatást támogató informatikai rendszerre, annak fizikai és személyi környezetére kiható súlyos üzemzavari és katasztrófa események megelőzéséről, kezeléséről, az érintettek értesítéséről és a rendszer visszaállításáról részletesen a Szolgáltató [32] Üzletmenet-folytonossági Terve intézkedik. Az Üzletmenet-folytonossági Tervben az üzletmenetet veszélyeztető, sértő, illetve azt leállító események súlyossági osztályokba vannak sorolva. A Terv részletes intézkedési forgatókönyveket tartalmaz a súlyos üzemzavari, illetve katasztrófa események kezelésére és részletesen szabályozza a Hitelesítő Központok szolgáltatói kulcsainak kompromittálódása esetén elvégzendő teendőket is Ez a dokumentum biztonsági okokból nem nyilvános.

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

5.8 A szolgáltatási tevékenység megszüntetése

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

A Szolgáltató gondoskodik a szolgáltatásainak megszüntetéséből fakadó zavarok minimalizálásáról. Különösképpen gondoskodik a tanúsítvány visszavonás kezelés és közzététel szolgáltatások folyamatos fenntartásáról.

Ennek érdekében a Szolgáltató mielőtt szolgáltatási tevékenységét leállítja:

a. legalább 30 nappal korábban értesíti az MK-PKI Tanácsadó Testületet és Internetes honlapján tájékoztatja a felhasználói közösség tagjait

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

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

A bejelentéssel egyidejűleg a Szolgáltató leállítja:

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

b. a kulcshordozó eszközön a titkosító kulcs elhelyezése szolgáltatást.

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

Ezzel egyidejűleg leállítja a visszavonás kezelési szolgáltatást.

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

6. Műszaki biztonsági óvintézkedések

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

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

6.1 Kulcs-pár előállítása és telepítése

6.1.1. Kulcs-pár előállítás

A Szolgáltató maga generálja a kulcspárt. Nem fogad el az Előfizető által generált titkosító magánkulcsot, illetve kulcshordozó eszközt.

A kulcspár generálását (előállítását) a Szolgáltató a fokozott biztonsági szintnek megfelelő védett környezetben, bizalmi munkakört betöltő személyzettel végezteti. A generált kulcspárt és a hozzá tartozó tanúsítványt a kulcsgenerálás befejező fázisában – biztonsági okokból – egy előre elkészített ún. transzport kulcspár publikus kulcsával titkosítja.

A kulcspár előállítási funkció végrehajtására felhatalmazott személyzet körét a Szolgáltató a lehető legkisebbre korlátozza.

A Szolgáltató a magánkulcsot csak a kulcspárhoz tartozó tanúsítvánnyal együtt helyezi el a kulcshordozó eszközön.

A Szolgáltató személyes típusú tanúsítványokhoz a felhasználó kívánsága szerinti kulcshordozó eszközt (pl.: csipkártyát, tokent stb.) alkalmaz.

A Szolgáltató a kulcshordozó eszközhöz PIN kódot biztosít.

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

6.1.2. A titkosító magánkulcs eljuttatása a felhasználóhoz

a. a Szolgáltató titkosító magánkulcsokat a transzport kulcs publikus kulcsával titkosítva tárolja és adja át az előfizetőnek vagy megbízottjának,

b. a titkosító magánkulcsot az Előfizető (vagy képviselője) a Szolgáltatótól titkosított állapotban veszi át és a birtokában lévő transzport kulcs privát kulcsával állítja vissza,

c. a Szolgáltató a kulcshordozó eszköz PIN kódját biztonságosan készíti el és a kulcshordozó eszköztől elkülönítve tárolja.

Az Előfizetőnek 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. A nyilvános kulcsok eljuttatása a felhasználói közösséghez

A Szolgáltató a Hitelesítő Központok és az Előfizetők nyilvános kulcsait a kibocsátott tanúsítványokban helyezi el. A Hitelesítő Központok tanúsítványait a szolgáltatás honlapján, az Előfizetői tanúsítványokat a Tanúsítványtárában teszi a felhasználói közösség számára elérhetővé.

6.1.4. Kulcs méretek, használt algoritmusok

A Szolgáltató Hitelesítő Központja elektronikus aláírás létrehozására az RSA[2] algoritmust használja. Az Előfizetői tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

A titkosító magánkulcs felhasználók (Előfizetők) titkosító magánkulcsainak mérete: legalább 1024 bit

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

[2] Az RSA algoritmust (Rivest, Shamir and Adleman Algorithm) az alábbi szabvány írja le részletesen: International Organization for Standardization, “ISO/IEC 14888-3: Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms,” 1999.

