NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

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

Verziószám	**1.1**
OID szám	**0.2.216.1.200.1100.100.42.3.2.7.1.1**
Hatályba lépés dátuma	**2013.10.01.**
Hatósági nyilvántartásba vétel száma	**EF/50690-5/2013**
Dokumentum besorolása	**Publikus**

Változáskövetés

Ver-zió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2013.08.01.	Első változat	Pándi Boglárka Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.1	2013.09.02.	Audit észrevételei alapján módosított változat	Kővári Ferenc	Bódi Antal	Ferencz Attila

TARTALOMJEGYZÉK

1. Bevezetés

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban Szolgáltató) fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó Hitelesítési Rend (továbbiakban HR-NMT).

A fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatások (továbbiakban: Szolgáltatások) keretében Szolgáltató a 2001. évi XXXV. számú, elektronikus aláírásról szóló 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

Jelen Hitelesítési Rend a Szolgáltatások keretében kibocsátott tanúsítványok kezelésére (előállítás, kibocsátás, közzététel, megújítás, felfüggesztés, újraérvényesítés, visszavonás) vonatkozó követelményeket, a tanúsítványok tartalmának és érvényességének ellenőrzési eljárásait és a Szolgáltatások működtetésének követelményeit tartalmazza.

A Szolgáltató a Szolgáltatásokat a vele szerződéses viszonyban álló ügyfelek (Előfizetők illetve Aláírók) részére nyújtja, és egyes szolgáltatás elemeket hozzáférhetővé tesz az elektronikus aláírások hitelességét ellenőrző Érintett felek részére is.

1.1. Szolgáltató adatai

Jelen dokumentum szerint kibocsátott tanúsítványokkal kapcsolatos Szolgáltatásokat a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban Szolgáltató) nyújtja.

A Szolgáltató általános adatait, valamint a Szolgáltatásokért illetékes szervezetének, az Ügyfélkapcsolati Irodának elérhetőségét, nyitva tartását, a Szolgáltatóval való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a NISZ Zrt. „Szolgáltatási Szabályzat fokozott biztonságú elektronikus alárás-hitelesítés szolgáltatáshoz” c. szabályzata (továbbiakban HSZSZ-F) tartalmazza.

1.2. Áttekintés

1.2.1. A Hitelesítési Rend célja

A HR-NMT egy olyan szabálygyűjtemény, mely egy tanúsítványtípus 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 az aláírás létrehozó eszköz használatát nem megkövetelő, közigazgatásban nem használható, nyilvános körben kibocsátott nem-minősített, azaz fokozott biztonságú elektronikus aláíráshoz kapcsolódó tanúsítványokra [rövidítve: NMT] vonatkoznak.

Ezen tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat a Szolgáltató HSZSZ-F dokumentuma tartalmazza.

1.2.2. Jogszabályok, szabványok

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

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

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 Média- és 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.

A hitelesítési rend szerkezetére és tartalmára vonatkozóan:

RFC 2527 illetve 3647 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány és szolgáltatási szabályzat keretrendszer)

A tanúsítványok és visszavonási listák szerkezetére, tartalmára vonatkozóan:

International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer” ajánlás 3-as verziója.

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

Az informatikai biztonsági követelményekre vonatkozóan:

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

MeH ITB 12. ajánlása

A kriptográfiai modulra vonatkozóan:

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

1.3. Hitelesítési rend azonosítása

Jelen dokumentum teles neve: NISZ Zrt.„Hitelesítési Rend nyilvános körben kibocsátott nem minősített tanúsítványokra”

A dokumentum rövid neve: HR-NMT.

A dokumentum objektum azonosítója és verziószáma a címlapon található.

A dokumentum hatósági nyilvántartásba vételi száma: a címlapon található.

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

1.4. Felhasználó közösség, alkalmazhatóság

1.4.1. A Szolgáltató regisztrációs szervezete

A Szolgáltató – saját szervezetén belül – ügyfélkapcsolati és regisztrációs irodát működtet.

Az Ügyfélkapcsolati Iroda elvégzi az igénylők illetve Előfizetők adatainak felvételét, az igénylők személyazonosságának megállapítását, a tanúsítvány kérelmek összeállítását, és gondoskodik az elkészült aláírás létrehozó adatok illetve eszközök szétosztásáról, valamint az előfizetői szerződésben foglaltak teljesítéséről.

A Regisztrációs Iroda biztosítja az igénylők illetve Előfizetők technikai regisztrációját, a tanúsítványok előállításának, felfüggesztésének és visszavonásának jóváhagyását és kezelését, valamint az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezését.

A Szolgáltató saját szervezetén kívüli regisztrációs szervezeteket is működtethet, a vele szerződéses alapon együttműködő Társaságokkal (mint szerződött közreműködők) együtt. Ezen regisztrációs szervezetek elvégzik a saját igénylőik és előfizetőik adatainak rögzítését, ellenőrzését, az igénylők személyazonosságának megállapítását, a tanúsítvány kérelmek összeállítását és Szolgáltatóhoz történő továbbítását. Biztosítják a tanúsítványok és az aláírás létrehozó eszközök szétosztását, a tanúsítvány kibocsátását és visszavonását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

1.4.2. A Szolgáltató hitelesítő szervezete

A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítő központokból, a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, az ezt körülvevő 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 regisztrációs szervezettől érkező kiadási, megújítási, felfüggesztési, újraérvényesítési és visszavonási igényeknek a végrehajtása, a tanúsítványok állapotára vonatkozó információk előállítása és közlése, valamint a szolgáltatást támogató informatikai rendszer üzemeltetése.

1.4.3. Hitelesítési Rend és Szabályozási Csoport

A Hitelesítési Rend és Szabályozási Csoport a Szolgáltató által létrehozott virtuális szervezeti egység, amely a hitelesítés szolgáltatással kapcsolatos hitelesítési rendek, szolgáltatási szabályzatok és belső szabályzatok kialakításáért, ellenőrzéséért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős.

1.4.4. Előfizetők és Aláírók

Előfizető a Szolgáltatóval szerződéses viszonyban álló szervezet, amely megrendeli a Szolgáltatótól a Szolgáltatásokat, a vele kapcsolatban álló illetve a képviseletében eljáró Aláírók számára.

Aláíró az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult, valamint az a szervezet, amely az aláírás-létrehozó eszközt birtokolja, és akinek a nevé-

ben az őt képviselő természetes személy az elektronikus aláírást az elektronikus dokumentumon elhelyezi, valamint aki meghatározza, hogy a nevében jogszabályban meghatározott feltételeknek megfelelő informatikai eszköz elektronikus aláírást elektronikusan dokumentumon elhelyezzen.

1.4.5. 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.

1.4.6. Alkalmazhatóság

1.4.6.1. A hitelesítési rend hatálya

A hitelesítési rend személyi hatálya a Szolgáltatóra, annak a szolgáltatásban közreműködő munkatársaira és a felhasználói közösségre terjed ki (Előfizetők, Aláírók, Érintett felek).

A hitelesítési rend tárgyi hatálya kiterjed az 1. pontban meghatározott szolgáltatásokra, az 1.2.1 pontban meghatározott tanúsítványokra, valamint a Szolgáltatónak a hitelesítés szolgáltatással kapcsolatban álló összes objektumára és tárgyi eszközére.

