MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó
Zártkörűen Működő Részvénytársaság

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

Verziószám	**5.0**
OID szám	**1.3.6.1.4.1.14868.2.2.2.5**
Hatósági nyilvántartásba vétel napja	**2008. 01. 01.**
Hatósági nyilvántartásba vétel száma	**HL-7691-2/2008a**
Hatálybalépés dátuma	**2008. 01. 01.**

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

HR-MTT+BALE verziók

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2002. 12. 08.	A nyilvános körben kibocsátott biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványok (**MTT+BALE**) szolgáltatói minősítésére előkészített változat	Bodlaki Ákos		
1.1	2003. 01. 30.	A minősítési eljárásra átadott változat	Bodlaki Ákos, Benkó Tamás, Tóth Elemér, Vész Ferenc		
1.1	2003. 03. 31.	A minősítési eljárásra elfogadott változat	Bodlaki Ákos, Tóth Elemér		
2.0	2005. 07. 21.	OCSP[1]-vel bővített változat	Néder Ferenc		
3.0	2006. 03. 30.	Felülvizsgált, az NHH észrevételei alapján javított változat	Néder Ferenc		
4.0	2007. 08. 06.	Felülvizsgált, az NHH észrevételei alapján javított változat	Néder Ferenc	Kovács Árpád, PKI SZE vezető	Hosszú Sándor István, vezérigazgató
5.0	2008. 01. 01.	A Szolgáltató adatainak változásával korrigált változat	Néder Ferenc	Juhász György, PKI SZE vezető	Hosszú Sándor István, vezérigazgató

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

TARTALOMJEGYZÉK

1. Bevezetés

E dokumentum a MÁV INFORMATIKA Zrt. (továbbiakban Szolgáltató) minősített hitelesítés-szolgáltatása keretében kibocsátott minősített elektronikus aláírások ellenőrzésére szolgáló tanúsítványok kezelésére (előállítás, felfüggesztés, visszavonás, megújítás) vonatkozó eljárásrendet, a tanúsítványok szerkezetét, a tanúsítványok tartalmának és érvényességének ellenőrzési eljárásait és az egyéb működési szabályokat tartalmazza.

A Szolgáltató szolgáltatásait a vele előfizetői szerződéses viszonyban álló *Előfizetők* részére nyújtja. A Szolgáltató az elektronikus aláírások hitelességét ellenőrző *érintett felek* részére bizonyos szolgáltatási elemeket hozzáférhetővé tesz.

A jelen Hitelesítési Rendet (továbbiakban: HR-MTT+BALE) a következők használják:

a. a Szolgáltató személyzete, annak érdekében, hogy a szolgáltatási tevékenység a hatályos jogszabályokkal és a Szolgáltató belső szabályzataival összhangban valósuljon meg,

b. az ellenőrző hatóságok,

c. a belső és külső auditorok.

A 2001. évi XXXV. törvényben meghatározott minősített elektronikus aláírással kapcsolatos szolgáltatások közül (továbbiakban: szolgáltatások) a Szolgáltató a jelen hitelesítési rend keretei között az Előfizetők és velük kapcsolatban álló Aláírók részére a következő szolgáltatásokat nyújtja:

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

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

1.1. 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 köz-

vetlen 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

1.2. Áttekintés

1.2.1. A hitelesítési rend célja

A HR-MTT+BALE egy olyan szabálygyűjtemény, mely egy Tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazás számára, valamint rögzíti azokat a követelményeket, amelyeket a Szolgáltatónak a tanúsítvány kezelés folyamatában teljesítenie kell.

Jelen dokumentumban a követelmények a nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz (rövidítve: BALE) alkalmazását megkövetelő minősített tanúsítványokra [rövidítve: MTT+BALE] vonatkoznak.

A tanúsítványok végfelhasználóinak tevékenységére vonatkozóan jelen HR-MTT+BALE-től független egyéb belső szabályzatok is élhetnek előírásokkal. Amennyiben e szabályzatok bármely vonatkozásban ellentmondást vagy eltérő kikötést tartalmaznának, jelen HR-MTT+BALE előírásai tekinthetők magasabb szintűnek, s ezek alkalmazandók.

1.2.2. Jogszabályok, szabványok

A jelen hitelesítési rend a következő jogszabályokat, szabványokat és ajánlásokat veszi figyelembe a hitelesítési rend teljes tartalmára vonatkozóan:

2001. évi XXXV. törvény az elektronikus aláírásról (a továbbiakban: Eat.),

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

ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3 részek)

A hitelesítési rend szerkezetére és tartalmára vonatkozóan:

RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány és szolgáltatási szabályzat keretrendszer)

Európai Unió ETSI TS 101 456 szabvány,

American Bar Association (ABA),

PKI Assessment Guidelines (PAG),

A minősített tanúsítványok, visszavonási listák szerkezetére és tartalmára vonatkozóan:

International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer”

Minősített tanúsítvány minták minősített hitelesítés-szolgáltatók számára, 1.0 verzió. Hírközlési Felügyelet.

ETSI TS 101 862 Minősített tanúsítvány profil

RFC 2459 illetve RFC 3280 (Internet X.509 Nyilvános kulcsú infrastruktúra – Tanúsítvány és Tanúsítvány visszavonási lista profil)

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

RFC 3739 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)

ISO 3166 szabvány

A minősített hitelesítés-szolgáltatókra vonatkozóan:

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

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

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

ETSI TS 101 456 (Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények).

Az OCSP szolgáltatásra vonatkozóan:

IETF RFC 2560 szabvány

Az informatikai biztonsági követelményekre vonatkozóan:

ITSEC[2], CC[3]

A kriptográfiai modulra, az aláírás-létrehozó eszközre vonatkozóan:

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

ITSEC, CC,

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

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

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

1.3. Hitelesítési rend azonosítás

A jelen hitelesítési rend a nyilvános körben kibocsátott és BALE eszköz alkalmazását megkövetelő minősített tanúsítványokra vonatkozó [MTT+BALE] követelményeket és ezzel kapcsolatos szabályokat írja le.

A nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítvány a következő tulajdonságokkal rendelkezik:

a. megfelel az Eat. 2. számú mellékletében meghatározott követelményeknek,

b. olyan hitelesítés-szolgáltató adta ki, amely teljesíti az Eat. 3. számú mellékletében meghatározott követelményeket,

c. olyan biztonságos aláírás-létrehozó eszköz került felhasználásra, amely eleget tesz az Eat. 1. számú mellékletében meghatározott követelményeknek,

d. nyilvános körben került kibocsátásra.

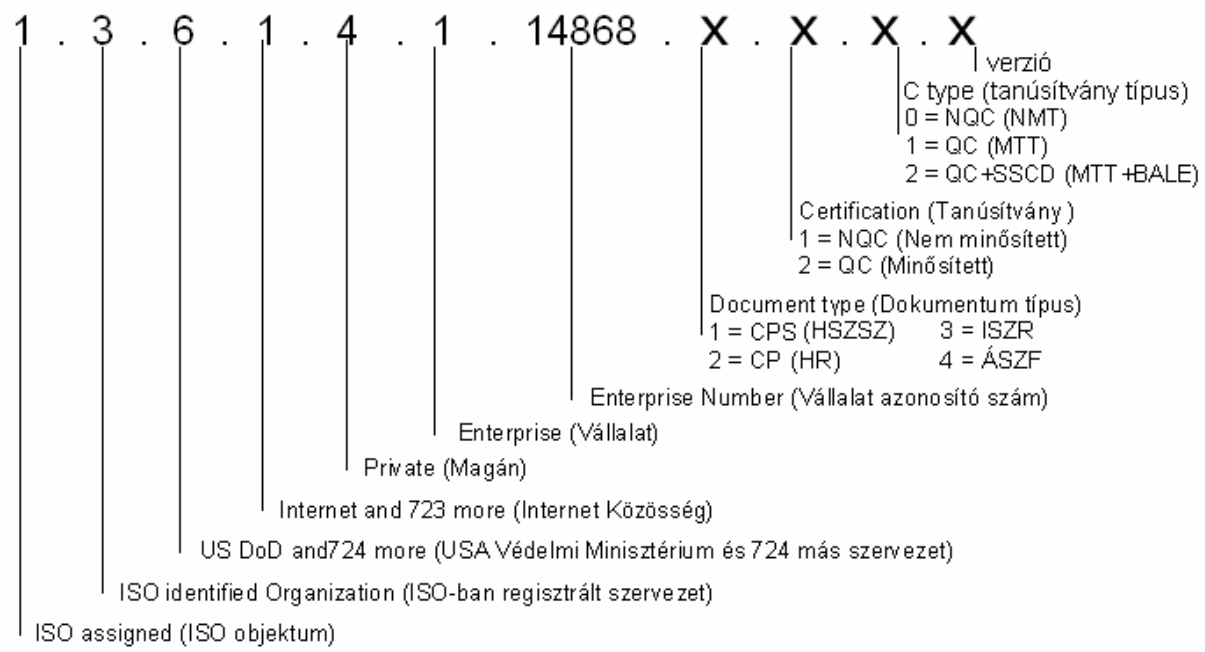
Az így kibocsátott minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon elégítik ki, mint egy kézírásos aláírás a papír-alapú adatok vonatkozásában[4].

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

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

[4] Vagyis minősített aláírásokhoz (lásd az Eat. 29.§ (1) bekezdését).

A nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítvány objektum azonosítója a következők szerint épül fel:



Jelen dokumentum teljes neve:

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

A jelen dokumentumban HR-MTT+BALE-ként történik rá hivatkozás.

Jelen HR-MTT+BALE-nek csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

1.4. Hitelesítés szolgáltató és felhasználói közösség, alkalmazhatóság

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösség a következő:

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

b. az Előfizetők és az Aláírók

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

d. az érintett felek

OCSP vonatkozásában a közösséget következő csoportok alkotják:

a. az Előfizetők

b. az OCSP szolgáltató

c. az OCSP válaszokat felhasználó (igénybevevő[5]) fél

d. az érintett felek

1.4.1. A Szolgáltató regisztráló és hitelesítő egységei

A Szolgáltató regisztráló és hitelesítő egységei:

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

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

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

A Szolgáltató regisztráló és hitelesítő egységei részletes feladatait a jelen hitelesítési rend 1.sz. melléklete írja le.

1.4.1.1. Regisztráló szervezet

A regisztráló szervezetek a Szolgáltató és a vele szerződéses alapon együtt működő Társaságok (mint szerződött közreműködők) azon szervezeti egységei, amelyek az előfizetők adatainak regisztrációját, ellenőrzését, az előfizető személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a regisztráló szervezethez történő továbbítását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

Egy regisztráló szervezethez tartozó előfizetők önálló közösséget alkothatnak, melyre a Szolgáltató, vagy a vele szerződéses alapon együtt működő Társaságok (mint szerződött közreműködők) további szabályokat is alkalmazhatnak. A regisztráló szervezetek által létrehozott szabályok nem tartalmazhatnak olyan kikötést, amely ellentétben áll a Hitelesítési Rend és Szabályozási Csoport által jóváhagyott Szabályzatokkal.

A regisztráló szervezet az elektronikus aláírás hitelesítés-szolgáltatás keretein belül biztosítja az előfizetői regisztrációt, a tanúsítványok felfüggesztés és visszavonás kezelését és az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezését. Egyúttal közreműködik további elektronikus aláírással kapcsolatos szolgáltatások biztosításában: tanúsítvány előállítás, kibocsátás és visszavonási állapot közzététele.

1.4.1.2. Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi eleme, amely a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, azt ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata a különböző osztályú és típusú aláírás-létrehozó adatok és tanúsítványok előállítása, ezek publikálása, a regisztráló szervezettől érkező módosítási, felfüggesztési, újra aktivizálási, visszavonási és megszüntetési igényeknek a Szolgáltatási Szabályzat (továbbiakban: HSZSZ-M) szerinti végrehajtása és a szolgáltatást támogató informatikai rendszer üzemeltetése.

1.4.2. Hitelesítési Rend és Szabályozási Csoport

A Hitelesítési Rend és Szabályozási Csoport a Szolgáltató által létrehozott szervezeti egység, amely a hitelesítés szolgáltatással kapcsolatos hitelesítési rendek és szolgáltatási szabályzatok kialakításáért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős. A Hitelesítési Rend és Szabályozási Csoportnak függetlennek kell lennie a PKI Szolgáltató Egységtől. A Hitelesítési Rend és Szabályozási Csoport feladata általában a hitelesítés szolgáltatáshoz kapcsolódó házirendek és szabályzatok elkészítése. Amennyiben a PKI Szolgáltató Egység vagy bármely más szervezeti egység, illetve külső megbízott készít el házirendet vagy szabályzatot, akkor a Hitelesítési Rend és Szabályozási Csoportnak ellenőriznie kell azokat megfelelőség szempontjából.

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

1.4.3. Előfizetők és Aláírók (Felhasználók)

Előfizető a Szolgáltatóval szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató Tanúsítványt bocsát ki. Előfizető lehet természetes vagy jogi személy.

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

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

1.4.4. Érintett felek

Az Érintett fél (aláírás Ellenőrző) olyan természetes vagy jogi személy, aki vagy amely, az aláírt elektronikus dokumentum fogadója, és egy adott Tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az aláírás hitelességének ellenőrzésekor.

1.4.5. Alkalmazhatóság

1.4.5.1. A hitelesítési rend hatálya

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

A hitelesítési rend személyi hatálya a szolgáltatóra, annak a szolgáltatásban közreműködő munkatársaira és a felhasználói közösségre terjed ki.

A hitelesítési rend tárgyi hatálya a következőkre terjed ki:

a. az 1. pontban meghatározott szolgáltatásokra

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

1.4.5.2. Szolgáltatás szintje

A Szolgáltató az 1. pontban rögzített Eat. szerinti minősített szolgáltatásokat nyújtja, melyek az alábbi összetevőkből épülnek fel:

a. Ügyfél regisztráció,és egyedi (megkülönböztető) név meghatározás

b. Tanúsítvány kiadás és tanúsítvány közzététel

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

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

e. Tanúsítvány felfüggesztés és visszavonás kezelés

f. Tanúsítvány megújítás

g. OCSP szolgáltatás

1.4.5.3. Tanúsítványok alkalmazhatósága

Az előfizetői tanúsítványok alkalmazhatóságára a következő szabályok érvényesek:

Engedélyezett alkalmazási lehetőségek

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

Korlátozott alkalmazási lehetőségek

Szolgáltató területi, pénzügyi, stb. korlátozásokat szabhat az előfizetői szerződésben, amelyeket a kibocsátott előfizetői Tanúsítványban fel kell tüntetni.