6.1.5. Kulcs felhasználási célok

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

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

6.1.6. Nyilvános kulcs paraméterek előállítása, a paraméterek ellenőrzése

A Szolgáltató a nyilvános kulcs paraméterek előállítása és ellenőrzése során az érvényes hazai és nemzetközi szabványokat, ajánlásokat veszi figyelembe.

6.2 Magánkulcsok védelme

6.2.1. Kriptográfiai modulra vonatkozó szabványok

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

A titkosító magánkulcsot a Szolgáltató PIN kóddal védve bocsátja ki.

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

A Szolgáltató az előfizetői titkosító magánkulcsokat a kulcshordozó eszközre a következő módokon viheti fel:

1. Egy olyan biztonságos kulcshordozó eszközben tárolja, amely nem kompromittálja a magánkulcs biztonságát, megfelel az ISO/IEC 15408 1999/1.,2.,3. szabvány szerint kidolgozott SSCD-PP3 védelmi profil követelményeinek, és amely szerepel a Nemzeti Hírközlési Hatóság elektronikus aláírás termék listáján.
2. A titkosító magánkulcs a transzport nyilvános kulccsal titkosítva kerül a kulcshordozó eszközre, amelyet az Előfizető vagy a megbízott kapcsolattartó állít vissza a titkosító magánkulcs felhasználó jelenlétében.

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

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

6.2.3. Titkosító magánkulcs letét

A Szolgáltató az előfizetői titkosító magánkulcsot letétbe nem helyezi.

6.2.4. Titkosító magánkulcs biztonsági mentése

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

Szolgáltató az előfizetők titkosító magánkulcsait csak kulcsvisszaállítási céllal menti és a tanúsítvány lejáratáig, illetve az előfizetővel kötött szerződésben rögzített időpontig megőrzi.

6.2.5. Titkosító magánkulcs archiválása

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

6.2.6. Magánkulcsok aktivizálása

Az előfizetői titkosító magánkulcs aktivizálása a Felhasználó által történik a PIN kód megadásával, azokban az esetekben, amikor a titkosító magánkulcs használatára szükség van.

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

[3] 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

6.2.7. Magánkulcsok deaktivizálása

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

A szolgáltatói titkosító magánkulcsok megsemmisítése a Szolgáltató kötelessége.

6.2.9. Magánkulcs tárolása kriptográfiai modulban

A Szolgáltató szolgáltatói magánkulcsait egy külön hardver kriptográfiai modulban tárolja. Egyúttal hozzáférésvédelmet és ellenőrzéseket alkalmaz annak biztosítása érdekében, hogy a magánkulcsok a kriptográfiai modulon kívül ne legyenek hozzáférhetők.

6.3 A kulcspár kezelésének egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

A Szolgáltató a nyilvános kulcsokat a tanúsítványokkal együtt archiválja (lásd: 4.8 pont).

6.3.2. A tanúsítványok és kulcspárok használatának periódusa

A Szolgáltató szolgáltatói magánkulcsainak használati periódusa nem haladhatja meg azok érvényességi idejét.

6.4 Aktivizáló adatok (PIN kódok)

6.4.1. Aktivizáló adatok generálása és installációja

A kulcshordozó eszközök és a titkosító magánkulcs aktivizáló adatait (PIN kódjait) a PKI alkalmazás állítja elő.

6.4.2. Aktivizáló adatok védelme

1. A Szolgáltató a titkosító magánkulcs felhasználó hozzáférési jogosultságát ellenőrző adatot (PIN-kódot) csak abból a célból rögzítheti, hogy azt átadhassa[4].
2. A Szolgáltató kulcshordozó eszközök PIN kódjait műszaki és szervezési intézkedésekkel védi az Előfizetőnek vagy a titkosító magánkulcs felhasználó részére történő átadásig.
3. Az átvétel után a titkosító magánkulcs felhasználó a saját munkaállomásán megváltoztathatja a PIN kódot, amelyhez megfelelő ügynök programmal (CSP) kell rendelkeznie.
4. A titkosító magánkulcs felhasználó a későbbiekben is bármikor megváltoztathatja a PIN kódját.
5. A Szolgáltató a saját aktivizálási adatait fokozott biztonsági szinten védi.
6. Az aktivizáló adat elvesztése, elfelejtése vagy illetéktelen kezekbe történő jutása esetén minden esetben új kulcspárt és aktivizálási adatot kell előállítani.

