NISZ
NEMZETI INFOKOMMUNIKÁCIÓS SZOLGÁLTATÓ ZRT.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

Hitelesítési Rend titkosító és egyéb nem aláírás célú tanúsítványokra (HR-TET)

Verziószám	**1.2**
OID szám	**0.2.216.1.200.1100.100.42.3.5.9.1.2**
Hatályba lépés dátuma	**2014.05.14.**
Dokumentum besorolása	**Publikus**

Változáskövetés

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2013.08.01.	Első változat	Kővári Ferenc Joláthy Dániel	Kővári Ferenc	Ferencz Attila
1.1	2014.03.17.	CAB BR követelmények szerint módosított változat	Kővári Ferenc Joláthy Dániel	Kővári Ferenc	Ferencz Attila
1.2	2014.05.14.	Jogi hivatkozásokkal és pontosításokkal módosított változat	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila

TARTALOMJEGYZÉK

1. Bevezetés

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban Szolgáltató) kormányzati hitelesítés szolgáltatása keretében kiadott titkosító és egyéb nem aláírás célú tanúsítványokra vonatkozó Hitelesítési Rend (továbbiakban HR-TET).

A nem-aláírás célú tanúsítványok kiadásával kapcsolatban Szolgáltató a következő szolgáltatásokat nyújtja:

a. tanúsítványok kiadása

b. aláírás-létrehozó eszközön a magánkulcs elhelyezése (igény esetén)

c. kulcsletét (igény esetén, kizárólag titkosító tanúsítvány kiadás keretében)

A fenti szolgáltatások az a) és b) pont tekintetében hasonlóak a vonatkozó jogszabály[1] szerinti elektronikus aláírás hitelesítés szolgáltatáshoz, illetve a magánkulcs elhelyezése aláírás létrehozó eszközön szolgáltatáshoz, melyeket Szolgáltató szintén nyújt. Ezért a fenti szolgáltatásokat Szolgáltató a vonatkozó jogszabály szerinti szolgáltatásokkal azonos műszaki környezetben, azonos eszközökkel, folyamatokkal és eljárásrend alkalmazásával nyújtja.

Jelen Hitelesítési Rendben „Szolgáltatások" kifejezés alatt a tanúsítvány kiadást, illetve annak a b) és c) pont szerinti szolgáltatásokkal való értelemszerű kombinációját kell érteni. A b) és c) pont szerinti szolgáltatásokat Szolgáltató csak az a) pont szerinti szolgáltatással együtt nyújtja.

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, az aláírás-létrehozó eszközön a kulcs elhelyezésre, valamit a kulcsletétre vonatkozóan is.

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

1.1. Szolgáltató adatai

Jelen dokumentum szerint kibocsátott tanúsítványokkal kapcsolatos Szolgáltatásokat a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (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 nem aláírás célú tanúsítvány szolgáltatásokhoz" c. szabályzata (továbbiakban HSZSZ-T) tartalmazza.

1.2. Áttekintés

1.2.1. A Hitelesítési Rend célja

A HR-TET egy olyan szabálygyűjtemény, mely a nem aláírás célú tanúsítványtípusok felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazás számára, valamint rögzíti azokat a követelményeket, amelyeket a Szolgáltatónak ezen tanúsítványok kibocsátása során teljesítenie kell.

Jelen dokumentumban a követelmények a nyilvános körben kibocsátott, titkosító és egyéb nem aláírás célú (SSL szerver authentikációs, SSL kliens authentikációs, kód/üzenet aláíró) tanúsítványokra [rövidítve: TET] vonatkoznak.

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

1.2.2. Jogszabályok, szabványok, ajánlások

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

84/2012. (IV.21) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

83/2012 (IV.21) Korm. rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról

[1] 2001. évi XXXV. törvény az elektronikus aláírásról

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

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[2],

MeH ITB 12. ajánlása

A kriptográfiai modulra vonatkozóan:

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

Az SSL szerver tanúsítványok kiadására vonatkozóan:

A CA Browser Fórum Baseline Requirements aktuális dokumentuma

1.3. Hitelesítési rend azonosítása

Jelen dokumentum teles neve: NISZ Zrt.„Hitelesítési Rend titkosító és egyéb nem aláírás célú tanúsítványokra”

A dokumentum rövid neve: HR-TET.

A dokumentum objektum azonosítója és verziószáma a címlapon található.

Jelen HR-TET-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 tanúsítványok, a kapcsolódó magánkulcsok illetve aláírás létrehozó 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, az aláírás-létrehozó eszközön a magán kulcs elhelyezését, valamint a kulcsletét szolgáltatást a hitelesítő szervezettel együttműködve.

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, a kapcsolódó magánkulcsok illetve az aláírás létrehozó eszközök szétosztását, a tanúsítvány kibocsátását és visszavonását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el. Ezen külső regisztrációs szervezetek SSL szerver tanúsítványokkal nem foglalkozhatnak, mivel ezen tanúsítványok tekintetében csak Szolgáltató saját Ügyfélkapcsolati Irodája és Regisztrációs Szervezete az illetékes.