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

Tiltott alkalmazási lehetőségek

Az előfizetői tanúsítványokat tilos felhasználni más nyilvános kulcsú tanúsítványok aláírására, vagy bármilyen hitelesítés szolgáltatás nyújtásához.

A fentiek alapján a kibocsátott Tanúsítványok (illetve az ezekhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, amely támogatja a PKI technológián alapuló elektronikus aláírási, le nem

tagadhatósági funkciókat. A Szolgáltató nem vállal felelősséget az elektronikus aláírásra kibocsátott aláírás-ellenőrző adat, illetve az aláírás-létrehozó adat titkosításra, vagy más, az elektronikus aláírástól eltérő felhasználására vonatkozóan.

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

A tanúsítvány használatára vonatkozó kitételeket a Tanúsítványban is rögzíteni kell. A tanúsítvány kitételektől eltérő használata az Aláíró egyéni felelőssége és kockázata, ahogy az ilyen módon felhasznált tanúsítvány elfogadása is az érintett fél (aláírás Ellenőrző) felelőssége és kockázata.

1.5. Tanúsítvány osztályok és tanúsítvány fajták

A jelen hitelesítési rend a nyilvános körben kibocsátott minősített és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő tanúsítványokat és az ezzel kapcsolatos követelményeket írja le.

1.5.1. Minősített tanúsítványok jellemzői

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

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

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

Az MTT+BALE olyan minősített tanúsítvány, amely:

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

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

1.5.3. Tanúsítványok használati osztályainak jellemzői

1.5.3.1. Előfizetői tanúsítvány

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

Előfizetői tanúsítvány olyan természetes személyeknek vagy szervezeteknek adható ki, amelyeknél a Szolgáltató az Aláírót személyes megjelenés során hitelesítő dokumentumokra és írásos nyilatkozatokra alapozott biztonsági ellenőrzéssel azonosítja.

Ha az Aláíró természetes személy jogi személyt képvisel, akkor a képviseleti jogot írásos megbízói nyilatkozattal kell igazolni.

1.5.3.2. Szolgáltatói tanúsítvány

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

1.5.4. Tanúsítvány fajták és tulajdonságaik

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

1.5.4.1. „Személyes" tanúsítvány

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

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

Ha a tanúsítvány CN mezőjében nem az aláíró személyazonosító igazolványában szereplő név kerül megadásra, úgy ez a név álnévként kerül rögzítésre.

Az álnév jelzésére a tanúsítvány CN mezőjében található szöveg '~' (tilde) karakterrel kezdődik és végződik (pl. CN= „~Ludas Matyi~").

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

1.5.4.2. „Szervezeti személy" („Munkatársi") tanúsítvány

„Szervezeti személy" (vagy másképpen: „Munkatársi") tanúsítványokat természetes személy igényelhet egy adott szervezet alkalmazottjaként és/vagy tisztségviselőjeként.

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

A tanúsítvány „Country" mezőjében a szervezet telephelyének országkódja, az „Organization" mezőben a szervezet neve, a „Common Name" (CN) mezőben a munkatárs (aláíró) neve szerepel. Opcionálisan szerepel a „Locality" mezőben a szervezet telephelyének városa, az „Organizational Unit" mezőben a szervezeti egység neve és az „E" mezőben a munkatárs (aláíró) e-mail címe.

Ha a tanúsítvány CN mezőjében nem az aláíró személyazonosító igazolványában szereplő név kerül megadásra, úgy ez a név álnévként kerül rögzítésre.

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

2. Általános rendelkezések

2.1. Feladatok és hatáskörök

2.1.1. A Szolgáltató feladatai és hatásköre

1. A Szolgáltatónak gondoskodnia kell a hitelesítés-szolgáltatásra vonatkozó valamennyi, a jelen hitelesítési rendben részletezett állítás teljesüléséről, amennyiben azok az adott tanúsítványokra alkalmazhatók.
2. A Szolgáltatónak szolgáltatásait nyilvánosan elérhetővé kell tenni.
3. A Szolgáltató jogi személy.
4. A Szolgáltató köteles rendszeresen felülvizsgálni és újra kiadni a jelen hitelesítési rendet és szolgáltatási szabályzatait.
5. A Szolgáltató csak az Előfizető által szolgáltatott és az Ügyfélkapcsolati Irodák által elfogadott adatok alapján bocsáthatja ki a tanúsítványokat. A Szolgáltató a tanúsítvány kibocsátását követően a tanúsítvány adataiban nem változtathat.
6. A Szolgáltató köteles közzétenni Tanúsítványtárában az általa kibocsátott, a Tanúsítványok Visszavonási Listájában a felfüggesztett és visszavont előfizetői tanúsítványokat. A Tanúsítványtár, a Tanúsítványok Visszavonási Listája (CRL[6]) elérhetőségét a Szolgáltatónak 99,9%-os rendelkezésre állással kell biztosítania úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 3 órás időtartamot.
7. A Szolgáltató kötelezettséget vállal arra, hogy a regisztrációt követő napokban, de legkésőbb 30 munkanapon belül a tanúsítvány kiadására intézkedik és erről az Előfizetőt értesíti.
8. A Szolgáltatónak a szolgáltatások működtetése és menedzselése során ügyfélkapcsolati tevékenységet kell biztosítania.
9. A Szolgáltatónak rendkívüli üzemeltetési helyzetben is biztosítania kell tanúsítványtára és visszavonási nyilvántartásai elérhetőségét, visszavonás kezelési, visszavonási állapot közzétételi minden érdekelt fél számára. Ügyfélszolgálata útján folyamatos felügyeletet kell biztosítania a tanúsítvány visszavonási és felfüggesztési igények fogadására és kezelésére.
10. A Szolgáltatónak az Internetes honlapján keresztül bárki számára folyamatosan elérhetővé kell tenni a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó szolgáltatási szabályzatait.
11. A Szolgáltató a lejárat előtt értesítést küldhet a lejáró tanúsítványokról az Előfizető részére.
12. Szolgáltató a Tanúsítványban köteles feltünteti az Előfizetői Szerződésben rögzített, a tanúsítvány felhasználhatóságával kapcsolatos korlátozásokat.
13. A Szolgáltató közzétételi kötelezettség mellett felfüggesztheti vagy visszavonhatja a tanúsítványt ha azt a 4.9.1 fejezetben részletezett körülmények ezt indokolják
14. Szolgáltató köteles megőrizni a tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetőleg – amennyiben ezen időszakban az elektronikus aláírással vagy az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is köteles biztosítani, amellyel a kibocsátott tanúsítványok tartalma megállapítható.
15. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről legalább hatvan nappal korábban köteles értesíteni az Előfizetőket és a Nemzeti Hírközlési Hatóságot. A bejelentés időpontjától kezdve a Szolgáltató nem bocsáthat ki új Tanúsítványt. A Szolgáltató a tevékenység befejezése előtt köteles visszavonnni az általa kibocsátott és még érvényes tanúsítványokat. A Szolgáltató a tevékenysége befejezéséig köteles eleget tenni a nyilvánosságra hozatali kötelezettségének.
16. A Szolgáltató intézkedni köteles 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 – köteles átadni ezen szolgáltatónak.

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

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

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

[6] CRL: Certifcate Revocations List

A visszavonási állapot közzétételében való közreműködés keretén belül kötelesek fogadni a visszavonási kérelmeket, új tanúsítvány visszavonási listát készíteni és azt aláírással hitelesíteni.

Az 1. szintű „Root CA" alapvető feladata és hatásköre a 2. szintű „Produktív CA" hitelesítése, ezen belül feladatai tételesen a következők:

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

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

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

2.1.1.2. A Regisztrációs Iroda (RA) feladatai és hatásköre

A Regisztrációs Iroda fő feladata a biztonságos aláírás-létrehozó eszközön az aláírás-létrehozó adat generálása, a tanúsítvány előállítása és kibocsátása, valamint közreműködés a hitelesítés-szolgáltatás folyamataiban (regisztráció, felfüggesztés és visszavonás kezelés, visszavonási állapot közzététele).

1. előkészíti a biztonságos aláírás-létrehozó eszközt az aláírás-létrehozó eszközön történő kulcspár generáláshoz
2. a tanúsítvány kibocsátásához szükséges ellenőrzések sikeres lefolytatása után a tanúsítvány kibocsátás elindítása a Hitelesítő Központnál, (visszautasítja a tanúsítvány kiadását, amennyiben a tanúsítványigénylés nem felel meg az elvárt feltételeknek)
3. fogadja a Hitelesítő Központtól kapott előfizetői tanúsítványokat és ellenőrzi azok hitelességét és sértetlenségét,
4. kezdeményezi a tanúsítványok elküldését a Tanúsítványtárba
5. megszemélyesíti a biztonságos aláírás-létrehozó eszközt és azt eljuttatja az Ügyfélkapcsolati Irodához
6. előállítja a kezdeti aktivizáló adatot (PIN kódot), majd azt a biztonságos aláírás-létrehozó eszköztől elkülönítve eljuttatja az Ügyfélkapcsolati Irodához,
7. formai szempontból ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét, végrehajtja a szabályos tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket,
8. visszautasítja a szabálytalan tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket,
9. fogadja és feldolgozza a tanúsítvány megújítási kérelmeket.

2.1.1.3. Az OCSP egység feladata

1. a kérő által kezdeményezett biztonságos csatornán keresztül fogadja az OCSP kérelmeket,
2. azonosítja és hitelesíti az OCSP állapot kérőt, ellenőrzi a kérelem szabályosságát,
3. előállítja az OCSP választ, amennyiben a Szolgáltató rendszere a pontos időt biztosítani tudja,
4. a kérő által kezdeményezett biztonságos csatornán keresztül elküldi az OCSP választ a felhasználónak szabványos formában,
5. ellenőrzi az OCSP szerver belső órájának pontosságát;
6. amennyiben az óra a pontossági határon kívülre kerül, az OCSP szolgáltatást leállítja, és hibaüzenetet küld az Előfizetők felé,
7. az OCSP szerver belső órájának az ISZR-ben előírt pontosságú szinkronizációja hiteles külső UTC idő alapján történik,
8. a belső óra pontosságának folyamatos ellenőrzése,

9. az OCSP válasz aláíró kulcs fokozott biztonságú előállítása és tárolása a 2/2002. (IV.26) MeHVM irányelvnek megfelelően,
10. az OCSP válaszadással kapcsolatos események rögzítése, naplózása és archiválása.

2.1.1.4. Az Ügyfélkapcsolati Iroda feladatai és hatásköre

Az Ügyfélkapcsolati Iroda szolgáltatás igénylés és teljesítés keretén belül:

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

A visszavonás kezelés szolgáltatás keretén belül:

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

2.1.1.5. A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Rend és Szabályozási Csoport a hitelesítés-szolgáltatást nyújtó szervezeti egységtől függetlenül működik. Feladata a Szolgáltató és felhasználó Közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség működésére vonatkozó alapelvek lefektetése, s ebből levezetve a tagok tevékenységét részletesen szabályozó, az egész Szolgáltató szervezetre nézve közös szabályzatok, így a hitelesítési rendek, szolgáltatási és biztonsági szabályzatok készítése és rendszeres karbantartása.

A Hitelesítési Rend és Szabályozási Csoport feladatai tételesen a következők:

1. A hitelesítési rendek elkészítése és karbantartása.
2. A szolgáltatási szabályzatok elkészítése és karbantartása.
3. A hitelesítési rendek és szabályzatok közötti összhang biztosítása.
4. A szolgáltatói szabályzatok verzióinak nyilvántartása és megőrzése.
5. Nyilvános szabályzatok hitelesítése, publikálása.
6. A regisztrációs folyamat szabályozása, ellenőrzése, felülvizsgálata.

2.1.1.6. Az Ügyfélszolgálat feladata

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

2.1.2. Az Előfizető és az Aláíró feladata és jogköre

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

1. önmagát az Ügyfélkapcsolati Irodán hiteles okmányokkal igazolni,
2. a tanúsítvány igénylését és magánkulcsának felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse,
3. az Előfizető a regiszrtráció során aTanúsítvány kiadásához szükséges adatokat ellenőrizni,
4. az Aláíró biztosítani az aláírás-létrehozó eszközének és adatának, valamint a PIN kódjának védelmét,

5. az Előfizető, illetve az Aláíró 3 (három) munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a Tanúsítványba foglalt adatokra,
6. az Aláíró az aláírás-létrehozó adatát csak az előfizetői szerződésben rögzített korlátozásoknak megfelelően használhatja,
7. az Aláíró tudomásul venni, hogy magánkulcsának védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
8. az Előfizető az ÁSZF-PKI módosításáról szóló értesítést követően 72 órán belül az Aláírókat írásban tájékoztatni a változásokról;
9. az Aláíró azonnal intézkedni Tanúsítványának visszavonása, illetve felfüggesztése végett, ha az aláírás létrehozó adat és/vagy a PIN kód nem az Aláíró kizárólagos birtokában van (elveszett, ellopták, esetleg kompromittálták), vagy ennek alapos gyanúja áll fenn.
10. kompromittálódás esetén az Aláíró magánkulcsának használatát azonnal és véglegesen megszakítani,
11. az Aláíró vagy az Előfizető a Tanúsítvánnyal ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót,
12. az OCSP válasz felhasználók kötelesek a kért OCSP válaszok vétele után meggyőződni arról, hogy azt a Szolgáltató elektronikusan aláírta, az aláírás az OCSP válaszadásra szolgáló kulccsal történt-e és a hozzátartozó tanúsítvány érvényes-e;

Továbbá:

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

2.1.3. Érintett félre vonatkozó ajánlások

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

1. az elektronikus aláírás elfogadása előtt ajánlott megértenie az elektronikus aláírással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat,
2. ajánlott megismernie Szolgáltató nyilvánosan elérhető szabályzatait (HSZSZ-M, ÁSZF-PKI),
3. különösen ajánlott az elektronikus aláírás ellenőrzését elvégeznie az Aláíró Tanúsítványának segítségével, meggyőződve az üzenet eredetiségéről és az aláírás valódiságáról,
4. ajánlott egyértelműen meggyőződnie a Tanúsítványban feltűntetett azonosító és egyéb adatok alapján, illetve a törvényesen rendelkezésre álló módszerek segítségével az Aláíró személyéről,
5. a tanúsítvány érvényességét és hatályosságát indokolt ellenőriznie a nyilvánosan elérhető Tanúsítványban,
6. ajánlott elvégeznie a teljes tanúsítási lánc ellenőrzését az alábbiak szerint:
   - 6.1 meggyőződni a Kibocsátó kilétéről a tanúsítvány kibocsátójának azonosítója alapján;
   - 6.2 meggyőződni az Aláíró Tanúsítványának integritásáról a Szolgáltató (Kibocsátó) Tanúsítványának segítségével;
   - 6.3 indokolt ellenőriznie a tanúsítvány állapotát a tanúsítvány visszavonási listák (CRL) áttanulmányozásával vagy OCSP szolgáltatás igénybe vételével;
   - 6.4 ajánlott tanulmányoznia a tanúsítvány összes attribútumát, és az adott tranzakcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni az aláírás elfogadásáról,
7. ajánlott visszautasítani az elektronikus aláírás elfogadását, ha az elektronikus aláírás, az Aláíró Tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata, annak érvénytelenségére utal, illetve ha az az adott kontextusban nem elfogadható; az aláírás elfogadása nem jelentheti az aláírt üzenet tartalmának tudomásul vételét vagy elfogadását,
8. Az OCSP választ aláíró kulcs tanúsítványának az Érintett fél által történő ellenőrzésére vonatkozóan általában érvényesek a 2.2.3 pontban leírt, a tanúsítvány ellenőrzésre vonatkozó szabályok.
9. Egy OCSP válasszal ellátott állomány átvétele után az Érintett félnek ajánlott ellenőriznie a Szolgáltató általi aláírás megtörténtét, az Szolgáltató OCSP választ aláíró kulcsához tartozó tanúsítvány érvényességét a Visszavont Tanúsítványok Listája segítségével a 2.1.2 pontban leírt módon.
10. Az ellenőrzés a tanúsítvány érvényességének lejárta után is elvégezhető, mert az Eat. 9.§ (7. bek.) alapján a tanúsítványokat és a tanúsítványok ellenőrzéséhez szükséges adatokat a szolgáltatónál a tanúsítvány lejártát követő 10 évig, illetve az aláírt és/vagy OCSP válaszzal elátott dokumentummal kapcsolatban felmerült jogvita lezárásáig meg kell őrizni és hozzáférhetővé kell tenni. A tanúsítvány tartalmának megállapításához a Szolgáltatónak kell biztosítania a megfelelő eszközt.

2.2. Felelősségek

2.2.1. A Szolgáltató felelőssége

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

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

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

A Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott tanúsítvány a jelen hitelesítési rendben és a szollgáltatási 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 szolgáltatási szabályzata szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

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

2.2.2. Az Előfizető és az Aláíró felelőssége

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

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

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

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

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

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

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

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

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

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

2.2.3. Érintett fél felelőssége

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

Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány érvényességének ellenőrzése során nem a hatályos jogszabályoknak megfelelően vagy az adott helyzetben általában elvárható gondosságú magatartás szerint jár el.

2.3. Az anyagi felelősség mértéke

A Szolgáltató anyagi felelősségének mértékéről, illetve annak korlátairól az általános szerződési feltételekben kell rendelkezni.

A Szolgáltató az anyagi felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében köteles naplózni tevékenységeit, védeni a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrizni azokat.

2.4. Értelmezés és alkalmazás

2.4.1. Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően köteles végezni. Szerződéseire, szabályzataira és azok teljesítésére a magyar jog az irányadó és azok a magyar jog szerint kell értelmezni.

A Szolgáltató tevékenységére elsősorban a következő jogszabályok mérvadók:

2001. évi XXXV. törvény (Eat.),

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

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

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

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

4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

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

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

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

2.4.2. Hatályosság, megszűnés, értesítések

2.4.2.1. Hatályosság

A hitelesítési rend a szolgáltatási szabályzattal és az általános szerződési feltételekkel kiegészítve a felhasználói közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A fenti dokumentumok egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően. A hitelesítési rend csak írott és hitelesített formában módosítható, a Nemzeti Hírközlési Hatóság által vezetett nyilvántartásban való átvezetés mellett.

A hitelesítési rend időbeli hatálya a Nemzeti Hírközlési Hatóság általi nyilvántartásba vételének keltétől egy újabb verzió kiadásáig vagy a szolgáltatási tevékenység megszűntéig tart. A hitelesítési rend személyi és tárgyi hatályát az 1.4.5.1 pont tartalmazza.

2.4.2.2. Megszűnés

A hitelesítési rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

2.4.2.3. 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, az Aláírók és az Érintett felek vagy bármely harmadik fél megkeresheti az Ügyfélkapcsolati Irodát írásban postai úton, e-mail-ben vagy faxon, továbbá munkanapokon ügyfélfogadási időben személyesen vagy telefonon.

A Szolgáltató Ügyfélszolgálata (Help Desk) folyamatos (7x24 órás) szolgálattal áll rendelkezésre telefonos vagy e-mail megkeresés esetén. Az írásban vagy elektronikus úton történő kommunikáció esetében a feladó nevét és elérhetőségét fel kell tüntetni és a feladónak a küldeményt hitelesítenie kell.

2.4.3. Vitás kérdések kezelése

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

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

A jogviták esetén követendő eljárást az általános szerződési feltételekbe kell foglalni.

2.5. Díjak

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

Az Előfizetőkre vonatkozó hatályos szolgáltatási díjakat az Előfizetői Szerződésben kell rögzíteni.

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

2.5.1. Tanúsítvány kibocsátás

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

2.5.2. Tanúsítvány hozzáférés

Szolgáltató a közzétett tanúsítványok eléréséért nem számol fel díjat.

2.5.3. Visszavonási lista hozzáférés

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

2.5.4. OCSP szolgáltatás

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

2.5.5. Egyéb szolgáltatásokra vonatkozó díjak

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

2.5.6. Visszatérítési elvek

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

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

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

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

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem kötelezhető.

2.6. Közzététel

2.6.1. Szolgáltatói információk közzététele

A Szolgáltatónak gondoskodnia kell arról, hogy az általa kibocsátott tanúsítványok[7], a tanúsítványok használatának feltételei és egyéb közérdekű szolgáltatói információk az Előfizetők és az érintett felek részére folyamatosan rendelkezésére álljanak:

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

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

2.6.2. A közzététel gyakorisága

A Szolgáltató a kibocsátott előfizetői tanúsítványokat a Tanúsítványtárban 24 órán belül köteles közzétenni.

A Szolgáltató az általa működtetett hitelesítő központok szolgáltatói tanúsítványait 24 órán belül köteles közzétenni.

A Szolgáltató a Visszavont Tanúsítványok listáját a visszavonást követő 60 percen belül köteles közzétenni.

2.6.3. Elérési szabályok

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

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

2.6.4. Tanúsítványtár

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

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

2.7. A megfelelőség vizsgálata

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

A Nemzeti Hírközlési Hatóság a Szolgáltató bejelentése alapján a jelen hitelesítési rendet nyilvántartásába felvette.

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

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

A Szolgáltató a hitelesítés-szolgáltatási és OCSP szolgáltatási tevékenységét, a szolgáltatást támogató informatikai rendszert, valamint annak személyi és fizikai környezetének biztonságát köteles auditáltatni, illetve tanúsíttatni:

[7] Az előfizetői tanúsítványokat a Szolgáltató csak az Előfizető hozzájárulásával teheti közzé

a. a saját szervezetén belüli belső auditor szervezettel
b. független külső auditor céggel

A Szolgáltató a szolgáltatási rendszerének következő elemeit köteles auditáltatni:

a. Az előfizetői és szolgáltatói minősített tanúsítványok kezeléshez felhasznált elektronikus aláírási termékeit
b. Az előfizetői és szolgáltatói minősített tanúsítványok kezeléshez és az OCSP szolgáltatáshoz használt rendszereit és módszereit

2.7.1. Vizsgálatok gyakorisága

A Szolgáltató aláírás-létrehozó eszközözeinek tanúsítására a használatba vételt megelőzően kell sort keríteni.

A Szolgáltatónak az Előfizetők számára tanúsított biztonságos aláírás-létrehozó eszközöket (BALE) kell biztosítania.

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

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

2.7.2. Az átvizsgáló szervezet megnevezése/jellemzői

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

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

2.7.3. Hiányosságok kezelése

Az üzemszerű ellenőrzések, a belső és külső auditok, valamint a szakértői elemzések során feltárt hiányosságokat, hibás gyakorlatokat a Szolgáltató késlekedés nélkül megszünteti, intézkedéseit naplózza.

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

2.7.4. Eredmény kommunikációja

A hiányosságok felszámolásáról a Szolgáltató Nemzeti Hírközlési Hatóságot tájékoztatja.

A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni.

2.8. Bizalmasság – Adatkezelési szabályzat

2.8.1. Bizalmas információk

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

A Szolgáltató gondoskodni köteles a jogszabályoknak való megfelelésről. Ennek keretén belül:

a. A fontos bejegyzéseket védeni az elveszéstől, tönkretételtől és hamisítástól
b. megfelelő technikai és szervezeti intézkedéseket hozni a személyes adatok felhatalmazás nélküli, illetve törvénysértő kezelése ellen
c. nyilvántartásba venni az Előfizetővel aláírt szerződést, beleértve az Előfizető hozzájárulását az alábbiakhoz:
    - hozzájárulás a szolgáltatások során felhasznált adatok hitelesítés-szolgáltató által történő nyilvántartásba vételéhez
    - hozzájárulás a nyilvántartásba vett adatok harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén
    - a tanúsítvány közzétételéhez
c. csak annyi bizonyítékot követelhet meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához

d. gondoskodni az Előfizetőre és az Aláíróra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk[8] hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,

e. védeni a regisztrációs adatok bizalmasságát (és sértetlenségét) az Előfizetővel folytatott adatcsere során is

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

A Szolgáltató tevékenysége során a következő bizalmas adatköröket kezeli:

a. a Szolgáltató üzleti titkai

b. az Előfizető Társaságok által a Szolgáltatónak átadott üzleti titkok

c. az Előfizetők és az Aláírók személyes adatai

Az üzleti titkok kezelésére az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról és a Szolgáltató Titokvédelmi Szabályzata mérvadó. Így például egyik szerződő fél sem jogosult az Előfizetői Szerződés teljesítése kapcsán tudomására jutott bármely adatot, tényt, információt, tervet vagy dokumentumot a másik fél előzetes írásbeli hozzájárulása nélkül harmadik személynek átadni.

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

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

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

2.8.2. Nem bizalmas információk

A Szolgáltató a regisztrációs űrlapon köteles külön jelölni mindazon adatokat, melyek – az Előfizető hozzájárulásával - a Tanúsítványtárban hozzáférhető előfizetői tanúsítványban nyilvánosságra kerülnek.

2.8.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

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

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

2.8.4. Feltárás törvényi meghatalmazással rendelkezők részére

A Szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az érintett személyazonosságát igazoló adatok tekintetében – az Eat. 11.§ paragrafusa alapján köteles adatokat továbbítani a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak.

Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató sem az Előfizetőt sem az Aláírót nem tájékoztathatja.

2.8.5. Információszolgáltatás polgári eljárás keretében

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

A Szolgáltató köteles rögzíteni az információszolgáltatás tényét és arról az Előfizetőt tájékoztatni.

[8] vagy nevükben az Előfizető

2.8.6. Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson túl más Társaság üzleti titkát, az Előfizetők és az Aláírók nem nyilvános személyes adatait csak az Illető Társaság illetve Előfizető írásos meghatalmazása alapján tárhatja fel harmadik fél részére.

2.8.7. Feltárás más esetekben

Szolgáltatónak tevékenysége befejezésekor nyilvántartásait, a bizalmas adatokkal együtt, át kell adnia más - vele azonos besorolású – szolgáltató részére az Eat. 16. § (2.) bek. szerint.

2.9. Szellemi tulajdonhoz fűződő jogok

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

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

A visszavonási információ a Szolgáltató tulajdonát képezi.

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

A Tanúsítványban szereplő megkülönböztető név használatára a megnevezett Tulajdonos jogosult.

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

A Szolgáltató szabályzatai, szerződéses feltételei a Szolgáltató tulajdonát képezik.

A Tanúsítványban szereplő hitelesítő azonosító a Szolgáltató tulajdonát képezi.

3. Azonosítás és hitelesítés

3.1. Regisztráció

A Szolgáltatónak a tanúsítvány igényléséhez szükséges regisztráció során:

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

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

3.1.1. Nevek típusa

Valódi nevek:

A tanúsítványban szereplő valódi név (betű-, szóköz- és ékezet-helyesen) azonos a regisztráció során a személyazonosság igazolására elfogadott hatósági személyazonosító igazolványban (személyi igazolvány, jogosítvány vagy útlevél) feltüntetett névvel. Az ettől eltérő névmegadás álnévnek minősül.

Álnevek használata:

A Szolgáltató az Előfizető igénye esetén a tanúsítványban álnevet tüntet fel. Az álnév a tanúsítvány CN mezőjében '~' (tilde) karakterrel kezdődik és végződik (pl. CN=~Ludas Matyi~).

3.1.2. Nevek szemantikája

A tanúsítványokban szereplő névmegadás feleljen meg az ITU-T[9] X.500 ajánlásának.

A nevek megadásakor a következő szabályok szerint kell eljárni:

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

Nem természetes személy alany vagy álnév használata esetében a tanúsítványban feltüntetett név megegyezik az Előfizető által megadott névvel az UTF-8 kódolást használva.

A Szolgáltató fenntartja a jogot az egyes személyeket vagy csoportokat esetlegesen sértő (pl. jóízlést, szemérmet, etnikai hovatartozást sértő) álnevek és egyéb adatok megadásának elutasítására.