1.4.6.2. Tanúsítványok alkalmazhatósága

Engedélyezett alkalmazási lehetőségek

Az előfizetői tanúsítványokhoz kapcsolódó magánkulcsok kizárólag elektronikus aláírások megtételére használhatók. A magánkulcsokhoz tartozó nyilvános kulcsok és tanúsítványok az elektronikus aláírások ellenőrzésére használhatók fel.

Korlátozott alkalmazási lehetőségek

Az előfizetői tanúsítványok használatával kapcsolatban Szolgáltató pénzügyi korlátozásokat szabhat meg, amelyeket a kibocsátott tanúsítványokban is fel kell tüntetni.

Tiltott alkalmazási lehetőségek

Az előfizetői tanúsítványok titkosításra vagy authentikációra történő felhasználása, más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen hitelesítés szolgáltatás nyújtásához történő alkalmazása tilos.

1.5. Tanúsítvány fajták és jellemzőik

1.5.1. Tanúsítvány fajták

A jelen hitelesítési rend szerinti tanúsítványok felhasználási területe és célja szerint Szolgáltató megkülönböztet:

- előfizetői,
- szolgáltatói, és
- teszt tanúsítványokat.

Előfizetői tanúsítvány a Szolgáltatóval szerződéses viszonyban álló Előfizető (illetve a vele kapcsolatban álló Aláírók) számára kibocsátott tanúsítvány (végfelhasználói tanúsítvány).

Szolgáltatói tanúsítvány a Szolgáltató által saját célra illetve a Szolgáltatások nyújtásához kapcsolódóan kibocsátott tanúsítvány; Előfizető ezeket nem igényelheti.

Teszt tanúsítvány a Szolgáltató által kizárólag tesztelési célokból kiadott tanúsítvány.

Jelen hitelesítési rendben foglaltak az előfizetői tanúsítványokra vonatkoznak, kivéve, ahol a szövegben a szolgáltatói, vagy a teszt tanúsítványokra való konkrét utalás található.

A tanúsítványok tulajdonosa (alanya) alapján a Szolgáltató megkülönböztet:

- „személyes” tanúsítványokat
- „munkatársi” tanúsítványokat
- „szervezeti vagy eszköz” tanúsítványokat

Személyes tanúsítvány esetén az Aláíró olyan természetes személy, aki magánszemélyként kerül regisztrálásra és ennek megfelelően kerül feltüntetésre a tanúsítványban, Magánszemély a Szolgáltatótól közvetlenül nem igényelhet tanúsítványt.

Munkatársi tanúsítvány esetén az Aláíró olyan természetes személy, aki egy szervezethez tartozik és azt képviseli valamilyen minőségben (jellemzően Előfizető munkavállalójaként), és ennek megfelelően kerül regisztrálásra illetve feltüntetésre a tanúsítványban.

Szervezeti vagy eszköz tanúsítvány esetében az Aláíró nem természetes személy, hanem egy szervezet, vagy általa működtetett eszköz (gépi aláírás esetén), amely ennek megfelelően kerül regisztrálásra illetve feltüntetésre a tanúsítványban.

Az egyes tanúsítvány fajtákra vonatkozó további részleteket a Szolgáltató HSZSZ-F dokumentuma tartalmazza.

1.5.2. Tanúsítványok jellemzői

Jelen hitelesítési rend az 1.2.1 pontnak megfelelően az aláírás létrehozó eszköz használatát nem megkövetelő, közigazgatásban nem alkalmazható, nyilvános körben kibocsátott nem-minősített, azaz fokozott biztonságú elektronikus aláíráshoz kapcsolódó tanúsítványokra [NMT] vonatkozik. Ezek olyan tanúsítványok, amelyek:

- megfelelnek az Eat. vonatkozó előírásainak
- olyan Szolgáltató adta ki, amely szerepel az illetékes hatóság (Nemzeti Média- és Hírközlési Hatóság - NMHH) nyilvántartásában
- nyilvános körben került kibocsátásra.

Az előfizetői tanúsítványoknak tartalmazniuk kell az alábbiakat:

- a Szolgáltató és székhelyének (ország-) azonosítóját
- az Aláíró nevét (vagy egy álnevét, ennek jelzésével)
- a tanúsítvány szándékolt felhasználásától függően az Aláíró speciális jellemzőit
- az Aláíró által birtokolt aláírás-létrehozó adatnak megfelelő aláírás-ellenőrző adatot
- a tanúsítvány érvényességi idejének kezdetét és végét,
- a tanúsítvány azonosító kódját
- a tanúsítványt kibocsátó Szolgáltató fokozott biztonságú elektronikus aláírását
- a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat
- a tanúsítvány felhasználásának korlátjait, (beleértve a kötelezettségvállalás korlátait is)
- szervezet képviseletére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minőségét és a képviselt szervezet azonosító adatait.

Szolgáltató által kibocsátott előfizetői tanúsítványok érvényességi ideje 2 év, de ettől rövidebb is lehet (1 év), mely esetben az időtartamot az előfizetői szerződésben rögzíteni kell.

2. Általános rendelkezések

2.1. Feladatok és hatáskörök

2.1.1. A Szolgáltató feladatai és hatásköre

1. Szolgáltatónak az 1. fejezetben meghatározott Szolgáltatások nyújtása során általánosságban az alábbi szolgáltatás elemeket kell biztosítania:
   - regisztráció
   - tanúsítvány előállítás
   - tanúsítvány kiadás és szétosztás
   - visszavonás kezelés (ebben felfüggesztés és újraérvényesítés biztosítása)
   - visszavonási állapot közzététele
   - aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése
2. A Szolgáltatónak gondoskodnia kell a hitelesítés-szolgáltatásra vonatkozó valamennyi, a jelen hitelesítési rendben részletezett állítás teljesüléséről, amennyiben azok az adott tanúsítványra alkalmazhatók.
3. A Szolgáltatónak szolgáltatásait nyilvánosan elérhetővé kell tenni.
4. A Szolgáltató jogi személy.
5. A Szolgáltató köteles rendszeresen felülvizsgálni és újra kiadni a jelen hitelesítési rendet és a kapcsolódó szolgáltatási szabályzatát (HSZSZ-F).
6. Tanúsítvány előállítás és kiadás csak az igénylők illetve Előfizetők által szolgáltatott és a Regisztrációs Szervezet által ellenőrzött adatok alapján történhet. A Szolgáltató a tanúsítvány kibocsátását követően a tanúsítvány adataiban nem változtathat.
7. A Szolgáltató köteles Tanúsítványtárában közzétenni az általa kibocsátott előfizetői tanúsítványokat, továbbá köteles a tanúsítvány állapotára vonatkozó nyilvántartásokat (tanúsítvány visszavonási listákat) hozzáférhetővé tenni.
8. A Szolgáltató köteles a hiánytalan igénybejelentés és megrendelés esetén a regisztrációt követő napokban, de legkésőbb 30 munkanapon belül a tanúsítvány kiadásáról intézkedni és erről az Előfizetőt vagy az Aláírót értesíteni.
9. A Szolgáltatónak a szolgáltatások működtetése és menedzselése során ügyfélkapcsolati tevékenységet kell biztosítania.
10. A Szolgáltatónak az Internetes honlapján keresztül bárki számára folyamatosan elérhetővé kell tenni a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó szolgáltatási szabályzatát (HSZSZ-F) valamint általános szerződési feltételeit (ÁSZF-PKI).
11. A Szolgáltató a lejárat előtt értesítést küld a lejáró tanúsítványokról az Előfizető vagy az Aláíró részére.
12. Szolgáltató a tanúsítványban köteles feltüntetni az Előfizetői Szerződésben rögzített, a tanúsítvány felhasználhatóságával kapcsolatos korlátozásokat.
13. A Szolgáltató közzétételi kötelezettség mellett felfüggesztheti vagy visszavonhatja a tanúsítványt, ha azt a 4.4.1 fejezetben részletezett körülmények ezt indokolják
14. Szolgáltató köteles megőrizni a tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetőleg – amennyiben ezen időszakban az elektronikus aláírással vagy az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is köteles biztosítani, amellyel a kibocsátott tanúsítványok tartalma megállapítható.
15. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről legalább hatvan nappal korábban köteles értesíteni az Előfizetőket és az illetékes hatóságot (NMHH). 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.
16. A Szolgáltató intézkedni köteles az iránt, hogy legkésőbb a tevékenysége befejezésekor más - vele legalább azonos besorolású - szolgáltató átvegye nyilvántartásait, így különösen a visszavont tanúsítványok nyilvántartását, valamint ellássa a hatályos jogszabályokban foglalt feladatokat. A Szolgáltató a visszavont tanúsítványokkal kapcsolatos minden adatot - beleértve a személyes adatokat is – köteles átadni ezen szolgáltatónak.

