NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

Szolgáltatási szabályzat nem aláírás célú tanúsítvány szolgáltatásokhoz (HSZSZ-T)

Verziószám	**1.4**
OID szám	**0.2.216.1.200.1100.100.42.3.5.10.1.4**
Hatályba lépés dátuma	**2015.07.01.**
Dokumentum besorolása	**Publikus**

NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

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
1.3	2015.03.04	HSM és BALE tanúsítások átvezetése, bizalmi munkakörök kiegészítése	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila
1.4	2015.06.01	Új HSM modulok feltüntetése	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila

Tartalomjegyzék

1. BEVEZETÉS 9
1.1. ÁTTEKINTÉS 9
1.2. A DOKUMENTUM NEVE ÉS AZONOSÍTÓJA 10
1.3. A SZOLGÁLTATÓ ÉS A FELHASZNÁLÓI KÖZÖSSÉG 10
1.3.1. Szolgáltató adatai és elérhetőségei 10
1.3.2. Regisztrációs és hitelesítő szervezet 11
1.3.2.1. A Szolgáltató regisztrációs szervezete 11
1.3.2.2. A Szolgáltató hitelesítő szervezete 11
1.3.3. Felhasználói közösség 12
1.3.3.1. Előfizető 12
1.3.3.2. Tanúsítványtulajdonos (alany) 12
1.3.3.3. Érintett felek és szoftvergyártók 13
1.4. TANÚSÍTVÁNYHASZNÁLAT 13
1.4.1. A szolgáltatás szintje 13
1.4.2. Tanúsítványok alkalmazhatósága 13
1.5. A SZOLGÁLTATÁSI SZABÁLYZAT ADMINISZTRÁCIÓJA 14
1.5.1. Szabályzat hatálya 14
1.5.2. Szabályzatra vonatkozó változáskezelés 14
1.5.3. Közzétételi és tájékoztatási elvek 15
1.5.3.1. A HSZSZ-T-ben nem tárgyalt elemek 15
1.5.3.2. A HSZSZ-T közzététele 15
1.5.4. Elfogadási eljárások 15
1.6. MEGHATÁROZÁSOK 15
1.7. HIVATKOZÁSOK 19
1.8. TANÚSÍTVÁNYOK JELLEMZŐI 20
1.8.1. Tanúsítványok fajtái 21
1.8.1.1. Előfizetői tanúsítvány 21
1.8.1.2. Szolgáltatói tanúsítvány 21
1.8.1.3. Teszt tanúsítvány 21
1.8.1.4. „Személyes” tanúsítvány 22
1.8.1.5. „Munkatársi” tanúsítvány 22
1.8.1.6. „Szervezeti” vagy eszköz tanúsítvány 22
1.8.1.7. SSL szerver tanúsítvány 23
2. ÁLTALÁNOS RENDELKEZÉSEK 23
2.1. FELADATOK ÉS HATÁSKÖRÖK 23

2.1.1. A Szolgáltató feladatai és hatásköre ... 23
2.1.1.1. A Hitelesítő Szervezet feladatai és hatásköre ... 25
2.1.1.2. A Regisztrációs Iroda feladatai és hatásköre ... 26
2.1.1.3. Az Ügyfélkapcsolati Iroda feladatai és hatásköre ... 26
2.1.1.4. A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre ... 26
2.1.1.5. Az Ügyfélszolgálat feladata ... 26
2.1.2. Az Előfizető és a Tanúsítványtulajdonos feladatai és hatásköre ... 26
2.1.3. Az Érintett félre vonatkozó ajánlások tanúsítvány ellenőrzése során ... 26
2.2. FELELŐSSÉGEK ... 26
2.2.1. A Szolgáltató felelőssége ... 26
2.2.2. Az Előfizető és a Tanúsítványtulajdonos felelőssége ... 27
2.2.3. Az Érintett fél felelőssége ... 28
2.3. ÉRTELMEZÉS ÉS ALKALMAZÁS ... 28
2.3.1. Alkalmazott jogszabályok ... 28
2.3.2. Hatályosság, megszűnés, értesítések ... 28
2.3.2.1. Hatályosság ... 28
2.3.2.2. Megszűnés ... 28
2.3.2.3. Értesítések ... 28
2.3.3. Vitás kérdések kezelése ... 29
2.4. KÖZZÉTÉTEL ... 29
2.4.1. Adatbázisok ... 29
2.4.1.1. Tanúsítványtár ... 29
2.4.1.2. Naplók, regisztrációs adatok ... 29
2.4.1.3. Az adatbázisok elérésének szabályozása ... 29
2.4.2. A tanúsítványokra vonatkozó információk közzététele ... 29
2.4.3. A közzététel gyakorisága ... 30
3. AZONOSÍTÁSI ELJÁRÁSOK ... 30
3.1. MEGNEVEZÉSI KONVENCIÓK ... 30
3.1.1. Nevek típusa ... 30
3.1.2. Nevek szemantikája ... 31
3.1.3. Nevek egyedisége ... 31
3.1.4. Név igénylési viták feloldása ... 31
3.1.5. Álnevek használata ... 31
3.1.6. Védjegyek elismerésének módszere ... 32
3.2. REGISZTRÁCIÓ ... 32
3.2.1. Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere ... 32
3.2.2. Regisztráció „Személyes” tanúsítvány igénylése esetén ... 33
3.2.3. Regisztráció „Munkatársi” tanúsítvány igénylése esetén ... 33
3.2.4. Regisztráció „Szervezeti vagy eszköz” tanúsítvány igénylése esetén ... 34
3.2.5. Adategyeztetés ... 35

3.2.6. Regisztráció SSL szerver (és Wildcard) tanúsítvány igénylése esetén ... 35

4. A TANÚSÍTVÁNY-ÉLETCIKLUSRA VONATKOZÓ SZABÁLYOK ... 38

4.1. TANÚSÍTVÁNYIGÉNYLÉS ... 38

4.1.1. Ki nyújthat be tanúsítványkérelmet ... 38

4.1.2. A tanúsítványigénylés folyamata és a résztvevők felelőssége ... 38

4.2. A TANÚSÍTVÁNY KÉRELEM FELDOLGOZÁSA ... 39

4.2.1. Azonosítási funkciók megvalósítása ... 39

4.2.2. A tanúsítványkérelem jóváhagyása vagy visszautasítása ... 39

4.2.3. A tanúsítványigénylések feldolgozásának időtartama ... 39

4.3. TANÚSÍTVÁNY KIBOCSÁTÁS ... 39

4.4. TANÚSÍTVÁNY ELFOGADÁS ... 39

4.4.1. Tanúsítvány közzététele a Szolgáltató által ... 40

4.4.2. A további szereplők értesítése a tanúsítvány kibocsátásáról ... 40

4.5. KULCSPÁR ÉS TANÚSÍTVÁNY HASZNÁLAT ... 40

4.5.1. A Tanúsítványtulajdonos magánkulcs- és tanúsítvány használata ... 40

4.5.2. Az Érintett felek nyilvános kulcs- és tanúsítvány használata ... 40

4.6. TANÚSÍTVÁNYOK ÉRVÉNYESSÉGE, MEGÚJÍTÁSA (TANÚSÍTVÁNY FRISSÍTÉSE) ... 41

4.6.1. A tanúsítványok érvényessége ... 41

4.6.2. A tanúsítványok megújítása ... 41

4.6.3. Érvénytelen tanúsítványok megőrzése ... 41

4.7. KULCSCSERE ... 41

4.8. TANÚSÍTVÁNY-MÓDOSÍTÁS ... 42

4.9. TANÚSÍTVÁNY VISSZAVONÁS ÉS FELFÜGGESZTÉS ... 42

4.9.1. Visszavonáshoz/felfüggesztéshez vezető körülmények ... 42

4.9.2. Visszavonás kérelmezése ... 43

4.9.3. Visszavonási kérelemre vonatkozó eljárás ... 44

4.9.3.1. SSL szerver tanúsítványok visszavonásának különleges szabályai ... 44

4.9.4. A felfüggesztési kérelemre vonatkozó eljárás ... 45

4.9.4.1. Ki kérelmezheti a felfüggesztést ... 45

4.9.4.2. A felfüggesztési eljárás ... 45

4.9.4.3. A Szolgáltató függeszti fel a tanúsítványt ... 46

4.9.5. Kivárási idő visszavonási/felfüggesztési kérelem esetén ... 46

4.9.5.1. Kivárási idő felfüggesztési kérelem esetén ... 46

4.9.5.2. Kivárási idő visszavonási kérelem esetén ... 46

4.9.5.3. A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok ... 47

4.9.6. Felfüggesztett állapotra vonatkozó korlátozások, újraérvényesítés ... 47

4.9.6.1. A felfüggesztés megengedett időtartama ... 47

4.9.6.2. Felfüggesztés megszüntetése ... 47

4.9.7. A visszavonási információ ellenőrzése az Érintett felek részéről ... 48

4.9.8. Visszavonási listák (CRL) és kibocsátásuk gyakorisága ... 48

4.9.9. A visszavonási lista előállítása és közzététele közötti leghosszabb idő ... 48
4.9.10. Visszavonási listák ellenőrzése ... 48
4.9.11. Valósidejű tanúsítványállapot-ellenőrzés ... 48
4.9.12. Visszavonási állapot közlés más formái ... 49
4.9.13. Intézkedések magánkulcs kompromittálódás esetén ... 49
4.10. KULCSLETÉT ... 49
5. FIZIKAI, ELJÁRÁSRENDI ÉS HUMÁN BIZTONSÁGI SZABÁLYOZÁSOK ... 49
5.1. FIZIKAI BIZTONSÁGI SZABÁLYOZÁSOK ... 50
5.2. HUMÁN SZABÁLYOZÁSOK ... 51
5.2.1. Bizalmi munkakörök ... 51
5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok ... 53
5.2.3. A bizalmi munkakörökben elvárt azonosítás és hitelesítés ... 54
5.2.4. Egymást kizáró munkakörök ... 54
5.2.5. Személyzetre vonatkozó előírások ... 54
5.2.6. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények ... 54
5.2.7. Biztonsági háttér ellenőrzésekre vonatkozó eljárások ... 55
5.2.8. Képzési követelmények ... 55
5.2.9. A felhatalmazás nélküli tevékenységek büntető következményei ... 56
5.3. NAPLÓZÁSI ELJÁRÁSOK ... 56
5.3.1. Naplózott esemény típusok ... 56
5.3.2. Napló adatok védelme ... 56
5.3.3. A naplók feldolgozásának gyakorisága ... 57
5.3.4. Napló adatok tárolása ... 57
5.3.5. A napló fájlok megőrzési időtartama ... 57
5.4. ADATOK ARCHIVÁLÁSA ... 57
5.4.1. A tárolt adatok típusai ... 57
5.4.2. Az archívum megőrzési időtartama ... 57
5.4.3. Az archívum védelme ... 57
5.4.4. Az archívum hozzáférését és ellenőrzését végző eljárások ... 58
5.5. A SZOLGÁLTATÓ KULCSCSERÉJE ... 58
5.6. KATASZTRÓFA ELHÁRÍTÁS ... 58
5.6.1. A szolgáltatások azonnali felfüggesztése ... 58
5.6.2. Minimális szolgáltatás rendkívüli üzemeltetési helyzetben ... 58
5.6.3. Rendkívüli eseményekről történő értesítés ... 59
5.7. A SZOLGÁLTATÁSI TEVÉKENYSÉG MEGSZÜNTETÉSE ... 59
6. MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK ... 60
6.1. KULCSPÁR ELŐÁLLÍTÁS ÉS TELEPÍTÉS ... 60
6.1.1. Kulcspár előállítás ... 60
6.1.2. Az aláírás-létrehozó eszköz megszemélyesítése ... 61