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 tanúsítványok és a kapcsolódó kulcspárok előállítása, a tanúsítványok publikálása, a regisztrációs szervezettől érkező kiadási, megújítási, felfüggesztési, újraérvényesítési és visszavonási igényeknek a végrehajtása, a tanúsítványok állapotára vonatkozó információk előállítása és közlése, a kulcsletét biztosítása, valamint a Szolgáltatásokat támogató informatikai rendszer üzemeltetése.

[2] A 2/2002 MeHVM már nem hatályos, de az aktuális részeit Szolgáltató ajánlásként figyelembe veszi,

1.4.3. Hitelesítési Rend és Szabályozási Csoport

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

1.4.4. Előfizetők és Tanúsítványtulajdonosok

Előfizető a Szolgáltatóval szerződéses viszonyban álló szervezet, amely megrendeli a Szolgáltatótól a Szolgáltatásokat, a vele kapcsolatban álló Tanúsítványtulajdonosok számára.

Tanúsítványtulajdonos:

a) az a természetes személy, aki számára a titkosító vagy az egyéb nem aláírás célú tanúsítvány kiállításra kerül, és aki az ehhez kapcsolódó magánkulcsot birtokolja illetve az Előfizetővel egyeztetve tevékenységéhez felhasználja

b) a jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, amely számára a titkosító vagy az egyéb nem aláírás célú tanúsítvány kiállításra kerül, és amely szervezet a kapcsolódó magánkulcsot birtokolja valamint azt felhasználja tevékenysége során valamilyen informatikai eszköz útján, vagy egy ezzel megbízott természetes személy által

c) olyan informatikai eszköz (web-szerver), amelynek IP címét vagy domain nevét Előfizető jogosult használni, és amely számára ún. SSZ szerver authentikációs tanúsítvány kiállításra kerül.

1.4.5. Érintett felek és szoftvergyártók

Az Érintett fél olyan természetes vagy jogi személy, aki vagy amely a Szolgáltató által kiadott tanúsítvány érvényességét ellenőrzi, és erre hagyatkozva jár el.

A szoftvergyártók alatt jelen Hitelesítési Rendben olyan természetes vagy jogi személyeket kell érteni, akik Szolgáltató ún. főtanúsítványát (Root CA) Szolgáltató kérelmére vagy azzal egyeztetve saját szoftverükkel együtt terjesztik.

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, Tanúsítványtulajdonosok, Érintett felek és szoftvergyártók).

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

1.4.6.2. Tanúsítványok alkalmazhatósága

Engedélyezett alkalmazási lehetőségek

Titkosító tanúsítványok esetén a nyilvános kulcsok különböző adatok vagy üzenetek titkosítására (kódolására), a kapcsolódó magánkulcsok pedig a kódolt üzenetek vagy adatok visszafejtésére használhatók fel.

SSL kliens authentikációs tanúsítványok esetén a tanúsítványok illetve a kapcsolódó magánkulcsok személyek vagy szervezetek hiteles azonosítására használhatók fel, a vonatkozó műszaki szabványok és protokollok szerint.

SSL szerver authentikációs tanúsítványok esetén a tanúsítványok illetve a kapcsolódó magánkulcsok webszerverek illetve domain-nevek hiteles azonosítására valamint biztonságos kommunikációs csatorna kiépítésére használhatók fel, a vonatkozó műszaki szabványok és protokollok szerint.

Kód- illetve üzenet-aláíró tanúsítványok esetén a magánkulcsok számítógépes kódok illetve üzenetek műszaki értelemben vett aláírására[3] illetve eredetének igazolására használhatók fel, míg a tanúsítványok illetve a publikus kulcsok az aláírások illetve az eredet ellenőrzésére szolgálnak.

Korlátozott alkalmazási lehetőségek

Az előfizetői tanúsítványok használatával kapcsolatban Szolgáltató pénzügyi felelősségvállalási korlátozásokat szabhat meg, melyeket vagy az ÁSZF-PKI szabályzatban, vagy az előfizetői szerződésben rögzíteni kell.

Tiltott alkalmazási lehetőségek

A titkosító tanúsítványokhoz kapcsolódó kulcsokat tilos felhasználni titkosításra ill. visszafejtésre minden olyan esetben, amelyben valamilyen jogszabály korlátozásokat vagy tiltásokat ír elő (pl. állami tevékenységek).

[3] (a kód- illetve üzenet-aláírás nem felel meg az Eat. szerinti fokozott biztonságú elektronikus aláírásnak, sem a minősített aláírásnak)

Az authentikációs tanúsítványokat illetve a kapcsolódó kulcsokat tilos felhasználni bármilyen, az azonosságra vonatkozó csalárd indíttatású félrevezetési céllal, vagy szándékos megtévesztés céljából.

A kód- illetve üzenet-aláíró 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 Tanúsítványtulajdonosok) 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 a Tanúsítványtulajdonos olyan természetes személy, aki magánszemélyként kerül regisztrálásra és ennek megfelelően kerül feltüntetésre a tanúsítványban. Magánszemély a Szolgáltatótól közvetlenül nem igényelhet tanúsítványt.