3.1.3. Nevek egyedisége

A Szolgáltató biztosítja tanúsítványtárában a tulajdonosazonosítók egyediségét, azaz gondoskodik arról, hogy az általa kiadott tanúsítványokban használt megkülönböztető nevet (DN) sohasem fogja egy másik entitáshoz rendelni. Erről a Szolgáltató elsődlegesen az alany neve és e-mail címének a névmegadásban való szerepeltetésével gondoskodik. A Szolgáltató a megkülönböztető név kiosztásakor ellenőrzi, hogy az adott név és e-mail cím szerepel-e egy más alany részére korábban kibocsátott tanúsítványban. Ha igen, és a tanúsítvány egyéb névmezői sem biztosítják az egyediséget, akkor a Szolgáltató fenntartja magának a jogot a megkülönböztető név olyan megváltoztatására, amely továbbra is jellemző az alanyra, mint magánkulcs felhasználóra, de biztosítja a megkülönböztethetőséget..

3.1.4. Név igénylési viták feloldása

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

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

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

3.1.5. Védjegyek elismerésének és hitelesítésének módszere

A tanúsítványkérelemmel az Előfizető kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik fél jogait. Szolgáltatónak nem kötelessége a védjegyek jogos használatának ellenőrzése, és nem vállal

[9] „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.

3.1.6. Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere

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

3.1.7. Azonosítás „Személyes" tanúsítvány igénylése esetén

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

a. név,

b. álnév, amennyiben annak megjelölésére az Előfizető igényt tart,

c. személyazonosítására használt okmány száma (személyi igazolvány, jogosítvány vagy útlevél szám),

d. lakcím,

e. anyja neve,

f. születési hely és idő,

g. e-mail cím,

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

Természetes személyt az Ügyfélkapcsolati Iroda hatósági személyazonosító igazolvány (személyi igazolvány, jogosítvány vagy útlevél) személyes bemutatásával azonosít.

Az Ügyfélkapcsolati Iroda a bemutatott személyozonosító igazolvány érvényességét és hitelességét ellenőrzi (lásd: 3.1.10. 1. pont).

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

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

Az igénylő szervezetnek (Előfizetőnek) a tanúsítványkérelemhez csatolnia kell a Szolgáltató által biztosított regisztrációs űrlapot kitöltve, és a szervezet képviseletére jogosult vezető tisztségviselőinek az aláírásával ellátva.

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

a. az igénylő szervezet neve, székhelye

b. annak a szervezeti egységnek a megnevezése, ahol a szervezeti személy (továbbiakban: Aláíró) dolgozik

c. az Aláíró neve, aláírása

d. az Aláíró beosztása (az előfizető szervezet és szervezeti egység viszonya az Aláíróhoz)

e. az Aláíró személyi igazolvány vagy útlevél száma

f. az Aláíró telefon száma, e-mail címe

g. az Aláírót megbízó dokumentum cégszerűen aláírva (a dokumentum tartalmazza a megbízó szervezet vagy szervezeti egység nevét, e-mail címét, telefon+fax számát)

h. az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:

- a tanúsítvány kibocsátásra kerüljön
- a szervezet vagy szervezeti egysége neve a tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön
- az Aláíró neve a tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön
- a Szolgáltató a regisztráció során a szervezeti azonosság hitelesítésére elfogad minősített aláírással ellátott elektronikus okiratot is abban az esetben, ha az Előfizetővel ebben előzetesen megegyezik. Ez esetben az Előfizető szervezeti azonosságának hitelesítése, s a szervezeti adatok felvétele a megegyezés során történik, az elektronikus okirat „már csak" az Előfizető hozzájárulását tartalmazza az Aláíró részére történő tanúsítvány kibocsátásához
- az Előfizető kapcsolattartókat nevez meg a Szolgáltató részére, akik aláírási joggal rendelkeznek a tanúsítvány kibocsátását illetően; a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén

- az Előfizető szervezet kötelezettséget vállal arra, hogy:
  - a tanúsítvány kibocsátásával és fenntartásával kapcsolatos és minden egyéb járulékos költséget vállal
  - a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat

A fentieken kívül még a következőket kell megadni:

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

b. az engedélyező személy beosztása

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

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

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

b. képviseleti megbízás cégszerűen aláírva

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

d. nem cégbíróságnál nyilvántartott szervezetek esetében a nyilvántartó szervezet igazolása, pl. alapítványok esetében Fővárosi Bíróság, egyéni vállalkozók esetében az illetékes önkormányzat, ügyvédek esetében az Ügyvédi Kamara, könyvvizsgálók esetében a Könyvvizsgálói Kamara, igazságügyi szakértők esetében az Igazságügyi Minisztérium, stb.,

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

f. aláírási címpéldány, amely a szervezet aláírásra jogosult vezetőinek nevét és aláírását tartalmazza; gazdasági társaságok esetében a cégbírósági bejegyzést, más – nem gazdasági – szervezetek esetében a szervezet hivatalos bejegyzését is mellékelni kell a kérelemhez

Az Ügyfélkapcsolati Iroda a bemutatott iratok és okmányok érvényességét és hitelességét adategyeztetéssel (lásd: 3.1.10. pont) ellenőrzi.

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

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

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

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

d. a szervezet kiléte nem állapítható meg minden kétséget kizáróan

e. nem egyértelmű a szervezet felhatalmazása a tanúsítvány kibocsátására

3.1.9. Személyi és szervezeti azonosítás OCSP szolgáltatás igénylés esetén

OCSP szolgáltatást igényelhet:

a. természetes személy

b. jogi személy (szervezet)

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

Az OCSP szolgáltatás igénybe vételére vonatkozó előfizetői szerződéshez a Szolgáltató szolgáltatási szabályzatában egyszerűsített azonosítási módot határozhat meg.

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

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

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

3.1.10. Adategyeztetés

1.) A Szolgáltató jogosult megállapítani az aláíró személyazonosságát a személyazonosításra alkalmas okmánya alapján. A Szolgáltató a regisztráció során az aláíró személyazonosságának ellenőrzése céljából - megnevezésének és az adatfelhasználás céljának feltüntetése mellett - adategyeztetést végez a következő nyilvántartások közül legalább eggyel:

a. személyi adat- és lakcímnyilvántartás,

b. úti okmány-nyilvántartás,

c. járművezetői engedély-nyilvántartás;

2.) A Szolgáltató a regisztráció során cég nevében történő aláírási jogosultság ellenőrzése céljából adategyeztetést végez a cégnyilvántartással.

4. A tanúsítvány-életciklusra vonatkozó követelmények

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 szervezetet képviselő személy, aki személyazonosságát a regisztráció során hitelt érdemlően igazolta.

A Szolgáltató azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatja az Előfizetőt a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről. Ha az Aláíró (alany) nem azonos az Előfizetővel, úgy őt az Előfizető tájékoztatja kötelességeiről.

A Tájékoztató a szolgáltató internetes honlapján bárki számára elérhető.

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 Szolgáltató Internetes honlapjáról.

Az Előfizetői Szerződés aláírásával Előfizető egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, valamint saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Az Előfizető aláírása igazolja azt is, hogy:

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

Az Előfizetőnek a Szolgáltató felkérésére írásban kell nyilatkozni arról, hogy hozzájárul a szolgáltatások során felhasznált személyes adatai Szolgáltató által történő nyilvántartásba vételéhez, tanúsítványa és az azzal kapcsolatos állapot információk szolgáltatói tanúsítványtárban való közzétételéhez, s ezen adatok harmadik félhez történő továbbításához a Szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb, jogszabályok által meghatározott esetekben.

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

4.2. A tanúsítvány kérelem 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.

4.3. Tanúsítvány kibocsátás

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

Az elkészült tanúsítvány a következő módon jut el az Előfizetőhöz:

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

4.4. Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető részéről az átvétellel történik meg.

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

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

A visszaigazolás egyben a hitelesítési rendek, a jelen szolgáltatási szabályzat és az általános szerződési feltételek elfogadását is jelenti.

4.4.1. Tanúsítvány közzététele a hitelesítés-szolgáltató által

Az Előfizető hozzájárulása esetén 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 tanúsítvány elfogadása után (lásd 4.4 pont) 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 6.1.6, 7.1.2 és 7.1.3 pontok).

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 ajánlott ellenőriznie. Ennek során többek között az alábbiakra ajánlott figyelemmel lennie:

a. Az érintett félnek ajánlott csak olyan célokra és olyan alkalmazásokkal nyilvános kulcsokat elfogadni, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat” és „kiterjesztett kulcshasználat” mezőinek tartalmával.

b. Mielőtt egy tanúsítványba foglalt nyilvános kulcsot felhasználna, az érintett félnek ajánlott ellenőrizni 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 ajánlott figyelembe vennie a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban szerepel.

4.6. Tanúsítványok érvényessége, megújítása (tanúsítvány frissítése)

4.6.1. A tanúsítványok érvényessége

Szolgáltató által kibocsátott Előfizetői tanúsítványok érvényességi ideje legfeljebb 2 év. Az érvényesség kezdete (év, hónap, nap, óra, perc, másodperc) nem lehet korábbi, mint a kibocsátás napja. Az előfizetői tanúsítványok érvényessége az előfizető kérésére az érvényességi idő lejárata előtt legfeljebb egy alkalommal legfeljebb két évre meghosszabbítható.

4.6.2. A tanúsítványok megújítása (tanúsítványok frissítése)

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

Tanúsítvány megújítása akkor lehetséges, ha:

a. a tanúsítvány nem szerepel a visszavonási listában

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

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

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

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

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

4.6.3. Érvénytelen tanúsítványok megőrzése

A Szolgáltató a lejárt és a visszavont előfizetői tanúsítványokat a lejárattól, illetve a visszavonástól számított 10 évig, illetve a tanúsítványhoz kapcsolódó privát kulccsal elektronikusan aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi. A Szolgáltató ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható. E megőrzési kötelezettségnek a Szolgáltató minősített archiválási szolgáltató igénybevételével is eleget tehet.

4.7. Kulcscsere

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

Kulcscserére a következő esetekben lehet szükség:

a. a tanúsítvány valamilyen okból visszavonásra került,

b. a tanúsítvány lejárt,

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

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

4.8. Tanúsítvány-módosítás

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

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

A tanúsítvány-módosítást az Előfizető kezdeményezheti.

A kérelem benyújtásakor a Szolgáltató ellenőrzi a tanúsítvány létezését és érvényességét, valamint az alany azonosságának és jellemzőinek igazolására használt információk érvényességét a 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 (lásd 4.9.7.1 pont) után állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni.

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

Visszavont/felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

4.9.1. Visszavonáshoz/felfüggesztéshez vezető körülmények

A Szolgáltató felfüggeszti vagy visszavonja a tanúsítványt ha:

a. az Előfizető vagy az Aláíró ezt kéri

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

c. a Szolgáltató és az Előfizető között a szerződés megszűnt

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

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

f. a Szolgáltató a tevékenységét befejezte

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

a. a magánkulcs kompromittálódása, vagy annak gyanúja

b. az aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása

c. az aláírás-létrehozó eszközt védő aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja

d. a tanúsítványban feltűntetett hibás adatok

e. az Előfizető tanúsítványban feltűntetett adatainak megváltozása

f. az Aláíró tanúsítványban feltűntetett adatainak megváltozása

g. a tanúsítványban feltűntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszűnése[10].

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

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

a. a tanúsítvány felfüggesztési idejének lejárata

b. amennyiben a törvény erre kötelezi

c. az ÁSZF-PKI vagy az Előfizetői Szerződés megszegése az Előfizető és/vagy az Aláíró által

d. az Előfizető és/vagy az Aláíró kötelezettségeinek be nem tartása

e. az Előfizetői szerződés megszűnése

f. a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról

g. a tanúsítványban feltűntetett kibocsátó adatok megváltozása

h. a hitelesítési szolgáltatás megszűnése

i. a Szolgáltató valamely magánkulcsának kompromittálódása miatt.

4.9.2. Visszavonás kérelmezése

Tanúsítvány visszavonását az előző pontban feltüntetett körülmények alapján az Aláíró, az Előfizető vagy azok képviselője, a Szolgáltató, a Nemzeti Hírközlési Hatóság vagy más harmadik fél kezdeményezheti. Az Előfizetőnek és a Szolgáltatónak kötelessége, harmadik félnek joga az előző (4.9.1.) pontban feltűntetett esetekben a visszavonás azonnali kezdeményezése.

A visszavonási kérelem benyújtható személyesen vagy írásban a Szolgáltató Ügyfélkapcsolati Irodájánál. Ha a bejelentő akadályoztatása miatt a visszavonási igényét személyesen nem tudja bejelenteni vagy azonnali intézkedés szükséges, akkor a tanúsítvány felfüggesztése telefonon vagy elektronikusan aláírt e-mail-ben is kérhető az Ügyfélszolgálaton (a Szolgáltató Ügyfélszolgálata a nap 24 órájában, folyamatosan rendelkezésre áll). A tanúsítvány visszavonására az ettől számított 5 napon belül kell intézkedni.

A visszavonási kérelem teljesítéséhez a következő adatok szükségesek:

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

b. a visszavonást kérő azonosító adatai

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

d. a visszavonáshoz vezető körülmény

[10] Eat. 10. § (3)

4.9.3. Visszavonási kérelemre vonatkozó eljárás

A visszavonási eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt:

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

b. Írásban történt bejelentés esetén a Szolgáltató a bejelentő adatai alapján azonosítja és hitelesíti a visszavonás kérelmezőjét.

c. Ha a kérelmező azonosítás-hitelesítése megtörtént, a visszavonási okok megalapozottak, az adatok egyeznek és a kérelmező jogosult a tanúsítvány visszavonását kezdeményezni, vagyis ha a Szolgáltató a visszavonási kérelem jogosságáról meggyőződött, akkor azonnal elvégzi a tanúsítvány visszavonását.

d. Ha a kérelmező azonosítás-hitelesítése sikertelen, a visszavonási okok nem megalapozottak, az adatok helytelenek, vagy a kérelmezőnek a Szolgáltató információi alapján nincs joga a tanúsítvány visszavonatására, akkor a Szolgáltató a visszavonási kérelmet visszautasítja.

e. E-mail-ben vagy telefonon történt bejelentés esetén a Szolgáltató bekéri a felfüggesztési jelszót és lefolytatja a 4.9.4.2. pont szerinti felfüggesztési eljárást. A visszavonási kérelem elbírálásához felkéri a bejelentőt, hogy jelenjen meg ügyfélkapcsolati irodájában személyes azonosítás-hitelesítésre. A bejelentő akadályoztatása esetén a tanúsítvány a felfüggesztés megengedett időtartamára (lásd: 4.9.7.1. pont) felfüggesztési állapotban marad, majd ennek lejártával a Szolgáltató a tanúsítványt visszavonja.

