MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó
Korlátolt Felelősségű Társaság

Hitelesítési Rend nyilvános körben kibocsátott nem minősített tanúsítványokra (HR-NMT)

Verziószám	**2.0**
OID szám	**1.3.6.1.4.1.14868.2.2.0.2**
Hatósági nyilvántartásba vétel napja	**2006. április 7.**
Hatósági nyilvántartásba vétel száma	**HL-4889-3/2006.**
Hatálybalépés dátuma	**2006. április 7.**

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

HR-NMT verziók

Verzió	Dátum	A változás leírása	Készítette
1.0	2002.10.15.	A fokozott biztonságú szolgáltatói regisztrálásra előkészített változat.	Bodlaki Ákos
1.1	2003.05.28.	Változások: Eszköz tanúsítvány Nem cégbíróságnál nyilvántartott szervezetek azonosítása-hitelesítése	Bodlaki Ákos
2.0	2006.03.30.	Felülvizsgált, az NHH észrevételei alapján javított változat	Néder Ferenc

TARTALOMJEGYZÉK

1. Bevezetés

A jelen Hitelesítési Rend (továbbiakban (HR-NMT) a MÁV INFORMATIKA Kft. (továbbiakban Szolgáltató) fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatása keretében kibocsátott aláírás-létrehozó adatok hitelességét bizonyító tanúsítványok kezelésére (előállítás, kibocsátás, közzététel, felfüggesztés, visszavonás, megújítás stb.) vonatkozó követelményeket, a tanúsítványok szerkezetét, a tanúsítványok tartalmának és érvényességének ellenőrzési eljárásait és a szolgáltatás működtetésének követelményeit tartalmazza.

A Szolgáltató a hitelesítés szolgáltatást a vele előfizetői szerződéses viszonyban álló ügyfelei (*előfizetői*) és az elektronikus aláírások hitelességét ellenőrző *érintett felek* részére szolgáltatja.

A jelen Hitelesítési Rend érvényesítésében a következő szervezetek és személyek érintettek:

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

b. az ellenőrző hatóságok

c. a belső és külső auditorok

A Szolgáltató szolgáltatásait a vele előfizetői szerződéses viszonyban álló Előfizetők részére és az elektronikus aláírások hitelességét ellenőrző *érintett felek* részére nyújtja.

A fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatások (továbbiakban: szolgáltatások) keretében a Szolgáltató az Előfizetők és velük kapcsolatban álló Aláírók részére a 2001. évi XXXV. törvényben meghatározott szolgáltatások közül a következőket 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 Korlátolt Felelősségű Társaság

Cégjegyzék szám: 01-09-563711

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

Telefonszám: (36-1) 457-9300

Telefax szám: (36-1) 457-9500

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

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

Illetékes fogyasztóvédelmi felügyelőség:

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

Kapcsolat az ügyfelekkel:

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

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

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

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

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

Panaszok bejelentésének helye:

a. személyesen az Ügyfélkapcsolati Irodákban

b. írásban a Szolgáltató székhelyére címezve

c. telefonon az Ügyfélkapcsolati Irodákban vagy az Ügyfélszolgálatnál

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

1.2. Áttekintés

1.2.1. A Hitelesítési Rend célja

A HR-NMT 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 nem-minősített tanúsítványokra [rövidítve: NMT] vonatkoznak.

A nem minősített tanúsítványok kibocsátására és felhasználására vonatkozó szabályokat a Szolgáltató „Szolgáltatási Szabályzat fokozott biztonságú elektronikus aláírás-hitelesítés szolgáltatáshoz" c. szabályzata (továbbiakban: HSZSZ-F) tartalmazza.

A tanúsítványok végfelhasználóinak tevékenységére vonatkozóan jelen HR-NMT-től és Szolgáltatótól független belső szabályzatok is élhetnek előírásokkal. Amennyiben e szabályzatok bármely vonatkozásban ellentmondást vagy eltérő kikötést tartalmaznának, a jelen HR-NMT előírásai és az elektronikus aláírással kapcsolatos jogszabályok tekinthetők magasabb szintűnek, s ezek alkalmazandók.

1.2.2. Jogszabályok, szabványok

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

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

3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes 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 tanúsítványok, visszavonási listák szerkezetére és tartalmára vonatkozóan:

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

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

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

RFC 3039 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)

ISO 3166 szabvány

Az informatikai biztonsági követelményekre vonatkozóan:

MeH ITB 12. ajánlás, ITSEC[1], CC[2]

A kriptográfiai modulra, az aláírás-létrehozó eszközre vonatkozóan:

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

ITSEC, CC,

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

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

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

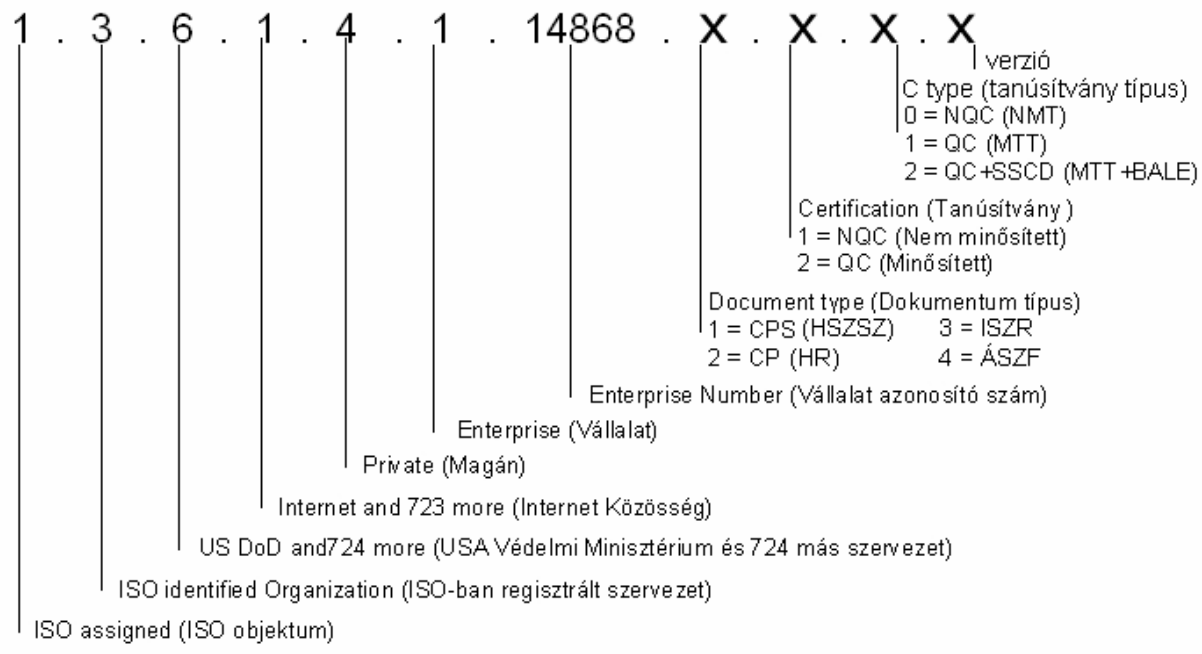
CEN 14167-3 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató kulcs előállítási szolgáltatásait megvalósító kriptográfiai modulra” (CMCKG-PP, HSM-PP)

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

1.3. Hitelesítési rend azonosítás

A HR-NMT a nem minősített tanúsítványok kezelését, az ezzel kapcsolatos eljárásokat és szabályokat írja le.

A nem minősített tanúsítvány objektum azonosítója:



Jelen dokumentum teljes neve:

Hitelesítési Rend nyilvános körben kibocsátott nem minősített tanúsítványokra.

Rövidített neve: Hitelesítési Rend nem minősített tanúsítványokra.

A jelen dokumentumban HR-NMT-ként történik rá hivatkozás. A HR-NMT a Szolgáltató belső dokumentuma.