Munkatársi tanúsítvány esetén a Tanúsítványtulajdonos 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 (pl. SSL szerver) tanúsítvány esetében a Tanúsítványtulajdonos nem természetes személy, hanem egy szervezet, amely ennek megfelelően kerül regisztrálásra illetve feltüntetésre a tanúsítványban.

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

1.5.2. Tanúsítványok jellemzői

Jelen hitelesítési rend az 1.2.1 pontnak megfelelően a nyilvános körben kibocsátott, titkosító és egyéb nem aláírás célú (SSL szerver authentikációs, SSL kliens authentikációs, kód/üzenet aláíró) tanúsítványokra [TET] vonatkozik. Ezek olyan tanúsítványok, amelyek:

- megfelelnek Szolgáltató jelen hitelesítési rendjének illetve a vonatkozó szakmai ajánlásoknak
- nyilvános körben került kibocsátásra
- nem aláírás célú tanúsítványok, azaz nem felelnek meg illetve nem használhatók fel az Eat. szerinti fokozott biztonságú vagy minősített elektronikus aláíráshoz

Az előfizetői tanúsítványoknak tartalmazniuk kell az alábbiakat:

- a Szolgáltató és székhelyének (ország-) azonosítóját
- a Tanúsítványtulajdonos nevét (vagy egy álnevét, ennek jelzésével)
- a tanúsítvány szándékolt felhasználásától függően a Tanúsítványtulajdonos speciális jellemzőit
- a Tanúsítványtulajdonos magánkulcsához tartozó publikus kulcsot
- a tanúsítvány érvényességi idejének kezdetét és végét,
- a tanúsítvány azonosító kódját
- a Szolgáltató elektronikus aláírását
- a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat

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.

Jelen hitelesítési rend szerinti SSL szerver tanúsítványok tekintetében Szolgáltatónak meg kell felelnie a CA Browser fórum Baseline Requirements dokumentuma aktuális verziójában foglalt előírásoknak (http://www.cabforum.org). Erre tekintettel SSL szerver tanúsítványokat Szolgáltató csak magyarországi szervezete részére bocsájt ki, olyan domain nevekre, amelyek Magyarországon kerültek bejegyzésre, magyarországi DNS (Domain Name System) regisztrátor által. Szolgáltató által kiadott SSL szerver tanúsítványok nem tartal-

mazhatnak IP címeket. Amennyiben jelen hitelesítési rend és a CAB BR dokumentum követelményei között ellentmondás van, akkor a CAB BR követelményei az irányadóak.

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 a magánkulcs elhelyezése (igény esetén)
   - kulcsletét (igény esetén, kizárólag titkosító tanúsítvány kiadás keretében)
2. A Szolgáltatónak gondoskodnia kell a Szolgáltatásokra 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-T).
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 a Tanúsítványtulajdonost 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 (Eat.) szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó szolgáltatási szabályzatát (HSZSZ-T) valamint általános szerződési feltételeit (ÁSZF-PKI).
11. A Szolgáltató a lejárat előtt értesítést kell küldjön a lejáró tanúsítványokról az Előfizető vagy a Tanúsítványtulajdonos részére.
12. Szolgáltató a tanúsítványban köteles feltünteti az Előfizetői Szerződésben rögzített, a tanúsítvány felhasználhatóságával kapcsolatos esetleges korlátozásokat.
13. A Szolgáltató közzétételi kötelezettség mellett felfüggesztheti vagy visszavonhatja a tanúsítványt, ha azt a 4.4.1 fejezetben részletezett körülmények 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 a tanúsítvánnyal kapcsolatban 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. 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.. 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
6. online tanúsítvány-állapotszolgáltatás (OCSP – Online Certificate Status Protocol) nyújtása a „Produktív CA" tanúsítványokra vonatkozóan

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-állapotszolgáltatás (OCSP – Online Certificate Status Protocol) nyújtása, ennek keretében a szabványos kérések fogadása és az OCSP válaszok megadása
6. Titkosító tanúsítvány esetén a kulcsletét szolgáltatás biztosítása.

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 a magánkulcs 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 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 összes példányát, miután a Tanúsítványtulajdonos részére az előállított kulcspárt átadta[4],
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.
11. kulcsletét szolgáltatás keretében ellenőrzi az igénylés jogosultságát és megfelelőség esetén biztonságos módon eljuttatja a kulcspárt illetve a kapcsolódó tanúsítványt az Ügyfélkapcsolati Irodához

[4] kivéve a titkosító tanúsítványokhoz kapcsolódó kulcsletét esetén

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 a Tanúsítványtulajdonos minden adatát, kivéve azokat, amelyek az Előfizető hozzájárulásával a tanúsítványba kerülnek
8. gondoskodik a magánkulcs illetve aláírás-létrehozó eszköz és a PIN boríték biztonságos kezeléséről és átadásáról,
9. tájékoztatja az Előfizetőt vagy Tanúsítványtulajdonost tanúsítványa lejáratát megelőzően legalább 15 nappal
10. a Tanúsítványtulajdonos 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.
16. kulcsletét szolgáltatás esetén fogadja az igényt, ellenőrzi az igénylőt és annak jogosultságát, megfelelőség esetén átadja a Regisztrációs Irodától kapott magánkulcsot az igénylőnek

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.