6.1.3. A magánkulcs eljuttatása a Tanúsítványtulajdonoshoz (Előfizetőhöz) *61*
6.1.4. A Tanúsítványtulajdonosok publikus kulcsának eljuttatása az érintett felekhez *61*
6.1.5. A Szolgáltató aláírás-ellenőrző adatainak eljuttatása a felhasználói közösséghez *61*
6.1.6. Kulcsméretek, használt algoritmusok *61*
6.1.7. Szolgáltatói kulcsgenerálás *62*
6.1.8. Kulcs felhasználási célok *62*
6.2. A MAGÁNKULCSOK VÉDELME 63
6.2.1. A magánkulcsokra vonatkozó szabályok *63*
6.2.2. Kriptográfiai modulra vonatkozó szabályok *63*
6.2.3. A többszereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése *63*
6.2.4. Kulcsletét, mentés, archiválás *63*
6.2.5. Magánkulcsok aktiválása *64*
6.2.6. Magánkulcs deaktiválása *64*
6.2.7. Magánkulcs megsemmisítése *64*
6.3. AZ ELŐFIZETŐI TANÚSÍTVÁNYOK MEGŐRZÉSE 64
6.4. AKTIVÁLÁSI ADATOK (PIN-KÓDOK) 64
6.5. INFORMATIKAI BIZTONSÁGI ELŐÍRÁSOK 65
6.5.1. Számítógép biztonsági követelmények *66*
6.5.2. Az informatikai biztonság értékelése *67*
6.6. ÉLETCIKLUSRA VONATKOZÓ MŰSZAKI ELŐÍRÁSOK 67
6.6.1. Rendszerfejlesztési szabályok *67*
6.6.2. Biztonságkezelési szabályok *68*
6.6.3. Életciklus biztonsági értékelések *68*
6.7. HÁLÓZATI BIZTONSÁGI SZABÁLYOK 68
6.8. KRIPTOGRÁFIAI MODUL ELLENŐRZÉSE 68
7. TANÚSÍTVÁNY ÉS TANÚSÍTVÁNY-VISSZAVONÁSI PROFIL 69
7.1. TANÚSÍTVÁNY PROFIL 69
7.1.1. Alap mezők *69*
7.1.2. Tanúsítvány kiterjesztések *70*
7.2. TANÚSÍTVÁNY-VISSZAVONÁSI PROFIL 71
8. A MEGFELELŐSÉG VIZSGÁLATA 72
8.1. AZ ELLENŐRZÉSEK GYAKORISÁGA ÉS KÖRÜLMÉNYEI 73
8.2. AZ AUDITOR ÉS SZÜKSÉGES KÉPESÍTÉSE 73
8.3. AZ AUDITOR ÉS AZ AUDITÁLT RENDSZERELEM FÜGGETLENSÉGE 73
8.4. AZ AUDITÁLÁS ÁLTAL LEFEDETT TERÜLETEK 73
8.5. A HIÁNYOSSÁGOK KEZELÉSE 73
8.6. AZ EREDMÉNYEK KÖZZÉTÉTELE 74
9. EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK 74
9.1. DÍJAK 74

9.1.1. Tanúsítványkibocsájtás és -megújítás *74*
9.1.2. Tanúsítvány hozzáférés *74*
9.1.3. Visszavonás és állapot információ hozzáférés *74*
9.1.4. Egyéb szolgáltatásokra vonatkozó díjak *75*
9.1.5. Visszatérítési elvek *75*
9.2. ANYAGI FELELŐSSÉG ÉS ANNAK KORLÁTAI 75
9.3. BIZALMASSÁG - ADATKEZELÉSI SZABÁLYOK 75
9.3.1. Bizalmas információk *75*
9.3.2. Nem bizalmas információk *77*
9.3.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése *77*
9.3.4. Feltárás törvényi meghatalmazással rendelkezők részére *77*
9.3.5. Feltárás bírósági meghatalmazással rendelkezők részére *77*
9.3.6. Feltárás tulajdonos kérésére *77*
9.3.7. Feltárás más esetekben *77*
9.4. A SZEMÉLYES ADATOK VÉDELME 77
9.5. SZELLEMI TULAJDONHOZ FŰZŐDŐ JOGOK 78
10. TEVÉKENYSÉGÉRT VISELT FELELŐSSÉG ÉS HELYTÁLLÁS 78
10.1. A SZOLGÁLTATÓI FELELŐSSÉG ÉS HELYTÁLLÁS 78
10.2. AZ ELŐFIZETŐI FELELŐSSÉG ÉS HELYTÁLLÁS 78
10.3. AZ ÉRINTETT FÉL FELELŐSSÉGE 78
10.4. ÉRVÉNYESSÉGI IDŐTARTAM 78
10.5. IRÁNYADÓ JOG 78

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 Hitelesítés Szolgáltatási Szabályzat (továbbiakban HSZSZ-T).

Jelen szabályzat a NISZ Zrt. kormányzati hitelesítés szolgáltatása keretében kiadott titkosító és egyéb nem aláírás célú tanúsítványokra vonatkozó eljárási és működési szabályokat tartalmazza.

A titkosító és egyéb 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 sszerinti 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.

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

1.1. Áttekintés

Jelen HSZSZ-T a [17] (Hitelesítési Rend titkosító és egyéb nem aláírás célú tanúsítványokra (HR-TET)) hatálya alá tartozó előfizetői tanúsítványokra vonatkozik.

Jelen HSZSZ-T célja, hogy összefogja azokat a szabályokat, adatokat és információkat, melyeket a Szolgáltató nem aláírás célú tanúsítványok kiadásával kapcsolatos szolgáltatásaival valamilyen módon kapcsolatba kerülő feleknek ismerni kell vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát, és lehetővé teszi a Szolgáltatásokat igénybe vevők számára, hogy megállapítsák azt, hogy az ismertetett szolgáltatási gyakorlat, valamint a kibocsátott tanúsítványok mennyiben felelnek meg az elvárásaiknak.

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

1.2. A dokumentum neve és azonosítója

Jelen dokumentum teljes neve: Szolgáltatási Szabályzat nem aláírás célú tanúsítvány szolgáltatásokhoz.

Jelen dokumentum rövid neve: HSZSZ-T

A dokumentum objektum-azonosítója (OID) és verziószáma a címlapon található.

A Szolgáltató jelen dokumentum valamint az egyéb kapcsolódó publikus dokumentumok egyedi azonosítója (OID) vonatkozásában az ISO/IEC [13] és az ITU [10] szabványok által előírt regisztrációs eljárásnak megfelelően jár el.

A HSZSZ-T nyomtatott formában a Szolgáltató PKI Ügyfélkapcsolati Irodájában, elektronikus változata a Szolgáltatások internetes honlapján érhető el. A szabályzatnak csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

1.3. A Szolgáltató és a felhasználói közösség

1.3.1. Szolgáltató adatai és elérhetőségei

Jelen dokumentummal kapcsolatos Szolgáltatásokat a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. nyújtja. A Szolgáltató általános adatai a következők:

Cégjegyzék szám:	01-10-041633
Székhely:	1081 Budapest, Csokonai u. 3.
Levélcím:	1389 Budapest, Pf.: 133.
Telefon:	+ 36 1 459-4200
Fax:	+ 36 1 303-1000
Internetes honlap címe:	www.nisz.hu

Kapcsolat az ügyfelekkel: PKI Ügyfélkapcsolati Iroda

Az ügyfelekkel való kapcsolattartás biztosítása érdekében a Szolgáltató ügyfélkapcsolati irodát tart fenn, mely egyben a Szolgáltatásokért illetékes szervezeti egység, és amelyet az ügyfelek személyesen illetve telefonon a nyitvatartási időben kereshetnek fel. A mindenkori nyitvatartási időket a Szolgáltató a Szolgáltatások internetes honlapján teszi közzé.

A PKI Ügyfélkapcsolati Iroda adatai a következők:

Cím:	1081 Budapest, Csokonai u. 3.
Telefon:	+ 36 1 795-7200, + 36 30 795-7200
Fax:	+36 1 795-0100
E-mail:	info@hiteles.gov.hu
Szolgáltatások internetes honlapjának címe:	http://hiteles.gov.hu

A tanúsítványok felfüggesztésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) biztosít. Az Ügyfélszolgálat elérhető a +36 1 795-7300 és a +36 30 795-7300 telefonszámokon, valamint elektronikus levélben az smc@nisz.hu címen.

Szolgáltatással kapcsolatos panaszok bejelentésének helye és módja

a. személyesen a Szolgáltató PKI Ügyfélkapcsolati Irodájában
b. írásban a Szolgáltató levelezési címére címezve
c. telefonon a PKI Ügyfélkapcsolati Irodában
d. elektronikus levélben az info@hiteles.gov.hu címen

Illetékes fogyasztóvédelmi felügyelőség

Nemzeti Fogyasztóvédelmi Hatóság Közép-magyarországi Regionális Felügyelősége
Cím: 1052 Budapest, Városház u. 7.
Telefon: +36 1 318-2681
Fax: +36 1 318-1639
Email: fogyasztovedelem@pest.b-m.hu

Fogyasztókapcsolati Iroda
Cím: 1088 Budapest, József krt. 6.
Telefon: + 36 1 459 4999, +36 1 459 4836
Ingyenes zöldszám: +36 80 201 205
Fax: +36 1 303 9075

1.3.2. Regisztrációs és hitelesítő szervezet

1.3.2.1. A Szolgáltató regisztrációs szervezete

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

Az Ügyfélkapcsolati Iroda (rövidítve ÜKI) 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 kapcsolódó adminisztrációval együtt.

A Regisztrációs Iroda (rövidítve RA) biztosítja az igénylők illetve Előfizetők technikai regisztrációját, a tanúsítványok előállításának, felfüggesztésének és visszavonásának jóváhagyását és kezelését, valamint az aláírás-létrehozó eszközön a magánkulcs 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 és 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.

1.3.2.2. A Szolgáltató hitelesítő szervezete

A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítő központokból (rövidítve: CA), 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 közzététele, 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.

1.3.3. Felhasználói közösség

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösség a következő:

a. a Szolgáltató regisztrációs és hitelesítő szervezete, illetve a szolgáltatásban részt vevő és erre feljogosított munkatársai
b. az Előfizetők és a velük kapcsolatban álló Tanúsítványtulajdonosok (természetes személyek vagy informatikai eszközök)
c. az Érintett felek

1.3.3.1. Előfizető

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

A szerződési feltételeket a [18] Általános Szerződési Feltételek a PKI szolgáltatásokhoz (továbbiakban: ÁSZF-PKI) tartalmazza.

Az Előfizető lehet jogi személy vagy jogi személyiség nélküli szervezet, a Tanúsítványtulajdonosok pedig jellemzően a szervezet munkatársai vagy informatikai eszközei (ld. következő pont)

1.3.3.2. Tanúsítványtulajdonos (alany)

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.