2.1.1.1. A Hitelesítő Szervezet feladatai és hatásköre

A Szolgáltató hitelesítő szervezetének, illetve az általa működtetett hitelesítő központoknak a feladata általánosságban a tanúsítványok előállítása és a visszavonási listák aláírásával közreműködés a visszavonási állapot közzétételében.

A tanúsítványok előállítása során a hitelesítő központok aláírják a tanúsítvány adatokat és gondoskodnak 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 a hitelesítő központok fogadják a visszavonási kérelmeket, új tanúsítvány visszavonási listát készítenek és azt aláírásukkal hitelesítik.

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

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

A 2. szintű „Produktív CA" hitelesítő központ alapvető feladata és hatásköre a Szolgáltató regisztrációs szervezete által regisztrált Előfizetők tanúsítványainak hitelesítése:

1. Saját szolgáltatói kulcspár generálása és magánkulcsának fokozott biztonságú védelme.
2. A Regisztrációs szervezettől kapott hitelesítési kérelmek fogadása és ellenőrzése.
3. Előfizetői kulcspár generálás és tanúsítvány előállítás, előfizetői tanúsítványok publikálása
4. Regisztrációs Irodától érkező tanúsítvány visszavonási, felfüggesztési, újraérvényesítési és tanúsítvány megújítási kérelmek feldolgozása, és tanúsítvány visszavonási listák publikálása.
5. online tanúsítvány-állapot szolgáltatás (OCSP – Online Certificate Status Protocol) nyújtása, ennek keretében a szabványos kérések fogadása és az OCSP válaszok megadása

2.1.1.2. A Regisztrációs Iroda feladatai és hatásköre

A Regisztrációs Iroda feladata általánosságban az igénylők illetve Előfizetők technikai regisztrációja, tanúsítványok előállításának, felfüggesztésének és visszavonásának jóváhagyása és kezelése, valamint az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése. Ezen belül a Regisztrációs Iroda feladatai tételesen a következők:

1. elvégzi a tanúsítvány kibocsátásához szükséges ellenőrzéseket, nem-megfelelőség esetén a tanúsítvány igényt visszautasítja, megfelelőség esetén elindítja a tanúsítvány kibocsátást a hitelesítő központ felé
2. fogadja a hitelesítő központtól kapott előfizetői tanúsítványokat és ellenőrzi azok hitelességét és sértetlenségét,
3. kezdeményezi a tanúsítványok elküldését a Tanúsítványtárba
4. igény esetén 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 illetve a kapcsolódó tanúsítványt az Ügyfélkapcsolati Irodához,
7. biztonságos módon megsemmisíti az előállított magánkulcs aláírás-létrehozó eszközön kívüli összes példányát, miután az Aláíró részére előállított kulcspárt átadta,
8. formai szempontból ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy újraérvényesítésére vonatkozó kérelmek hitelességét és érvényességét, végrehajtja a szabályos 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 fő feladata általánosságban az igénylők illetve Előfizetők adatainak felvétele, az igénylők személyazonosságának megállapítása, a tanúsítvány kérelmek összeállítása és az előfizetői szerződésben foglaltak biztosítása. Ezen belül az Ügyfélkapcsolati Iroda feladatai tételesen a következők:

1. gondoskodik az igénylők és Előfizetők megfelelő tájékoztatásáról az igények fogadásáról
2. ellenőrzi a 3 pontban előírt adatszolgáltatási követelmények szerint megadott adatok alapján az igénylő és Előfizető adatait
3. rögzíti a tanúsítványba kerülő adatokat, ellenőrzi az igényléshez átadott dokumentumok valódiságát, érvényességét, sértetlenségét és hitelességét,

4. előkészíti az Előfizetői Szerződést
5. előkészíti a Szolgáltatások díjainak a számlázását ,
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 adat illetve aláírás-létrehozó eszköz és a PIN boríték biztonságos kezeléséről és átadásáról,
9. tájékoztatja az Előfizetőt vagy Aláírót tanúsítványa lejáratát megelőzően legalább 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.
12. fogadja a tanúsítvány visszavonásra, felfüggesztésre, vagy újraérvényesítésre vonatkozó kérelmeket és ellenőrzi a kérelmező jogosultságát,
13. visszautasítja (az ok megjelölésével) a jogosulatlan vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy újraérvényesítésre vonatkozó kérelmeket,
14. a kérelem elfogadása után intézkedik a tanúsítvány visszavonásáról (felfüggesztéséről, vagy újraérvényesítéséről) az előírt időn belül,
15. tájékoztatja a visszavont tanúsítvány tulajdonosát tanúsítványa állapotának változásáról.

2.1.1.4. A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Rend és Szabályozási Csoport fő feladata a szolgáltatásokkal kapcsolatos hitelesítési rendek, szolgáltatási szabályzatok és belső szabályzatok kezelése. Hatáskörébe tartozik a Szolgáltató és a felhasználói 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 keresztül folyamatosan (napi 24 órában) fogadja, és a felfüggesztési kérelmeket végrehajtja.

2.1.2. Az Előfizető és Aláíró feladatai és hatásköre

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

1. önmagát az Ügyfélkapcsolati Irodán hiteles okmányokkal igazolni,
2. a tanúsítvány igénylését és magánkulcsának felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse,
3. a tanúsítvány igénylés és regisztráció során valós adatokat megadni,
4. biztosítani az aláírás-létrehozó eszközének és adatának, valamint a PIN kódjának védelmét,
5. három munkanapon belül jelezni Szolgáltatónál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a tanúsítványba foglalt adatokra,
6. az aláírás-létrehozó adatát jelen hitelesítési rendben és az előfizetői szerződésben rögzített korlátozásoknak megfelelően használni,
7. 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. 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.
9. kompromittálódás esetén a magánkulcsának használatát azonnal és véglegesen megszakítani,
10. a tanúsítvánnyal ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról haladéktalanul tájékoztatni a Szolgáltatót,
11. az Aláíró jogosult arra, hogy a magánkulcsot birtokolja és a jogszabályokban meghatározott módon elektronikus aláíráshoz felhasználja,

Előfizető köteles:

1. szervezeti adatait az Ügyfélkapcsolati Irodán hiteles okmányokkal igazolni
2. a tanúsítvány igénylés és regisztráció során valós adatokat megadni, harmadik fél jogainak megsértése nélkül
3. három munkanapon belül jelezni Szolgáltatónál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a tanúsítványba foglalt adatokra
4. azonnal intézkedni a vele kapcsolatban álló Aláírók tanúsítványainak 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
5. tájékoztatni a Szolgáltatót az aláírással vagy az elektronikusan aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt - a szolgáltatási szabályzatban (HSZSZ-F) meghatározott – rendellenességről, valamint a tanúsítvánnyal ellátott elektronikusan aláírt elektronikus dokumentummal kapcsolatos jogvita megindulásáról.
6. a Szolgáltatások díjait az előfizetői szerződésben foglaltak szerint megfizetni Szolgáltató számára

2.1.3. Az Érintett félre vonatkozó ajánlások

Az Érintett félnek ajánlott a Szolgáltató szabályzataiban leírtaknak megfelelően a legnagyobb gondossággal eljárni az elektronikus aláírás és a tanúsítvány érvényességének 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 (HR-NMT, HSZSZ-F, ÁSZF-PKI),
3. különösen ajánlott az elektronikus aláírás ellenőrzését elvégeznie az Aláíró tanúsítványának segítségével, meggyőződve az üzenet eredetiségéről és az aláírás valódiságáról,
4. ajánlott egyértelműen meggyőződnie a tanúsítványban feltüntetett azonosító és egyéb adatok alapján, illetve a törvényesen rendelkezésre álló módszerek segítségével az Aláíró személyéről,
5. a tanúsítvány érvényességét illetve hatályosságát indokolt ellenőriznie a tanúsítványban,
6. ajánlott elvégeznie a teljes tanúsítási lánc ellenőrzését az alábbiak szerint:
   6.1. meggyőződni a Kibocsátó kilétéről a tanúsítvány kibocsátójának azonosítója alapján;
   6.2. meggyőződni az Aláíró tanúsítványának integritásáról a Szolgáltató (Kibocsátó) tanúsítványának segítségével;
   6.3. indokolt ellenőriznie a tanúsítvány állapotát a tanúsítvány visszavonási listák (CRL) áttanulmányozásával vagy OCSP szolgáltatás igénybevételével;
   6.4. ajánlott tanulmányoznia a tanúsítvány összes attribútumát, és az adott tranzakcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni az aláírás elfogadásáról,
7. ajánlott visszautasítani az elektronikus aláírás elfogadását, ha az elektronikus aláírás, az Aláíró tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata annak érvénytelenségére utal, illetve ha az az adott kontextusban nem elfogadható; az aláírás elfogadása nem jelentheti az aláírt üzenet tartalmának tudomásul vételét vagy elfogadását,
8. Az OCSP választ aláíró kulcs tanúsítványának az Érintett fél által történő ellenőrzésére vonatkozóan általában érvényesek a fentiekben leírt, a tanúsítvány és a tanúsítási lánc ellenőrzésre vonatkozó szabályok.
9. Egy OCSP válasszal ellátott állomány átvétele után az Érintett félnek ajánlott ellenőriznie a Szolgáltató általi aláírás megtörténtét, az Szolgáltató OCSP választ aláíró kulcsához tartozó tanúsítvány érvényességét a Visszavont Tanúsítványok Listája segítségével a fentiekben leírt módon
10. 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 le-

het 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 szolgáltatási szabályzatban (HSZSZ-F), az általános szerződési feltételekben (ÁSZF-PKI) 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 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. 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.

2.2.2. Előfizető és az Aláíró felelőssége

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

Az Előfizetőnek és az Aláírónak 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 Aláíró a magánkulcsát nem a szolgáltatási szabályzatban és a vonatkozó jogszabályokban meghatározott módon és célra használta.

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

Az OCSP választ kérő fél felelős az OCSP válaszon található elektronikus aláírás helyességének és az OCSP választ aláíró kulcs tanúsítványa érvényességének az ellenőrzésért

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.

Aláíró felelősséget visel és tudomásul veszi, hogy a magánkulcsával készített elektronikus aláírás a saját elektronikus aláírásának minősül, és viseli ennek jogkövetkezményeit.

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 (ÁSZF-PKI) kell rendelkezni.

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

2.4. Értelmezés és alkalmazás

2.4.1. Irányadó jog

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

A Szolgáltató tevékenységére elsősorban az 1.2.2 pontban felsorolt jogszabályok mérvadók.

Ezeken túlmenően a Szolgáltatónak az üzleti titkok vonatkozásában a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény szerint, a személyes adatok vonatkozásban az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) szerint kell eljárni.

Szolgáltató figyelembe veszi még az Európai Parlament és Európa Tanács az elektronikus aláírások közösségi programjáról szóló 1999/93/EK irányelvét is.

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 személyi és tárgyi hatályát az 1.4.6.1 pont tartalmazza.

A hitelesítési rend időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és határozatlan időre szól. Időbeli hatálya megszűnik a szolgáltatási tevékenység beszüntetésekor, illetve egy újabb verzió hatályba lépésével. A hitelesítés rend módosítását a vonatkozó jogszabályok szerint 30 nappal előzetesen be kell jelenteni az illetékes hatóság (NMHH) részére nyilvántartásba vétel céljából.

2.4.2.2. Megszűnés

A hitelesítési rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

2.4.2.3. Értesítések

A Szolgáltató az Aláírókat, Előfizetőket és Érintett feleket a Szolgáltatások internetes honlapján történő közzétellel, illetve az Ügyfélkapcsolati Irodában elérhető dokumentumokkal tájékoztatja. Az Ügyfélkapcsolati Iroda az Előfizetőket és Aláírókat esetenként írásban vagy elektronikus úton is értesítheti.

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. Az írásban vagy elektronikus úton történő kommunikáció esetében a feladó nevét és elérhetőségét fel kell tüntetni és a feladónak a küldeményt hitelesítenie kell.

2.4.3. Vitás kérdések kezelése

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

Panaszt az Ügyfélkapcsolati Irodán lehet írásban vagy szóban előterjeszteni. A panaszt a Szolgáltató köteles az előterjesztéstől számított 15 munkanapon belül kivizsgálni és ennek eredményéről a panaszost írásban tájékoztatni.

A jogviták esetén követendő eljárást az általános szerződési feltételekbe (ÁSZF-PKI) kell foglalni.

2.5. Díjak

A Szolgáltató jogosult önálló üzletpolitikát kialakítani és Szolgáltatásaiért díjat szedni. A díjazására vonatkozó információkat a szolgáltatási szabályzat tartalmazza. A 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 előfizetői és szolgáltatói tanúsítványok, a tanúsítványokkal kapcsolatos szabályzatok, a tanúsítványok felfüggesztett vagy visszavont állapotára vonatkozó

információk, valamint az egyéb közérdekű szolgáltatói információk az Előfizetők, Aláírók és az Érintett felek részére folyamatosan rendelkezésre álljanak.

A Szolgáltatónak a szolgáltatói információkat a Szolgáltatások Internetes honlapján keresztül kell elérhetővé tennie. Szolgáltatónak csak saját elektronikus aláírásával ellátott szabályzatai tekinthetők hitelesnek. A honlapról letöltött dokumentumok nyomtatott változatai semmilyen formában sem tekinthetők hivatalos példánynak.

2.6.2. A közzététel gyakorisága

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

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

A Szolgáltató a Visszavont Tanúsítványok listáját a visszavonást (vagy felfüggesztést, illetve az újraérvényesítést) követő 60 percen belül köteles közzétenni.