SSL szerver tanúsítvány esetén - az Ügyfélkapcsolati Iroda munkaidején túl - a Szolgáltató Ügyfélszolgálata a tanúsítványok visszavonását is elvégzi.

2.1.2. Az Előfizető és Tanúsítványtulajdonos feladatai és hatásköre

Az Előfizető és a Tanúsítványtulajdonos feladata általánosságban a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a Szolgáltatások igénybevétele során. Ennek során a Tanúsítványtulajdonos 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. a tanúsítványát illetve a magánkulcsát jelen hitelesítési rendben és az előfizetői szerződésben rögzített korlátozásoknak megfelelően használni,
7. tudomásul venni, hogy magánkulcsának védelme 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 a magánkulcs és/vagy a PIN kód nem a Tanúsítványtulajdonos 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 kapcsolatos jogvita megindulásáról haladéktalanul tájékoztatni a Szolgáltatót,
11. a Tanúsítványtulajdonos jogosult arra, hogy a magánkulcsot birtokolja és a jelen szabályzatban illetve a HSZSZ—T dokumentumban meghatározottak szerint azt 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 Tanúsítványtulajdonosok tanúsítványainak visszavonása, illetve felfüggesztése végett, ha a magánkulcs és/vagy a PIN kód nem a Tanúsítványtulajdonos kizárólagos birtokában van (elveszett, ellopták, esetleg kompromittálták), vagy ennek alapos gyanúja áll fenn
5. tájékoztatni a Szolgáltatót a tanúsítvánnyal kapcsolatban észlelt rendellenességről, valamint a tanúsítvánnyal kapcsolatos jogvita megindulásáról.
6. a Szolgáltatások díjait az előfizetői szerződésben foglaltak szerint megfizetni Szolgáltató számára

Szolgáltató kérésére Előfizető illetve Tanúsítványtulajdonos köteles a jelzett határidőn belül választ adni a magán kulcsának kompromittálódására vagy tanúsítvány nem rendeltetésszerű felhasználásával kapcsolatos szolgáltatói kérdésekre.

2.1.3. Az Érintett félre vonatkozó ajánlások

Az Érintett félnek ajánlott a Szolgáltató szabályzataiban leírtaknak megfelelően a legnagyobb gondossággal eljárni a tanúsítvány érvényességének elbírálásakor, ezen belül:

1. a tanúsítvány elfogadása előtt ajánlott megértenie az azzal kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat,
2. ajánlott megismernie Szolgáltató nyilvánosan elérhető szabályzatait (HR-TET, HSZSZ-T, ÁSZF-PKI),
3. kód- illetve üzenet-aláíró tanúsítvány esetében ajánlott az aláírás ellenőrzését elvégeznie a Tanúsítványtulajdonos 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 a Tanúsítványtulajdonos 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 a Tanúsítványtulajdonos 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 a tanúsítvány elfogadását, ha a Tanúsítványtulajdonos tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata annak érvénytelenségére utal, illetve ha az az adott kontextusban nem elfogadható;
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 a tanúsítvánnyal 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 2013. évi V. törvény 6:519. §-a szerint, az Előfizetővel szemben pedig a szerződésszegésért való felelősség szabályai – Ptk. 6:142.§ - szerint felelős a Szolgáltatások nyújtásával okozott kárért, ha megszegte a szolgáltatási szabályzatban (HSZSZ-T), az általános szerződési feltételekben (ÁSZF-PKI) vagy az Előfizetői Szerződésben előírtakat. 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 szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

Szolgáltató a tanúsítványok kibocsájtása keretében felelősséget vállal a tanúsítványokba bekerülő adatokért, azok pontosságáért, adott esetben a domainnevek és ezek igénylőinek ellenőrzéséért, azért, hogy a tanúsítványok kizárólag előfizetői szerződéses jogviszony keretében kerülnek kibocsájtásra, valamint a tanúsítványra vonatkozó állapotinformációk (beleértve a visszavonási rendelkezésre állás) valóságnak megfelelő szolgáltatásáért.

2.2.2. Előfizető és a Tanúsítványtulajdonos felelőssége

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

Az Előfizetőnek és a Tanúsítványtulajdonosnak 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 Tanúsítványtulajdonos a magánkulcsát nem a szolgáltatási szabályzatban és a vonatkozó jogszabályokban meghatározott módon és célra használta.

Az Előfizető és a Tanúsítványtulajdonos felelős az aláírás-létrehozó eszköz átvételét követően annak biztonságos megőrzéséért, a magánkulcs 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

Az Előfizető illetve Tanúsítványtulajdonos részére történő átadást követően Szolgáltató nem vállalhat felelősséget az aláírás-létrehozó eszköz elvesztéséből, vagy a magánkulcs biztonságának egyéb módon történő sérüléséből, illetve a PIN kód illetéktelen személy tudomására jutásából származó károkért.