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

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

4.9.4. A felfüggesztési kérelemre vonatkozó eljárás

4.9.4.1. Ki kérelmezheti a felfüggesztést

A felfüggesztést kérelmezheti az Aláíró vagy az Előfizető illetve annak képviselője, valamint harmadik személy.

Felfüggesztést a következő körülmények fennállása esetén kell kezdeményezni:

a. a magánkulcs kompromittálódásának gyanúja,

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

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

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

Tanúsítvány felfüggesztési igény telefonon is bejelenthető a Szolgáltató Ügyfélszolgálatán. Telefonon történt bejelentés esetén a Szolgáltató a személyes adatok bemondása után felfüggesztési jelszóval azonosítja a felfüggesztés kérelmezőjét, majd elvégzi a felfüggesztési kérelem formai és tartalmi ellenőrzését, illetve ezek sikeressége esetén a tanúsítvány felfüggesztését.

4.9.4.2. A felfüggesztési eljárás

a. A felfüggesztési eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt, majd mérlegeli a felfüggesztési okokat. Ha a felfüggesztési kérelmet az Előfizető terjesztette be, az Előfizető azonosítása után a Szolgáltatónak nincs mérlegelési joga a felfüggesztés tekintetében

b. ha a felfüggesztési okok megalapozottak és az ellenőrzések sikeresek, vagyis ha a Szolgáltató a felfüggesztési kérelem jogosságáról meggyőződött, akkor azonnal elvégzi a tanúsítvány felfüggesztését

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

d. Szolgáltató a felfüggesztés megtörténtéről vagy visszautasításáról értesíti az Előfizetőt, az Aláírót 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 az Aláíró kérésére a felfüggesztési időn belül visszaállítja érvényesre.

4.9.4.3. A Szolgáltató függeszti fel a tanúsítványt

A Szolgáltató felfüggeszti a tanúsítványt, ha:

a. a Szolgáltató tudomására jutott alapos gyanú a regisztrációs adatok valótlanságáról,

b. az Előfizető vagy az aláíró visszavonási kérelme kiegészítésre szorul.

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

4.9.5. Kivárási idő visszavonási/felfüggesztési kérelem esetén

A visszavonási/felfüggesztési kérelem esetén a Szolgáltató ennek végrehajtását soron kívül végrehajtja a kérelem elfogadása után. A Szolgáltató akkor tekinti a visszavonási/felfüggesztési kérelmet elfogadottnak, ha annak jogosságáról meggyőződött.

4.9.5.1. Kivárási idő felfüggesztési kérelem esetén

a. Felfüggesztési kérelem esetén a kérelem elfogadására a Szolgáltató nem alkalmaz kivárási időt. A felfüggesztési kérelem elfogadását követően azonnal intézkedik a tanúsítvány felfüggesztésére, a tanúsítvány-állapot megváltozását nyilvántartásában átvezeti és a felfüggesztési kérelem szerint módosított felfüggesztési állapotot 1 órán belül közzéteszi.

b. Ha a Szolgáltatónak a felfüggesztési kérelem hitelességéről kétségei merülnek fel, akkor a felfüggesztési kérelmet azonnal visszautasítja.

4.9.5.2. Kivárási idő visszavonási kérelem esetén

Visszavonási kérelem esetén a kérelem elfogadására a Szolgáltató kivárási időt alkalmaz:

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

b. Ha a Szolgáltató a visszavonási kérelem érvényességéről 3 órán belül nem tud kétséget kizáróan meggyőződni, akkor erről a kérelmezőt értesíti és a tanúsítványt nem visszavonja, hanem 4.9.4.2 pont szerint felfüggeszti. A visszavonást később – a kérelmező hiteles azonosítását követően végzi el.

c. A visszavonási kérelem elfogadását követően a Szolgáltató a visszavonási kérelem szerint módosított visszavonási állapotot 1 órán belül közzéteszi.

4.9.6. A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok

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

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

c. A felfüggesztett/visszavont tanúsítványnak a visszavont tanúsítványok listájában való megjelenése után az Érintett fél felelős a felmerülő károkért.

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

4.9.7. Felfüggesztett állapotra vonatkozó korlátozások, újraérvényesítés

4.9.7.1. A felfüggesztés megengedett időtartama

Tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig lehet.

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

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

4.9.7.2. A felfüggesztés megszüntetése

A felfüggesztés megszüntetésének, és ezzel a tanúsítvány újraérvényesítésének 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 megszüntetését kérő személy azonosító adatai,

c. a felfüggesztés megszüntetésének oka.

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

4.9.8. A visszavonási információ ellenőrzése az érintett felek részéről

Ha az érintett felek kellő gondossággal kívánnak eljárni a tanúsítvány visszavonási állapotának ellenőrzésekor, akkor indokolt meggyőződniük a tanúsítvány visszavonási információ hitelességéről is.

4.9.9. Visszavonási lista (CRL) és kibocsátásának 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 listáják 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.

4.9.10. A visszavonási lista előállítása és közzététele közötti közötti leghosszabb idő

A visszavonási lista előállítása és közzététele közötti közötti leghosszabb idő 1 óra.

4.9.11. A visszavonási listák ellenőrzése

A visszavonási listákat az érintett feleknek ajánlott ellenőrizni - saját felelősségükre - a tanúsítványok elfogadását megelőzően. A tanúsítványhoz tartozó visszavonási lista elérhetőségét a tanúsítvány tartalmazza. A lista ellenőrzése abból áll, hogy a kérdéses tanúsítványt a lista tartalmazza-e (és ha igen, milyen időponttól), a lista hiteles és sértetlen-e, s a kérdéses tranzakció szempontjából időben releváns-e.

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

4.9.12. Visszavonási állapot közlés más formái

A Szolgáltató a visszavonási listák közzététele mellett online visszavonási információs szolgáltatást (OCSP) nyújt.

4.9.13. Intézkedések magánkulcs kompromittálódás esetén

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

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

4.10. Kulcsletét

A Szolgáltató kulcsletétet nem szolgáltat.

4.11. OCSP szolgáltatás

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

Az OCSP kérelmek teljesítését a Szolgáltató OCSP egysége automatikusan végzi:

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

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

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

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

5. Fizikai, eljárásrendi, és személyi biztonsági szabályozások

A szolgáltatásokat támogató informatikai rendszer személyi és fizikai környezete kialakítása során meg kell felelni a 2/2002 MeHVM irányelvben rögzített biztonsági követelményeknek.

A Szolgáltatónak gondoskodnia kell arról, hogy kellő, az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra. Ezen belül:

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

b. A Szolgáltató felelősséget vállal minden elektronikus aláírással kapcsolatos szolgáltatásért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki.
A Szolgáltató egyértelműen meghatározza a harmadik felek felelősségét, és megfelelő konstrukciók biztosítják azt, hogy a harmadik felek a Szolgáltató által megkövetelt összes ellenőrzés végrehajtására legyenek szorítva. A Szolgáltató felelősséget vállal valamennyi fél fentiekre vonatkozó gyakorlatának nyilvánosságra hozására.

c. A Szolgáltató vezetősége (mely felelős a Szolgáltató informatikai biztonság politikájának meghatározásáért, és e házirend által érintett valamennyi alkalmazott részére történő közzétételért) az információ biztonságára vonatkozó útmutatót hagyott jóvá és adott ki.

d. A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetőségének kell jóváhagynia.

e. A Szolgáltató a Biztonsági Szabályzatában dokumentálta, majd megvalósította és folyamatosan fenntartja a hitelesítési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait[11].

f. A Szolgáltató gondoskodik az informatika biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez, illetve egységhez lettek kiadva.

g. A Szolgáltató biztonsági műveleteiért a végső felelősség a felső vezetőségéé. Ezen biztonsági műveletek közé az alábbiak tartoznak:

- üzemeltetési eljárások és felelősségek
- biztonsági rendszerek tervezése és elfogadása
- káros szoftver elleni védelem
- erőforrás gazdálkodás
- hálózat menedzselés
- a biztonsági napló aktív felügyelete, eseményelemzések és nyomkövetések
- adathordozó eszköz kezelése és biztonsága
- adat és szoftver csere

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

A Szolgáltatónak gondoskodnia kell arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek. A Szolgáltató valamennyi informatikai értékéről leltárt kell vezetni, ezek védelmi követelményeit az elvégzett kockázat elemzéssel összhangban osztályokba kell sorolni.

A Szolgáltató fizikai, eljárásrendi és személyi biztonsági szabályozásait a PKI Szolgáltatások Biztonsági Szabályzatában kell rögzíteni.

5.1. Fizikai biztonsági szabályozások

A Szolgáltató általános tevékenységével kapcsolatosan a Szolgáltatónak:

a. biztosítania kell az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.

[11] Ajánlott, hogy az információbiztonsági szabályzat azonosítsa a nyújtott szolgáltatásokkal kapcsolatos valamennyi fontos célt és potenciális veszélyt, valamint az ezen veszélyek hatásainak elkerülése, illetve korlátozása érdekében szükséges védelmi intézkedéseket. Ajánlott leírnia az arra vonatkozó szabályokat, irányelveket és eljárásokat, hogy a meghatározott szolgáltatásokat és az ezekkel kapcsolatos biztonsági garanciákat hogyan biztosítják.

b. óvintézkedéseket kell tennie az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

A kulcspár generálásasal, tanúsítvány előállítással, aláírók BALE eszközzel való ellátásával,és a visszavonás kezeléssel kapcsolatosan a Szolgáltatónak egy egyértelműen meghatározott biztonsági körlet létrehozásával fizikai védelmet kell biztosítani az alábbi szolgáltatások számára:

a. kulcspár generálás

b. tanúsítvány előállítás,

c. az aláírók BALE-val való ellátása,

d. visszavonás kezelés.

Bármely más szervezettel megosztott rész e körleten kívül kell essen.

A Szolgáltatónak óvintézkedéseket kell tennie a fizikai és környezetbiztonsági rendszer erőforrások, illetve a működésük támogatására használt berendezések megvédése érdekében. A Szolgáltató szolgáltatásainak fizikai- és környezetbiztonsági programjaiban kell rögzíteni a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelem és tűzbiztonság tényezőivel, a támogató eszközök (ezen belül az áram és klíma berendezések) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, katasztrófa utáni helyreállítással, stb. kapcsolatos tevékenységeire.

A Szolgáltatónak óvintézkedéseket kell megvalósítani annak megakadályozása érdekében, hogy a minősített elektronikus aláírás-hitelesítéssel kapcsolatos szolgáltatásaihoz szükséges berendezéseket, információkat, adathordozókat vagy szoftvereket jogosulatlanul elvigyék a helyszínről[12].

5.1.1. Hitelesítő Központok

A hitelesítő központok legmagasabb védelmi szintet képező objektuma a Bizalmi Központ, amely a biztonsági szempontból legkritikusabb hardver/szoftver egységeket tartalmazza. A Bizalmi Központban történik a kulcspárok és a tanúsítványok előállítása, a biztonságos aláírás-létrehozó eszközök megszemélyesítése. A Bizalmi Központ védelmét a 2/2002 MeHVM irányelv ide vonatkozó ajánlása szerint kell biztosítani.

5.1.2. Regisztrációs Iroda

A regisztrációs irodában találhatók a regisztrációs munkahelyek és munkaállomások. Az iroda védelmét is a 2/2002 MeHVM irányelv ide vonatkozó ajánlása szerint kell biztosítani.

5.2. Eljárásrendi szabályozások

A Szolgáltató eljárásrendi szabályait a következő szabályzatok tartalmazzák:

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

b. a Szolgáltatási Szabályzat, mely a Szolgáltató és a felhasználói közösség (előfizetők, aláírók, érintett felek stb.) viszonyát szabályozza

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

5.3. Humán szabályozások

5.3.1. Bizalmi munkakörök

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

h. a Szolgáltató informatikai rendszeréért általánosan felelős vezető,

i. biztonsági tisztségviselő,

j. rendszeradminisztrátor,

k. rendszerüzemeltető,

l. független rendszervizsgáló,

m. regisztrációs felelős.

[12] A biztonsági körletben egyéb funkciók is támogathatók, a hozzáférések jogosult személyzetre való korlátozás biztosításával.

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

Munkakör	Feladatkör	Felelősségi kör	Hatáskör
A Szolgáltató infokommunikációs divíziójának vezetője	A Szolgáltató szervezet irányítása és ellenőrzése	Folyamatos és biztonságos szolgáltatás. A Szolgáltató informatikai rendszeréért általánosan felelős vezető	A Szolgáltató szervezet szintjén dönt
A PKI Szolgáltató Egység vezetője	A Szolgáltató hitelesítés-szolgáltatási tevékenységének irányítása	Folyamatos és biztonságos szolgáltatás. A PKI Rendszer működtetésének egyszemélyi felelős vezetője	A Szolgáltató Egység szintjén dönt, intézkedik.
Ügyfélkapcsolati Iroda vezetője	Az ügyfélkapcsolati tevékenység irányítása és ellenőrzése.	Az ügyfelek biztonságos azonosítása. Előfizetői szerződések előkészítése	Az ügyfélkapcsolati tevékenység ellenőrzése.
A Szolgáltató IB vezetője (biztonsági tisztségviselő)	IB tevékenység irányítása, ellenőrzése a Szolgáltató minden területén.	A szolgáltatás biztonságáért általánosan felelős személy	IB intézkedések, IB belső ellenőrzés.
Rendszerüzemeltető	Üzemeltetési adminisztráció, hibaelhárítás, karbantartás	A PKI Rendszer folyamatos üzemeltetése, mentése és helyreállítása	Operatív intézkedés az üzemeltetés területén
Rendszeradminisztrátor	Biztonsági beállítások, adminisztráció, karbantartás	A PKI Rendszer telepítése, konfigurálása, karbantartása	Operatív ellenőrzés, operatív intézkedés
Hitelesítő biztonsági felügyelő (Security Officer /SO/) (regisztrációs felelős)	RO kulcsok, tanúsítványok létrehozása	Szolgáltatói kulcsok, PKI alkalmazás és adatok biztonsága	Szolgáltatói (pl.: RO) kulcspárok, tanúsítványok létrehozása
Regisztrációs felügyelő (Registration Officer /RO/) (regisztrációs felelős)	Regisztrációs Iroda irányítása. Előfizető regisztráció, kulcs, tanúsítvány igénylése, kulcs megszemélyesítése	Regisztrációs Iroda folyamatos működtetése.	Regisztrációs Irodán intézkedési jog. SO hatásköre nem lehet.
Rendszervizsgáló (auditor)	Operatív funkcionális és biztonsági ellenőrzések (naplózott, illetve archivált állományok vizsgálata).	Funkcionális és biztonsági hiányosságok, visszaélések felfedése. Kontroll intézkedések betartásának ellenőrzése.	Biztonsági és audit naplók ellenőrzése.