6.5 Informatikai biztonsági előírások

6.5.1. Számítógép biztonsági követelmények

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

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

Az operációs rendszerek által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás (a biztonsági napló védelme, az ahhoz való hozzáférés korlátozása),

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

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

A PKI alkalmazás által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás (a rendszerüzemeltetői hozzáférések és tevékenységek rögzítése),
b. kommunikáció (a Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása),
c. a felhasználói adatok védelme (az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják),

A kriptográfiai hardver modulok által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás,
b. kriptográfiai támogatás (kriptográfiai kulcsok generálása, védelme és megsemmisítése; bizalmasságot, sértetlenséget, hitelességet és letagadhatatlanságot biztosító kriptográfiai eljárások megvalósítása),
c. a felhasználói adatok védelme (hozzáférés ellenőrzési szabályok érvényre juttatása),
d. azonosítás és hitelesítés,
e. biztonságkezelés (a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
f. a biztonsági funkciók megbízható védelme (a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása),

A tűzfal és a behatolás-detektáló által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás (a hálózati kommunikáció naplózása, a biztonsági napló védelme, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),
b. a felhasználói adatok védelme (az információ áramlás ellenőrzési szabályok érvényre juttatása/szűrés, a tiltott információ áramlás megakadályozása, megfigyelése),

6.6 Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési szabályok

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

6.6.2. Biztonságkezelési szabályok

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

6.7 Hálózati biztonsági szabályok

1. A hálózati védelmi intézkedések fokozott biztonsági szintnek felelnek meg.
2. A Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikációt biztosító belső hálózat PKIX kapcsolattal védett a sértetlenség és letagadhatatlanság érdekében, illetve bizalmasság elvesztése ellen.
3. A Szolgáltató hitelesítés-szolgáltatást támogató informatikai rendszerénél a védett belső és a külső hálózatok biztonságos elválasztását tűzfal és behatolás érzékelő rendszer (IDS) biztosítja.
4. A Hitelesítő Központ nem folytat közvetlen külső kommunikációt a végfelhasználókkal.

6.8 Kriptográfiai modul ellenőrzése

A Szolgáltató a titkosító tanúsítvány szolgáltatáshoz alkalmazott hardveres kriptográfiai modult rendszeresen ellenőrzi.

7. Tanúsítvány és tanúsítvány-visszavonási profil

A Szolgáltató által kibocsátott tanúsítvány és tanúsítvány-visszavonási profilok megfelelnek az ITU-T X.509 szabvány 3. változatának. Az alkalmazott tanúsítványtípus mezői és azok értelmezése e szabványokat követi.

7.1 Tanúsítvány profil

7.1.1. Alap mezők

A Szolgáltató az RFC 3280 bis 08-nak megfelelő tanúsítványokat bocsát ki.

7.1.2. Tanúsítvány kiterjesztések

A Szolgáltató az ITU X.509 szabvány 3. változatának, az EU ETSI TS 101 862 és az RFC 3739 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.

7.2 Tanúsítvány-visszavonási profil

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

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

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

8. Megfelelőségi audit és egyéb ellenőrzések

8.1 Az ellenőrzések gyakorisága és körülményei

A megfelelőségi ellenőrzéseket 2 évente meg kell ismételni. Ezek az ellenőrzések lehetnek belső auditok is.

8.2 Az auditor és szükséges képesítése

A külső és belső auditálást végző személyeknek függetlennek kell lenniük a szolgáltatás üzemeltetését végző személyektől.

A külső és belső auditálást csak a megfelelő szakmai ismeretek birtokában lévő, tapasztalt szakemberek végezhetik.

8.3 Az auditor és az auditált rendszerelem függetlensége

Az auditornak függetlennek kell lennie az általa ellenőrzött rendszertől.

8.4 Az auditálás által lefedett területek

Az auditálásnak le kell fedni az alábbi területeket:

a. fizikai biztonság

b. dokumentálás és folyamatok biztonsága

c. a személyi állomány biztonsági ellenőrzése

d. adatvédelem

e. műszaki biztonság

8.5 A hiányosságok kezelése

A hiányosságok kezelése a [31] biztonsági szabályzat szerint történik.

8.6 Az eredmények közzététele

A külső és belső rendszervizsgáló csak a megbízójának adhat információt a szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a szolgáltató bizalmas üzleti információi, ezért azokat [26] titokvédelmi szabályzat szerint kell kezelni.

9. Egyéb üzleti és jogi kérdések

9.1 Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató a szolgáltatás internetes honlapján 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.

9.1.1. Tanúsítványok kibocsátása

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

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

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

c. a titkosító tanúsítványok és kulcspárok biztonságos megőrzésének 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 megőrzését és tárolását, továbbá szükség esetén, - a korábbi titkosított állományok visszaállítása érdekében - a tanúsítványok és a titkosító kulcspárok kiadását az Előfizetőnek.