Fentiek alapján Tanúsítványtulajdonos:

- bármely természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítványnak megfelelően, a jelen szabályzat 3.2 pontjában előírtak szerint igazolta. A HR-TET [17] illetve a vonatkozó jogszabályi előírás alapján magánszemély a Szolgáltatótól közvetlenül nem igényelhet tanúsítványt.
- bármely természetes személy, aki részére a tanúsítvány azzal a céllal kerül kibocsátásra, hogy jogi személy vagy szervezet képviseletében azt felhasználja tevékenysége során, és akinek - a személyazonossága ellenőrzése mellett - a regisztráció során a 3.2.3 pontban meghatározott módon a képviseleti jogosultságot illetve az Előfizetőhöz, mint szervezethez tartozást is ellenőrizni kell.
- olyan szervezet (Előfizető), amely részére szervezeti vagy eszköz tanúsítvány kerül kibocsátásra, és amely szervezet nevében egy kijelölt személy vagy informatikai eszköz (mint felhasználó) a tanúsítványhoz tartozó magánkulcsot felhasználja. Szervezeti vagy eszköz tanúsítvány esetében az igényléskor meg kell nevezni azt a természetes személyt, aki az Előfizető részéről eljár a tanúsítvány igényléssel kapcsolatban (pl. az eszköz üzemeltetéséért felelős rendszergazda), és akinek a

regisztráció során a személyazonosságát és képviseleti jogosultságát a 3.2, 3.2.4 és 3.2.6 pontokban meghatározott módon ellenőrizni kell

1.3.3.3. 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 szabályzatban olyan természetes vagy jogi személyeket kell érteni, akik Szolgáltató ún. főtanúsítványát (Root CA) Szolgáltató kérelmére vagy azzal egyeztetve saját szoftverükkel együtt terjesztik.

1.4. Tanúsítványhasználat

1.4.1. A szolgáltatás szintje

A Szolgáltató jelen szabályozás keretében nem aláírás célú tanúsítvány kiadással kapcsolatos szolgáltatásokat nyújt, azaz a jelen szabályzat szerint kiadott tanúsítványok nem az [1] Eat. 2.§. 15. pontjában meghatározott fokozott biztonságú vagy minősített elektronikus aláíráshoz kapcsolódó tanúsítványok.

1.4.2. Tanúsítványok alkalmazhatósága

Engedélyezett tanúsítványhasználat

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 web-szerverek 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[2] 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 szabályzatában, vagy az előfizetői szerződésben rögzít.

Az Előfizető szervezet is élhet korlátozásokkal a Tanúsítványtulajdonosok és az Érintett felek tanúsítvány felhasználási tevékenységével kapcsolatosan.

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

Tiltott tanúsítványhasználat

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

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

A kód- illetve üzenet-aláíró tanúsítványok titkosításra vagy azonosításra történő felhasználása, más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen hitelesítés szolgáltatás nyújtásához történő alkalmazása tilos.

Egyéb szabályok

A fentieken túl a Szolgáltató által kibocsátott tanúsítványok (illetve az ezekhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, amelyek támogatják a PKI technológián alapuló titkosítási és azonosítási illetve műszaki értelemben vett aláírási funkciókat.

A Szolgáltató nem vállal felelősséget a kibocsátott tanúsítványok, illetve az ezekhez kapcsolódó kulcspárok fentiekben meghatározott céltól eltérő felhasználásáért.

A tanúsítványok elfogadása, a feltüntetett használati információktól eltérő bármely módú használata az Előfizetők, Tanúsítványtulajdonosok és az Érintett fél egyéni felelőssége és kockázata.

1.5. A szolgáltatási szabályzat adminisztrációja

1.5.1. Szabályzat hatálya

A HSZSZ-T aktuális verziójának időbeli hatálya a címoldalon jelzett hatálybalépés dátumával kezdődik, és határozatlan időre szól. Időbeli hatálya megszűnik egy újabb szabályzat verzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor.

A HSZSZ-T személyi hatálya a Szolgáltatóra, annak a Szolgáltatásokban közreműködő munkatársaira, valamint az Előfizetőkre és a Tanúsítványtulajdonosokra terjed ki. A HSZSZ-T az Érintett felekkel kapcsolatban ajánlásokat fogalmaz meg.

A HSZSZ-T tárgyi hatálya kiterjed az 1. pontban meghatározott Szolgáltatásokra illetve ezek keretében kibocsájtott tanúsítványokra, valamint Szolgáltatónak a fenti Szolgáltatásokkal kapcsolatban álló összes objektumára és tárgyi eszközére.

1.5.2. Szabályzatra vonatkozó változáskezelés

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoport működik, amely a HSZSZ-T karbantartásáért felelős. A szolgáltatási szabályzat hitelesítési rendeknek való megfeleléséért a Hitelesítési Rend és Szabályozási Csoport, illetve annak vezetője felel. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, az új szabályzat verziókat jóváhagyásra előterjeszti, elektronikus aláírással hitelesíti, a hatályon kívül helyezett szabályzatokat archiválja és 10 évig, illetőleg a kiadott tanúsítvánnyal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi.

A szabályzatot a Szolgáltató vezetése hagyja jóvá és lépteti hatályba.

A szolgáltatási szabályzat módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

A szabályzattal, illetve a szolgáltatással kapcsolatos észrevételeket a Szolgáltató vezetésének kell címezni. A Szolgáltató részéről a kapcsolattartó személy a PKI szolgáltatásokért általánosan felelős vezető. Elérhetőségét, valamint a jelen szabályzattal kapcsolatos észrevételek fogadását Szolgáltató a PKI Ügyfélkapcsolati Irodán keresztül biztosítja.

1.5.3. Közzétételi és tájékoztatási elvek

1.5.3.1. A HSZSZ-T-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a Szolgáltatások biztonságát nem veszélyezteti ([17], [18]). A Szolgáltató több belső biztonsági és egyéb szabályzattal ([14], [15]) illetve operatív szintű előírással rendelkezik ([16], [19]), melyeket bizalmasan, üzleti titokként kezel.

1.5.3.2. A HSZSZ-T közzététele

A Szolgáltató jelen szabályzatát a Szolgáltatások internetes honlapján teszi közzé, nyomtatott formában pedig PKI Ügyfélkapcsolati Irodában biztosít hozzáférést a szabályzathoz.

1.5.4. Elfogadási eljárások

A jelen HSZSZ-T szerkezetében és tartalmában követi az RFC 3647 szabványt [11] azzal az eltéréssel, hogy a szabályzat nem tartalmazza a nem értelmezhető, vagy lényegi előírásokat nem tartalmazó fejezeteket, illetve tartalmaz az RFC-ben nem tárgyalt fejezeteket is.

A Szolgáltató a jelen szabályzatát indokolt esetben, de legalább évente egyszer felülvizsgálja.

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 HSZSZ-T jogszabályoknak és a vonatkozó szakmai előírásoknak illetve ajánlásoknak való megfelelőségét Szolgáltató által megbízott küldő auditor is megvizsgálja.

1.6. Meghatározások

Alany: a Szolgáltató által kiadott tanúsítványban azonosított entitás, aki/amely a tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

Aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró a magánkulcsok felhasználásával az elektronikus aláírást létrehozza. Nem aláírás célú tanúsítványok esetében olyan hardver illetve szoftver eszköz, mely a tanúsítványhoz kapcsolódó magánkulcs biztonságos tárolását, hordozását és használatát biztosítja

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.

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

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

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

Elektronikus aláírás: elektronikusan aláírt elektronikus dokumentumhoz azonosítási célból logikailag hozzárendelt, vagy ahhoz elválaszthatatlanul összekapcsolt elektronikus adat.

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

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

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes.

Előfizető: Az a szervezet, amely Szolgáltatóval érvényes előfizetői szerződéssel rendelkezik a Szolgáltatások igénybe vételére

Elsődleges hitelesítő központ (ROOT CA, vagy Főtanúsítvány kiadó): az elsőnek létrehozott, fizikailag is működő hitelesítő központ, amely az alája rendelt másodlagos (produktív) hitelesítő központokat hitelesíti,

Érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített aláírás, illetve időbélyeg, valamint az azokhoz kapcsolódó tanúsítvány az aláírás és időbélyeg elhelyezésének időpontjában érvényes volt. Nem aláírás célú tanúsítványok esetében olyan egymáshoz rendelhető információk sorozata, amelyek segítségével megállapítható ezen tanúsítványok érvényessége egy adott időpontban.

Érintett fél: Az a természetes személy vagy szervezet, aki/amely az elektronikusan aláírt dokumentum fogadója, és az adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az aláírás hitelességének ellenőrzésekor. Nem aláírás célú tanúsítványok esetén az Érintett fél olyan természetes vagy jogi személy, aki vagy amely a Szolgáltató által kiadott tanúsítvány érvényességét ellenőrzi, és erre hagyatkozva jár el.

Fokozott biztonságú elektronikus aláírás: elektronikus aláírás, amely megfelel a következő követelményeknek: alkalmas az aláíró azonosítására, egyedülállóan az aláíróhoz köthető, olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak és a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető

Felhasználó (végfelhasználó): olyan entitás, aki/amely a Szolgáltatások keretében előállított kulcsokat és tanúsítványokat rendeltetésüknek megfelelően használja.

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

Hitelesítő központ (CA): a Szolgáltató azon egysége, amely a végfelhasználók számára a tanúsítványok kiállításával kapcsolatos tevékenységet végzi. A CA fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.

Hitelesítés-szolgáltatás: az [1] Eat. 6.§ (2) szerint meghatározott szolgáltatás, melynek keretében a hitelesítés-szolgáltató azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány aktuális állapotára (különösen esetleges felfüggesztésére vagy visszavonására) vonatkozó információkat.

Hitelesítés-szolgáltató: az [1] Eat. 6.§ (2) szerint meghatározott hitelesítés-szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet. Lásd még: **Szolgáltató**

Igénylő: Az a személy, amely Szolgáltatóhoz fordul a szolgáltatás igénybe vétele céljából.

Informatikai rendszer: a Szolgáltató által a szolgáltatói kulcspár kezeléséhez, a magánkulcs előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezelési szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt eszközök és termékek

Időbélyeg: elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegzés időpontjában változatlan formában létezett.

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

Kulcsletét: Szolgáltató által kiadott titkosító tanúsítványokhoz kapcsolódó tevékenység, melynek keretében Szolgáltató az általa előállított magánkulcsból – annak az Előfizető illetve Tanúsítványtulajdonos részére történő átadását követően - egy másolatot biztonságos módon megőriz, és azt az Előfizető vagy Tanúsítványtulajdonos kérésére számunkra ismételten átadja, díj ellenében

Kompromittálódás: Az az eset, amikor a magánkulcs illetve az aláírás-létrehozó eszköz használatára arra nem jogosított személy képessé válik.

Kriptográfiai modul (Hardware Security Module – HSM): Hardver alapú biztonsági megoldás, amely alkalmas beépített eljárások segítségével biztonságos kulcsgenerálásra és tárolásra.

Lenyomat: olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket: a képzett lenyomat egyértelműen származtatható az adott elektronikus dokumentumból; a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés; a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, amelyre alkalmazva a lenyomatképző eljárás eredményeképp az adott lenyomat keletkezik

Magánkulcs aktiválása: A magánkulcs aktiválása az a folyamat, melynek során a jogosult – különböző azonosító elemek pl. jelszó, PIN-kód megadásával – engedélyezi, hogy a leolvasóba helyezett magánkulcs megkezdje üzemszerű működését. Az aktiválás általában a

magánkulcsot igénylő környezetben (dokumentumkezelő, levelező rendszer) történik, és érvényes lehet a visszavonásig (deaktiválásig) illetve egyszeri használatra.

Magánkulcs deaktiválása: A magánkulcs deaktiválása az a folyamat, melynek során a magánkulcs üzemszerű működése megszüntetésre kerül.

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

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

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

Regisztrációs adatok: Azon információk, adatok összessége, amelyeket a Szolgáltató a tanúsítványkiadás érdekében az Előfizetőről illetve a Tanúsítványtulajdonosokról begyűjt.

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

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

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

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

Szolgáltatási szabályzat: A Szolgáltató szolgáltatási tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.

Szolgáltató: elektronikus aláírással kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet. Nem aláírás célú tanúsítványok esetén ezen tanúsítványok kiadásával kapcsolatos szolgáltatásokat nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet.