A Szolgáltató a Tanúsítvány visszavonási listát (CRL - Certificate Revocation List) legfeljebb 24 óránként frissíti, azaz, két CRL megjelenése közötti idő nem haladhatja meg a 24 órát.

2.6.3. Elérési szabályok

A Szolgáltató minden Aláíró, Előfizető és Érintett fél számára köteles elérhetővé tenni a Szolgáltatások Internetes honlapját, a szolgáltatási információk közzététele céljából.

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 és tanúsítvány visszavonási lista

A Szolgáltató az általa kibocsátott előfizetői tanúsítványokat Tanúsítványtárban tárolja és a Szolgáltatások Internetes honlapján teszi hozzáférhetővé. A Szolgáltató keresési lehetőséget biztosíthat a Tanúsítványtárban az Aláíró illetve Előfizető tanúsítványban foglalt adatai alapján.

A Szolgáltató a tanúsítványok felfüggesztett vagy visszavont állapotára vonatkozó információkat a Szolgáltatások Internetes honlapján a visszavont tanúsítványok listája (CRL – Certificate Revocation List) révén teszi hozzáférhetővé. Ezen felül egy adott tanúsítvány állapotára vonatkozó információt Szolgáltató az OCSP szolgáltatása keretében is hozzáférhetővé teszi.

2.7. A megfelelőség vizsgálata

Szolgáltatónak megfelelőségi vizsgálatokat és ellenőrzéseket kell elvégeznie illetve elvégeztetnie annak érdekében, hogy a Szolgáltatásaival kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljenek a vonatkozó jogszabályi és szakmai követelményeknek.

2.7.1. Vizsgálatok gyakorisága

A megfelelőségi vizsgálatokat a szolgáltatási tevékenység kezdetekor el kell végezni, és évente meg kell ismételni. A vizsgálatokat a jogszabályi feltételek vagy Szolgáltatásokban bekövetkezett jelentősebb változások alkalmával is el kell végezni.

2.7.2. Az átvizsgáló szervezet és a vizsgált fél kapcsolata

A Szolgáltató megfelelőségi vizsgálatai lehetnek külső vagy belső ellenőrzések illetve auditok.

A vizsgálatokat végző szervezeteknek, személyeknek függetlennek kell lenniük a Szolgáltató Szolgáltatásokért felelős szervezeti egységétől.

A vizsgálatokat csak megfelelő szakmai ismeretek birtokában lévő, tapasztalt szakemberek végezhetik.

2.7.3. A vizsgálatok kiterjedése

A megfelelőségi vizsgálatoknak ki kell terjedniük az alábbiakra:

- dokumentálás és folyamatok megfelelősége, adatvédelem
- a személyi állomány ellenőrzése
- eszközök, termékek megfelelősége
- fizikai környezet és szolgáltatói rendszerek biztonsága

2.7.4. Hiányosságok kezelése

A vizsgálatok során feltárt hiányosságok kezelésére és megszüntetésére Szolgáltatónak eljárásokat kell kialakítania, és ezeket a szolgáltatási szabályzatában (HSZSZ-F) ismertetnie kell.

2.8. Bizalmasság – Adatkezelési elvek

Szolgáltatónak gondoskodnia kell a jogszabályoknak való megfelelésről. Ennek keretén belül:

- a felvett adatokat és a fontos bejegyzéseket védenie kell az elveszéstől, tönkretételtől és hamisítástól. A jogszabályoknak való megfelelés, valamint az alapvető üzleti tevékenységek támogatása érdekében szükség van bizonyos bejegyzések biztonságos megőrzésére is.
- biztosítania kell az adatvédelmi törvényeknek való megfelelést
- megfelelő technikai és szervezeti intézkedéseket kell hoznia a személyes adatok felhatalmazás nélküli, illetve törvénytelen kezelése ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen,
- gondoskodnia kell az Aláíróra vonatkozó adatok és információk bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk hozzájárulnak, vagy ha bíróság illetve jogszabály ezt előírja

2.8.1. Bizalmas információk

Szolgáltató bizalmas információként kell kezelje az Aláírók valamint Előfizetők (tanúsítványba foglalt adatai kivételével) minden olyan adatát, amely nem nyilvános adat. Szolgáltató ezen kívül bizalmas információként kezelje a következő adatokat és dokumentumokat:

- magánkulcsok és aktivizáló kódok,
- tanúsítványigénylések és szerződések,
- tranzakciós és napló adatok,
- nem nyilvános szabályzatok, illetve minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

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 illetve OCSP szolgáltatás keretében teszi közzé.

A Szolgáltató a tanúsítvány visszavonás okát a vonatkozó szakmai ajánlásoknak megfelelően fel kell tüntesse a visszavonási listában. Ezen kívül a visszavonással kapcsolatos minden egyéb információt, adatot bizalmasan kell kezeljen.

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 Aláírók 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.) bekezdése 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 regisztráció során:

a. gondoskodnia kell arról, hogy az igénylők illetve Előfizetők tanúsítvány kérelmei illetve megrendelései 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[1] X.500 ajánlásának.

3.1.2. Nevek szemantikája

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

A tanúsítványban szereplő adatok magyar írásmód szerint, a magyar ABC írásjeleit felhasználva, speciális és vezérlő karakterek nélkül kerüljenek 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) valódi nevek kell legyenek, de lehetnek álnevek is Előfizető erre vonatkozó kifejezett igénye alapján. Ez utóbbi esetben az álnevet a tanúsítványban jelezni kell.

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

3.1.3. Nevek egyedisége

A Szolgáltató köteles biztosítani tanúsítványokban használt megkülönböztető nevek (DN) egyediségét. Erről elsődlegesen az Aláíró nevének valamint egy Szolgáltató által alkalmazott egyedi azonosítónak a „Tulajdonos" mezőben való szerepeltetésével kell gondoskodnia. A megkülönböztető nevek egyediségére Aláíró email címe is felhasználható, a „Tulajdonos alternatív neve" mezőben való szerepeltetéssel.

3.1.4. Név igénylési viták feloldása

Szolgáltatónak a név igénylési viták feloldásával kapcsolatos eljárását a szolgáltatási szabályzatában (HSZSZ-F) ismertetnie kell.

3.1.5. Védjegyek elismerésének és hitelesítésének módszere

Szolgáltatónak a védjegyek elismerésével és hitelesítésével kapcsolatos eljárását a szolgáltatási szabályzatában (HSZSZ-F) ismertetnie kell.

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 Szolgáltatások keretében és a Szolgáltató által kell történjen, kiemelt biztonságú környezetben. Erre tekintettel az aláírás-létrehozó adat és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán az aláírás-létrehozó adat illetve az aláírás-létrehozó eszköz átvételének igazolása szükséges. Az aláírás-létrehozó adat illetve aláírás-létrehozó eszköz átvételénél az Előfizető aláírásával igazolja ezek valamint a kapcsolódó aktivizáló adat (PIN kód) átvételét.

3.1.7. Személyazonosság megállapítása

A tanúsítványok igénylésekor az Előfizető részéről eljáró természetes személy igénylőt (munkatársi tanúsítvány esetén az Aláírót, szervezeti vagy eszköz tanúsítvány esetén a kapcsolattartót) az Eat. 12. § értelmében a Szolgáltató köteles ellenőrizni illetve a személyazonosságát megállapítani.

A személyazonosság megállapításához nincs szükség személyes megjelenésre, az történhet személyazonosító igazolvány, útlevél, gépjármű vezetői engedély vagy egyéb, személyazonosításra alkalmas okmány alapján, melyek adatait a regisztrációs űrlap tartalmazza.