Jelen HR-NMT-nek csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

1.4. Felhasználó 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

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.

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 fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatáshoz (továbbiakban: HSZSZ-F) 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.

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.

Eszköz tanúsítvány esetében az aláíró egy számítástechnikai eszköz.

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 a 2001. évi XXXV. törvény az elektronikus aláírásról (Eat.) szerinti szolgáltatásokat nyújtja fokozott biztonságú szinten, melyek az alábbi összetevőkből épülnek fel:

a. Tanúsítvány kialakítási szolgáltatás, ebben regisztráló szolgáltatás és egyedi-név szolgáltatás, valamint megszemélyesítési szolgáltatás

b. Tanúsítvány kiadás és tanúsítvány szétosztási szolgáltatás

c. Felfüggesztési és visszavonás kezelési szolgáltatás

d. Tanúsítvány megújítási szolgáltatás

e. Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése

f. Aláírás-létrehozó eszköz fizikai megszemélyesítése (arculati elemek elhelyezése az eszközön)

1.4.5.3. Tanúsítványok alkalmazhatósága

Az előfizetői tanúsítványok alkalmazhatóságára a következő szabályok érvényesek:

Engedélyezett alkalmazási lehetőségek

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

Korlátozott alkalmazási lehetőségek

Szolgáltató területi, pénzügyi, stb. korlátozásokat szabhat saját belső hitelesítési rendje szerint, 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 tanúsítványok más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen hitelesítés szolgáltatás nyújtásához történő alkalmazása tilos.

A fentiek alapján a kibocsátott Tanúsítványok (illetve az ezekhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, amely támogatja a PKI technológián alapuló elektronikus aláírási, le nem tagadhatósági funkciókat. A Szolgáltató nem vállal 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 nem minősített tanúsítványokat és az ezzel kapcsolatos követelményeket írja le.

Szolgáltató által kibocsátott Előfizetői tanúsítványok érvényességi ideje 1 év.

1.5.1. Tanúsítványok jellemzői

A tanúsítványoknak tartalmazniuk kell az alábbiakat:

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

1.5.2. Nyilvános körben kibocsátott nem minősített tanúsítvány (NMT)

Az NMT olyan tanúsítvány, amely:

a. megfelel az Eat. előírásainak
b. olyan Szolgáltató adta ki, amely szerepel az NHH nyilvántartásában
c. nyilvános körben került kibocsátásra.

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 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 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 Aláíró lakóhelyének országkódja és helységneve, a „Common Name" mezőben az Aláíró neve vagy álneve, az „E" mezőben az Aláíró e-mail címe szerepel. Amennyiben az Aláíró hozzájárul, a tanúsítvány „STREET" mezőjében az Aláíró lakcímében szereplő utca neve és a házszáma, a „PostalCode" mezőjében az Aláíró lakcímében szereplő irányítószám is szerepel. A tanúsítvány „Organization" és „Organization Unit" mezői üresen maradnak.

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

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

1.5.4.2. „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 szervezetet képviselő Aláíróra.

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

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

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

1.5.4.3. Eszköz tanúsítvány

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

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

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

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

2. Általános rendelkezések

2.1. 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 tanúsítványra 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 Tanúsítványtárában közzétenni az általa kibocsátott, felfüggesztett és visszavont előfizetői tanúsítványokat.
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 az Internetes honlapján keresztül bárki számára folyamatosan elérhetővé kell tenni a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó szolgáltatási szabályzatait.
10. A Szolgáltató a lejárat előtt értesítést küldhet a lejáró tanúsítványokról az Előfizető részére.
11. Szolgáltató a Tanúsítványban köteles feltünteti az Előfizetői Szerződésben rögzített, a tanúsítvány felhasználhatóságával kapcsolatos korlátozásokat.
12. A Szolgáltató közzétételi kötelezettség mellett felfüggesztheti vagy visszavonhatja a tanúsítványt ha azt a 4.4.1 fejezetben részletezett körülmények ezt indokolják
13. 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.
14. 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 visszavonni az általa kibocsátott és még érvényes tanúsítványokat. A Szolgáltató a tevékenysége befejezéséig köteles eleget tenni a nyilvánosságra hozatali kötelezettségének.
15. 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 feladatai és hatásköre

A Szolgáltató által működtetett hitelesítő központok feladata a tanúsítványok előállítása és 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.

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” és az időbélyegző egység 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 feladatai és hatásköre

A Regisztrációs Iroda fő feladata a hitelesítés-szolgáltatás (regisztráció, kulcsgenerálás, az előfizetői tanúsítvány előállítás, kibocsátás) és az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése. Egyúttal közreműködik az előfizetői tanúsítvány felfüggesztés és visszavonás kezelés szolgáltatásokban.

1. a tanúsítvány kibocsátásához szükséges ellenőrzések sikeres lefolytatása után a tanúsítvány kibocsátás elindítása a Hitelesítő Központnál, (visszautasítja a tanúsítvány kiadását, amennyiben a tanúsítvány-igénylés nem felel meg az elvárt feltételeknek)
2. fogadja a Hitelesítő Központtól kapott előfizetői tanúsítványokat és ellenőrzi azok hitelességét és sértetlenségét,
3. kezdeményezi a tanúsítványok elküldését a Tanúsítványtárba
4. megszemélyesíti az aláírás-létrehozó eszközt és azt eljuttatja az Ügyfélkapcsolati Irodához
5. előállítja a kezdeti aktivizáló adatot (PIN kódot), majd azt az aláírás-létrehozó eszköztől elkülönítve eljuttatja az Ügyfélkapcsolati Irodához,
6. szoftveres úton történő kulcspár generálás esetén biztonságos módon eljuttatja a kulcspárt az aláírás-létrehozó eszközbe, olyan biztonságos útvonal kiépítésével, mely kriptográfiai mechanizmusok felhasználásával forráshitelesítést, sértetlenséget és bizalmasságot biztosít,
7. biztonságos módon megsemmisíti az előállított magánkulcs aláírás-létrehozó eszközön kívüli összes példányát, miután az Aláíró részére előállított kulcspárt elhelyezte az aláírás-létrehozó eszközben),
8. 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,
9. visszautasítja a szabálytalan tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket,
10. fogadja és feldolgozza a tanúsítvány megújítási kérelmeket.

2.1.1.3. 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 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. előkészíti az Előfizetői Szerződést
5. elszámolja és kiszámlázza a szolgáltatások ellenértékét,
6. nyilvántartásba veszi a regisztráció során felvett adatokat és megőrzi azokat.
7. bizalmas információként kezeli az Előfizető és az Aláíró minden adatát, kivéve azokat, amelyek az Előfizető hozzájárulásával a tanúsítványba kerülnek
8. gondoskodik az aláírás-létrehozó eszköz és a PIN boríték biztonságos kezeléséről és átadásáról,
9. tájékoztatja az Előfizetőt tanúsítványa lejáratát megelőzően 15 nappal

10. 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.
11. 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.

2.1.1.4. A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Rend és Szabályozási Csoport a hitelesítés-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 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.

2.1.1.5. 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 Igénylő, az Előfizető és Aláíró feladatai és hatásköre

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

1. önmagát az Ügyfélkapcsolati Irodán okmányokkal igazolni,
2. a tanúsítvány igénylését és magánkulcsának felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse,
3. az Előfizető a regisztráció során a Tanúsítvány 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-F 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,

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 fél feladatai és hatásköre

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-F, ÁSZF-F),
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;
   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. Ha az ellenőrzés a tanúsítvány érvényességének lejárta után történik, akkor az Eat. 9.§ (7. bek.) alapján a szolgáltatónál 10 évig, illetve az aláírt dokumentummal kapcsolatban felmerült jogvita lezárásáig megőrzött, a tanúsítványokkal kapcsolatos elektronikus információkat és ahhoz kapcsolódó személyes adatokat elő lehet keresni és ellenőrizni lehet a tanúsítvány érvényességét. 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, az Előfizetővel szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért, ha megszegte a HSZSZ-F-ben, az ÁSZF-F-ben 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 rögzíteni.

A Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott tanúsítvány a jelen hitelesítési rendben és a szolgáltatási 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. 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 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.

A Szolgáltató nem vállalhat felelősséget az 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 tanúsítvány, a szolgáltatási szabályzat, illetve a hatályos jogszabályok 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 (lásd: 4.5.1 és 4.5.4 fejezetek).

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.),

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

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

Az Előfizetők, az Aláírók és az Érintett felek vagy bármely harmadik fél megkeresheti az Ügyfélkapcsolati Irodát munkanapokon ügyfélfogadási időben személyesen vagy telefonon, postai úton írásban, e-mail-ben vagy faxon. A Szolgáltató Ügyfélszolgálata (Help Desk) folyamatos (7x24 órás) szolgálattal áll rendelkezésre telefonos vagy e-mail megkeresés esetén. Az írásban vagy elektronikus úton történő kommunikáció esetében a feladó nevét és elérhetőségét fel kell tüntetni és a feladónak a küldeményt hitelesítenie kell.

A Szolgáltató az Előfizetőket és Érintett feleket tipikusan az Internetes honlapján (web oldalain) történő közzétellel, illetve az ügyfélkapcsolati irodákban elérhető dokumentumokkal tájékoztatja. Az ügyfélkapcsolati irodák az Előfizetőket esetenként írásban vagy elektronikus úton is értesíthetik.

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 Szolgáltató jogosult önálló üzletpolitikát kialakítani és szolgáltatásaiért díjat szedni.

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató Internetes honlapján keresztül is közzéteheti.

2.6. Közzététel

2.6.1. Szolgáltatói információk közzététele

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

a. tanúsítvány típusok
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 – saját elektronikus aláírásával hitelesítve - Internetes honlapján keresztül is elérhetővé kell tennie. Szolgáltatónak csak saját elektronikus aláírásával ellátott dokumentumai tekinthetők eredetinek. A honlapról letöltött dokumentumok nyomtatott változatai semmilyen formában sem tekinthetők hivatalos példánynak.

2.6.2. A közzététel gyakorisága

A Szolgáltató Tanúsítványtárát és a Tanúsítvány visszavonási listát 24 óránként frissíti.

A Szolgáltató az általa működtetett hitelesítő központok szolgáltatói tanúsítványait 24 órán 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 az 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, a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, valamint a tanúsítvány visszavonási listákat Tanúsítványtárban tárolja és teszi hozzáférhetővé.

2.7. A megfelelőség vizsgálata

A Szolgáltatót fokozott biztonságú szolgáltatóként 2002. október 30.-án a Nemzeti Hírközlési Hatóság nyilvántartásba vette.

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

2.7.1. Vizsgálatok gyakorisága

A vizsgálatokat a Szolgáltató évente egyszer megismételteti, illetve a törvényi feltételek vagy szolgáltatásban bekövetkezett jelentősebb változások alkalmával soron kívül elvégezteti.

2.7.2. Az átvizsgáló szervezet és a vizsgált fél kapcsolata

A belső auditot a Szolgáltató hitelesítés szolgáltatást végző szervezeti egységétől független informatikai biztonsági menedzser, a külső auditot nyilvános kulcsú infrastruktúra illetve informatikai biztonsági termék és szállítótól független külső auditor cég végzi el**.**

2.7.3. A vizsgálatok kiterjedése

Az auditorok két fő területet, a hitelesítés szolgáltatás és az informatikai biztonság területét vizsgálják, abból a szempontból, hogy Szolgáltató hitelesítő és biztonsági rendszere, annak személyi és fizikai környezete megfelele a mindenkori hatályos törvényi előírásoknak, valamint a Szolgáltató saját szabályzatainak, első sorban a hitelesítési rendnek, a szolgáltatási és a biztonsági szabályzatoknak.

2.7.4. Hiányosságok kezelése

Az auditor a vizsgálati jelentést a Szolgáltató vezetőjének nyújtja be.

A jelentésben megállapított hiányosságok következménye:

1. A hiányosságok nem sértik alapvetően a Szolgáltató tevékenységébe vetett bizalmat, vagy az informatikai biztonságot. A Szolgáltató változatlan formában folytatja tevékenységét, de köteles a hiányosságokat 30 napon belül megszüntetni.
2. Ha a hiányosságok alapvetően érintik a Szolgáltató egyes tevékenységeit, vagy az informatikai biztonság egyes területeit, a Szolgáltatónak fel kell függesztenie a hiányosságok által érintett tevékenységeit a hiányosságok megszüntetéséig. Amennyiben ez a létrehozandó aláírás-létrehozó adatok, eszközök biztonságát vagy a tanúsítványok, visszavonási listák hitelességét veszélyezteti, akkor ezen tevékenységet és a kibocsátott tanúsítványokat fel kell függeszteni.

3. Amennyiben a hiányosságok a Szolgáltatóba vetett bizalmat alapvetően megingatják, a teljes tevékenységét fel kell függeszteni és a kibocsátott tanúsítványokat vissza kell vonni.

Eredmény kommunikációja

A vizsgálati jelentés belső használatra szolgáló anyag. Azt a Szervezeti és Működési Szabályzatban meghatározott szervezeti egységek vezetői kapják meg. A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni, de azok alapot adhatnak a Szolgáltató kötelezettségszegésének bizonyítására.

2.8. Bizalmasság – Adatkezelési szabályzat

2.8.1. Bizalmas információk

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

1. A felvett adatokat védi az elveszéstől, tönkretételtől és hamisítástól. A jogszabályoknak való megfelelés, valamint az alapvető üzleti tevékenységek támogatása érdekében szükség van bizonyos bejegyzések biztonságos megőrzésére is.
2. gondoskodik az adatvédelmi törvényeknek való megfelelésről,
3. megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen kezelése ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen,
4. nyilvántartásba veszi az előfizetővel aláírt megállapodást, beleértve az alábbiakat:
    4.1. hozzájárulás a szolgáltatások során felhasznált adatok hitelesítés-szolgáltató által történő nyilvántartásba vételéhez,
    4.2. hozzájárulás a nyilvántartásba vett adatok harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén, az erre az esetre vonatkozó szabályzat megkövetelt feltételei szerint,
    4.3. az előfizető hozzájárulását a tanúsítvány közzétételéhez,
5. gondoskodik arról, hogy a regisztrációs eljárás során az adatvédelmi jogszabályok követelményei érvényesüljenek,
6. hitelesítési rendje csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához,
7. gondoskodik az Aláíróra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz az előfizető hozzájárult, vagy ha bíróság vagy egyéb jogi követelmény ezt előírja,
8. A legmagasabb érzékenységi szintet bizalmasság szempontjából az Aláírók és a hitelesítés szolgáltatók aláírás-létrehozó adatai képezik, ezen belül a legérzékenyebb a szolgáltatói aláírás-létrehozó adat, mert kompromittálódása a Szolgáltató tevékenységének azonnali felfüggesztésével jár. Ezért ezeket az adatokat, illetve az ezeket hordozó eszközöket fokozott biztonsággal kell tárolni és használni. Az aláírás- létrehozó adat biztonságáért a teljes felelősséget az adat tulajdonosa viseli.

A Szolgáltató 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 felek az üzleti titok megsértésével okozott kárért a polgári jog általános szabályai szerint felelnek.

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 előírásait kell érvényesíteni.

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 írásos hozzájárulása nélkül nem adhatja át, kivéve a 2.8.4 pontban meghatározott eseteket.