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

9.1.2. Tanúsítvány hozzáférés

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

9.1.3. Visszavonás és állapot információ hozzáférés

Szolgáltató a közzétett visszavonási információ eléréséért nem számol fel díjat.

9.1.4. Egyéb szolgáltatásokra vonatkozó díjak

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

9.1.5. 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 kulcshordozó eszközön szereplő adatok a Szolgáltató hibájából fakadóan nem megfelelők,[5]

d. a kibocsátott kulcshordozó eszköz, az aktivizáló adat 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.

9.2 Anyagi felelősség és annak korlátai

A Szolgáltató anyagi felelősségéről és annak korlátairól a [30] Általános Szerződési Feltételek (ÁSZF-PKI) rendelkezik.

9.3 Bizalmasság – Adatkezelési szabályzat

9.3.1. Bizalmas információk

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

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

1. A titkosító magánkulcs letétben tárolt példányát és 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 és a titkosító magánkulcs felhasználó hozzájárulását az alábbiakhoz:
   3.1. hozzájárulás a szolgáltatások során felhasznált adatok szolgáltató által történő nyilvántartásba vételéhez,

[5] Pl. a magánkulcs hordozó kártya fizikai megszemélyesítése nem megfelelő

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 a titkosító magánkulcs felhasználóra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz ő maga hozzájárul, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,
6. biztosítja a regisztrációs adatok bizalmasságát és sértetlenségét az előfizetővel folytatott adatcsere során is.

A Szolgáltató az előfizetők és a titkosító magánkulcs felhasználók személyes adatait csak a közöttük fennálló előfizetői szerződéssel összhangban levő célokra használhatja fel, harmadik félnek azokat az Előfizetők és a magánkulcs felhasználók írásos hozzájárulása nélkül nem adhatja át, kivéve a 9.3.4 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 a titkosító magánkulcs felhasználó azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

9.3.2. Nem bizalmas információk

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

9.3.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

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

9.3.4. Feltárás törvényi meghatalmazással rendelkezők részére

A Szolgáltató a tanúsítvány felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – meghatalmazás birtokában – adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét a Szolgáltatónak rögzíteni kell, de az adatátadásról az előfizetőt vagy a magánkulcs felhasználót nem tájékoztathatja.

9.3.5. Információszolgáltatás polgári eljárás keretében

A Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - a titkosító magánkulcs felhasználó személyazonosságát igazoló adatokat átadhatja az ellenérdekű peres félnek vagy képviselőjének feltárhat bizalmas felhasználói információkat, illetőleg azt közölheti a megkereső bírósággal. A Szolgáltató rögzíti az információszolgáltatás tényét, és arról tájékoztatja az Előfizetőt.

9.3.6. Feltárás tulajdonos kérésére

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

9.4 A személyes adatok védelme

a) A Szolgáltató gondoskodik az adatvédelem és az adatbiztonság területén a szabályszerű működésről, a jogok, kötelezettségek és felelősségek meghatározásáról

b) A Szolgáltató működése és szabályzatai megfelelnek a Személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992 évi XLIII. törvény követelményeinek.

9.5 Szellemi tulajdonhoz fűződő jogok

A Szolgáltató által előfizetői részére kibocsátott tanúsítványok és az azokhoz tartozó kulcspárok tulajdonosa az Előfizető, teljes jogú használója pedig a titkosító magánkulcs felhasználó (alany), 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, szerződéses feltételei

d. a Tanúsítványban szereplő hitelesítő azonosító.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltatói felelősség és helytállás

A Szolgáltató felelősségét a jelen szolgáltatási szabályzat 2.2.1 fejezete, helytállására vonatkozó kötelezettségeit a [30] Általános Szerződési Feltételek (ÁSZF-PKI) tartalmazza.

9.6.2. Az előfizetői felelősség és helytállás

Az előfizetői felelősség és helytállás mértékére a jelen szolgáltatási szabályzat 2.2.2 fejezete, az előfizetői szerződés és a [30] Általános Szerződési Feltételek (ÁSZF-PKI) előírásai érvényesek.

9.6.3. Az érintett fél felelőssége

Az érintett fél felelősségét a jelen szolgáltatási szabályzat 2.2.3 fejezete tartalmazza

9.6.4. Érvényességi időtartam

Jelen szabályzat visszavonásig, illetve egy újabb verzió hatályba lépéséig érvényes.

9.6.5. Irányadó jog

A Szolgáltató működésére a Magyar Köztársaság törvényei az irányadók.