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

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

A személyazonosság hitelesítésének eljárását Szolgáltatónak a szolgáltatási szabályzatában (HSZSZ-F) kell ismertetnie.

3.1.8. Szervezeti azonosság és hovatartozás megállapítása

Az tanúsítványok igénylésekor a személyazonosság megállapításán túl az Előfizető (mint képviselt szervezet) azonosítását is el kell végezni, mivel a szervezet adatai is bekerülnek a tanúsítványba.

Igazolni kell azt is, hogy az Előfizető részéről eljáró természetes személy valóban az Előfizető szervezetéhez tartozik illetve hogy jogosult a szervezet nevében az adott tanúsítványt igényelni.

A szervezet azonosítása történhet 30 napnál nem régebbi cégkivonat vagy – nem gazdasági társaság esetén – egyéb hivatalos szervezeti dokumentum alapján. A szervezethez tartozás illetve az igénylési jogosultság a szervezet erre vonatkozó nyilatkozata és a hivatalos képviselő aláírási címpéldánya alapján igazolható.

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

A szervezet azonosításának eljárását Szolgáltatónak a szolgáltatási szabályzatban (HSZSZ-F) kell ismertetnie.

3.1.9. Eszköz azonosság megállapítása

Amennyiben az Aláíró nem természetes személy hanem egy szervezet vagy általa működtetett eszköz, a tanúsítvány igénylésekor, az Előfizető részéről eljáró természetes személynek (kapcsolattartónak) valamint a szervezetnek az azonosítása mellett szükséges az Előfizető írásos nyilatkozata is az eszköz megnevezéséről valamint hozzájárulásáról ahhoz, hogy a kapcsolattartó jogosult a szervezet nevében az adott tanúsítványt igényelni.

A tanúsítvány megrendelés nem fogadható el, ha az azonosítás-hitelesítés vagy az azt követő ellenőrzések során a kapcsolattartónak vagy az eszköznek az Előfizetőhöz tartozásával kapcsolatban kétség merül fel.

3.2. Érvényes tanúsítvány megújítása

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

Tanúsítvány megújítás 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 vagy az Aláíró írásban nyilatkozik.

A Szolgáltató az Előfizető vagy Aláíró 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 lehetőségéről a lejárat előtt értesítést küldhet az Előfizetőnek vagy Aláírónak.

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 illetve a 4.4.5 pontban rögzíti a tanúsítványok visszavonásának illetve felfüggesztésének azonosítására és hitelesítésére vonatkozó követelményeket.

4. A működésre vonatkozó követelmények

4.1. Tanúsítványigénylés

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

Tanúsítvány igényléséhez ki kell tölteni egy Szolgáltató által erre a célra rendszeresített regisztrációs űrlapot és le kell folytatni a szolgáltatási szabályzatban részletezett regisztrációs eljárást. Az űrlap igényelhető az Ügyfélkapcsolati Irodánál, vagy letölthető a Szolgáltatások 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. A regisztrációs űrlap aláírásával a tanúsítványigénylő hozzájárul a szolgáltatások során felhasznált adatoknak a Szolgáltató által történő nyilvántartásba vételéhez, tanúsítványa és az azzal kapcsolatos állapot információk szolgáltatói tanúsítványtárban való közzétételéhez, s ezen adatok harmadik félhez történő továbbításához a Szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb, jogszabályok által meghatározott esetekben.

Az Előfizető illetőleg igénylő 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 dokumentumokat és az azok érvényességével kapcsolatos esetleges korlátozásokat.

4.2. Tanúsítvány kibocsátás

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

Az elkészült tanúsítványt az Aláíró vagy Előfizető kijelölt kapcsolattartója személyesen átveszi az Ügyfélkapcsolati Irodán.

Megújított tanúsítvány esetén az elkészült tanúsítványt Aláíró vagy Előfizető kijelölt kapcsolattartója letölti a Szolgáltató Tanúsítványtárából.

4.3. Tanúsítvány elfogadás

A tanúsítvány elfogadása az Aláíró vagy Előfizető kijelölt kapcsolattartója részéről az átvétellel történik meg.

Az aláírás-létrehozó adat használatba vétele előtt az Aláírónak illetve Előfizető kijelölt kapcsolattartójának kötelessége ellenőrizni a tanúsítványban feltüntetett adatok 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. Ennek keretében a tanúsítvány visszavonási és felfüggesztési kérelmeket köteles feldolgozni és az állapotváltozást valamint a visszavonási információkat köteles közzétenni az előírások szerinti időn belül.

Az erre vonatkozó részletes eljárásrendet Szolgáltatónak a szolgáltatási szabályzatában (HSZSZ-F) ismertetnie kell.

4.4.1. Visszavonáshoz/felfüggesztéshez vezető körülmények

A Szolgáltatónak a szolgáltatási szabályzatában (HSZSZ-F) ismertetnie kell, hogy a 2001. / XXXV. számú, elektronikus aláírásról szóló törvényben (Eat), felsorolt eseteken túl milyen körülmények között lehet, illetve kell visszavonási illetve felfüggesztési kérelmet benyújtani.

4.4.2. Visszavonás/felfüggesztés kérelmezése

Tanúsítvány visszavonását/felfüggesztését az Aláíró, az Előfizető vagy annak regisztráció során nyilvántartásba vett kapcsolattartója, a Szolgáltató, vagy hatósági szervezet kezdeményezheti.

Az Előfizetőnek, Aláírónak és a Szolgáltatónak kötelessége, harmadik félnek joga az előző (4.4.1) pontban feltűntetett jogszabály alapján és annak megfelelően a visszavonás azonnali kezdeményezése.

4.4.3. Visszavonási eljárás

Visszavonási igényt levélben vagy személyesen kell benyújtani Szolgáltató részére

Szolgáltatónak ellenőriznie kell a kérelmező jogosultságát, valamint a kérelemben foglalt tanúsítvány adatait, és meg kell állapítani a visszavonási okát.

Ha a visszavonási okok megalapozottak és az ellenőrzések sikeresek, a Szolgáltató el kell végezze a tanúsítvány visszavonását és ezt közzé kell tegye a visszavont tanúsítványok listájában.

Szolgáltatónak a visszavonás megtörténtéről vagy visszautasításáról értesítenie kell az Aláírót, az Előfizetőt illetve a visszavonás kérelmezőjét.

Tanúsítvány visszamenőleges visszavonása nem megengedett. Szolgáltató a már egyszer végérvényesen visszavont tanúsítvány érvényességét nem állíthatja vissza érvényesre.

4.4.4. Visszavonási kérelemre vonatkozó türelmi idő és felelősségi szabályok

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 szabad felhasználni.

A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok:

a. A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig és elfogadásáig az Előfizető illetve Aláíró 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 egy adott tanúsítvány érvénytelenségére utaló információ, nem hagyatkozhat kizárólag a visszavont tanúsítványok listában 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 5 naptári napig lehet.

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

Ha a felfüggesztésről a Szolgáltató határozott, akkor 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 Aláíró, Előfizető vagy annak a regisztráció során nyilvántartásba vett kapcsolattartója 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. A visszavont tanúsítványok listájának közzétételében az eseti szolgáltatás kiesés nem haladhatja meg a 24 órát, a közzététel rendelkezésre állása 99 %.