Az Előfizető és az Aláíró a tanúsítvány igénylésével hozzájárul ahhoz, hogy a Szolgáltató személyes adatait tárolja és kezelje. A hozzájárulás egyaránt vonatkozik az adatok aláíróval és előfizetővel való megosztására (ha a két fél különbözik), s nyilvántartásba vett adatok harmadik félhez történő továbbítására, a szolgáltató szolgáltatásainak leállítása esetén. A tanúsítványigénylő űrlapon az Előfizetőnek jeleznie kell a tanúsítvány nyilvánosságra hozatalához történő hozzájárulását.

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

2.8.2. Nem bizalmas információk

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

2.8.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

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

A Szolgáltató a tanúsítvány visszavonás okát feltünteti a visszavonási listában. Ezen kívül a visszavonással kapcsolatos minden egyéb információt, 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 adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak.

Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató 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.

2.8.6. Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson túl ügyfelei üzleti titkát, az Előfizetők és az Aláírók nem nyilvános személyes adatait csak az ügyfelek vagy az 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 Aláíró jogosult.

Az Aláíró egyedi azonosítójában szereplő bármilyen védjegy, szervezeti- és személynév, vagy egyéb adat az Előfizető vagy az 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 regisztrálás során:

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

b. megfelelő, illetékes 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

A tanúsítványokban szereplő névmegadás feleljen meg az ITU-T[3] X.500 ajánlásának.

3.1.2. Nevek szemantikája

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

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

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

3.1.3. Nevek egyedisége

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

3.1.4. Név igénylési viták feloldása

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

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

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

3.1.5. Védjegyek elismerésének és hitelesítésének módszere

A 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 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 kiemelt biztonságú környezetben 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] „Information Technology - Open Systems Interconnection - The directory: Overview of concepts, models and services”

3.1.7. Személyazonosság megállapítása

Az Eat. 12. § értelmében a Szolgáltató jogosult az Aláíró személyazonosságát megállapítani. Ezért az előfizetői tanúsítványok igénylésekor a személyes azonosságot igazolni kell.

A személyazonosság megállapítása történhet személyi igazolvány, útlevél, gépjármű vezetői engedély vagy egyéb, személyazonosításra alkalmas okmány alapján.

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

A személyazonosság hitelesítésének eljárását a szolgáltatási szabályzatban kell részletezni.

3.1.8. Szervezeti hovatartozás megállapítása

Szervezeti típusú tanúsítványok igénylésekor a személyazonosság megállapításán túl a szervezet azonosítását is el kell végezni.

A szervezet azonosítása történhet 30 napnál nem régebbi cégkivonattal, aláírási címpéldánnyal vagy egyéb, azonosításra alkalmas dokumentum alapján.

A tanúsítvány kérelem nem fogadható el, amennyiben a dokumentumok szervezethez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel.

A szervezet azonosításának eljárását a szolgáltatási szabályzatban kell részletezni.

3.1.9. Eszköz azonosság megállapítása

Eszköz tanúsítvány igénylésekor az eszköz azonosításához és hitelesítéséhez az előfizető személyazonosítása mellett szükségeses az Előfizető írásos nyilatkozata az eszköz birtoklásáról és annak azonosítójáról.

A Szolgáltató köteles a szerződéskötéstől elállni, ha az azonosítás-hitelesítés vagy az azt követő ellenőrzések során az eszköznek az Előfizetőhöz tartozásával vagy annak eredetiségével kapcsolatban kétség merül fel.

3.2. Érvényes tanúsítvány megújítása (tanúsítvány frissítése)

Érvényességi idejének lejárata előtt a Szolgáltató a tanúsítvány érvényességét újabb egy évre meghosszabbíthatja.

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

Előfizetői tanúsítvány megújítása akkor lehetséges, ha:

a. a tanúsítvány nem szerepel a Visszavont Tanúsítványok Listájában

b. a tanúsítványban rögzített adatok 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.

3.3. Érvénytelen tanúsítvány megújítása

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

3.4. Felfüggesztés és visszavonási kérés

A Szolgáltatónak gondoskodnia kell arról, hogy az általa kibocsátott tanúsítványok érvényességét az Előfizető vagy az Aláíró kérésére felfüggessze vagy a tanúsítványt visszavonja. Ennek érdekében a Szolgáltató a 4.4.3 pontban rögzíti a tanúsítványok visszavonásának és felfüggesztésének (4.4.5 pont) eljárásait.

4. A működésre vonatkozó követelmények

4.1. Tanúsítványigénylés

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

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

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

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

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

A Tájékoztatót a szolgáltató internetes honlapján minden érdeklődő számára elérhetővé kell tenni.

4.2. Tanúsítvány kibocsátás

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

Az elkészült Tanúsítvány a következő módon juthat 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

4.3. Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető részéről az átadással történik meg.

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

4.4. Tanúsítvány felfüggesztés és visszavonás

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatást köteles nyújtani. 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: 4.4.6 pont) után állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni.

A felfüggesztési és visszavonási kérelmeket félfogadási időben az Ügyfélkapcsolati irodák fogadják. Emellett a Szolgáltató köteles 24 órás folyamatos ügyeletet biztosítani a felfüggesztési kérelmek fogadására és azoknak a sikeres végrehajtására.

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

e. 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[4].

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

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

d. az Előfizetői szerződés megszűnése

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

f. a Tanúsítványban feltűntetett kibocsátó adatok megváltozása

g. a hitelesítési szolgáltatás megszűnése

h. a Szolgáltató valamely magánkulcsának kompromittálódása miatt

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

4.4.2. Visszavonás/felfüggesztés kérelmezése

Tanúsítvány visszavonását/felfüggesztését az előző pontban feltüntetett körülmények alapján az Aláíró, az Előfizető vagy annak regisztráció során nyilvántartásba vett képviselője, a Szolgáltató, hatósági szervezet vagy más harmadik fél kezdeményezheti. Az Előfizetőnek és a Szolgáltatónak kötelessége, harmadik félnek joga az előző (4.4.1) pontban feltűntetett esetekben a visszavonás azonnali kezdeményezése.

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

A visszavonási/felfüggesztési kérelem teljesítéséhez a következő adatok szükségesek:

a. a Tanúsítvány sorszáma,

b. a visszavonást kérő azonosító adatai,

c. a visszavonás oka.

4.4.3. Visszavonási eljárás

Visszavonási igényt Aláírói tanúsítványra lehet levélben vagy személyesen benyújtani.

A visszavonási eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt:

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

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

[4] Eat. 10. § (3)

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

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

A visszavont Tanúsítvány bekerül a következő alkalommal kibocsátott Visszavont Tanúsítványok Listájába.

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

4.4.4. Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási/felfüggesztési kérelem esetén a Szolgáltató ennek végrehajtását soron kívül köteles végrehajtani a kérelem elfogadása után. A legnagyobb késedelem a visszavonási/felfüggesztési kérelem elfogadása és a visszavonási állapot közzététele között: 24 óra lehet.

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

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

Visszavont/felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok:

a. A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig és elfogadásáig az 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 Szolgáltatót felelősség nem terheli.

c. A 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.

4.4.5. Felfüggesztési eljárás

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

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

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

4.4.6. Felfüggesztett állapotra vonatkozó korlátozások

Tanúsítvány felfüggesztett állapotban legfeljebb 30 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 30 napon belül dönt a Tanúsítvány visszavonásáról is. Amennyiben Szolgáltató nem képes ezen időszak alatt a körülmények kivizsgálására, akkor a tanúsítványt visszavonja, valamint az Előfizető igénye estén részére térítésmentesen új Tanúsítványt bocsát ki.

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

Az újraérvényesítés feltételei a következők:

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

b. Az újraérvényesítést kérő személyt azonosítani és hitelesíteni kell.

Az újraérvényesítés kéréséhez a következő adatokat kell megadni:

a. a felfüggesztett Tanúsítvány sorszáma,

b. a felfüggesztés megszüntetést kérő azonosító adatai,

c. a felfüggesztés megszüntetés kérés oka.