Tanúsítványtulajdonos felelősséget visel a titkosító tanúsítvány felhasználásával végzett titkosításért, és viseli ennek jogkövetkezményeit.

2.2.3. Érintett fél felelőssége

Az Érintett fél illetve a szoftvergyártók a Szolgáltató által kibocsátott tanúsítványok elfogadása során a tőle elvárható gondossággal járnak el és az adott helyzetben általában elvárható magatartást tanúsítják. Az Érintett Félnek

illetve a szoftvergyártóknak e tekintetben javasolt megismernie a jelen szabályzatban rájuk vonatkozó ajánlásokat.

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 Ptk. 2:46.§ és 2:47.§ 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.

2.4.2.2. Megszűnés

A hitelesítési rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

2.4.2.3. Értesítések

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

Az Előfizetők, a Tanúsítványtulajdonosok és az Érintett felek vagy bármely harmadik fél megkeresheti az Ügyfélkapcsolati Irodát munkanapokon ügyfélfogadási időben személyesen vagy telefonon, postai úton írásban, e-mailben 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 a Tanúsítványtulajdonosnak 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 szóbeli panaszt azonnal meg kell vizsgálni és szükség szerint orvosolni kell. Ha az Előfizető a panasz kezelésével nem ért egyet, vagy az azonnali intézkedésre nincs mód, úgy a panaszról, a kezelés módjáról a Szolgáltató jegyzőkönyvet vesz fel. 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, Tanúsítványtulajdonosok és az Érintett felek illetve szoftvergyártók 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 Tanúsítványtulajdonos, 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 a Tanúsítványtulajdonos 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-T) 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 a Tanúsítványtulajdonosra vonatkozó adatok és információk bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk hozzájárulnak, vagy ha arra jogosult hatóság, bíróság illetve jogszabály ezt előírja

2.8.1. Bizalmas információk

Szolgáltató bizalmas információként köteles kezelni a Tanúsítványtulajdonosok 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.
- kulcsletétbe helyezett kulcsok

2.8.2. Nem bizalmas információk

A Szolgáltató a regisztrációs űrlapon köteles külön jelölni mindazon adatokat, melyek – az Előfizető vagy a Tanúsítványtulajdonos 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 köteles feltüntetni a visszavonási listában. Ezen kívül a visszavonással kapcsolatos minden egyéb információt, adatot köteles bizalmasan kezelni.

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 a Tanúsítványtulajdonost 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 - a Tanúsítványtulajdonos 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 a Tanúsítványtulajdonosok nem nyilvános személyes adatait csak a Tanúsítványtulajdonosok 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 a Tanúsítványtulajdonos, 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 a Tanúsítványtulajdonos részére kibocsátott egyedi azonosító a Szolgáltató tulajdonát képezi.

A tanúsítványban szereplő megkülönböztető név használatára a megnevezett Tanúsítványtulajdonos jogosult.

A Tanúsítványtulajdonos egyedi azonosítójában szereplő bármilyen védjegy, szervezeti- és személynév, vagy egyéb adat az Előfizető vagy a Tanúsítványtulajdonos 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 a Tanúsítványtulajdonosok 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[5] 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 a tanúsítványokban használt megkülönböztető nevek (DN) egyediségét. Erről elsődlegesen a Tanúsítványtulajdonos nevének valamint egy Szolgáltató által alkalmazott egyedi azonosítónak a „Tulajdonos” mezőben való szerepeltetésével kell gondoskodnia. A megkülönböztető nevek egyediségére Tanúsítványtulajdonos email címe is felhasználható, a „Tulajdonos alternatív neve” mezőben való szerepeltetéssel, kivéve, ha ezt valamely ajánlás vagy előírás tiltja.

3.1.4. Név igénylési viták feloldása

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

3.1.5. Védjegyek elismerésének és hitelesítésének módszere

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

3.1.6. A magánkulcs birtoklásának ellenőrzése

A Tanúsítványtulajdonos számára a magánkulcs és publikus kulcs (kriptográfiai kulcspár) előállítása a Szolgáltatások keretében és a Szolgáltató által kell történjen, kiemelt biztonságú környezetben. Erre tekintettel a magánkulcs és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán a magánkulcs illetve az aláírás-létrehozó eszköz átvételének igazolása szükséges.

Fentiek alól kivételt képez az SSL szerver tanúsítványok esete, amikor is Előfizető jogosult maga előállítani a kriptográfiai kulcspárt. Ilyenkor a magánkulcs birtoklását Előfizető szabványos (pkcs10) kérelem benyújtásával köteles igazolni Szolgáltató felé.

3.1.7. Személyazonosság megállapítása

A tanúsítványok igénylésekor az Előfizető részéről eljáró természetes személy igénylőt (munkatársi tanúsítvány esetén a Tanúsítványtulajdonost, szervezeti vagy SSL szerver tanúsítvány esetén a kapcsolattartót) Szolgáltató köteles ellenőrizni illetve a személyazonosságát megállapítani.