Szolgáltatói kulcspár: a szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs

Szolgáltatói magánkulcs: olyan kriptográfiai magánkulcs, amelyet a szolgáltató saját elektronikus aláírással kapcsolatos szolgáltatásainak igazolására, így különösen a tanúsítványok kibocsátásához, a visszavonási nyilvántartásokhoz, illetve a naplózáshoz használ

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

Tanúsítvány: A Szolgáltató által kibocsátott igazolás, amely a nyilvános kulcsot az elektronikus aláírásról szóló törvény szerint egy meghatározott személyhez kapcsolja és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget. Nem aláírás célú tanúsítványok esetén a Szolgáltató által kibocsátott igazolás, amely a nyilvános kulcsot a HSZSZ-T és HR-TET szerint egy meghatározott személyhez kapcsolja és igazolja e személy személyazonosságát vagy valamely más tény fennállását.

Tanúsítványok fajták: A tanúsítványok tulajdonosa vagy felhasználása szerinti megkülönböztetése (pl. személyes, munkatársi, szervezeti, vagy előfizetői, szolgáltatói, teszt).

Tanúsítvány kibocsátása: a tanúsítvány átadása az arra jogosult személynek (pl. Tanúsítványtulajdonosnak), valamint a tanúsítvány elérhetővé tétele a tanúsítványtárban

Tanúsítványtár: X. 500 szabvány alapú címtár, amelyben a tanúsítványok rendszeresen frissülnek. Tartalma nyilvánosan elérhető LDAP-al vagy web lapról.

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

Visszavonás kezelése: a HSZSZ-T és HR-TET szabályzatokban meghatározott esetekben a kibocsátott tanúsítványok visszavonására és felfüggesztésére vonatkozó eljárások lefolytatása;

Visszavonási nyilvántartások: olyan nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját (év, hó, nap, óra, másodpercben)

1.7. Hivatkozások

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

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

[2] 84/2012. (IV.21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

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

[4] 78/2010. (III.25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól

[5] 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

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

[7] 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

[8] 7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

[9] 2/2002. (IV. 26) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről*

* A 2/2002. (IV.26) MeHVM irányelv nem hatályos jogszabály, de az aktuális részeit Szolgáltató ajánlásként figyelembe veszi a fokozott elektronikus aláírással kapcsolatos szolgáltatásaihoz

Hivatkozott ajánlások, szabványok:

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

[11] Internet Közösség RFC 2459, RFC 3280, RFC 822, RFC 2560 és RFC 3647 ajánlásai

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

[13] MSZ ISO/IEC 27001 szabvány

A Szolgáltató hivatkozott dokumentumai:

[14] A NISZ Zrt. Szervezeti és Működési Szabályzata

[15] A NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája

[16] A NISZ Zrt. PKI szolgáltatások biztonsági szabályzata

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

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

[19] A PKI szolgáltatások üzletmenet-folytonossági terve

[20] Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz

Egyéb hivatkozott dokumentumok

[21] CA Browser Forum Baseline Requirements

Ezeken túlmenően a Szolgáltató az üzleti titkok vonatkozásában a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény, a személyes adatok vonatkozásban az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény szerint jár el.

1.8. Tanúsítványok jellemzői

Jelen HSZSZ-T a nyilvános körben kibocsátott, titkosító és egyéb nem aláírás célú (SSL szerver authentikációs, SSL kliens authentikációs, kód/üzenet aláíró) tanúsítványokra vonatkozik.

Ezen tanúsítványok jellemzőit a Szolgáltató [17] Hitelesítési Rend titkosító és egyéb nem aláírás célú tanúsítványokra (HR-TET) dokumentumának 1.5.2 pontja írja le.

A nem aláírás célú tanúsítvány a CWA 14167-1:2001 [12] ajánlásnak megfelelően a Tanúsítványtulajdonos és nyilvános kulcsának összetartozását tanúsítja.

A tanúsítványok tartalmazzák:

- 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 szabályzat szerint kiadott SSL szerver tanúsítványok tekintetében Szolgáltató megfelel a [21] CA Browser Fórum Baseline Requirement dokumentumában foglalt előírásoknak. Erre tekintettel SSL szerver tanúsítványokat Szolgáltató csak magyarországi szervezete részére bocsájt ki, olyan domain nevekre, amelyek Magyarországon kerültek bejegyzésre (azaz .hu végződésű nevek), magyarországi DNS (Domain Name System) regisztrátor által. Szolgáltató által kiadott SSL szerver tanúsítványok nem tartalmazhatnak IP címeket.

Szolgáltató láncolt tanúsítványkiadó egységek felülhitelesítését nem támogatja, így a jelen szabályzat szerinti tanúsítványok mind Szolgáltató által kiadott tanúsítványok.

1.8.1. Tanúsítványok fajtái

A jelen szabályzat szerint kiadott tanúsítványok felhasználási területe és célja szerint Szolgáltató megkülönböztet:

- előfizetői,
- szolgáltatói, és
- teszt tanúsítványokat.

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

A jelen szabályzat szerint kiadott előfizetői tanúsítványok tulajdonosa (alanya) alapján a Szolgáltató megkülönböztet:

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

1.8.1.1. Előfizetői tanúsítvány

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

Az előfizetői tanúsítványokhoz kapcsolódó hitelesítési rend ([17] Hitelesítési Rend titkosító és egyéb nem aláírás célú tanúsítványokra (HR-TET)) objektum-azonosítója (OID): 0.2.216.1.200.1100.100.42.3.5.9.X (ahol X a dokumentum verziója, pl. 1.1).

1.8.1.2. Szolgáltatói tanúsítvány

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

A saját kiadású Szolgáltatói tanúsítványok hitelesítési rendjének objektum-azonosítója (OID): 0.2.216.1.200.1100.100.42.3.1.5.1

1.8.1.3. Teszt tanúsítvány

A Szolgáltató teszt tanúsítványokat kizárólag tesztelési célokból ad ki.

A teszt tanúsítványok a Tanúsítványtulajdonosok által semmilyen olyan célra nem használhatók, amely esetében a tanúsítvány használatábóla magánkulcs vagy eszköz

illetéktelen kezekbe történő jutásából a Tanúsítványtulajdonosnak vagy Szolgáltatónak bármilyen kára származna. Teszt tanúsítványok használatából eredő károkért a Szolgáltató semmilyen felelősséget nem vállal.

A Teszt tanúsítványok azonosíthatók az alapján, hogy a tanúsítványok „Subject" / „Common Name" (CN) vagy valamelyik másik mezőjében megtalálható az erre való utalás (pl. 'teszt' vagy 'Teszt', vagy „kizárólag tesztelésre" szövegrészlet).

1.8.1.4. „Személyes" tanúsítvány

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

Ha a tanúsítvány CN mezőjében nem a Tanúsítványtulajdonos személyazonosító okmányában szereplő név kerül megadásra, úgy ez a név álnévként kerül rögzítésre.

A tanúsítvány egyéb adatokat is tartalmazhat, különböző kiterjesztés mezőkben, Szolgáltató erre vonatkozó dokumentuma ([20] Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz) szerint.

1.8.1.5. „Munkatársi" tanúsítvány

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.

„Munkatársi" tanúsítványok jogi személy vagy jogi személyiség nélküli szervezet munkatársai, tisztségviselői számára kerülnek kibocsátásra. Az Előfizető ebben az esetben a jogi személy vagy szervezet, a Tanúsítványtulajdonos pedig a szervezet munkatársa, tisztségviselője.

A tanúsítvány „Country" mezőjében a szervezet székhelyének (vagy telephelyének) országkódja, az „Organization" mezőben a szervezet neve, a „Common Name" (CN) mezőben a munkatárs (Tanúsítványtulajdonos) neve szerepel. A „Locality" mezőben a szervezet székhelyének (vagy telephelyének) városa, az opcionális „Organizational Unit" mezőben a szervezeti egység neve, a „SubjectAltName" mezőben a munkatárs (Tanúsítványtulajdonos) e-mail címe szerepel.

Ha a tanúsítvány CN mezőjében nem a Tanúsítványtulajdonos személyazonosító okmányában szereplő név kerül megadásra, úgy ez a név álnévként kerül rögzítésre.

A tanúsítvány egyéb adatokat is tartalmazhat, különböző kiterjesztés mezőkben, Szolgáltató erre vonatkozó dokumentuma ([20] Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz) szerint.

1.8.1.6. „Szervezeti" vagy eszköz tanúsítvány

Szervezeti vagy eszköz tanúsítvány esetében a Tanúsítványtulajdonos nem természetes személy, hanem egy szervezet, amely ennek megfelelően kerül regisztrálásra illetve feltüntetésre a tanúsítványban.

„Szervezeti" vagy „eszköz" tanúsítványok jogi személy vagy jogi személyiség nélküli szervezet, illetve annak szervezeti egységei, szerepkörei vagy informatikai eszközei számára kerülnek kibocsátásra.

A tanúsítvány „Country” mezőjében a szervezet székhelyének (vagy telephelyének) országkódja, az „Organization” mezőben a szervezet neve, a „Common Name” (CN) mezőjében a szervezet illetve szervezeti egység hivatalos neve, vagy a szerepkör illetőleg az informatikai eszköz igénylőlapon megadott neve szerepel. A „Locality” mezőben a szervezet székhelyének (vagy telephelyének) városa, az „Organizational Unit” mezőben a szervezeti egység neve és a „SubjectAltName” mezőben a szervezeti egység e-mail címe szerepel.

A tanúsítvány egyéb adatokat is tartalmazhat, különböző kiterjesztés mezőkben, Szolgáltató erre vonatkozó dokumentuma ([20] Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz) szerint.

1.8.1.7. SSL szerver tanúsítvány

SSL szerver tanúsítvány esetében a Tanúsítványtulajdonos nem természetes személy, hanem egy szervezet domain neve, amely ennek megfelelően kerül regisztrálásra illetve feltüntetésre a tanúsítványban.

SSL szerver tanúsítványok jogi személy vagy jogi személyiség nélküli szervezetek web-szerverei számára kerülnek kibocsátásra.

A tanúsítvány „Country” mezőjében csak HU bejegyzés szerepelhet, azaz Szolgáltató csak magyarországi domain nevekre ad ki SSL szerver tanúsítványt. Az „Organization” mezőben a domain-név tulajdonosi jogaival rendelkező szervezet neve, a „Common Name” (CN) mezőjében a DNS szerint bejegyzett domain név (vagy wildcard-os név) szerepel. A „Locality” mezőben domain-név tulajdonosi jogaival rendelkező szervezet székhelyének (vagy telephelyének) városa, az „Organizational Unit” opcionális mezőben a szervezeti egység neve, a „SubjectAltName” mezőben pedig szintén a domain név (vagy wildcard-os név) szerepel.

A tanúsítvány egyéb adatokat is tartalmazhat, különböző kiterjesztés mezőkben, Szolgáltató erre vonatkozó dokumentuma ([20] Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz) szerint.

2. Általános rendelkezések

2.1. Feladatok és hatáskörök

2.1.1. A Szolgáltató feladatai és hatásköre

1. Szolgáltató az 1. fejezetben meghatározott Szolgáltatások nyújtása során az alábbi szolgáltatás elemeket biztosítja, a [17] HR-TET követelményeinek megfelelően:
   - regisztráció
   - tanúsítvány előállítás
   - tanúsítvány kiadás és szétosztás
   - visszavonás kezelés (ebben felfüggesztés és újraérvényesítés biztosítása)
   - visszavonási állapot közzététele
   - aláírás-létrehozó eszközön a magánkulcs elhelyezése
   - kulcsletét (igény esetén, kizárólag titkosító tanúsítvány kiadás keretében)
2. A Szolgáltató gondoskodik a Szolgáltatásokra vonatkozó valamennyi, a jelen HSZSZ-T-ben részletezett feltétel teljesüléséről, amennyiben azok az adott tanúsítványra alkalmazhatók.
3. A Szolgáltató szolgáltatásait nyilvánosan elérhetővé teszi.