4.4.7. Visszavont Tanúsítványok Listája (CRL) és kibocsátásának gyakorisága

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

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

4.4.8. Visszavont Tanúsítványok Listája ellenőrzése

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

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

4.4.9. Visszavonási állapot közlés más formái

A Szolgáltató nem köteles a Tanúsítvány visszavonási listától különböző visszavonási állapot közlő eljárást működtetni.

A tanúsítványt igénybe vevő Érintett feleknek ugyanakkor, minden hagyományosan alkalmazott, és ésszerűen elvárható módszert igénybe kell venniük az általuk tanúsítvány segítségével ellenőrzött műveletek biztonsága érdekében. Amennyiben módjuk van az aláírás és tanúsítvány érvényességének más forrásból való ellenőrzésére, akkor azt a tanúsítvány állapotától függetlenül is meg kell tenniük.

Amennyiben Érintett fél más forrásból tudomást szerezhet, vagy ésszerű és elvárható gondossággal más forrásból megbizonyosodhat a tanúsítvánnyal igazolt művelet érvényességéről, akkor ezeket a lépéseket a tanúsítvány állapotától függetlenül is meg kell tennie. Szolgáltató ilyen esetekben nem felelős a bekövetkező károkért.

4.4.10. Intézkedések magánkulcs kompromittálódás esetén

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

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

4.5. Biztonsági audit eljárások

A Szolgáltató hitelesítés támogató informatikai rendszerének biztonsági naplózását és annak auditálását biztonsági szabályzatban kell részletezni a jelen dokumentumban leírt követelmények alapján. A Szolgáltató biztosítja a regisztrációs információk, a hitelesítés-szolgáltató kulcsgondozási és tanúsítványgondozási eseményeire vonatkozó fontosabb információk naplózását, melyben:

a. A Szolgáltató a környezetére, kulcs- és tanúsítvány gondozására vonatkozó fontosabb események pontos időpontját is rögzíti.

b. A Szolgáltató biztosítja személyzete felelősségre vonhatóságát tevékenységéért, többek között az eseménynapló megőrzésén és védelmén keresztül.

4.5.1. Naplózott esemény típusok

A Szolgáltató általános tevékenységével kapcsolatosan:

- A naplózandó eseményeket és adatokat a Szolgáltató biztonsági szabályzatai rögzítik.

A regisztrációval kapcsolatosan:

- A Szolgáltató gondoskodik arról, hogy naplózásra kerüljön valamennyi regisztrációval kapcsolatos esemény, beleértve a Tanúsítvány megújítására vonatkozó kérelmeket is.

A tanúsítvány előállítással kapcsolatosan:

- A Szolgáltató naplózza a szolgáltatói kulcsok életciklusával kapcsolatos összes eseményt.

- A Szolgáltató naplózza a tanúsítványok életciklusával kapcsolatos összes eseményt.

Az Aláírók aláírás-létrehozó eszközzel való ellátásával kapcsolatosan[5]:

- A Szolgáltató naplóz minden általa gondozott kulcs életciklusával kapcsolatos eseményt.
- a Szolgáltató naplózza az aláírás-létrehozó eszközök készítésével kapcsolatos valamennyi eseményt.

A visszavonás kezeléssel kapcsolatosan:

- A Szolgáltató gondoskodik a visszavonással kapcsolatos összes kérés, valamint az ezek eredményét képező összes tevékenység naplózásáról.

4.5.2. Napló adatok tárolása

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

4.5.3. Adatarchiválás

A Szolgáltatónak gondoskodnia kell arról, hogy a Tanúsítványra vonatkozó minden lényeges információ megfelelő ideig rögzítésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

4.5.4. Az archívum megőrzési időtartama

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

4.5.5. Az archívum védelme

A Szolgáltató fenntartja a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét.

A Szolgáltató a fontos bejegyzéseket megvédi az elveszéstől, tönkretételtől és hamisítástól.

A Szolgáltató megfelelő műszaki és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen feldolgozása ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen.

Az archívumba történő hagyományos vagy elektronikus adattovábbítás csak biztonságos megoldással történhet.

4.6. Katasztrófa elhárítás

4.6.1. A hitelesítés-szolgáltatás azonnali felfüggesztése

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

A Szolgáltató gondoskodik arról, hogy katasztrófa esetén, beleértve a saját aláírás-létrehozó magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, az üzemeltetés amint csak lehetséges helyreálljon és a szolgáltatás meginduljon.

4.6.2. Hardver, szoftver, vagy adatsérülés esete

A Szolgáltató Üzletmenet-folytonossági Terve a kritikus szoftver/hardver komponensek sérülésével, mint katasztrófa helyzettel foglalkozik. Ilyen esetekben a tervezett eljárásokat életbe lépteti annak érdekében, hogy az üzemeltetés, amint csak lehetséges, helyreálljon.

A Szolgáltató minimalizálja a biztonsági események és hibás működések által okozott kárt, eseményjelentés és válaszadás eljárások használatán keresztül.

A Szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Ennek érdekében valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.

[5] Az „aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése” szolgáltatás keretén belül.

4.7. Hitelesítés szolgáltató tevékenység megszüntetése

A Szolgáltatónak a tervezett megszűnés előtt megállapodást kell kötni más szolgáltatóval a szolgáltatások átvételéről. A megállapodásról tájékoztatnia kell a felhasználói közösséget.

A Szolgáltatónak gondoskodnia kell a szolgáltatásainak megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról, különösképpen a tanúsítvány visszavonás kezelés és közzététel szolgáltatások folyamatos fenntartásáról.

Ennek érdekében a Szolgáltatónak mielőtt hitelesítés-szolgáltatási tevékenységét leállítja:

a. értesítenie kell a Nemzeti Hírközlési Hatóságot és Internetes honlapján tájékoztatnia kell a felhasználói közösség tagjait

b. meg kell szűntetnie a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások összes felhatalmazását

c. fel kell készülnie a regisztrációs adatok és az eseménynapló archívumok fenntartására vonatkozó kötelezettségei átruházására

A bejelentéssel egyidejűleg a Szolgáltató leállíthatja:

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

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

Szolgáltatónak a tervezett megszűnés előtt intézkednie kell az előfizetői tanúsítványok és szolgáltatói tanúsítványai visszavonásáról.

Ezzel egyidejűleg leállíthatja a visszavonás kezelési szolgáltatását.

Regisztrációs Iroda megszűnése esetén:

a. A Szolgáltató a Regisztrációs Iroda megszűnése előtt 60 nappal köteles értesíteni azon Előfizetőket, akik a megszűnő Regisztrációs Irodánál kötöttek szerződést és a Szolgáltató által kibocsátott érvényes tanúsítvánnyal rendelkeznek.

b. A Regisztrációs Iroda megszűnéséről a felhasználói közösség tagjait a Szolgáltató a web oldalain történő közzététel útján köteles tájékoztatni.

5. Fizikai, eljárásrendi, és humán biztonsági szabályozások

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

a. 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.

b. 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.

c. A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetőségének kell jóváhagynia[6].

d. 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[7].

e. 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.

f. 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.

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

A következő pontok csak a vonatkozó lényeges intézkedéseket tartalmazzák.

[6] Az informatika biztonság kezelésével kapcsolatban útmutatásként lásd a MeH ITB 12. ajánlást és az ISO/IEC 17799-et.

[7] Ajánlott, hogy a Biztonsági 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.

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.

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

A kulcspár generálással, tanúsítvány előállítással, aláírók 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 aláírás-létrehozó eszközzel 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.[8] kapcsolatos tevékenységeire.

A Szolgáltatónak óvintézkedéseket kell megvalósítani annak megakadályozása érdekében, hogy a fokozott biztonságú elektronikus aláírás-hitelesítéssel kapcsolatos szolgáltatásaihoz szükséges berendezéseket, információkat, adathordozókat vagy szoftvereket jogosulatlanul elvigyék a helyszínről[9].

5.2. Eljárásrendi szabályozások

A Szolgáltató gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék.