1. táblázat

5.3.2. Az egyes feladatokhoz szükséges személyzeti létszámok

A PKI rendszerben minden rendszer-telepítési, hardver-konfigurálást és szoftver-frissítést igénylő beavatkozást csak két munkatárs egyidejű jelenlétében lehet elvégezni. A műveletek sikerességét auditoroknak kell ellenőrizni és hitelesíteni.

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

a. a PKI alkalmazás installásához szükséges szolgáltatói kulcspárok generálása
b. a hitelesítő központok szolgáltatói tanúsítványaihoz tartozó kulcspárjainak generálása
c. a szolgáltatói nyilvános kulcsokat tartalmazó token Root CA-hoz való továbbítása, illetve a Root CA által kibocsátott tanúsítványok visszaszállítása
d. a Root CA nyilvános kulcsát tartalmazó tokennek a Produktív CA-hoz való továbbítása
e. Root CRL generálás

Továbbá csak két SO együttesen végezheti az alábbi feladatokat:

a. a szolgáltatói magánkulcsok biztonsági mentése

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

5.3.3. A bizalmi munkakörökben elvárt azonosítás és hitelesítés

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

5.3.4. Egymást kizáró munkakörök

A bizalmi munkakörök közötti személyi átfedésekre az alábbi korlátozások vonatkoznak:

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

5.3.5. Személyzetre vonatkozó előírások

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

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

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

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

5.3.6. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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

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

5.3.7. Biztonsági háttér ellenőrzésekre vonatkozó eljárások

Az alább meghatározott szerepkörök betöltését az átlagosnál magasabb szintű személyi biztonsági ellenőrzésnek kell megelőzni:

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

A személyi biztonsági ellenőrzéshez a szerepkörre kijelölt személy hozzájárulása szükséges. Nem tölthet be bizalmi munkakört az a személy, akinél a biztonsági ellenőrzés kockázatot tár fel.

A szerepkörök betöltéséhez szükséges képzettség és gyakorlat követelményei:

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

biztonsági tisztviselő (IB adminisztrátor, SO):

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

regisztrációs biztonsági tisztviselő (RO):

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

működtető adminisztrátor, rendszer auditor:

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

A szerepkör betöltőinek a szerepkör átvétele előtt:

a. át kell adni munkaköri leírását,

b. alá kekk írnia egy titoktartási nyilatkozatot, amelyben 3 év titoktartási kötelezettség szerepel a Szolgáltatótól történő kilépés utáni időponttól számítva,

c. biztonsági oktatást kell tartani annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és azt gyakorolni tudja.

Kilépéskor a szerpkör betöltőjétől:

a. a kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságait azonnal meg kell szüntetni,

b. tanúsítványát vissza kell vonni, aláírás-létrehozó eszközét vissza kell venni,

c. számítógépes tevékenységét legalább két hétre visszamenőlegesen le kell ellenőrizni,

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

5.3.8. Képzési követelmények

A Hitelesítő Központ, a Regisztrációs Iroda, az Ügyfélkapcsolati Iroda és az Ügyfélszolgálat területén dolgozó valamennyi munkatársnak felvételét követően, illetve a szolgáltatások indítását megelőzően, a saját munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzést kell biztosítani.

Rendszerüzemeltetői munkakörbe kinevezett munkatárs a kinevezést követő 3 hónapig csak megfelelő gyakorlattal rendelkező munkatárs felügyelete mellett dolgozhat.

5.3.9. Továbbképzési gyakoriságok és követelmények

Abban az esetben, amikor a szolgáltatásban jelentős változás[13] következik be, valamennyi munkatársat, az őt érintő mélységben továbbképzésben kell részesíteni, és át kell adni a számára szükséges dokumentációkat.[14]

A kisebb változásokról azok[15] bekövetkezése előtt a munkatársakat írásban kell tájékoztatatni a változásokról.

5.3.10. A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatársat tájékoztatni kell azokról a munkajogi vagy büntető következményekről, melyek a munkaköri kötelezettségek, illetve törvények megsértését szankcionálják.

5.3.11. A szerződéses alkalmazottakra vonatkozó követelmények

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

---

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

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

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

Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződésben foglalkoztatott személyeket a Szolgáltató csak az „ellenőrzött beszállítók” listájáról választ. Az ellenőrzött beszállítókkal a Szolgáltatónak írásos megállapodást kell kötni, amelyben rögzíteni kell a biztonsági szabályokat is, így a titoktartásra vonakozó kikötéseket.

5.3.12. A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentációt a 9.1 pont sorolja fel.

6. Műszaki biztonsági óvintézkedések

A Szolgáltatónak megbízható, az informatikai biztonság szempontjából értékelt és minősített termékekből álló, egységes informatikai rendszert kell használni szolgáltatásai nyújtásához.

A rendszer szállítója csak a hitelesítés-szolgáltatási és OCSP szolgáltatási rendszer kiépítésében jelentős tapasztalatokkal rendelkező, nemzetközileg elismert technológiát alkalmazó vállalkozás lehet.

6.1. Kriptográfiai kulcspár előállítás és aláírás-létrehozó eszköz megszemélyesítés

6.1.1. Kulcspár előállítás

A Szolgáltató maga generálja a szolgáltatói kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben, nagy biztonságú hardver modulban (HSM[16]) vagy biztonságos aláírás-létrehozó eszközön (BALE). A nagy biztonságú hardver modul és a BALE eszköz is hazai tanúsítvánnyal rendelkezik és szerepel a Nemzeti Hírközlési Hatóság által jóváhagyott minősített elektronikus aláírási termékek listájában. A kulcspárok generálását olyan algoritmussal végzi, amely szerepel a Nemzeti Hírközlési Hatóság HL-20336-7/2005. sz. határozatának 1. sz. mellékletében.

A szolgáltatói aláírás-létrehozó adatok teljes életciklusuk alatt a nagy biztonságú hardver modulban, illetve a biztonságos aláírás-létrehozó eszközön maradnak.

Az előfizetői kulcspárokat a Szolgáltató PKI alkalmazása magán a biztonságos aláírás-létrehozó eszközön generálja. A Szolgáltató nem fogadhat el az Előfizető által generált kulcspárt.

Az az OCSP választ aláíró szolgáltatói kulcspárt tanúsított HSM modul generálja és tárolja. Az aláíró kulcs teljes életciklusa alatt ezen eszközben marad.

6.1.2. Az aláírás-létrehozó eszköz megszemélyesítése

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

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

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

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

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

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

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

Az aláírás-létrehozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

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

A Szolgáltató az Aláírók aláírás-ellenőrző adatát (nyilvános kulcsát) az Előfizetői Tanúsítványba foglalva a Tanúsítványtárán keresztül köteles mindenki számára elérhetővé tenni.

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

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

A tanúsítványok letölthetők és a felhasználó kliens-alkalmazásába installálhatók.

[16] Hardware Security Module

6.1.6. Kulcs méretek, algoritmusok, paraméterek

A Szolgáltató Hitelesítő Központja a hitelesítés-szolgáltatás területén olyan algoritmust és paramétereket használ, amelyek szerpelnek a Nemzeti Hírközlési Hatóság HL-20336-7/2005. sz. határozatának 1. sz. mellékletében..

Az Elsődleges (1. szintű) Hitelesítő Központ ("Root CA") aláíró kulcsának mérete:	2048 bit
kommunikációs kulcsának mérete:	1024 bit
A 2. szintű Hitelesítő Központ („Produktív CA”) aláíró kulcsának mérete:	2048 bit
kommunikációs kulcsának mérete:	1024 bit
A Regisztrációs Iroda kommunikációs kulcsának mérete:	1024 bit
Az OCSP választ aláíró kulcs mérete:	2048 bit
Az Aláírók aláíró kulcsainak (aláírás-létrehozó adatának) mérete:	legalább 1024 bit

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

6.1.7. Előfizetői aláírás-ellenőrző adat előállításához használt paraméterek előállítása

Az előfizetői tanúsítványok az RSA[17] aláíró algoritmusokhoz használhatók.

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

6.1.8. Szolgáltatói kulcsgenerálás

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

A produktív hitelesítő központok aláíró kulcsainak tanúsítványait a Szolgáltató 1. szintű hitelesítő központja (Root CA-ja) hitelesíti.

6.1.9. Kulcs felhasználási célok

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

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

A Szolgáltató szervezeti egységei esetében a „Key Usage” mezők lehetséges (egyúttal kötelezően kitöltendő) értékeit a következő táblázatok mutatják.

Hitelesítő Központ:

Kulcs megnevezése	Kulcs használati („Key Usage”) mező értéke	Kritikus/Nem kritikus
Hitelesítő Központ (CA) aláíró kulcsa	KeyCertSign, CRLSign	**K**
OCSP válasz egység aláíró kulcsa	DigitalSign, DataEncipherment, KeyEncipherment	**K**
	Az „Extended Key Usage” mezőbe: OCSP signing	**NK**
A CA PKIX kommunikációs kulcs (Regisztrációs Irodával való biztonságos kommunikáció megteremtésére)	DigitalSign, DataEncipherment, KeyEncipherment	**K**

17 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.

Regisztrációs Iroda:

Kulcs megnevezése	Kulcs használati („Key Usage") mező értéke	Kritikus/Nem kritikus
CA PKIX kommunikációs kulcs (a Hitelesítő Központtal való biztonságos kommunikáció megteremtésére)	DigitalSign, DataEncipherment, KeyEncipherment	**K**

6.2. Aláírás-létrehozó adat védelme

6.2.1. A HSM-re vonatkozó szabványok

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

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

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

A Szolgáltató biztonsági megfontolásból alkalmazza az „n-ből m" ellenőrzést a Root CA kulcsgondozási funkcióinak aktivizálásánál.

6.2.3. Aláírás-létrehozó adat letét

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

6.2.4. Aláírás-létrehozó adat mentése, duplikálása

A Szolgáltató az Előfizető aláírás-létrehozó adatot semmilyen formában sem mentheti vagy tárolhatja.

A Szolgáltatónál a Hitelesítő Központ aláíró magánkulcsai[18] biztonsági okokból duplikálásra kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik.

6.2.5. Aláírás-létrehozó adat BALE eszközön, kriptográfiai modulban

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

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

HSM modulban generált – nem minősített szolgáltatói tanúsítványokhoz tartozó – szolgáltatói kulcspárok esetében a magánkulcs nyílt (titkosítatlan) formában semmilyen körülmények között sem hagyhatja el a HSM modult. A szolgáltatói magánkulcsok csak a modul (token) mentésénél, duplikálásánál hagyják el a modult. A mentési (klón) modulba ilyen esetekben a magánkulcs rejtjeles védelem alatt másolódik át.

6.2.6. Aláírás-létrehozó adat aktiválása

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

6.2.7. Aláírás-létrehozó adat deaktiválása

Az aláírás-létrehozó adat deaktiválását az Aláíró alkalmazása végzi kijelentkezéskor vagy amikor az Aláíró a biztonságos aláírás-létrehozó eszközt eltávolítja az olvasóból.

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

6.2.8. Aláírás-létrehozó adat megsemmisítése

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

A szolgáltatói aláírás-létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3. Kulcspár kezelés egyéb aspektusai

6.3.1. Aláírás-ellenőrző adat archiválása

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

Az archiválást tanúsítványokról biztonsági mentést is kell készíteni.

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

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

Root CA aláíró kulcs és tanúsítvány érvényessége:	10 év
OCSP válasz egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
Produktív CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
RO kommunikációs kulcs és tanúsítvány érvényessége:	legfeljebb 3 év
Előfizetői aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 2 év

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

6.4. Aktiválási adatok

6.4.1. Aktiválási adatok generálása és installációja

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

6.4.2. Aktiválási adatok védelme

A Szolgáltató az Aláíró hozzáférési jogosultságát ellenőrző adatot (PIN-kódot) csak abból a célból rögzítheti, hogy azt az Aláíró számára - másolat megőrzése nélkül - átadhassa[19].

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

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

Az Előfizető a későbbiekben is bármikor megváltoztathatja a PIN kódját.

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

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

A Szolgáltató a saját aktiválási adatait a MÁV INFORMATIKA Zrt. Információbiztonsági szabályzata által meghatározott fokozott biztonsági szinten védi.

[19] 3/2005. (III. 18.) IHM rendelet 40. §, 4. bek. szerint.

6.4.3. Aktiválási adatok egyéb aspektusai

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

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

6.5. Számítógép biztonsági szabályok

6.5.1. Számítógép biztonság technikai követelményei

A Számítógép biztonság technikai követelményeit a MÁV INFORMATIKA Zrt. Információbiztonsági szabályzata szerinti fokozott biztonsági osztálybasorolás határozza meg.

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

A PKI alkalmazás által megvalósított biztonsági funkciók az alábbiak:

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

Az OCSP szolgáltatásra vonatkozó biztonsági követelmények az alábbiak:

a. Az OCSP választ aláíró kulcsok tárolása a tanúsítással rendelkező HSM egység(ek)ben történik. Az OCSP szerverek külön biztonsági zónában történő üzemeltetése.
b. biztonsági naplózás,
c. Az OCSP választ kibocsátó szervereket többszörös tűzfal rendszer védi a külső hálózatokról érkező fenyegetésektől.