4. A Szolgáltató jogi személy, ennek megfelelően felelősséget vállal a nyújtott Szolgáltatásokért.
5. A Szolgáltató rendszeresen felülvizsgálja HSZSZ-T-jét valamint a kapcsolódó publikus dokumentumokat ([17] HR-TET és [18] ÁSZF-PKI).
6. A Szolgáltató mindenkor az igénylők illetve Előfizetők által átadott és a regisztrációs szervezet által ellenőrzött adatok alapján bocsátja ki a tanúsítványokat. A Szolgáltató a tanúsítvány kibocsátását követően a tanúsítvány adatait nem változtatja meg.
7. A Szolgáltató a Tanúsítványtárában teszi közzé az általa kibocsátott tanúsítványokat, a visszavonási listákban pedig a felfüggesztett és visszavont előfizetői tanúsítványokat. A Tanúsítványtár és a visszavonási listák elérhetőségét a Szolgáltató 99%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 24 órás időtartamot.
8. A Szolgáltató kötelezettséget vállal arra, hogy hiánytalan igénybejelentés és megrendelés esetén a regisztrációt követően 30 napon belül a tanúsítvány kiadására intézkedik és erről az Előfizetőt vagy Tanúsítványtulajdonost értesíti.
9. A Szolgáltató a Szolgáltatások működtetése során az ügyfélkapcsolati tevékenységet Ügyfélkapcsolati Iroda illetve ügyfélszolgálat által biztosítja.
10. A Szolgáltató rendkívüli üzemeltetési helyzetben is biztosítja tanúsítványtára és visszavonási listái elérhetőségét, visszavonás kezelési, visszavonási állapot közzétételi szolgáltatását minden érdekelt fél számára. Ügyfélszolgálata útján folyamatos felügyeletet biztosít a tanúsítvány visszavonási és felfüggesztési igények kezelésére.
11. A Szolgáltató vezeti és a Szolgáltatások Internetes honlapján keresztül bárki számára folyamatosan elérhetővé teszi a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó saját szabályzatait (jelen HSZSZ-T, HR-TET [17], ÁSZF-PKI [18]). A szabályzatok közzétételét Szolgáltató 99%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 24 órás időtartamot.
12. A Szolgáltató a lejárat előtti 30 napban értesítést küld a lejáró tanúsítványokról az Előfizető vagy Tanúsítványtulajdonos részére.
13. Szolgáltató a tanúsítványban feltünteti az előfizetői szerződésben vagy más szabályozásban rögzített, a tanúsítvány felhasználhatóságával kapcsolatos esetleges korlátozásokat.
14. A Szolgáltató indokolt esetben felfüggeszti vagy visszavonja a tanúsítvány érvényességét és ezt a Szolgáltatások internetes honlapján közzéteszi.
15. Szolgáltató megőrzi a tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetőleg – amennyiben ezen időszakban a tanúsítvánnyal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.
16. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről legalább hatvan nappal korábban értesíti az Előfizetőket. A bejelentés időpontjától kezdve a Szolgáltató nem bocsáthat ki új tanúsítványt. A Szolgáltató a tevékenység befejezése előtt legalább húsz nappal visszavonja az általa kibocsátott és még érvényes tanúsítványokat. A Szolgáltató a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének eleget tesz.
17. Szolgáltató tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést készít. A mentett adatállományokat védi a jogosulatlan módosítástól, illetve biztosítja, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá, valamint, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

18. A Szolgáltató intézkedik 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 – átadja ezen szolgáltatónak.
19. Amennyiben szolgáltatásaihoz kapcsolódó egyes feladatait Szolgáltató kiadja alvállalkozóknak, úgy köteles ezen alvállalkozók ezirányú tevékenységét ellenőrizni. Ez esetben is Szolgáltató felelős elsődlegesen az alvállalkozók tevékenységéért, a vonatkozó jogszabályok szerint.

2.1.1.1. A Hitelesítő Szervezet feladatai és hatásköre

A Szolgáltató hitelesítő szervezete, illetve az általa működtetett hitelesítő központok – a [17] HR-TET követelményeinek megfelelően - biztosítják a tanúsítványok illetve a magánkulcsok kiadását, a visszavonási listák előállítását valamint közreműködnek ezek 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 hitelesítő központ (Főtanúsítványkiadó - „Root CA”) végzi a 2. szintű hitelesítő központ („Produktív CA”) hitelesítését, ezen belül tételesen a következőket:

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 központ ("Produktív CA”) hitelesítési kérelmeinek fogadása és ellenőrzése, részére 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-állapot szolgáltatás (OCSP – Online Certificate Status Protocol) nyújtása a „Produktív CA” tanúsítványokra vonatkozóan

A 2. szintű „Produktív CA” hitelesítő központ végzi az Előfizetők tanúsítványainak előállítását és hitelesítését:

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

2.1.1.2. A Regisztrációs Iroda feladatai és hatásköre

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

A Regisztrációs Iroda feladatait tételesen a [17] HR-TET dokumentum tartalmazza.

2.1.1.3. Az Ügyfélkapcsolati Iroda feladatai és hatásköre

Az Ügyfélkapcsolati Iroda elvégzi az igénylők illetve Előfizetők adatainak felvételét, az igénylők személyazonosságának megállapítását, a tanúsítvány kérelmek összeállítását és az előfizetői szerződésben foglaltak biztosítását.

Az Ügyfélkapcsolati Iroda feladatait tételesen a [17] HR-TET dokumentum tartalmazza.

2.1.1.4. A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Rend és Szabályozási Csoport elvégzi a Szolgáltatásokkal kapcsolatos hitelesítési rend, szolgáltatási szabályzat, valamint a belső szabályzatok kezelését. 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 rend, szolgáltatási szabályzat, az ÁSZF és a belső biztonsági szabályzatok készítése és rendszeres karbantartása.

A Hitelesítési Rend és Szabályozási Csoport feladatait tételesen a [17] HR-TET dokumentum tartalmazza.

2.1.1.5. Az Ügyfélszolgálat feladata

A tanúsítványokkal kapcsolatos felfüggesztési, illetve visszavonási kérelmeket a Szolgáltató Ügyfélszolgálata telefonon keresztül folyamatosan (napi 24 órában) fogadja, a felfüggesztési kérelmeket végrehajtja, valamint erről telefonon illetve emailben tájékoztatja a kérelmezőt illetve az Ügyfélkapcsolati Irodát.

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

2.1.2. Az Előfizető és a Tanúsítványtulajdonos feladatai és hatásköre

Az Előfizető és a Tanúsítványtulajdonos feladata és kötelessége általánosságban a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a Szolgáltatások igénybe vétele során. Az Előfizető és Tanúsítványtulajdonos feladatait tételesen [17] HR-TET dokumentum tartalmazza.

2.1.3. Az Érintett félre vonatkozó ajánlások tanúsítvány ellenőrzése során

Az Érintett félnek ajánlott a Szolgáltató szabályzataiban leírtaknak megfelelően a legnagyobb gondossággal eljárni a tanúsítvány illetve ennek érvényessége elbírálásakor.

Az Érintett félre vonatkozó ajánlásokat tételesen a [17] HR-TET dokumentum tartalmazza.

2.2. Felelősségek

2.2.1. A Szolgáltató felelőssége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-T szerint kiadott tanúsítványt – és ezzel jelzi a felhasználó közösség és az érintett felek felé ezen HSZSZ-T használatát – azért vállalja a felelősséget, hogy az igénylők regisztrációja, a tanúsítvány előállítása, kibocsátása, közzététele, visszavonása, a Tanúsítvány Visszavonási Lista (CRL) közzététele, a kulcsletét

szolgáltatás, valamint az OCSP tevékenységek a jelen HSZSZ-T-ben előírtaknak teljes mértékben megfelelnek, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltató maga és az Előfizetők is a jelen HSZSZ-T előírásainak megfelelően járjanak el.

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 - Ptk. 6:142.§ - szabályai szerint felelős a Szolgáltatások nyújtásával okozott kárért, ha megszegte a szolgáltatási szabályzatban (HSZSZ-T), az általános szerződési feltételekben ([18] ÁSZF-PKI) vagy az Előfizetői Szerződésben előírtakat. E szabályok megtartását kétség esetén a Szolgáltatónak kell bizonyítania.

A Szolgáltató általi felelősségvállalás mértéke az ÁSZF-PKI ([18]) 2.2 pontjával összhangban alapesetben 500 000 Ft.. Szolgáltató az Előfizetői Szerződésben ettől eltérő összegben is megállapodhat az Előfizetővel.

A Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott tanúsítvány a [17] HR-TET dokumentumban vagy jelen HSZSZ-T-ben 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.

A Szolgáltató felelősséget vállal minden – jelen HSZSZ-T-ben tárgyalt – tanúsítványokkal kapcsolatos szolgáltatásért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki.

2.2.2. Az 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 HSZSZ-T-ben, az ÁSZF-PKI-ban [18] és a vonatkozó jogszabályban ([1]) meghatározott módon és célra használta.

Fentiek alapján az Előfizető vagy a Tanúsítványtulajdonos köteles haladéktalanul tájékoztatni a Szolgáltatót:

a. az azonosításához szükséges személyazonosító adatokról, más személy (szervezet) képviseletében történő tanúsítvány használat esetén a képviseletre jogosult személy személyazonosító adatairól, a cégadatokról, továbbá mindezek változásáról;
b. a tanúsítvánnyal kapcsolatban észlelt - a szolgáltatási szabályzatban meghatározott - rendellenességről;

Az Előfizető és a Tanúsítványtulajdonos felelős a magánkulcs - illetve ha volt, 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 vállal felelősséget a magánkulcs vagy hordozójának elvesztéséből, vagy a kulcs biztonságának egyéb módon történő sérüléséből, elvesztéséből, illetve a PIN-kód illetéktelen tudomásra jutásból származó károkért.

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

Előfizető illetve Tanúsítványtulajdonos az SSL szerver és eszköz tanúsítványokat csak arra a szerverre/eszközre telepítheti, amelyikhez igényelték (különös tekintettel a Subject/Altname mező tartalmára is).

2.2.3. Az 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. Értelmezés és alkalmazás

2.3.1. Alkalmazott jogszabályok

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. Szerződéseire és szabályzataira, és azok teljesítésére, a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők. A Szolgáltató tevékenységére vonatkozó fő jogszabályok felsorolását az 1.7 fejezet tartalmazza.

Ezeken túlmenően a Szolgáltatónak az üzleti titkok vonatkozásában a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény szerint, a személyes adatok vonatkozásban az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) szerint, a szerződésszegéssel kapcsolatban a Magyar Köztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény 339. §-a szerint kell eljárnia.

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

2.3.2. Hatályosság, megszűnés, értesítések

2.3.2.1. Hatályosság

Jelen szabályzat személyi, tárgyi és időbeli hatályát az 1.5.1 pont tartalmazza.

Jelen szabályzat a vonatkozó hitelesítési renddel ([17] HR-TET) és az általános szerződési feltételekkel ([18] ÁSZF-PKI) kiegészítve a felhasználói közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza. Jelen szabályzat vagy az ÁSZF-PKI egyetlen pontja sem értelmezhető a hitelesítési rendben (HR-TET) foglalt értelmezéstől eltérően.