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

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

Amennyiben az igény emelt szintű regisztrációra vonatkozik, a személyazonosító okmány ellenőrzésén túl szükség van az Előfizető részéről eljáró természetes személy személyes megjelenésére is Szolgáltató regisztrációs irodájában (vagy felár ellenében az ún. kihelyezett regisztráció keretében).

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-T) 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-T) kell ismertetnie.

3.1.9. Eszköz azonosság megállapítása

Amennyiben a Tanúsítványtulajdonos nem természetes személy, hanem egy szervezet illetve informatikai eszköz (pl. SSL szerver), a tanúsítvány igénylésekor az Előfizető részéről eljáró természetes személynek (kapcsolattartónak) valamint a szervezetnek az azonosítása mellett szükséges az Előfizető írásos nyilatkozata is a szerver megnevezéséről valamint hozzájárulásáról ahhoz, hogy a kapcsolattartó jogosult a szervezet nevében az adott tanúsítványt igényelni.

SSL szerver esetén a domain név Előfizetőhöz tartozását is igazolni kell, a DNS (Domain Name System) regisztrátor által kiállított hivatalos igazolás Szolgáltatóhoz történő benyújtásával. Szolgáltató meg kell győződjön arról, hogy az igényelt domain az Előfizető birtokában van és azt jogosult használni.

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 a Tanúsítványtulajdonos 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 a Tanúsítványtulajdonos írásban nyilatkozik.

A Szolgáltató az Előfizető vagy Tanúsítványtulajdonos 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 Tanúsítványtulajdonosnak.

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 a Tanúsítványtulajdonos 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 a Tanúsítványtulajdonosokat) 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 magánkulcs használatát, védelmét
b. garantálja feltüntetett adatainak valódiságát
c. megfizeti a szolgáltatások díját
d. az adatok későbbi változásairól a Szolgáltatót értesíti.

A regisztráció során az Ügyfélkapcsolati Iroda nyilvántartásba veszi a Tanúsítványtulajdonos 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 a Tanúsítványtulajdonos vagy Előfizető kijelölt kapcsolattartója személyesen átveszi az Ügyfélkapcsolati Irodán.

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

4.3. Tanúsítvány elfogadás

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

A magánkulcs használatba vétele előtt a Tanúsítványtulajdonosnak illetve Előfizető kijelölt kapcsolattartójának kötelessége ellenőrizni a tanúsítványban feltüntetett adatok helyességét. Amennyiben bármilyen rendellenességet talál, magánkulcsot 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-T) ismertetnie kell. SSI szerver tanúsítványokra a HSZSZ-T különleges szabályokat állapíthat meg.

4.4.1. Visszavonáshoz/felfüggesztéshez vezető körülmények

A Szolgáltatónak a szolgáltatási szabályzatában (HSZSZ-T) ismertetnie kell, hogy milyen körülmények között lehet, illetve kell visszavonási illetve felfüggesztési kérelmet benyújtani.

4.4.2. Visszavonás/felfüggesztés kérelmezése

Tanúsítvány visszavonását/felfüggesztését a Tanúsítványtulajdonos, az Előfizető vagy annak regisztráció során nyilvántartásba vett kapcsolattartója, a Szolgáltató, vagy más harmadik fél is kezdeményezheti.

Az Előfizetőnek, Tanúsítványtulajdonosnak 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 a Tanúsítványtulajdonost, 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 (kivéve az SSL szerver tanúsítványokat, ahol 1 nap). 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 Tanúsítványtulajdonos 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 rosszhiszemű 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.

SSL szerver tanúsítvány a CA Browser Fórum előírásainak megfelelően nem lehet felfüggesztett állapotban.

4.4.6. Felfüggesztett állapotra vonatkozó korlátozások

Tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig lehet. Kivételt képez az SSL szerver tanúsítvány, amely nem lehet felfüggesztett állapotban (csak a visszavont állapot megengedett).

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

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

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 a Tanúsítványtulajdonos, 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 Listájának 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-T) tartalmazza.

4.4.10. Intézkedések magánkulcs kompromittálódás esetén

A magánkulcs kompromittálódása, vagy vélelmezett kompromittálódása esetén a tanúsítvány visszavonásáról azonnal intézkedni kell. Alapos gyanú esetén a magánkulcs használatát azonnal be kell szüntetni.

Az Előfizetőnek és a Tanúsítványtulajdonosnak kötelessége a kompromittálódott magánkulcs 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, a kulcsletét biztosítás, 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.

A Tanúsítványtulajdonosok aláírás-létrehozó eszközzel való ellátásával kapcsolatosan[6]:

- 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.

A kulcsletét kezeléssel kapcsolatosan:

- A Szolgáltató naplóz minden eseményt, mely egy kulcsletétbe helyezett magánkulcs Előfizető részére történő átadásával kapcsolatos

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 köteles fenntartani a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét.