A kriptográfiai hardver modulokra vonatkozó biztonsági követelmények az alábbiak:

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

A tűzfalra és a behatolásdetektálóra vonatkozó biztonsági követelmények az alábbiak:

a. biztonsági naplózás (a hálózati kommunikáció naplózása, a biztonsági napló védelme, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),
b. a felhasználói adatok védelme (az információ áramlás ellenőrzési szabályok érvényre juttatása/szűrés, a tiltott információ áramlás megakadályozása, megfigyelése),
c. azonosítás és hitelesítés,
d. a biztonsági funkciók megbízható védelme (az információ áramlás ellenőrzés megkerülhetetlenségének biztosítása),

6.5.2. Számítógép biztonsági értékelések

A számítógép biztonsági értékelések rendszerét a 2. táblázat kell felépíteni.

BIZTONSÁGI ELLENŐRZÉS TÍPUSA		VÉGZI	RENDSZERESSÉG
Operatív	IT infrastruktúra	Informatikai biztonsági adminisztrátor	Naponta
	PKI alkalmazás	Rendszer auditor	Naponta
Belső ellenőrzés	IT infrastruktúra	Informatikai biztonsági menedzser	Félévente egyszer
	PKI alkalmazás	Hitelesítési Rend és Szabályozási Csoport	Félévente egyszer
Külső ellenőrzés	IT infrastruktúra	Külső auditor	Évente egyszer
	PKI alkalmazás	Külső auditor	Évente egyszer

2. táblázat

6.6. Életciklus technikai szabályok

6.6.1. Rendszerfejlesztési szabályok

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató társasági szintű információbiztonsági szabályzata tartalmazza, amely pontosan meghatározza 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 és rendszer szintű információbiztonsági szabályzatai tartalmazzák.

6.6.3. Életciklus biztonsági értékelések

A Szolgáltató által alkalmazott megbízható informatikai rendszerek a MÁV INFORMATIKA Zrt. Információbiztonsági szabályzata fokozott biztonsági osztálya követelményeinek felelnek meg, amely azonos szintű az ITSEC F-B1/E3, illetve a Common Criteria EAL4 szintnek. Az életciklus biztonsági értékeléseket a 2. táblázat szerinti rendszerben kell elvégezni.

6.6.4. 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 a visszavonási listákban.

Rendkívüli üzemeltetési helyzetben a Szolgáltató minden egyéb szolgáltatást szüneteltet.

6.6.5. A hitelesítés-szolgáltatás azonnali felfüggesztése

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

6.7. Hálózati biztonsági szabályok

A hálózati védelmi intézkedéseket a MÁV INFORMATIKA Zrt. Információbiztonsági szabályzata fokozott biztonsági osztálya biztonsági szintnek megfelelően kell megvalósítani.

A Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikációt biztosító belső hálózatot védeni kell a sértetlenség és letagadhatatlanság érdekében, illetve bizalmasság elvesztése ellen.

A Szolgáltató hitelesítés-szolgáltatást és OCSP-t támogató informatikai rendszerénél a védett belső és a külső hálózatok biztonságos elválasztását tűzfallal és betörés figyelő rendszerrel (IDS) kell biztosítani.

A Hitelesítő Központ nem folytathat közvetlen külső kommunikációt a végfelhasználókkal.

6.8. Kriptográfiai (HSM) modul ellenőrzése

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

a. a memóriájában levő magánkulcsot törli

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

7. Tanúsítvány és tanúsítvány-visszavonási profil

A Szolgáltató által kibocsátott minősített tanúsítvány profilok és tanúsítvány-visszavonási profilok megfelelnek a 2/2002 (IV.26.) MeHVM irányelvnek, az ITU-T X.509 szabvány 3. változatának, az EU ETSI TS 101 862 (*Minősített tanúsítvány profil*) szabványnak és az RFC 3739 (*Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil*) Internet szabványnak. Az alkalmazott minősített tanúsítvány mezői és azok értelmezése e szabványokat követi.

7.1. Tanúsítvány profil

7.1.1. Alap mezők

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

7.1.2. Tanúsítvány kiterjesztések

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

7.3. OCSP profil

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

8. Hitelesítési Rend adminisztráció

8.1. Változatkezelési eljárások

8.1.1. Változtatási eljárások

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoport működik, amely többek között a jelen hitelesítési rend karbantartásáért is felelős. A változtatási igényeket e csoport gyűjti egybe, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

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

A hitelesítési rend módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

8.2. Közzétételi és tájékoztatási elvek

8.2.1. A HR-MTT+BALE-ben nem tárgyalt elemek

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

8.2.2. A HR-MTT+BALE közzététele

A Szolgáltató a jelen szabályzatát Internetes honlapján teszi közzé.

8.3. HR-MTT+BALE elfogadási eljárások

A jelen HR-MTT+BALE megfelel az RFC 2527 szabványnak. A megfelelőségi vizsgálatot a Szolgáltató, illetve a külső auditor is elvégzi a 2. táblázatban megadott rendszerességgel.

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

Módosítás esetén a Szolgáltató a HR-MTT+BALE változtatásokkal egybeszerkesztett új verziójának tervezetét hatósági felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Hírközlési Hatóságnak. A Szolgáltató alkalmanként ezt megelőzően is konzultál a Nemzeti Hírközlési Hatósággal a tervezett változtatásairól. Az új verzió hatályba léptetésének feltétele, hogy azt a Nemzeti Hírközlési Hatóság nyilvántartásba vegye.

9. Hivatkozások és Meghatározások

9.1. Hivatkozások

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

A Szolgáltató hivatkozott szabályzatai:

A MÁV INFORMATIKA Zrt. Szervezeti és Működési Szabályzata,

A MÁV INFORMATIKA Zrt. Iratkezelési Szabályzata

A MÁV INFORMATIKA Zrt. Titokvédelmi Szabályzata

A MÁV INFORMATIKA Zrt. Adatvédelmi és adatbiztonsági szabályzata

A MÁV INFORMATIKA Zrt. Információbiztonsági szabályzata

Általános Szerződési Feltételek PKI szolgáltatásokhoz (ÁSZF-PKI)

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

A PKI Szolgáltatások Biztonsági Szabályzata

A PKI Szolgáltatások Üzletmenet-folytonossági Terve

A PK Szolgáltatások Üzemeltetési Kézikönyve

9.2. Meghatározások

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

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

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

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

Biztonságos aláírás-létrehozó eszköz: az Eat. 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz

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

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

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

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

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

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

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

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

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes

Érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás-ellenőrző adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsít-

ványt kibocsátó szolgáltató elektronikus aláírás-ellenőrző adatára és annak visszavonására vonatkozó információk), amely alapján megállapítható, hogy az elektonikus dokumentumon elhelyezett fokozott biztonságú vagy minősített aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítványok az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt

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

a. alkalmas az aláíró azonosítására,

b. egyedülállóan az aláíróhoz köthető,

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

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

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

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

Igénylő: a minősített tanúsítvány iránti igényt benyújtó személy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Szolgáltatói kulcspár: a szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs

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

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

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

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

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

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

Mellékletek

1. sz. melléklet

A Szolgáltató feladatai, hatásköre és felelőssége részletesen

A Szolgáltató feladatai és hatásköre

A Szolgáltató kötelezettséget vállal arra, hogy a Szervezeti és Működési Szabályzatában, a mindenkori hitelesítési rendekben, szolgáltatási szabályzataiban, általános szerződési feltételeiben, az előfizetői szerződéseiben és a biztonsági szabályzataiban meghatározottak szerint jár el az előfizetők tanúsítványainak kiadásakor és kezelésekor. Ezek keretében kötelezettséget vállal az alábbiakra:

1. A Szolgáltató (az Ügyfélkapcsolati Irodák, a Regisztrációs Iroda, a Hitelesítő Központ és az Ügyfélszolgálat együttes tevékenységével) minősített elektronikus aláírás-hitelesítés szolgáltatást nyújt
2. A Szolgáltató szolgáltatásait hozzáférhetővé teszi minden olyan igénylő számára, akinek tevékenysége kinyilvánított működési területére esik
3. A Szolgáltató megfelelően dokumentált megállapodásokkal és szerződéses kapcsolatokkal rendelkezik azon esetekre, amikor a szolgáltatások nyújtása alvállalkozókat, illetve más, harmadik felekkel kötött megegyezéseket érint
4. A Szolgáltató Ügyfélszolgálata útján folyamatos felügyeletet biztosít a tanúsítvány visszavonási és felfüggesztési igények fogadására. 99,9%-os rendelkezésre állással biztosít minden tanúsítványállapot szolgáltatást és a CRL publikálást minden érdekelt fél számára.
5. Szolgáltató megőrzi a tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a Tanúsítvány érvényességének lejáratától számított 10 évig, illetőleg – amennyiben ezen időszakban az elektronikus aláírással vagy az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merült fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott Tanúsítvány tartalma megállapítható
6. 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

Az Ügyfélkapcsolati Iroda feladatai és hatásköre

Az Ügyfélkapcsolati Iroda az Igénylők, az előfizetők és az aláírók részére nyújtott ügyfélkapcsolati szolgáltatásán belül:

1. gondoskodik az Igénylő azonosításáról, illetve arról, hogy a Tanúsítványt igénylő formanyomtatványok teljesek, pontosak és kellőképpen hitelesek legyenek
2. ellenőrzi a megadott adatok és a bemutatott dokumentumok alapján az Igénylő személyazonosságát és a leendő Aláíró adatait
3. összegyűjti, illetve meghatározza a Tanúsítványba kerülő adatokat, ellenőrzi az Igénylő által átadott dokumentumok érvényességét, sértetlenségét és hitelességét
4. összeveti egymással és a valósággal az egyes iratokon szereplő adatokat (így különösen a Tanúsítványt személyesen igénylő ügyfél igazolvány-képét az arcával, aláírását a helyszíni aláírásával)
5. lehetősége szerint ellenőrzi a dokumentumok érvényességét valós idejű nyilvántartásokban is
6. nyilvántartásba veszi a regisztráció során felvett adatokat
7. szerződést köt
8. elszámolja és kiszámlázza a szolgáltatások ellenértékét
9. megőrzi a nyilvántartásokat a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig
10. A Szolgáltató az Előfizető és az Aláíró minden adatát a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli
11. korlátozás nélkül biztosítja az Aláíró számára a rá vonatkozó regisztrációs és egyéb adatokhoz történő hozzáférést

Az Ügyfélkapcsolati Iroda a tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:

1. kezdeti tanúsítvány előállítás esetén ellenőrzi a Tanúsítványba kerülő adatokat az adott tanúsítványtípushoz kapcsolódó hitelesítési, ellenőrzési eljárás szerint
2. az Aláíró adatainak változása esetén ellenőrzi a már korábban nyilvántartásba vett adatokat és intézkedik a változások átvezetésre

Az Ügyfélkapcsolati Iroda az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:

1. gondoskodik az aláírás-létrehozó eszköz és a PIN boríték biztonságos kezeléséről és az Előfizetőnek/Aláírónak történő biztonságos átadásáról
2. biztosítja, hogy a Szolgáltató alkalmazottai nem élhetnek vissza az aláírás-létrehozó eszközzel

Az Ügyfélkapcsolati Iroda a visszavonás kezelés szolgáltatás keretén belül:

1. ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy a felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét
2. visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket
3. a visszavonási kérelem elfogadása után haladéktalanul intézkedik a tanúsítvány visszavonásáról
4. tájékoztatja a visszavont, illetve felfüggesztett Tanúsítvány tulajdonosát Tanúsítványa állapotának változásáról

A Regisztrációs Iroda (RA) feladatai és hatásköre

A Regisztrációs Iroda biztosítja az alábbi szolgáltatásokat:

a. elektronikus aláírás-hitelesítés szolgáltatás, ezen belül:

regisztráció,

felfüggesztés és visszavonás kezelés,

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

Egyúttal közreműködik az alábbi szolgáltatások biztosításában:

a. tanúsítvány előállítás,
b. tanúsítvány kibocsátás
c. visszavonási állapot közzététele

A Regisztrációs Iroda a regisztráció szolgáltatás keretén belül:

1. formai szempontból ellenőrzi a tanúsítvány igénylésre vonatkozó kérelmeket
2. visszautasítja a Tanúsítvány kiadását, ha a tanúsítvány igénylés nem teljes, nem helyes, vagy egyéb módon nem felel meg az elvárt feltételeknek
3. bizalmas információként kezeli az Előfizető és az Aláíró minden adatát,

A Regisztrációs Iroda a tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:

1. a Tanúsítvány előállításához szükséges ellenőrzések és visszaigazolások sikeres befejeződése után a Hitelesítő Központ felé tanúsítvány kibocsátási kérelem üzenetet indít el,
2. feldolgozza a tanúsítvány megújítási kérelmeket az alábbi módon:
   2.1. tanúsítványfrissítés kérelme esetén az Aláíró korábbi Tanúsítványában szereplő érvényességi időt meghosszabbítja, a többi adat és kulcspár változatlan megtartása mellett,
   2.2. tanúsítvány aktualizálás kérelme esetén nyilvántartásba veszi az Aláíró megváltozott új adatait, a korábbi Tanúsítványt visszavonja és a megváltozott adatokkal új Tanúsítványt állít elő,
3. biztosítja az aláírandó Tanúsítványt is tartalmazó tanúsítvány kérelem üzenet sértetlenségét, hitelességét és bizalmasságát.

A Regisztrációs Iroda a tanúsítvány kibocsátás szolgáltatásban való közreműködés keretén belül:

1. fogadja a Hitelesítő Központtól kapott új tanúsítványokat, valamint ellenőrzi ezek hitelességét és sértetlenségét,
2. kezdeményezi az új tanúsítványok elküldését a Tanúsítványtárhoz, biztosítva a kérést tartalmazó üzenet hitelességét és sértetlenségét.