2.3.2.2. Megszűnés

Jelen szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

2.3.2.3. Értesítések

A Szolgáltató a Tanúsítványtulajdonosokat, Előfizetőket és Érintett feleket a Szolgáltatás internetes honlapján történő közzététellel, illetve az Ügyfélkapcsolati Irodában elérhető

dokumentumokkal tájékoztatja. Az Ügyfélkapcsolati Iroda az Előfizetőket és Tanúsítványtulajdonosokat esetenként írásban vagy elektronikus úton is értesíti.

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-mail-ben vagy faxon.

2.3.3. Vitás kérdések kezelése

Bármely vitás kérdés felmerülése esetén a Tanúsítványtulajdonosnak és/vagy 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. Az írásban vagy elektronikus úton történő kommunikáció esetében a feladó nevét és elérhetőségét fel kell tüntetni és a feladónak a küldeményt hitelesítenie kell. A panaszt a Szolgáltató az előterjesztéstől számított 15 munkanapon belül kivizsgálja és ennek eredményéről a panaszost írásban tájékoztatja.

A jogvitáik rendezésére vonatkozó szabályokat az ÁSZF-PKI [18] tartalmazza.

2.4. Közzététel

2.4.1. Adatbázisok

2.4.1.1. Tanúsítványtár

A Szolgáltató az általa kibocsátott előfizetői tanúsítványokat a Tanúsítványtárában helyezi el.

Az Tanúsítványtulajdonos vagy az Érintett fél a Szolgáltatások internetes honlapján keresztül érheti el a Tanúsítványtár adatait. A szolgáltatói tanúsítványok szintén a Szolgáltatások internetes honlapján érhetők el.

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

2.4.1.2. Naplók, regisztrációs adatok

A Szolgáltató a működése során keletkező naplófájlokat, regisztrációs adatokat belső adatbázisokban, fokozottan védett körülmények között tárolja. Ezen adatok nem kerülnek közzétételre.

2.4.1.3. Az adatbázisok elérésének szabályozása

A Szolgáltató minden Előfizető és Érintett fél számára elérhetővé teszi a Szolgáltatások internetes honlapját, azon keresztül Tanúsítványtárát és visszavonási listáit, olvasás céljából. A Tanúsítványtárban keresési lehetőséget biztosít a tanúsítványokban tárolt adatok alapján.

A Szolgáltató belső adatbázisait és egyéb adatállományait a jogszabályokban meghatározott kötelezettségeken túl csak és kizárólag a Szolgáltató biztonsági szabályzata [16] által meghatározott szerepkörű és jogosultságú munkatársai érhetik el.

2.4.2. A tanúsítványokra vonatkozó információk közzététele

A Szolgáltató gondoskodik arról, hogy a tanúsítványok és az azokhoz kapcsolódó információk, kikötések és egyéb feltételek az Előfizetők és az Érintett felek rendelkezésére álljanak. Ezek közé tartoznak különösképpen:

a. a hitelesítési rend ([17] HR-TET), valamint a jelen szolgáltatási szabályzat és a kapcsolódó ÁSZF-PKI

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

A Szolgáltató a szolgáltatói információkat elektronikus formában, a Szolgáltatások internetes honlapján keresztül teszi elérhetővé. Hitelesnek csak a Szolgáltató saját elektronikus aláírásával ellátott szabályzatai tekinthetők.

Hiteles dokumentumaihoz nyomtatott formában a Szolgáltató az Ügyfélkapcsolati Irodában biztosít hozzáférést.

Amennyiben a szolgáltatói tanúsítványok tekintetében kereszthitelesítésre kerül sor, úgy az erre vonatkozó információkat a Szolgáltató publikusan közzéteszi a honlapján.

Amennyiben a másodlagos („produktív CA") hitelesítő központok szolgáltatói tanúsítványa visszavonásra kerül, úgy az erre vonatkozó állapot információt Szolgáltató 24 órán belül mind a visszavonási lista, mind az OCSP szolgáltatása által közzéteszi.

2.4.3. A közzététel gyakorisága

Szolgáltató a kibocsátott előfizetői tanúsítványokat - az érintett Tanúsítványtulajdonos, illetve Előfizető hozzájárulása esetén - a Tanúsítványtárban a tanúsítvány előállítását követően 24 órán belül közzéteszi.

A Szolgáltató az általa működtetett hitelesítő központok szolgáltatói tanúsítványait a Szolgáltatások internetes honlapján a tanúsítványok használatba vételét követően 24 órán belül közzéteszi.

Amennyiben a másodlagos („produktív CA") hitelesítő központok szolgáltatói tanúsítványa visszavonásra kerül, úgy az erre vonatkozó állapot információt Szolgáltató 24 órán belül mind a visszavonási lista, mind az OCSP szolgáltatása által közzéteszi.

A tanúsítványokra vonatkozó szabályzatait Szolgáltató azok módosításakor, egyéb szolgáltatói közleményeit pedig eseti jelleggel teszi közzé, a Szolgáltatások internetes honlapján.

A visszavonási állapot információk nyilvánosságra hozatala tekintetében Szolgáltató a Tanúsítvány visszavonási listát (Certificate Revocation List - CRL) legfeljebb 24 óránként frissíti, azaz, két CRL megjelenése közötti idő nem haladja meg a 24 órát. Amennyiben egy tanúsítvány állapota megváltozik, a Szolgáltató a változást követő 1 órán belül új CRL-t állít elő és tesz közzé.

3. Azonosítási eljárások

3.1. Megnevezési konvenciók

3.1.1. Nevek típusa

A tanúsítványokban szereplő névmegadás az ITU-T[3] X.500 ajánlásának felel meg: X.500 formátum (ITU-T X.501 /ISO/IEC 9594-2:1997, RFC 2459).

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

Természetes személy alany esetén a tanúsítványban szereplő név (betű-, szóköz- és ékezet-helyesen) megegyezik a személyazonosság igazolására elfogadott hatósági okmányban (személyi igazolvány, jogosítvány vagy útlevél) feltüntetett valódi névvel.

Az ettől eltérő névmegadás álnévnek minősül.

3.1.2. Nevek szemantikája

Természetes személy alany esetében a tanúsítványban feltüntetett név megegyezik a személyazonosság igazolására elfogadott hatósági okmányban foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve a CN mezőben (CN = Vezetéknév + Keresztnév), az UTF-8 kódolást használva.

A Szolgáltató a személyazonosság igazolására elfogadott hatósági okmányban foglalt névtől eltérő nevet álnévként kezel és rögzít.

Nem természetes személy alany, valamint álnév használata esetében a tanúsítvány CN mezőjében feltüntetett név megegyezik az Előfizető által az igényléskor megadott névvel, az UTF-8 kódolást használva.

Titkosító, SSL kliens authentikációs, illetve kód/üzenet aláíró tanúsítvány „SubjectAltname” mezőjében az alanyhoz kapcsolódó elektronikus levelezési cím szerepel, melynek struktúrája megfelel az RFC 822 előírásainak. SSL szerver tanúsítvány esetén a subjectAltname mezőben a vonatkozó szakmai ajánlások ([11] és [21]) szerinti domain név szerepel.

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 biztosítja Tanúsítványtárában a tulajdonosazonosítók egyediségét, azaz gondoskodik arról, hogy az általa kiadott tanúsítványokban használt megkülönböztető nevet (DN) sohasem fogja egy másik entitáshoz rendelni.

Erről elsődlegesen a Tanúsítványtulajdonos nevének a „Subject/CommonName” almezőjében, valamint az entitáshoz rendelt egyedi azonosítónak a „Subject/Serialnumber” almezőjében való szerepeltetésével gondoskodik.

Az egyedi azonosítót az Ügyfélkapcsolati Iroda munkatársai az általuk használt ügyfélnyilvántartó rendszerben hozzák létre és rögzítik az adott entitáshoz.

3.1.4. Név igénylési viták feloldása

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

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

3.1.5. Álnevek használata

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

Álnév használata esetén a CN mezőben található szöveg '~' (tilde) karakterrel kezdődik és végződik (pl. CN= ~Ludas Matyi~).

3.1.6. Védjegyek elismerésének módszere

A tanúsítvány megrendeléssel illetve regisztrálással az Előfizető kifejezi, hogy a tanúsítványban foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik fél jogait. Szolgáltatónak – SSL tanúsítványok kivételével - nem kötelessége a védjegyek jogos használatának ellenőrzése, és nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában. Szolgáltató nem garantálja Előfizetők számára védjegyeik feltüntetését a tanúsítványban.

SSL szerver tanúsítványok esetén amennyiben Előfizető védjegyek, márkanevek, vagy egyéb olyan név megjelentetését igényli a tanúsítványban, amelyhez harmadik félnek joga fűződhet, Szolgáltató az igénylést csak akkor fogadja el, ha ezekről Előfizető hiteles igazolást nyújtott be, és az igazolás illetve az adatokat helyességét Szolgáltató saját maga is ellenőrizte.

3.2. Regisztráció

A regisztrációs folyamat lépései általánosságban a következők:

1. Az igénylő (Tanúsítványtulajdonos vagy Előfizető kapcsolattartója) kitölti a Szolgáltató által rendelkezésre bocsájtott regisztrációs űrlapot, saját kezűleg aláírja, majd aláíratja az Előfizető cégjegyzésre jogosult vezetőivel is, és végül az Ügyfélkapcsolati Iroda részére átadja személyesen vagy megküldi e-mailben vagy levélben, a Szolgáltató állal kért csatolmányokkal együtt (pl. aláírási címpéldány és 30 napnál nem régebbi cégkivonat másolata)
2. a regisztrációs űrlapot valamint csatolmányait a Szolgáltató Ügyfélkapcsolati Irodája ellenőrzi, és szükség esetén hiánypótlást kér. Hiánytalan igénylés esetén Szolgáltató gondoskodik az Előfizetői Szerződés előkészítéséről, a szükséges ellenőrzésekről, és intézkedik az előfizetői kulcspár és a tanúsítvány elkészítéséről (igény esetén az aláírás-létrehozó eszközzel együtt),
3. Az előfizetői tanúsítvány elkészültével értesíti a Tanúsítványtulajdonost és egyezteti vele a tanúsítvány, az előfizetői kulcspár és az Előfizetői Szerződés átvételének módját. Amennyiben az igény emelt szintű regisztrációra vonatkozott, az átadás-átvételéhez a Tanúsítványtulajdonos személyes megjelenése is kötelező a Szolgáltató Ügyfélkapcsolati Irodájában (vagy kihelyezett regisztráció keretében külön díj ellenében).

3.2.1. Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere

A Szolgáltató a Tanúsítványtulajdonos kriptográfiai kulcspárját a Szolgáltatások keretében maga állítja elő, vagy ún. kriptográfiai modulban (HSM), vagy pedig biztonságos aláírás létrehozó eszközön, kiemelt biztonságú környezetben, ezért a magánkulcs és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán a magánkulcs illetve eszköz (és a hozzá tartozó aktivizáló adat – PIN-kód) átvételének igazolása szükséges.

Az aláírás-létrehozó adat illetve eszköz átadása Szolgáltató ügyfélkapcsolati munkatársa által személyesen történik, az Előfizető részéről pedig a Tanúsítványtulajdonos vagy az Előfizető kijelölt kapcsolattartója személyesen kell jelen legyen és aláírásával igazolja a magánkulcs illetve eszköz valamint a kapcsolódó PIN-kód átvételét.

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.

Amennyiben Tanúsítványtulajdonos természetes személy és az átvételnél nem ő jelenik meg személyesen, Szolgáltató kérheti, hogy az Előfizető kapcsolattartója rendelkezzen Tanúsítványtulajdonos általi meghatalmazással az átvételre vonatkozóan. Ez csak az alap szintű regisztrációnál engedélyezett (emelt szintű regisztrációnál nem).

3.2.2. Regisztráció „Személyes" tanúsítvány igénylése esetén

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.