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

A Szolgáltató megfelelő műszaki és szervezeti intézkedéseket köteles foganatosítani 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 katasztrófa esemény jelzése

Amennyiben a Szolgáltató rendszerében olyan jellegű hiba illetve esemény következik be, amely 24 óránál nagyobb szolgáltatás kieséssel jár, akkor az eseményről Szolgáltatónak értesítenie kell 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.

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

4.7. Szolgáltatói tevékenység megszüntetése

A Szolgáltatónak a tervezett megszűnés előtt megállapodást javasolt kötni más szolgáltatóval a szolgáltatások átvételéről. Amennyiben ilyen megállapodás megszületik, erről 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 illetve a Szolgáltatások internetes honlapján keresztül tájékoztatnia kell a felhasználói közösség tagjait

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

c. fel kell készülnie a regisztrációs adatok, a kulcsletétbe helyezett kulcsok és az eseménynapló archívumok átruházására (amennyiben erre vonatkozó megállapodás megszületett)

A bejelentéssel egyidejűleg a Szolgáltató leállíthatja:

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

b. az aláírás-létrehozó eszközön a magánkulcs 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 Szolgáltatásokkal kapcsolatos személyi és fizikai biztonság követelményeit.

A következő pontok csak a vonatkozó lényeges követelményeket tartalmazzák.

5.1. Fizikai biztonsági szabályozások

A Szolgáltatónak az általános tevékenységével kapcsolatosan :

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, kulcsletét biztosításával 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. a Tanúsítványtulajdonosok aláírás-létrehozó eszközzel való ellátása,

d. visszavonás kezelés.

e. kulcsletét (kizárólag titkosító tanúsítvány esetén)

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 Szolgáltatások biztonsága függ. Ezeket a bizalmi munkaköröket és felelősségeket belső leírásokban dokumentálni kell.

A bizalmi munkakörök közé az alábbiak tartoznak:

A kormányzati 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 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

e. kulcsletétbe elhelyezett kulcs kivétele

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 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 (magánkulcsokat illetve a publikus kulcsokat), 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. Fenti szabályok alól kivételt képez az SSL szerver tanúsítványokhoz tartozó kulcspár, amit Előfizető is előállíthat a saját környezetében, és azt az általa kijelölt személy szabványos formában (pkcs10 kérésben) átadhatja Szolgáltató részére.

A magánkulcs láírás-létrehozó eszközön (pl.: chipkártyán) történő elhelyezésére a Szolgáltató csak tanúsítvány kibocsátással együtt vállalkozhat.

A szolgáltatói magánkulcsok 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 a magánkulcs illetve az aláírás-létrehozó eszköz aktivizálásához PIN kódot kell biztosítson. A PIN kódot fizikailag védett környezetben kell előállítania és biztonságos módon kell tárolnia egészen az átadásig.

6.1.3. A magánkulcs eljuttatása a Tanúsítványtulajdonoshoz (Előfizetőhöz)

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

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

A magánkulcs vagy az aláírás-létrehozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

6.1.4. A Tanúsítványtulajdonosok publikus kulcsainak eljuttatása az érintett felekhez

A Szolgáltató a Tanúsítványtulajdonosok nyilvános kulcsát a tanúsítványba foglalva a Szolgáltatások internetes honlapján levő Tanúsítványtárán keresztül köteles mindenki számára elérhetővé tenni.

6.1.5. A Szolgáltató publikus kulcsainak eljuttatása a felhasználói közösséghez

A Szolgáltató köteles a hitelesítő központok (Root CA, Produktív CA) 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 jelen hitelesítési rend szerinti előfizetői tanúsítványokhoz tartozó kulcs felhasználási célja a következő:

Titkosító tanúsítványok esetén a nyilvános kulcsok különböző adatok vagy üzenetek titkosítására (kódolására), a kapcsolódó magánkulcsok pedig a kódolt üzenetek vagy adatok visszafejtésére használhatók fel.

SSL kliens authentikációs tanúsítványok esetén a magánkulcsok személyek vagy szervezetek azonosítására használhatók fel, a vonatkozó műszaki szabványok és protokollok szerint.

SSL szerver authentikációs tanúsítványok esetén a kapcsolódó magánkulcsok web-szerverek illetve domainnevek azonosítására valamint biztonságos kommunikációs csatorna kiépítésére használhatók fel, a vonatkozó műszaki szabványok és protokollok szerint.

Kód- illetve üzenet-aláíró tanúsítványok esetén a magánkulcsok számítógépes kódok illetve üzenetek műszaki értelemben vett aláírására[7] illetve eredetének igazolására használhatók fel, míg a publikus kulcsok az aláírások illetve az eredet ellenőrzésére szolgálnak

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

6.2. A magánkulcsok védelme

A Szolgáltatónak gondoskodnia kell valamennyi általa (saját maga vagy a Tanúsítványtulajdonosok számára) előállított magánkulcs titkosságáról és sértetlenségéről.