A Szolgáltató személyzete olyan adminisztratív és kezelési eljárásokat és folyamatokat végez, amely szinkronban van a Szolgáltató Biztonsági Szabályzatának eljárásaival.

5.2.1. Az egyes munkakörökben elvárt azonosítás és hitelesítés

A Szolgáltató személyzete csak sikeres azonosítás és hitelesítés után használhatja a kulcs- és tanúsítványgondozással kapcsolatos kritikus alkalmazásokat.

5.3. Humán szabályozások

5.3.1. Bizalmi munkakörök

A Szolgáltató egyértelműen azonosítja azokat a munkaköröket, amelyektől a hitelesítés-szolgáltatás biztonsága függ. Ezeket a bizalmi munkaköröket és felelősségeket munkaköri leírásokban dokumentálja.

A bizalmi munkakörök közé az alábbiak tartoznak:

A hitelesítés-szolgáltató informatikai rendszeréért általánosan felelős vezető

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

Rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.

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

Független rendszervizsgáló: a hitelesítés-szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a hitelesítés-szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések

[8] A fizikai és környezeti biztonsággal kapcsolatban útmutatóként lásd a MeH ITB 12. ajánlását és az ISO/IEC 17799 dokumentumot.

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

betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

Regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

Bizalmi munkakörökbe a biztonságért felelős felső vezetésnek kell formálisan kineveznie a hitelesítés-szolgáltató munkatársait.

Üzemeltetési eljárásokat kell kidolgozni valamennyi olyan bizalmi és adminisztratív feladatra, amely hatást gyakorol a hitelesítési szolgáltatásokra, s ezeket az eljárásokat be kell tartani.

A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia a hitelesítés-szolgáltatóval.

5.3.2. Az egyes feladatokhoz szükséges személyzeti létszámok

A hitelesítés-szolgáltató munkatársai munkaköri leírásainak támogatniuk kell a feladatok szétválasztásának és a legkisebb meghatalmazás elvének szempontjait. A leírásoknak többek között meg kell határozniuk az egyes feladatokhoz szükséges létszámot is.

Csak védett környezetben legalább két, bizalmi munkakört betöltő, erre feljogosított személy együttes részvételével, más személyek jelenlétét kizárva kerülhet sor az alábbi funkciók végrehajtására:

a. a hitelesítés-szolgáltató saját szolgáltatói kulcsának előállítása

b. a hitelesítés-szolgáltató szolgáltatói magánkulcsának mentése

c. a hitelesítés-szolgáltató szolgáltatói magánkulcsának visszaállítása

d. a hitelesítés-szolgáltató szolgáltatói magánkulcsának megsemmisítése

5.3.3. Az egyes munkakörökben elvárt azonosítás és hitelesítés

A hitelesítés-szolgáltató személyzetét megfelelően azonosítani és hitelesíteni kell, mielőtt a tanúsítvány kezeléssel kapcsolatos kritikus alkalmazásokat használnák.

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 hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy személyzeti gyakorlata fokozza és támogassa a hitelesítés-szolgáltató működésének megbízhatóságát. Különösképpen:

A hitelesítés-szolgáltatónak kellő számú, a hitelesítési szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet kell alkalmaznia.

A hitelesítés-szolgáltató valamennyi bizalmi munkakört betöltő munkatársának függetlennek kell lennie minden olyan ütköző érdektől, ami hátrányosan érinthetné a hitelesítés-szolgáltató tevékenységeinek semlegességét, a szolgáltatás megbízhatóságát és biztonságát.

A hitelesítés-szolgáltató (ideiglenes és állandó) munkatársainak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaleírásokkal kell rendelkezniük. A munkaleírásoknak meg kell határozniuk a beosztás érzékenységét, a feladatok elvégzéséhez szükséges hozzáférési jogosultságok alapján. Ahol erre szükség van, meg kell különböztetni az általános funkciókat és a hitelesítés-szolgáltató specifikus funkciókat. A munkaleírásoknak meg kell határozniuk az egyes feladatokhoz szükséges létszámot is. Ajánlott, hogy a munkaleírások 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. Előélet vizsgálatára vonatkozó eljárások

A hitelesítés-szolgáltatónak nem szabad bizalmi munkakörbe, illetve a vezetőségbe kineveznie olyan személyt, aki bűncselekményért, illetve más olyan vétségért el lett ítélve, amely illető alkalmasságát befolyásolja. A munkatársaknak nem szabad hozzáférniük biztonsági funkciókhoz mindaddig, amíg a szükséges, személyükre és alkalmasságukra vonatkozó ellenőrzések végrehajtása meg nem történik.

5.3.8. Kiképzési követelmények

Az üzemeltető személyzetet a rendszer használatba vétele előtt ki kell képezni

a. a nyilvános kulcsú infrastruktúra elméletéből,

b. a rendszer használatáról,

c. a regisztrációs, tanúsítási és visszavonási eljárásrendekről,

d. az egyes tevékenységek jogi következményeiről,

e. az informatikai biztonsági követelményekről,

f. a Hitelesítési rend és a Szolgáltatási Szabályzat alkalmazásának jelentőségéről.

A képzést meg kell ismételni minden, a rendszerben történő változás után (a változás által érintett területen).

.

6. Műszaki biztonsági óvintézkedések

A Szolgáltató az Eat. 7.§ (5) bekezdésének megfelelő megbízható, biztonságtechnikailag értékelt és minősített termékekből álló rendszert használ szolgáltatásai nyújtásához.

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

6.1. Kulcspár előállítás és telepítés

6.1.1. Kulcspár előállítás

A Szolgáltató maga generálja a kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben. A kulcspárok generálását olyan algoritmussal végzi, melyet jogszabály ismer el erre a célra alkalmasnak[10].

A Szolgáltató nem fogadhat el az Előfizető által generált kulcspárt.

Az aláírás-létrehozó adat aláírás-létrehozó eszközön (pl.: csipkártyán) történő elhelyezésére a Szolgáltató csak tanúsítvány kibocsátással együtt vállalkozhat. Ezzel együtt a csipkártyán elhelyezi a kibocsátott Tanúsítványt is.

A szolgáltatói magánkulcsok (aláírás-létrehozó adatok) teljes életciklusuk alatt nagy biztonságú hardver modulban, illetve az aláírás-létrehozó eszközön maradnak, amennyiben ilyen módon kerültek generálásra.

6.1.2. Aláírás-létrehozó eszköz megszemélyesítés

Az aláírás-létrehozó eszköz (csip kártya) megszemélyesítését a Szolgáltató maga végzi fizikailag védett környezetben üzemelő kártya-megszemélyesítő rendszeren.

A csip 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 csip 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 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 Előfizetőnek vagy az Előfizető képviselőjének.

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) – hozzájárulásuk esetén -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 nyilvános kulcsokat tartalmazó tanúsítványok letölthetők és a felhasználó kliens-alkalmazásába installálhatók.

6.1.6. Kulcs méretek, használt algoritmusok

A Szolgáltató Hitelesítő Központja elektronikus aláírás létrehozására az RSA[11] algoritmust használja. Az Előfizetői tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

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

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

[11] 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.

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

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

6.1.7. Kulcs felhasználási célok

A Szolgáltató Előfizetők részére kulcspárt illetőleg Tanúsítványt elektronikus aláírási céllal bocsát ki.

Ennek érdekében az Előfizetők részére kibocsátott tanúsítványok egyes attribútumaira felhasználási területtől és céltól függően kialakított beállításokat alkalmaz.

A kulcspár kizárólag arra a célra használható, amelyre a Szolgáltató kibocsátotta.

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

6.2. Az aláírás-létrehozó adat védelme

A Szolgáltató gondoskodik valamennyi általa (saját maga, regisztráló szervezet, az Aláírók számára) előállított magánkulcs titkosságáról és sértetlenségéről.