3.2.3. Regisztráció „Munkatársi" tanúsítvány igénylése esetén

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.

Munkatársi tanúsítványt a regisztrációs űrlap kitöltésével lehet igényelni, a 3.2 pontban leírt folyamatlépések szerint.

A regisztrációs űrlapon a következő adatokat lehet, illetve kell megadni:

1. Az igényelt tanúsítványra, a regisztrációs szintre, és az esetleges eszköz(ök)re vonatkozó adatok
2. Az Előfizető tekintetében:
   2.1. az Előfizető szervezet neve, székhelye és egyéb közcélú adatai
   2.2. az Előfizető szervezet képviseletére jogosult személy(ek) neve, beosztása
3. Az Tanúsítványtulajdonos (tanúsítványigénylő) tekintetében:
   3.1. annak a szervezeti egységnek a megnevezése, ahol a Tanúsítványtulajdonos dolgozik,
   3.2. annak a szervezeti egységnek a telephelye, ahol a Tanúsítványtulajdonos dolgozik
   3.3. Tanúsítványtulajdonos neve
   3.4. Tanúsítványtulajdonos álneve, ha annak megjelölésére a Tanúsítványtulajdonos igényt tart és azt számára az Előfizető engedélyezte
   3.5. a Tanúsítványtulajdonos anyja neve
   3.6. Tanúsítványtulajdonos születési helye és ideje,
   3.7. Tanúsítványtulajdonos állampolgársága és neme
   3.8. a Tanúsítványtulajdonos beosztása, telefonszáma, email címe
   3.9. a Tanúsítványtulajdonos személyazonosítására használt okmány típusa, száma
4. A megrendeléssel kapcsolatos egyéb adatok (pl. sürgősségi eljárás, helyszíni átadás)
5. A megrendeléshez csatolt dokumentumokra vonatkozó adatok

A regisztrációs űrlap tartalmazza Tanúsítványtulajdonos nyilatkozatát a Szolgáltatások igényléséhez megadott adatainak helyességére, valamint Szolgáltató feltételeinek elfogadására vonatkozóan. Hasonlóan, a regisztrációs űrlap tartalmazza az Előfizető képviseletére jogosult személy nyilatkozatát arról, hogy Tanúsítványtulajdonos a szervezethez tartozik, és a tanúsítványt használhatja és a szervezet képviseletében eljárjon. A regisztrációs űrlapot – mely az előfizetői szerződés mellékletének minősül - a Szolgáltató biztosítja; azon további adatok és információk megadására vonatkozó mezők is rendszeresíthetők.

Az Előfizető nevében eljáró, a cég- vagy szervezet képviseletére jogosult személy képviseleti jogát az Előfizetőnek a regisztráció során igazolnia kell. Ez 30 napnál nem régebbi cégkivonattal

(vagy egyéb hivatalos okmánnyal) és aláírási címpéldánnyal történik, melyek másolatát az igényléskor be kell küldeni Szolgáltató részére, majd a tanúsítvány átvételekor az eredeti dokumentumokat is be kell mutatni az Ügyfélkapcsolati Irodán.

Az előfizetői szerződés megkötése során az Előfizető kapcsolattartót nevezhet meg a Szolgáltató részére, aki aláírási joggal rendelkezik a tanúsítványok kibocsátását illetően; a Szolgáltató később e személynek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén. A Szolgáltató ez esetben jogosult a kapcsolattartó azonosítás-hitelesítését személyazonosítói igazolvány személyes bemutatásával elvégezni.

Amennyiben az igény nem emelt szintű regisztrációra szólt, a Tanúsítványtulajdonos személyazonosításához nincs szükség személyes megjelenésre; az ellenőrzést a regisztrációs űrlapon megadott személyazonosító adatok alapján végzi el az Ügyfélkapcsolati Iroda. Ilyen esetben viszont Tanúsítványtulajdonos meghatalmazottat kell megjelöljön Szolgáltató részére, aki az elkészült tanúsítványt és a magánkulcsot (a kapcsolódó eszközzel és/vagy aktivizáló adattal együtt) átveszi. Ilyenkor a meghatalmazás mellé Szolgáltató bekéri Tanúsítványtulajdonos írásos nyilatkozatát is a tanúsítvány használatával kapcsolatos kikötések és szabályok elfogadására vonatkozóan.

Amennyiben az igény emelt szintű regisztrációra szólt, a Tanúsítványtulajdonos ellenőrzéséhez szükség van a személyes megjelenésre is, alapesetben Szolgáltató Ügyfélkapcsolati Irodájában, vagy – ez irányú igény esetén – az Előfizető által megadott helyszínen (külső regisztráció keretében, külön díj ellenében). A személyes megjelenés illetve ellenőrzés történhet a tanúsítvány és a magánkulcs átadásakor is („feltételes regisztráció").

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

Az Ügyfélkapcsolati Iroda a bemutatott iratok és okmányok érvényessége és hitelessége, a Tanúsítványtulajdonos(ok) személyazonosságának megállapítása, valamint az aláírási jogosultság ellenőrzése céljából adategyeztetést végez (lásd: 3.2.5. pont).

A Szolgáltató megtagadja a tanúsítvány kibocsátását, ha a Tanúsítványtulajdonos(ok) személyazonosító adatokkal, az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétségek merülnek fel.

Hasonlóan, a Szolgáltató megtagadhatja a tanúsítvány és a megrendelt eszközök átadását, ha a bemutatott személyazonosító okmányával kapcsolatban, vagy az Előfizető szervezetére vonatkozóan bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel.

A tanúsítvány és a megrendelt eszközök átadásakor az Ügyfélkapcsolati Iroda munkatársának aláírásával kell igazolnia, hogy az átvevő személy (Tanúsítványtulajdonos vagy meghatalmazottja) azonosítását annak bemutatott személyazonosító okmánya alapján elvégezte.

A Szolgáltató a fentiekben leírtak alapján , nem emelt szintű regisztráció esetén eltekint a személyes megjelenéstől és a Tanúsítványtulajdonos személyes azonosításától; ugyanakkor az ebből fakadó károkért a felelősséget elhárítja. A Szolgáltató felelőssége az adatok teljeskörűségének ellenőrzésére, azok egyeztetésére (lásd 3.2.5 pont), illetve annak eldöntésére vonatkozik, hogy a rendelkezésre álló adatok alapján a tanúsítvány kibocsátható-e és az aláírás létrehozó adat (illetve eszköz) a kapcsolódó PIN-kóddal a megfelelő személynek (Tanúsítványtulajdonosnak vagy meghatalmazottjának) került-e átadásra.

3.2.4. Regisztráció „Szervezeti vagy eszköz" tanúsítvány igénylése esetén

Szervezeti vagy eszköz tanúsítvány esetében a Tanúsítványtulajdonos nem természetes személy, hanem egy szervezet vagy ennek egy eszköze, adott esetben egy webszerver illetve kapcsolódó domain név. Ennek megfelelően a tanúsítvány igénylésekor eljáró

természetes személy Előfizető kapcsolattartójaként értelmezendő, és jellemzően ő fogja használni vagy átvenni a tanúsítványt.

Szervezeti vagy eszköz tanúsítványt a regisztrációs űrlap kitöltésével lehet igényelni, a 3.2 pontban leírt folyamatlépések szerint.

A regisztrációs űrlapon a 3.2.3 pontban jelzett adatokat lehet illetve kell megadni, az alábbi különbségekkel:

1. Az Tanúsítványtulajdonos helyett a tanúsítványigénylő (természetes személy) adatait kell megadni
2. Az űrlapon meg kell adni a tanúsítvány CN mezőjébe kerülő szervezet vagy eszköz megnevezését
3. Meg kell adni a tanúsítvány SubjectAltname mezőjébe kerülő email címet.

Az Ügyfélkapcsolati Iroda a 3.2.3 pontban leírt - Tanúsítványtulajdonosra vonatkozó - ellenőrzéseket szervezeti vagy eszköz tanúsítvány esetén a tanúsítványigénylőre vonatkozóan végzi el. A regisztrációs űrlapon szereplő adatok ellenőrzése, az azonosítás rendje egyebekben a 3.2.3 pontokban feltüntetett módon történik, azzal a megjegyzéssel, hogy meghatalmazott illetve Előfizető képviselője itt nem értelmezhető.

3.2.5. Adategyeztetés

A Szolgáltató jogosult megállapítani a Tanúsítványtulajdonos (természetes személy) vagy Előfizető képviselője (szervezeti vagy eszköz tanúsítvány esetén) személyazonosságát a személyazonosításra alkalmas okmánya alapján.

Amennyiben a nem aláírás célú tanúsítvány igénylés mellett Előfizető benyújtott egy igényt fokozott biztonságú vagy minősített tanúsítványra vonatkozóan is, Szolgáltató a természetes személy igénylő személyazonosságának ellenőrzése céljából - megnevezésének és az adatfelhasználás céljának feltüntetése mellett - adategyeztetést végez a következő nyilvántartások közül legalább eggyel:

a. személyi adat- és lakcímnyilvántartás,
b. úti okmány-nyilvántartás,
c. járművezetői engedély-nyilvántartás;

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

3.2.6. Regisztráció SSL szerver (és Wildcard) tanúsítvány igénylése esetén

SSL szerver tanúsítvány esetében a Tanúsítványtulajdonos nem természetes személy, és a tanúsítványban egy szervezet domain nevét igazolja a Szolgáltató a publikus kulcshoz tartozás szempontjából. Ennek megfelelően a tanúsítvány igénylésekor eljáró természetes személy Előfizető kapcsolattartójaként értelmezendő, és jellemzően ő fogja átvenni a tanúsítványt illetve telepíteni a szervezet web-szerverére. Előfizetőnek Szolgáltató lehetővé teszi, hogy meghatalmazás alapján kijelölje a tanúsítványigényléssel megbízott kapcsolattartóját. Ilyen esetben Szolgáltató csak ettől a személytől fogadhat el tanúsítványkéréseket. A meghatalmazottak listáját Előfizető kérésére Szolgáltató átadja Előfizető részére.

SSL szerver (és Wildcard) tanúsítványt a regisztrációs űrlap kitöltésével lehet igényelni, a 3.2 pontban leírt folyamatlépések szerint.

A regisztrációs űrlapon a 3.2.3 pontban jelzett adatokat lehet illetve kell megadni, az alábbi különbségekkel:

1. Az Tanúsítványtulajdonos helyett a tanúsítványigénylő (természetes személy) adatait kell megadni
2. Az űrlapon meg kell adni a tanúsítvány CN mezőjébe kerülő domain nevet (vagy neveket, Wildcard tanúsítvány esetén)

Az Ügyfélkapcsolati Iroda a 3.2.3 pontban leírt - Tanúsítványtulajdonosra vonatkozó - ellenőrzéseket szervezeti vagy eszköz tanúsítvány esetén a tanúsítványigénylőre vonatkozóan végzi el. A regisztrációs űrlapon szereplő adatok ellenőrzése, az azonosítás rendje egyebekben a 3.2.3 pontokban feltüntetett módon történik.