4.4.8. Visszavont Tanúsítványok Listája ellenőrzése

A Visszavont Tanúsítványok Listájának ellenőrzése az Érintett felek felelőssége a tanúsítványok elfogadását megelőzően. A tanúsítványokhoz tartozó visszavonási lista elérhetőségét Szolgáltatónak a tanúsítványban szerepeltetnie kell. 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 visszavont tanúsítványok listájában a Szolgáltató által közzétett érvénytelen, vagy felfüggesztett tanúsítvány elfogadásából keletkező bárminemű kár Érintett felet terheli.

4.4.9. Visszavonási állapot közlés más formái

A visszavont tanúsítványok listája mellett Szolgáltató online tanúsítvány-állapot szolgáltatást (OCSP – Online Certificate Status Protocol) is nyújt jelen hitelesítési rend szerint kiadott tanúsítványaihoz.

Az OCSP szolgáltatás részleteit Szolgáltató szolgáltatási szabályzata (HSZSZ-F) tartalmazza.

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-szolgáltatását támogató informatikai rendszerének biztonsági naplózását és annak ellenőrzését belső biztonsági szabályzatban kell részletezni. A Szolgáltatónak biztosítania kell a regisztrációs információk, a hitelesítés-szolgáltató kulcsok kezelésére, valamint a tanúsítványok kezelésére vonatkozó fontosabb információk naplózását, oly módon, hogy:

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

b. A Szolgáltató biztosítsa 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 szabályzata rögzíti.

A regisztrációval kapcsolatosan:

- A Szolgáltató gondoskodik arról, hogy naplózásra kerüljön a regisztrációval kapcsolatos valamennyi lényeges 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[2:]

- 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 tanúsítványokra vonatkozó minden lényeges információ megfelelő ideig rögzítésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

4.5.4. Az adatok megőrzési időtartama

A Szolgáltató a tanúsítványokra vonatkozó 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 fenn kell tartsa a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét.

A Szolgáltató a fontos bejegyzéseket meg kell védje az elveszéstől, tönkretételtől és hamisítástól.

A Szolgáltató megfelelő műszaki és szervezeti intézkedéseket kell foganatosítson 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 Média- és Hírközlési Hatóságot és lehetőségei szerint a felhasználó Közösség tagjait.

4.6.2. Hardver, szoftver, vagy adatsérülés esete

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

4.7. Hitelesítés-szolgáltatói 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 Média- és Hírközlési Hatóságot és a Szolgáltatások internetes honlapján tájékoztatnia kell a felhasználói közösség tagjait

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

b. meg kell szűntetnie a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások (amennyiben vannak) 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.

A 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 személyi és fizikai biztonság követelményeit.

A következő pontok csak a vonatkozó lényeges követelményeket tartalmazzák.

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, aláírás létrehozó eszköz megszemélyesítéssel és a visszavonás kezeléssel kapcsolatosan a Szolgáltatónak megfelelő biztonsági környezet 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, úgymint fizikai hozzáférés szabályozás, a természeti katasztrófa elleni védelem, a villámvédelem és tűzbiztonság tényezőivel, a támogató eszközök (ezen belül az áram és klíma berendezések) meghibásodásával, vízvezeték szivárgással, lopás, betörés és behatolás elleni védelem.

5.2. Eljárásrendi szabályozások

A Szolgáltatónak gondoskodnia kell 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 belső biztonsági szabályzatának eljárásaival.

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

5.3. Humán szabályozások

5.3.1. Bizalmi munkakörök

A Szolgáltatónak egyértelműen azonosítania kell azokat a munkaköröket, amelyektől a hitelesítés-szolgáltatás biztonsága függ. Ezeket a bizalmi munkaköröket és felelősségeket belső leírásokban dokumentálni kell.

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

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 Szolgáltató felső vezetősége kell kinevezze a hitelesítés-szolgáltató munkatársait.

A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia a Szolgáltatóval.

5.3.2. Az egyes feladatokhoz szükséges személyzeti létszámok

A Szolgáltató bizalmi 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 Szolgáltató bizalmi munkaköröket betöltő 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 Szolgáltatónak be kell tartani a vonatkozó jogszabályi (3/2005. IHM rendelet szerinti) kizárásokat.

5.3.5. Személyzetre vonatkozó előírások

A Szolgáltatónak gondoskodnia kell arról, hogy személyzeti gyakorlata fokozza és támogassa a Szolgáltatások működésének megbízhatóságát.

5.3.6. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A Szolgáltató a bizalmi munkakörökben olyan személyzetet foglalkoztathat, amely rendelkezik a nyújtott Szolgáltatásokhoz szükséges képzettséggel, gyakorlattal, és megfelelt a Szolgáltató által lefolytatott biztonsági ellenőrzéseken.

5.3.7. Előélet vizsgálatára vonatkozó eljárások

A Szolgáltatónak nem szabad bizalmi munkakörbe olyan személyt kinevezni, aki bűncselekményért, illetve más olyan vétségért el lett ítélve, amely az illető alkalmasságát befolyásolja. A munkatársak nem szabad ellássanak biztonsági feladatokat mindaddig, amíg a személyükre és alkalmasságukra vonatkozó ellenőrzések végrehajtása meg nem történik.

5.3.8. Képzési 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. a hitelesítés szolgáltatás jogi következményeiről,

e. a Hitelesítési Rend és a Szolgáltatási Szabályzat alkalmazásának jelentőségéről

f. a rendszer használatáról és az informatikai biztonsági követelményekről,

A képzést vagy annak elemeit meg kell ismételni minden lényeges, 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 termékeket használ a tanúsítványok előállításához illetve a Szolgáltatások nyújtásához.

6.1. Kulcspár előállítás és telepítés

6.1.1. Kulcspár előállítás

A Szolgáltató maga kell előállítsa a kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat), fizikailag védett környezetben. A kulcspárok generálását olyan algoritmussal végezheti, melyet jogszabály illetve az illetékes hatóság (NMHH) határozata erre a célra alkalmasnak jelöl.

A Szolgáltató nem fogadhat el Előfizető által generált kulcspárt.

Az aláírás-létrehozó adat aláírás-létrehozó eszközön (pl.: chipkártyán) történő elhelyezésére a Szolgáltató csak tanúsítvány kibocsátással együtt vállalkozhat.

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

6.1.2. Aláírás-létrehozó eszköz megszemélyesítés

Amennyiben az Előfizető aláírás-létrehozó eszköz (pl. chip kártya) alapú tanúsítványt igényelt, az eszköz megszemélyesítését a Szolgáltató fizikailag védett környezetben üzemelő kártya-megszemélyesítő rendszeren kell végezze.

A Szolgáltató az aláírás-létrehozó adat illetve az aláírás-létrehozó eszköz aktivizálásához PIN kódot kell biztosítson. A PIN kódot fizikailag védett környezetben kell előállítania és a kódot tartalmazó PIN-borítékot az aláírás-létrehozó eszköztől elkülönítve kell tárolnia.

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

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

A Szolgáltató az aláírás-létrehozó adatot illetve eszközt és a PIN kódot tartalmazó borítékot személyesen adja át az Aláírónak vagy az Előfizető kapcsolattartójának.

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) a tanúsítványba foglalva a Szolgáltatások internetes honlapján levő 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 Szolgáltatások internetes honlapján keresztül mindenki számára elérhetővé tenni.