A Regisztrációs Iroda az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:

1. gondoskodik a kulcspár előállítás biztonságosságáról, a magánkulcsok titkosságáról,
2. a kulcspárt:
   2.1. olyan kriptográfiai eszközzel állítja elő, amely hazai tanúsítvánnyal igazolt és egyben szerepel a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, tanúsított elektronikus aláírási termékek listáján is,
   2.2. olyan algoritmus felhasználásával állítja elő, melyet a Nemzeti Hírközlési Hatóság az elfogadott kriptográfiai algoritmusok között megfelelő kulcs generáló algoritmusként ismer el,

2.3. olyan aláíró algoritmushoz és olyan kulcshosszúságban állítja elő, melyet a Nemzeti Hírközlési Hatóság az elfogadott kriptográfiai algoritmusok között megfelelő aláíró algoritmusként, illetve megfelelő paraméterként tart nyilván,

3. Minősített tanúsítvánnyal (MTT) kísért, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő kulcspár generálását megfelelően biztonságos környezetben hajtja végre, (a biztonságos aláírás-létrehozó eszközön történő kulcspár generálás esetén az aláírás-létrehozó adat az aláírás-létrehozó eszközön jön létre és azt az semmilyen körülmények között nem hagyja el),
4. gondoskodik az általa megszemélyesített aláírás-létrehozó eszköznek az Ügyfélkapcsolati Irodához történő biztonságos továbbításáról,
5. biztonságos módon előállítja a kezdeti aktivizáló adatot (PIN kódot), majd azt az aláírás-létrehozó eszköztől elkülönítve eljuttatja az Ügyfélkapcsolati Irodához,
6. biztosítja, hogy a Szolgáltató alkalmazottai nem élhetnek vissza az aláírás-létrehozó eszközzel,
7. biztosítja saját aláírás-létrehozó adatainak biztonságos használatát és tárolását.

A Regisztrációs Iroda a visszavonás kezelés szolgáltatás keretén belül:

1. formai szempontból ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét
2. haladéktalanul végrehajtja a szabályos visszavonási, felfüggesztési vagy felfüggesztés megszüntetési kérelmeket (vagyis a kérelmezett változást átvezeti a Tanúsítványtár alapját képező tanúsítvány állapot adatbázisába),
3. visszautasítja a szabálytalan kérelmeket,

A Regisztrációs Iroda a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:

1. rendkívüli esetben új Tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, mely tartalmazza a visszavonási lista lejáratának idejét is,
2. kéri a Hitelesítő Központtól az új Tanúsítvány visszavonási lista kibocsátását, (a visszavonási lista aláírási kérelemben), biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét,

A Hitelesítő Központok („CA”-k) feladatai és hatásköre

A Hitelesítő Központok:

1. ellenőrzik a regisztrációs irodától érkező tanúsítvány kérelmet, benne az aláírandó tanúsítvány adatokat tartalmazó üzenet sértetlenségét és hitelességét,
2. aláírják a tanúsítvány adatokat és feldolgozzák a regisztrációs irodától érkező tanúsítvány kérelmet, melynek keretén belül előállítják a Tanúsítványt (aláírják a megadott tanúsítvány adatokat),
3. csak tanúsítványok aláírására használják fel a Tanúsítvány aláírására szolgáló magánkulcsukat,
4. csak olyan tanúsítványokat állítanak elő, amelyek megfelelnek a HSZSZ-M-ben meghatározott, támogatott tanúsítványtípusoknak,
5. gondoskodnak arról, hogy a Tanúsítványban foglalt megkülönböztetett név egyedi legyen a Szolgáltató szolgáltatási körén belül,
6. gondoskodnak arról, hogy a Szolgáltató teljes szolgáltatási körén belül kibocsátott tanúsítványokhoz tartozó kulcsok mindvégig egyediek maradjanak,
7. elküldik a Regisztrációs Irodának az előállított Tanúsítványt, biztosítva a válaszüzenet sértetlenségét és hitelességét.

A Hitelesítő Központok a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:

1. ellenőrzik a Regisztrációs Irodától érkező visszavonási lista aláírási kérelmet, s ebben az aláírandó Tanúsítvány visszavonási lista sértetlenségét és hitelességét,
2. feldolgozzák a visszavonási lista aláírási kérelmet, melynek során új Tanúsítvány visszavonási listát készítenek és azt aláírással hitelesítik
3. a szolgáltatási szabályzatban meghatározott frissítési időponthoz igazodóan rendszeresen új Tanúsítvány visszavonási listát készítenek, mely tartalmazza a következő lista tervezett kibocsátási idejét is,
4. aláírják a tanúsítvány visszavonási listákat,
5. megválaszolják a Regisztrációs Irodától kapott visszavonási lista aláírási kérelmet, biztosítva a válaszüzenet sértetlenségét és hitelességét.

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

1. Saját szolgáltatói kulcspár generálása.
2. Saját magánkulcsának MÁV INFORMATIKA Zrt. Információbiztonsági szabályzata szerinti fokozott biztonságú védelme.
3. Saját Tanúsítvány előállítása önhitelesítéssel.
4. Saját Tanúsítvány nyilvánosságra hozatala.
5. Szolgáltatói (Produktív CA) Hitelesítő Központok hitelesítési kérelmeinek fogadása és ellenőrzése.
6. Tanúsítvány előállítás Produktív Hitelesítő Központok részére.
7. Produktív Hitelesítő Központok Tanúsítvány visszavonási kérelmeinek feldolgozása.
8. Produktív Hitelesítő Központok Tanúsítvány megújítási kérelmeinek feldolgozása.
9. Tanúsítvány eljuttatása a Produktív Hitelesítő Központhoz.
10. Produktív Hitelesítő Központok Tanúsítványainak és visszavonási listáinak publikálása a Tanúsítványtárban.
11. Produktív Hitelesítő Központ Tanúsítványának visszavonása, illetve felfüggesztése, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn.
12. Az általa tanúsított Hitelesítő Központok bizalmi és biztonsági ellenőrzése.

A 2. szintű „Produktív CA" Hitelesítő Központ alapvető feladat és hatásköre a Regisztrációs Iroda ("RA") és a regisztrált előfizetők hitelesítése; ezen belül a feladatok tételesen a következők:

1. Saját magánkulcs generálás.
2. A saját magánkulcsának MÁV INFORMATIKA Zrt. Információbiztonsági szabályzata szerinti fokozott biztonságú védelme.
3. A Regisztrációs Iroda hitelesítési kérelmeinek fogadása és ellenőrzése.
4. A Regisztrációs Iroda és az Ügyfélkapcsolati Iroda tájékoztatása a tanúsítványkérelmek státuszáról.
5. Kulcspár generálás és Tanúsítvány előállítás a Regisztrációs Irodák részére.
6. Kulcspár és Tanúsítvány eljuttatása a Regisztrációs Irodákhoz.
7. Regisztrációs Irodáktól előfizetői hitelesítési kérelmek fogadása és ellenőrzése.
8. Tanúsítvány előállítás az előfizetők részére.
9. Regisztrációs Irodától érkező tanúsítvány visszavonási, felfüggesztési és újraérvényesítési kérelmek feldolgozása.
10. Regisztrációs Irodától érkező tanúsítvány megújítási kérelmek feldolgozása.
11. Tanúsítványok és tanúsítvány visszavonási listák publikálása a Tanúsítványtárban.
12. Intézkedés tanúsítványok visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn.
13. Folyamatos üzem[20] biztosítása a tanúsítvány felfüggesztési és visszavonási kérelmek végrehajtása érdekében, 99,9%-os rendelkezésre állással.
14. A Regisztrációs Irodák bizalmi és biztonsági ellenőrzése.

A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Rend és Szabályozási Csoport a szolgáltatást nyújtó szervezeti egységtől függetlenül működik. Kötelessége a Szolgáltató és a felhasználó Közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség működésére vonatkozó alapelvek lefektetése, s ebből levezetve a közösség tevékenységét részletesen szabályozó, az egész Szolgáltató szervezetre nézve közös szabályzatok, így a hitelesítési rendek, szolgátatási szabályzatok és biztonsági szabályzatok készítése és rendszeres karbantartása.

A Hitelesítési Rend és Szabályozási Csoport feladatai tételesen a következők:

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

[20] A hét 7 napján, a nap 24 órájában.

A Hitelesítő Központok felelőssége

A Hitelesítő Központok felelősségének belső megosztása nem érinti a szolgáltató társaság egységes jogi felelősségét.

Az 1. szintű „Root CA”

a. felelős az általa kibocsátott tanúsítványok hitelességéért

b. felelős a közvetlenül alá rendelt produktív hitelesítő központok hitelesítésért,

A 2. szintű „Produktív CA” felelős:

a. az általa kibocsátott tanúsítványok hitelességéért

b. az általa létrehozott alárendelt hitelesítő központok hitelesítésért,

c. az alárendelt regisztrációs irodák működéséért.

nem felelős:

a. az Előfizetők aláírási és más hitelesítő központok által kibocsátott magánkulcsok és tanúsítványok felhasználási tevékenységért,

b. nem felelős az érintett felek aláírás ellenőrzési és tanúsítvány elbírálási tevékenységért.

A Szolgáltató felelőssége a hitelesítés-szolgáltatás vonatkozásában

A Szolgáltató felelősségét a hitelesítés-szolgáltatás vonatkozásában az Általános Szerződési Feltételek tartlmazzák.

Hitelesítési Rend és Szabályozási Csoport felelőssége

A Hitelesítési Rend és Szabályozási Csoport felelős a Szolgáltató által kibocsátott szabályzatok ellentmondásmentességéért, megfelelő értelmezhetőségéért és használhatóságáért, azok törvényi megfelelőségéért, érvényesítésért és betartatásáért.

A Hitelesítési Rend és Szabályozási Csoport nem felelős az Előfizetők, az érintett felek, és a felhasználó közösség szervezetei által kibocsátott szabályzatokért.

A Regisztrációs Iroda felelőssége

A Regisztrációs Iroda felelős:

a. a regisztrációs adatok ellenőrzéséért,

b. az általa generált kulcspárok megfelelőségéért, az aláírás-létrehozó adat, az aláírás-ellenőrző adat és a tanúsítvány összetartozásáért és a Tanúsítvánnyal együtt történő aláírás-létrehozó eszközre írásért,

c. az aláírás-létrehozó eszköz és az aktivizáló (PIN) kód összetartozásáért.

Az Ügyfélkapcsolati Iroda felelőssége

Az Ügyfélkapcsolati Iroda felelős:

a. az Előfizetők személyazonosságának és szervezeti identitásának megállapításáért és a bemutatott dokumentumok alapján történő ellenőrzéséért,

b. a felvett regisztrációs adatok ellenőrzéséért,

c. a regisztrációs adatoknak a Regisztrációs Irodához történő bizalmas, hiteles és sértetlen eljuttatásáért,

d. a tanúsítvány visszavonási igény bejelentője személyazonosságának és szervezeti identitásának megállapításáért és a bemutatott dokumentumok alapján történő ellenőrzéséért,

e. az előfizetői pénzek kezeléséért.

Hardver, szoftver, vagy adatsérülés esete

A hardver és/vagy szoftver meghibásodások, valamint egyéb üzemzavarok osztálybasorolástól függő intézkedéseket vonnak maguk után. Katasztrófa helyzetben az Üzletmenet-folytonossági Tervben előírt „azonnali reakció” intézkedéseket kell foganatosítani, azaz értesíteni kell:

a. a Szolgáltató meghatározott felső vezetőit,

b. a Válságstáb vezetőjét és tagjait,

c. szükség esetén a szerződéssel lekötött szerviz cégeknek, az Üzletmenet-folytonossági Tervben megnevezett munkatársait.

A Válságstáb első intézkedései:

a. a katasztrófa esemény azonosítása és behatárolása,

b. A katasztrófa esemény további hatásainak korlátozása,

c. A károk azonosítása, a további károk keletkezésének megakadályozása, illetve mérséklése és a kárérték becslése.

A Válságstáb további intézkedései a hitelesítés-szolgáltatást támogató informatikai rendszer részleges visszaállítására vonatkoznak a tartalék helyszínen.

A visszaállítás egyik alapfeltétele a megfelelő program és adatmentések rendelkezésre állása. A PKI rendszerterve részletesen tartalmazza a hitelesítés-szolgáltatást támogató informatikai rendszer egyes részrendszereire:

a. a teljes rendszer mentés gyakoriságát és időpontját,

b. az inkrementális mentések gyakoriságát és időpontját,

c. a program, file, könyvtár, tranzakció mentések gyakoriságát és időpontját

d. a szükséges adathordozó típust és kapacitást.

Minden mentés három példányban készül. Az első példány a Szolgáltató archívumában, a második, biztonsági példány a Biztonsági Adattárban, a harmadik példányok a katasztrófa helyszínen kerülnek tárolásra. A mentések bizalmasság sérülés elleni védelemmel ellátva, időponttal ellátva és elektronikusan aláírva kerülnek tárolásra.

Egy szolgáltatói egység tanúsítványának visszavonása

Egy szolgáltatói tanúsítvány visszavonása esetén a Szolgáltató az alábbiakat vállalja:

a. a visszavonásról tájékoztatja az összes Előfizetőt és érintett felet,

b. jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információk már nem érvényes(ek).

A Szolgáltató a szolgáltatói tanúsítvány visszavonását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet – amennyiben az sérült –, valamint a végfelhasználók számára új nyilvános kulcsot biztosít új tanúsítvány kiadásával.

Egy szolgáltatói egység kulcsának kompromittálódása

Egy szolgáltatói kulcs kompromittálódása esetén a Szolgáltató az alábbiakat vállalja:

a. a kompromittálódásról tájékoztatja az összes Előfizetőt és érintett felet,

b. jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok és visszavonási állapot információk már nem érvényesek.

A Szolgáltató a szolgáltatói kulcs kompromittálódását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint szükség esetén új kulccsal és új tanúsítvánnyal látja el szolgáltatói egységét, valamint a kompromittálódás által érintett Aláírókat.

Katasztrófa esemény lehet például az Elsődleges Hitelesítő Központ („Root CA”), illetve a Szolgáltató operatív hitelesítő aláírás-létrehozó adatainak, az aktiváló adatoknak és a hardver biztonsági moduloknak az együttes kompromittálódása. Az Üzletmenet-folytonossági Terv forgatókönyvet tartalmaz az ilyen típusú katasztrófa események kezelésére.

A katasztrófa esemény a szolgáltatás azonnali felfüggesztésével jár és amennyiben a kompromittálódás ténye bizonyítást nyer, úgy az összes érintett tanúsítványt vissza kell vonni. A szolgáltatások felfüggesztésének tényéről a Szolgáltató értesíti a felhasználó Közösség tagjait, valamint a Nemzeti Hírközlési Hatóságot.