A Szolgáltató külön aláíró magánkulcsot használ Tanúsítvány aláírásra, és Tanúsítvány visszavonási lista aláírásra, egyúttal ezen kulcsokat semmilyen más célra nem használja.

A Szolgáltató a tanúsítványokat, illetve a tanúsítvány visszavonási listákat aláíró magánkulcsait fizikailag biztonságos helyszínen használja.

6.2.1. A több-szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése

A Szolgáltatónál legalább a Hitelesítő Központban alkalmazni kell az „n-ből m” ellenőrzést.

6.2.2. Aláírás-létrehozó adat letét, mentés, archiválás

Szolgáltató nem nyújthat aláírás-létrehozó adat letét szolgáltatást. Szolgáltató az Előfizető aláírás-létrehozó adatát semmilyen formában nem mentheti vagy archiválhatja; annak előállítására, visszafejtésére alkalmas programot, adatot nem tárolhat.

6.2.3. Aláírás-létrehozó adat aktiválása

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

6.2.4. Aláírás-létrehozó adat deaktiválása

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

6.2.5. 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 archivált 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:

Produktív CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
Előfizetői aláíró kulcs és tanúsítvány érvényessége:	1 év

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

6.4. Aktivizáló adatok (PIN kódok)

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

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

Az Előfizető bármikor megváltoztathatja PIN kódját.

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

A PIN kód elvesztése, elfelejtése vagy illetéktelen kezekbe történő jutása esetén minden esetben új PIN kódot kell előállítani, amely esetenként új aláírás-létrehozó adat illetve tanúsítvány előállítását is feltételezi.

6.5. Számítógép biztonsági szabályok

6.5.1. Számítógép biztonság technikai követelményei

A Számítógép biztonság technikai követelményeit a MeH ITB 12. ajánlás szerinti fokozott biztonsági osztálybasorolás határozza meg.

A Szolgáltató gondoskodnia kell arról, hogy az informatikai rendszeréhez való hozzáférés kellően felhatalmazott egyénekre legyen korlátozva. Különösképpen:

1. A Szolgáltató védi rendszerei és információi sértetlenségét vírusok, káros és engedély nélküli szoftverek ellen.
2. A Szolgáltató biztonságosan kezeli adathordozó eszközeit a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.
3. A Szolgáltató gondoskodik a felhasználói[12] hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.
4. A Szolgáltató gondoskodik arról, hogy az információhoz és az alkalmazói rendszer funkciókhoz történő hozzáférés, a hozzáférés ellenőrzési szabályzatnak megfelelően korlátozott legyen, és hogy a hitelesítés-szolgáltató rendszere megfelelő számítógép-biztonsági ellenőrzéseket nyújtson a hitelesítés-szolgáltató szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében, beleértve a biztonsági adminisztrátori és üzemeltetési funkció elkülönítését. Különösképpen a rendszer szolgáltatási programok használatát korlátozza és ellenőrzi szigorúan.
5. A Szolgáltató gondoskodik arról, hogy személyzetét sikeresen azonosítsák és hitelesítsék, mielőtt a tanúsítvány gondozásával kapcsolatos kritikus alkalmazásokat használhatnák.
6. A Szolgáltató eljárásokat dolgoztat ki és hajtat végre valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására.
7. A Szolgáltató műszaki óvintézkedéseket juttat érvényre (például tűzfalak[13] segítségével), hogy a hitelesítés-szolgáltató belső hálózati tartományai védettek legyenek a harmadik felek számára elérhető külső hálózati tartományoktól.
8. A Szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.
9. A Szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni és regisztrálni az erőforrásaihoz való jogosulatlan és/vagy szabálytalan hozzáférési kísérleteket, valamint képes legyen ezekre időben reagálni[14].

[12] A felhasználó fogalma itt felöleli a rendszer operátorokat, rendszer adminisztrátorokat és bármely olyan felhasználót, akinek közvetlen hozzáférése van a rendszerhez.

[13] Ajánlott, hogy a tűzfalakat úgy konfigurálják, hogy azok a hitelesítés-szolgáltató működéséhez nem szükséges protokollokat és hozzáféréseket kiiktassák.

10. A Szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.
11. A Szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ (hálózatról történő) módosítására vonatkozóan.
12. A Szolgáltató gondoskodik arról, hogy az érzékeny adatokat[15] megvédjék az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.
13. A Szolgáltató biztosítja a személyzet tevékenységéért való felelősségre vonhatóságát.16

6.6. Életciklus technikai szabályok

6.6.1. Rendszerfejlesztési szabályok

A Szolgáltató gondoskodik arról, hogy az általa, illetve a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény-meghatározási fázisban figyelembe vegyék, annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

A Szolgáltató konfiguráció kezelési eljárásokat alkalmaz valamennyi működő szoftvere esetében a kibocsátásokra, a módosításokra és a sürgős szoftver javításokra vonatkozóan.

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

6.6.2. Biztonságkezelési szabályok

A Szolgáltató olyan eszközöket és eljárásokat alkalmaz, melyek garantálják a kritikus szolgáltatásait megvalósító megbízható informatikai rendszereire az operációs rendszer beállítások, valamint a hálózati konfiguráció biztonságát, egyúttal az alkalmazott biztonsági mechanizmusok sértetlenségének, helyes működésének ellenőrzését.

A biztonságkezelési szabályok a Szolgáltató társasági szintű Informatikai biztonságpolitikája, valamint a társasági és a rendszer szintűi biztonsági szabályzatok tartalmazzák.

6.7. Hálózati biztonsági szabályok

A Szolgáltató gondoskodik arról, hogy informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerüljön sor. Az érzékeny adatokat megvédi, amikor azok átvitele nem biztonságos hálózatokon keresztül történik.

A regisztrálással kapcsolatosan:

1. A regisztrációs adatok bizalmasságát és sértetlenségét megvédik, különösen az Előfizetővel/Aláíróval folytatott külső, illetve a Szolgáltató egyes komponensei közötti belső adatcsere során.
2. A Szolgáltató (a hitelesítő szervezeten keresztül) ellenőrzéssel biztosítja, hogy regisztrációs adatokat csak általa elismert, azonosságában hitelesített regisztrációs szolgáltatókkal cserél.

A tanúsítvány előállítással és visszavonás kezeléssel kapcsolatosan:

3. A Szolgáltató gondoskodik arról, hogy a helyi hálózati komponensek fizikailag biztonságos környezetben legyenek és konfigurációikat időszakonként auditálják.
4. A Szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni, regisztrálni az erőforrásaihoz a hálózatról történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre.

A tanúsítvány kibocsátásával kapcsolatosan:

5. A Szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.

A tanúsítvány visszavonás kezeléssel kapcsolatosan:

[14] A hitelesítés-szolgáltató erre használhat például egy behatolás észlelő rendszert, vagy hozzáférés ellenőrzést felügyelő és riasztási eszközöket.

[15] Az érzékeny adatok közé tartoznak a regisztrációs információk is.

[16] Például az eseménynapló megőrzésén keresztül.

6. A Szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ hálózatról történő módosítására vonatkozóan.

6.8. Kriptográfiai modul ellenőrzése

A Szolgáltató gondoskodik a kriptográfiai hardver biztonságáról annak teljes élettartama alatt. Különösképpen gondoskodik arról, hogy:

1. a Tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert ne manipulálhassák szállítás közben,
2. a Tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálhassák tárolás közben,
3. a Szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktivizálása, mentése és visszaállítása legalább két bizalmi munkakört betöltő alkalmazott együttes jelenlétét kívánja meg,
4. a Tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardver helyesen működik,
5. a Szolgáltató kriptográfiai hardverén tárolt szolgáltatói magán aláíró kulcsokat az eszköz visszavonásakor megsemmisítik.

7. Tanúsítvány és tanúsítvány-visszavonási profil

A Szolgáltató által kibocsátott tanúsítványok megfelelnek az RFC 2527 szabványban leírt X. 509 3-as verziójú tanúsítványoknak.