6.1.6. Kulcs méretek, használt algoritmusok

A Szolgáltató a Szolgáltatások nyújtása során – mind a szolgáltatói, mind pedig az előfizetői kulcsok, algoritmusok és paraméterek tekintetében - az illetékes hatóság (NMHH) vonatkozó határozatának megfelelő szabványos kulcsméreteket és algoritmuskészletet kell használjon. Az alkalmazott kulcsméreteket és algoritmus készletet a Szolgáltató szolgáltatási szabályzata tartalmazza.

6.1.7. Kulcs felhasználási célok

A Szolgáltató jelen hitelesítési rend szerinti előfizetői tanúsítványokhoz előállított kulcsokat kizárólag elektronikus aláírási célra bocsát ki.

A szolgáltatói magánkulcsok használati célja kizárólag tanúsítványok, visszavonási listák illetve OCSP válaszok aláírása.

6.2. Az aláírás-létrehozó adat védelme

A Szolgáltatónak gondoskodnia kell valamennyi általa (saját maga, az Aláírók számára) előállított magánkulcs titkosságáról és sértetlenségéről.

A Szolgáltató külön aláíró magánkulcsot kell használjon a tanúsítványok és a visszavonási listák aláírására, és ezt a kulcsot semmilyen más célra nem használja fel.

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 Aláíró illetve 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 aláírás-létrehozó adat aktiválása az Aláíró vagy Előfizető kijelölt felhasználója által történhet a Szolgáltatótól kapott PIN kód megadásával, azokban az esetekben, amikor az aláírás-létrehozó adat használatára szükség van. A szolgáltatói magánkulcs aktiválása hasonlóan jelszóval vagy PIN-kóddal történhet, az erre kijelölt bizalmi munkaköröket betöltő személyek által.

6.2.4. Aláírás-létrehozó adat deaktiválása

Az előfizetői aláírás-létrehozó adatok deaktiválása az Aláíró vagy Előfizető kijelölt felhasználója által történhet, az aláíró alkalmazásból való kijelentkezéskor, vagy – pl. chipkártya esetén – amikor az Aláíró az aláírás-létrehozó eszközt eltávolítja az olvasóból. A szolgáltatói magánkulcs deaktiválása az aláíró tevékenység vagy alkalmazás leállításával történhet, az erre kijelölt bizalmi munkaköröket betöltő személyek által.

6.2.5. Aláírás-létrehozó adat megsemmisítése

Az előfizetői tanúsítvány lejárta után az aláírás-létrehozó adat fizikai megsemmisítését az Aláírónak saját felelősségi körében kell elvégezni úgy, 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

A Szolgáltató köteles minden általa előállított és kibocsátott aláírás-ellenőrző adatot az adott tanúsítványba foglalva megőrizni illetve 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:

Root CA aláíró kulcs és tanúsítvány érvényessége:	20 év
OCSP válasz egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 30 nap
Produktív CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
Előfizetői aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 2 év

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

6.4. Aktivizáló adatok (PIN kódok)

Az aláírás-létrehozó adatok illetve eszközök aktivizáló adatait (PIN kódjait) a Szolgáltató biztonságos körülmények között, véletlenszám generátor segítségével kell előállítsa.

A Szolgáltató a PIN kódokat műszaki és szervezési intézkedésekkel kell megvédje, és kizárólag az Aláíró illetve Előfizető kapcsolattartója részére adhatja át, személyesen, az aláírás-létrehozó eszköztől elkülönítve. Az átvételt követően az Előfizetőnek saját felelősségi körében kell biztosítania PIN kód kizárólagos birtoklását.

Az Előfizető bármikor megváltoztathatja PIN kódját.

6.5. Informatikai biztonsági előírások

6.5.1. Számítógép biztonsági követelmények

A Szolgáltatónak olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technológiákat kell kialakítania és üzemeltetnie, amelyek biztosítják a Szolgáltató megbízható működését a Szolgáltatások nyújtásához. Ennek ismertetését Szolgáltató részben a nyilvános szolgáltatási szabályzatában (HSZSZ-F), részben a belső szabályzataiban írja le.

6.6. Életciklus technikai szabályok

6.6.1. Rendszerfejlesztési szabályok

A Szolgáltatónak gondoskodnia kell 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 kell alkalmazzon valamennyi működő szoftvere esetében a kibocsátásokra, a módosításokra és a sürgős szoftver javításokra vonatkozóan.

6.6.2. Biztonságkezelési szabályok

A Szolgáltató olyan eszközöket és eljárásokat kell alkalmazzon, 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.

6.7. Hálózati biztonsági szabályok

A Szolgáltatónak gondoskodnia kell arról, hogy informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerüljön sor. Az érzékeny adatokat meg kell védeni, amikor azok átvitele nem biztonságos hálózatokon keresztül történik.

6.8. Kriptográfiai modul ellenőrzése

A Szolgáltatónak gondoskodnia kell a kriptográfiai hardver modul biztonságáról annak teljes élettartama alatt.

7. Tanúsítvány, CRL és OCSP profil

7.1. Tanúsítvány profil

A Szolgáltató által kibocsátott tanúsítványok feleljenek meg az RFC 3280 ajánlásban leírt X. 509 3-as verziójú tanúsítványoknak. A további információkat a Szolgáltató szolgáltatási szabályzata (HSZSZ-F) tartalmazza.

7.2. Tanúsítvány-visszavonási profil

A Szolgáltató által kibocsátott tanúsítványok visszavonási listák feleljenek meg az RFC 3280 ajánlásban leírt X. 509 2-es verziójú tanúsítvány visszavonási listáknak. A további információkat a Szolgáltató szolgáltatási szabályzata (HSZSZ-F) tartalmazza.

7.3. Online tanúsítvány-állapot szolgáltatás (OCSP) profil

A Szolgáltató szolgáltatási szabályzata (HSZSZ-F) tartalmazza.

8. Hitelesítési Rend adminisztráció

8.1. Változáskezelés

A Szolgáltatónak felülvizsgálati folyamatot kell meghatároznia, a szervezetén belül mely kiterjed a HR-NMT gondozására is.

8.2. Közzétételi és tájékoztatási elvek

A Szolgáltató jelen HR-NMT-t és egyéb kapcsolódó dokumentumait az Aláírók, Előfizetők és az Érintett felek rendelkezésére kell bocsássa, a tanúsítványtípusnak való megfelelés felméréséhez szükséges mértékig.

A Szolgáltató a tanúsítvány használatával kapcsolatos kikötéseit és feltételeit az Aláírók, Előfizetők és Érintett felek számára megismerhetővé teszi.

8.3. HR-NMT elfogadási eljárások

A HR-NMT jóváhagyása előtt Szolgáltató meg kell vizsgálja a hitelesítési rend tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és szakmai ajánlások – különösképpen az RFC 3647 - tekintetében.

A HR-NMT ellenőrzésére illetve jóváhagyására a Szolgáltató belső szervezete illetve a Szolgáltatásokért felelős vezetője rendelkezik hatáskörrel és felelősséggel.

A HR-NMT jogszabályoknak való megfelelőségét a Nemzeti Média- és Hírközlési Hatóság is ellenőrzi.

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

9. Hivatkozások

A Szolgáltató hivatkozott dokumentumai:

A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Szervezeti és Működési Szabályzata

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. PKI szolgáltatások Informatikai Biztonságpolitikája (PKI-IBP)

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. PKI szolgáltatások Biztonsági Szabályzata (PKI-IBSZ)

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt Szolgáltatási Szabályzat fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatásokhoz (HSZSZ-F))

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt Általános Szerződési Feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI)

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt PKI szolgáltatások Üzletmenet-folytonossági terve (PKI-BCP/-DRP)