A Szolgáltató külön magánkulcsot kell használjon a tanúsítványok és a visszavonási listák aláírására, és ezt a kulcsot semmilyen más célra nem használhatja 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. Kulcsletét, mentés, archiválás

Szolgáltató kizárólag a titkosító tanúsítványokhoz nyújt kulcsletét szolgáltatást. A kulcsletétet fizikailag biztonságos módon menti és archiválja, megfelelő jogosultság és hozzáférés védelmet biztosítva a kapcsolódó környezethez. A letétben őrzött kulcsokat Szolgáltató a tanúsítvány lejártáig köteles őrizni, azt követően jogosult törölni a kulcsletét adatbázisából.

Szolgáltató az egyéb végfelhasználói tanúsítványokhoz tartozó magánkulcsokat semmilyen formában nem mentheti vagy archiválhatja; annak előállítására, visszafejtésére alkalmas programot, adatot nem tárolhat.

6.2.3. Magánkulcs aktiválása

Az előfizetői magánkulcs aktiválása a Tanúsítványtulajdonos vagy Előfizető kijelölt felhasználója által történhet a Szolgáltatótól kapott PIN kód megadásával vagy – Előfizető által az SSL szerver tanúsítványokhoz generált kulcspár esetén – az előfizetői által ismert jelszó megadásával.

A szolgáltatói magánkulcs aktiválása hasonlóan jelszóval vagy PIN-kóddal történhet, az erre kijelölt bizalmi munkaköröket betöltő személyek által.

6.2.4. Magánkulcs deaktiválása

Az előfizetői magánkulcsok deaktiválása a Tanúsítványtulajdonos vagy Előfizető kijelölt felhasználója által történhet, a Tanúsítványtulajdonos alkalmazásból való kijelentkezéskor, vagy – pl. chipkártya esetén – amikor a Tanúsítványtulajdonos az aláírás-létrehozó eszközt eltávolítja az olvasóból.

A szolgáltatói magánkulcs deaktiválása a tanúsítvány aláíró vagy CRL aláíró alkalmazás leállításával történhet, az erre kijelölt bizalmi munkaköröket betöltő személyek által.

6.2.5. Magánkulcs megsemmisítése

Az előfizetői tanúsítvány lejárta után a magánkulcs fizikai megsemmisítését a Tanúsítványtulajdonosnak 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. Publikus kulcs archiválása

A Szolgáltató köteles minden általa kibocsátott tanúsítványt illetve az ahhoz kapcsolódó publikus kulcsot megőrizni illetve archiválni az érvényesség lejártától számított 10 évig.

Az archivált tanúsítványokról biztonsági mentést is kell készíteni.

[7] (a kód- illetve üzenet-aláírás nem felel meg az Eat. szerinti fokozott biztonságú elektronikus aláírásnak, sem a minősített aláírásnak)

6.3.2. Kulcsok felhasználási ideje

A tanúsítványokhoz kapcsolódó magánkulcsok és nyilvános kulcsok érvényességi ideje megegyezik a kulcsok hitelességét igazoló tanúsítvány érvényességi idejével:

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

Előfizetői tanúsítvány megújítás esetén értelemszerűen a kulcs felhasználási ideje a megújított tanúsítvány érvényességéhez igazodik.

6.4. Aktivizáló adatok (PIN kódok)

Az előfizetői tanúsítványokhoz tartozó magánkulcsok illetve aláíró 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 a Tanúsítványtulajdonos illetve Előfizető kapcsolattartója részére adhatja át, személyesen. Az átvételt követően az Előfizetőnek illetve Tanúsítványtulajdonosnak saját felelősségi körében kell biztosítania a 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-T), 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 meg kell feleljenek az RFC 3280 ajánlásban leírt X. 509 3-as verziójú tanúsítványoknak. A további információkat a Szolgáltató szolgáltatási szabályzata (HSZSZ-T) tartalmazza.

7.2. Tanúsítvány-visszavonási profil

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

7.3. Online tanúsítvány-állapot szolgáltatás (OCSP) profil

A Szolgáltató szolgáltatási szabályzata (HSZSZ-T) tartalmazza.

8. Hitelesítési Rend adminisztráció

8.1. Változáskezelés

A Szolgáltatónak felülvizsgálati folyamatot kell meghatároznia a szervezetén belül, mely kiterjed a jelen hitelesítési rend (HR-TET) gondozására is.

8.2. Közzétételi és tájékoztatási elvek

A Szolgáltató jelen hitelesítési rendjét és egyéb kapcsolódó dokumentumait a Tanúsítványtulajdonosok, Előfizetők és az Érintett felek rendelkezésére kell bocsássa, a tanúsítványtípusnak való megfelelés felméréséhez szükséges mértékig.

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

8.3. HR-TET elfogadási eljárások

A HR-TET 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.

Módosítás esetén a HR-TET ellenőrzésére illetve jóváhagyására a Szolgáltató belső virtuális szervezete (Hitelesítési Rend és Szabályozási Csoport) illetve a Szolgáltatásokért felelős vezetője rendelkezik hatáskörrel és felelősséggel.

A HR-TET jogszabályoknak illetve a szakmai előírásoknak való megfelelőségét Szolgáltató által megbízott külső auditor is ellenőrzi.

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 nem aláírás célú tanúsítvány szolgáltatásokhoz (HSZSZ-T)

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)