7.1. Tanúsítvány profil

7.1.1. Alap mezők

A Szolgáltató által kibocsátott előfizetői tanúsítványok alap mezői a következő minta alapján kerülnek kitöltésre:

Mezőnév	Szabály
Verzió Version	Szolgáltató az RFC 2459-nek megfelelő tanúsítványokat bocsát ki. Az Előfizető és Érintett fél által alkalmazott eljárásoknak és alkalmazásoknak támogatnia kell az ilyen típusú tanúsítványok helyes kezelését. Szolgáltató a kibocsátott tanúsítványok „Version” mezőjébe V3 értéket ír.
Sorozatszám Serial Number	A kibocsátó hitelesítő szervezeten belül egyedi szám 12 karakter hosszúságú.
Algoritmus azonosító Signature Algorithm Identifier	Szolgáltató tanúsítványt hitelesítő elektronikus aláírásának algoritmus azonosítója..
Aláírás Signature	Szolgáltató tanúsítványt hitelesítő elektronikus aláírása az RFC 2459 szerint generálva és kódolva.
Kibocsátó Issuer	A tanúsítványt kibocsátó hitelesítő szervezet és egység egyedi azonosítója egyedi X.500 név formátumot szerint, UTF8String formátumban.
Érvényesség Valid From & Valid To	A tanúsítvány érvényességének kezdete és vége. UCT szerinti érték, az RFC 2459 szerinti kódolással.
Tulajdonosazonosító Subject	A Tulajdonos egyedi neve egyedi X.500 név formátumot szerint, UTF8String formátumban.
Tulajdonos nyilvános kulcsának algoritmus azonosítója Subject Public Key Algorithm Identifier	A Tulajdonos nyilvános kulcs algoritmusának azonosítója.
Tulajdonos nyilvános kulcsa Subject Public Key Value	A Tulajdonos nyilvános kulcsa.
Kibocsátó egyedi azonosító Issuer Unique Identifier	Nem kitöltött.
Tulajdonos egyedi azonosítója Subject Unique Identifier	Nem kitöltött.

7.1.2. Tanúsítvány kiterjesztések

A Szolgáltató az ITU-T X.509 ajánlás 3. verziójának megfelelő tanúsítvány kiterjesztéseket támogatja. Például:

Mezőnév	Szabály	Kritikus
Tanúsítvány-típusok Certificate Policies	PolicyIdentifier [17] PolicyQualifier UserNotice	IGEN
Alapvető megkötések Basic Constraints	Subject type = End Entity Path Length Constraint = None	Nem
Kulcshasználat Key Usage		IGEN
Kulcshasználat kiterjesztés[18]		IGEN

[17] Ide kerül a hivatkozott tanúsítványtípus azonosítója

Mezőnév	Szabály	Kritikus
Key Usage		
CRL szétosztási pont CRL Distribution Points		IGEN
ETSI Tranzakciós limit OID:0.4.0.1862.1.2		IGEN

A szabályzat kiterjesztés 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 által kibocsátott visszavonási listák alap mezői a következők lehetnek:

Mezőnév	Érték vagy szabály
Verzió Version	A visszavonási lista a ITU X.509 ajánlás 2. verziójának felel meg.
Algoritmus azonosító Signature Algorithm Identifier	Szolgáltató visszavonási listát hitelesítő elektronikus aláírásának algoritmus azonosítója: sha1RSA (OID=1.2.840.113549.1.1.5).
Aláírás Signature	Szolgáltató visszavonási listát hitelesítő elektronikus aláírása, RFC 2459 szerint generálva és kódolva.
Kibocsátó Issuer	A visszavonási listát kibocsátó hitelesítő szervezet egyedi azonosítója.
Hatályba lépés Effective Date	A visszavonási lista hatályba lépésének kezdete. A Szolgáltató által kibocsátott tanúsítványok esetében ez megegyezik a kibocsátás idejével. UCT szerinti érték, RFC 2459 szerinti kódolással.
Következő kibocsátás Next Update	A következő visszavonási lista kibocsátásának ideje. UCT szerinti érték, RFC 2459 szerinti kódolással.
Visszavont tanúsítványok Revoked Certificates	A visszavont tanúsítványok listája a tanúsítvány sorozatszámával és a visszavonás idejével.

7.2.1. „Tanúsítvány visszavonási lista” és „Tanúsítvány visszavonási lista bejegyzési” kiterjesztések

A Szolgáltató által használt visszavonás bejegyzési kiterjesztések a következők lehetnek:

Mezőnév	**Érték vagy szabály**	**Kritikus**
Visszavonás oka reasonCode	A visszavonás oka	IGEN
Érvénytelenség ideje Invalidity Date	A magánkulcs megbízhatatlanná válásának ideje	IGEN
Útmutató old Instruction	A felfüggesztett tanúsítvány kezelése	Nem

A Szolgáltató a nem kritikus kiterjesztéseket nem köteles kitölteni.

[18] Csak azonosítás-hitelesítés célú felhasználás esetén kell megadni.

A Szolgáltató által kitöltött visszavonási lista kiterjesztések a következők:

Mezőnév	Érték vagy szabály	Kritikus
CRL sorozatszám *CRL number*	A visszavonási lista egyesével növekvő sorozatszáma	IGEN

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

8. HR-NMT adminisztráció

8.1. A HR-NMT változáskezelés

A Szolgáltató egy felülvizsgálati folyamatot határoz meg, mely kiterjed a HR-NMT gondozására is.

8.2. Közzétételi és tájékoztatási elvek

A Szolgáltató az általa támogatott HR-NMT-t és egyéb más fontos dokumentációját az előfizetők és az érintett felek rendelkezésére bocsátja, a tanúsítványtípusnak való megfelelés felméréséhez szükséges mértékig.

A Szolgáltató a tanúsítvány használatával kapcsolatos kikötéseit és feltételeit az összes előfizető és potenciális érintett fél számára megismerhetővé teszi.

8.3. HR-NMT elfogadási eljárások

A HR-NMT formailag megfelel az RFC 2527 szabványnak.

A Szolgáltató jóváhagyás előtt megvizsgálja a HR-NMT előző pontokban meghatározott követelményeknek való megfelelőségét.

A HR-NMT jóváhagyására a Szolgáltató felsőszintű irányító testülete rendelkezik végső hatáskörrel és felelősséggel.

A HR-NMT törvényeknek való megfelelőségét a Nemzeti Hírközlési Hatóság is vizsgálja.

Módosítás esetén a Szolgáltató a HR-NMT változtatásokkal egybeszerkesztett új verziójának tervezetét hatósági felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Hírközlési Hatóságnak. Az új verzió hatályba léptetésének feltétele, hogy azt a Nemzeti Hírközlési Hatóság nyilvántartásba vegye.

9. Hivatkozások és Meghatározások

9.1. Hivatkozások

A Szolgáltató hivatkozott dokumentumai:

A MÁV INFORMATIKA Kft. Szervezeti és Működési Szabályzata

A MÁV INFORMATIKA Kft. Iratkezelési Szabályzata

A MÁV INFORMATIKA Kft. Titokvédelmi Szabályzata

A MÁV INFORMATIKA Kft. Informatikai Biztonságpolitikája

A MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata

Szolgáltatási Szabályzat fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatáshoz (HSZSZ-F))

Általános Szerződési Feltételek fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatáshoz (ÁSZF-F)

A PKI Szolgáltatások Biztonsági Szabályzata

A PKI 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 elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ

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

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

Biztonsági tisztviselő, biztonsági menedzser: a hitelesítés-szolgáltatás biztonságáért, 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 elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával

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

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

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

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

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

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes

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

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

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

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

a) alkalmas az aláíró azonosítására,

b) egyedülállóan az aláíróhoz köthető,

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

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

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

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

Igénylő: a 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

Rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását 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 aláírás-ellenőrző adatot az Eat. 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget

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

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

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