További különleges szabályok SSL szerver tanúsítvány esetén.

a. igazolni kell a domain név Előfizetőhöz tartozását, a DNS (Domain Name System) regisztrátor által kiállított hivatalos igazolás Szolgáltatóhoz történő benyújtásával, melyből megállapítható, hogy az Előfizető a tanúsítványba bekerülő domain tulajdonosa. Ez alapján Szolgáltató meggyőződik arról, hogy az igényelt domain valóban az Előfizető birtokában van és azt jogosult használni.

b. a Szolgáltató meggyőződik arról is, hogy az igénylő jogosultsága valóban fennáll-e az igényben jelzett domain esetén. Ehhez be kell nyújtani
- vagy az internet szolgáltató (domain regisztrátor) által kiállított igazolást, melyből megállapítható, hogy az igénylő szervezet a tanúsítványba bekerülő domain tulajdonosa,
- vagy a domain tulajdonos által kiállított hivatalos dokumentumot (nyilatkozat, vagy meghatalmazás), mely igazolja az igénylő jogosultságát az adott domainre vonatkozó igénylés benyújtására és a tanúsítvány átvételére

c. Fenti esetekben benyújtott igazolások alapján Szolgáltató meggyőződik azok valóságtartalmáról, az igénylőtől és Előfizetőtől függetlenül megszerzett információk alapján történő ellenőrzéssel:
- Ha Szolgáltató az igénylő jogosultságát az internet szolgáltató (vagy domain regisztrátor) által kiállított igazolás alapján kívánja megállapítani, akkor ellenőriznie kell a dokumentum eredetiségét (kizárandó, hogy az előfizető hamis igazolást nyújtva kapjon tanúsítványt); ezt telefonos és/vagy emailes megkereséssel ellenőrizheti közvetlenül a domain regisztrátornál (nem az igénylő által megadott hozzáférhetőségeken, hanem a domain regisztrátor publikus web-lapján jelzett elérhetőségeken)
- Szolgáltató felhívja (vagy emailen megkeresi) a DNS regisztrátort, és megkérdezi, hogy az adott domaint valóban az igénylő illetve Előfizető regisztráltatta-e nála. A hívás dátuma és időpontja, a hívott fél neve és telefonszáma, valamint a telefonos ellenőrzés eredménye rögzítésre kerül.
- Szolgáltató felhívja (vagy emailen megkeresi) az igényelt domain tulajdonosát azon a telefonszámon, amit a DNS regisztrátortól kapott, és rákérdez, hogy valóban ők igényeltek-e SSL tanúsítványt az adott domainre, vagy ők bízták-e meg igénylőt az adott domainra vonatkozó igény benyújtásával
- Szolgáltató felhívja (vagy emailen megkeresi) a Whois adatbázisban az adott domainhez bejegyzett technikai / adminisztratív személyt, és rákérdez, hogy valóban ők igényeltek-e SSL tanúsítványt az adott domainre, vagy ők bízták-e meg igénylőt az adott domainra vonatkozó igény benyújtásával

- Szolgáltató küld egy emailt azon email címekre, melyek az igényelt domainhez tartoznak és a következő előtagokkal rendelkeznek: ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’, ‘postmaster ’. Az emailben kéri a címzettek, hogy küldjön válaszüzenetet számára 10 napon belül. Amennyiben az összes emailcím esetében az a válaszüzenet jön, hogy az email cím nem létezik, akkor Szolgáltató megtagadja az adott domainre a tanúsítvány kiállítását. Amennyiben 10 napon belül nem jön válaszüzenet, Szolgáltató megtagadhatja a tanúsítvány kiadását.
- Szolgáltató fentiek mellett egyéb módon is meggyőződhet a kérelmező domainra használatra vonatkozó jogosultságáról[4]

d. a Szolgáltató [17] szabályzata (HR-TET) 1.5.2. pontjának megfelelően Szolgáltató ellenőrzi, hogy az igényelt domaint Magyarországon jegyezték-e be[5], a domain regisztrátor által szolgáltatott országkód valóban C=HU, és csak akkor adja ki a tanúsítványt az igényelt domain-ra, ha az ellenőrzés pozitív eredménnyel zárult

e. Szolgáltató az igénylés során beadott dokumentumokat (pl. a domain regisztrátor által kiadott igazolást) csak akkor fogadja el, ha azok még hatályosak illetve nem régebbiek 1 évnél.

f. védjegyek tekintetében Szolgáltató a 3.1.6 pontban leírt ellenőrzést is megteszi, hogy meggyőződjön az igény jogosságáról. A kiadott SSL szerver tanúsítvány nem tartalmazhat védjegyet, márkanevet vagy egyéb ilyen jellegű nevet anélkül, hogy azok helyességét és használatára vonatkozó jogosultságot igénylő illetve Előfizető ne igazolta volna és Szolgáltató ne ellenőrizte volna.

g. Szolgáltató nem adhat ki olyan web-szerver tanúsítványt, amely esetében az igényelt domain az ICANN[6] szervezetnél ún. elfogadásra váró gTLD domainként szerepel (generic TopLevelDomain, pl. a .info domain)

h. Szolgáltató havonta ellenőrzi, hogy az ICANN kiadott-e új gTLD domaint, és ellenőrzi, hogy van-e érvényes kiadott tanúsítvány erre a domain-ra. Amennyiben igen, ezt vissza kell vonnia 120 napon belül, hacsak az Előfizető igazolni tudja, hogy jogosult használni az adott gTLD-t

i. Szolgáltató a benyújtott igényléseket megvizsgálva jogosult bizonyos igényeket Magas Kockázatú Kérelmeknek minősíteni. Ezen Magas Kockázatú Kérelmek esetében az igényléseket további intézkedésekkel ellenőrizheti: a Szolgáltató ügyfélmenedzsere vagy az Ügyfélkapcsolati Iroda munkatársa kimegy az igénylőhöz, és helyszíni szemle keretében győződik meg a kérelmező adatainak hitelességéről, melynek eredményét dokumentálnia kell (feljegyzés készítésével és Ügyfélkapcsolati Iroda általi megőrzéssel)

További különleges szabályok Wildcard SSL szerver tanúsítványok esetén

a. egy Wildcard-os tanúsítvány kibocsájtását megelőzően Szolgáltatónak fel kell ismernie és ki kell szűrnie, ha a * karakter egy top level domain (pl. *.hu) vagy egy nyilvános általános domain (pl. *.com vagy *.co.uk) mellett közvetlenül helyezkedne el (attól balra)

b. a nyilvános általános domainek esetén Szolgáltató megvizsgálja a “public suffix listát”a http://publicsuffix.org címen

[4] www.iplocation.net,

[5] Country Code Top-Level Domain alapján

[6] Internet Corporation for Assigned Names and Numbers

c. Szolgáltató nem adhat ki olyan wildcard-os tanúsítványt, amely az előző pontban kiszűrésre került (hacsak az igénylő nem igazolja a teljes domain név tartományra vonatkozó jogát)

Szolgáltató az elutasított igényléseket (valamint a visszavont tanúsítványokat) nyilvántartja, a csalások és visszaélések elkerülése érdekében.

Amennyiben Szolgáltató az igények elbírálásakor illetve az adatok ellenőrzésekor a közhiteles adatforrásokon túli egyéb adatforrásokat is felhasznál (pl. RIPE NCC[7], IANA[8]), akkor ezek pontosságát és megbízhatóságát felhasználás előtt megvizsgálja (milyen gyakran frissítik az adatforrásokat, mennyire hamisítható az adatforrás, és mennyire nyilvános az adatforrás). Ilyen tekintetben a Szolgáltató saját adatforrásai nem használhatók az az igénylő illetve Előfizető által benyújtott adatok ellenőrzéséhez.

4. A tanúsítvány-életciklusra vonatkozó szabályok

4.1. Tanúsítványigénylés

4.1.1. Ki nyújthat be tanúsítványkérelmet

Tanúsítványkérelmet azok az Előfizetők nyújthatnak be, akik előzetesen a Szolgáltatóval szerződéses kapcsolatot létesítettek. A kérelmező csak az adott szervezetet képviselő személy lehet, aki személyazonosságát a regisztráció során hitelt érdemlően igazolta (lásd: 3.2.3.-3.2.6. pontok).

A Szolgáltató azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatja az Előfizetőt illetve a Tanúsítványtulajdonost a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről. Ez alapesetben a Szolgáltatások internetes honlapján közzétett Tájékoztatóval és szabályzatokkal történik, de igény esetén az Ügyfélkapcsolati Iroda munkatársai telefonon illetve személyesen is tájékoztatják az igénylőket.

4.1.2. A tanúsítványigénylés folyamata és a résztvevők felelőssége

Tanúsítvány igényléséhez ki kell tölteni a Szolgáltató által rendelkezésre bocsájtott regisztrációs űrlapot és le kell folytatni a regisztrációs eljárást. Az űrlap nyomtatott vagy elektronikus formában igényelhető az Ügyfélkapcsolati Irodánál, vagy elektronikus formában letölthető a Szolgáltatások internetes honlapjáról.

Az Előfizetői Szerződés aláírásával Előfizető egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, valamint saját kötelezettségei vonatkozásában tájékozódott, azokat elfogadja.

Az Előfizető illetve a Tanúsítványtulajdonos aláírásával igazolja azt is, hogy:

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

Az Tanúsítványtulajdonosnak (tanúsítványigénylőnek) a Szolgáltató felkérésére írásban kell nyilatkozni arról, hogy hozzájárul a Szolgáltatások során felhasznált személyes adatai Szolgáltató által történő nyilvántartásba vételéhez, tanúsítványa és az azzal kapcsolatos

[7] Réseaux IP Européens Network Coordination Centre

[8] Internet Assigned Numbers Authority

állapot információk szolgáltatói tanúsítványtárban való közzétételéhez, s ezen adatok harmadik félhez történő továbbításához a Szolgáltató Szolgáltatásainak leállítása esetén, illetve egyéb, jogszabályok által meghatározott esetekben. Ez a nyilatkozat a regisztrációs űrlap aláírásával történik.

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. A tanúsítvány kérelem feldolgozása

4.2.1. Azonosítási funkciók megvalósítása

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

4.2.2. A tanúsítványkérelem jóváhagyása vagy visszautasítása

A Szolgáltató az előfizetői szerződés aláírásával hagyja jóvá a tanúsítványkérelmet.

A tanúsítványkérelem visszautasítása esetén a Szolgáltató az igénylővel előfizetői szerződést nem köt.

4.2.3. A tanúsítványigénylések feldolgozásának időtartama

A tanúsítványigénylések feldolgozásának időtartama legfeljebb 30 nap.

4.3. Tanúsítvány kibocsátás

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

Az elkészült tanúsítvány a következő módon jut el az Előfizetőhöz:

a. az Előfizető kijelölt kapcsolattartója, a Tanúsítványtulajdonos vagy annak meghatalmazottja (aki előfizető kijelölt kapcsolattartója is lehet egyben) személyesen átveszi az Ügyfélkapcsolati Irodán, a magánkulccsal illetve adott esetben az aláírás-létrehozó eszközzel és a kapcsolódó PIN-kóddal együtt, vagy

b. az Előfizető kapcsolattartója vagy a Tanúsítványtulajdonos letölti a Szolgáltató nyilvános Tanúsítványtárából

A tanúsítvány valamint a magánkulcs (illetve aláírás-létrehozó eszköz) és PIN-kód átadását megelőzően az Ügyfélkapcsolati Iroda ellenőrzi az átvevő személyét és jogosultságát, a 3.2.3., 3.2.4 és 3.2.6 pontoknak megfelelően.

4.4. Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető illetve a Tanúsítványtulajdonos részéről az átvétellel történik meg.

A tanúsítvány illetve a magánkulcs használatba vétele előtt az Előfizető kijelölt kapcsolattartójának illetve a Tanúsítványtulajdonosnak kötelessége ellenőrizni a tanúsítványban feltüntetett adatainak helyességét és visszaigazolni a tanúsítvány átvételét. Amennyiben bármilyen rendellenességet talál, a magánkulcsot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonására.

A tanúsítvány elfogadását a Szolgáltató erre rendszeresített nyomtatványának aláírásával igazolja az átvevő, amely egyben a hitelesítési rend, a jelen szolgáltatási szabályzat és az általános szerződési feltételek elfogadását is jelenti.

4.4.1. Tanúsítvány közzététele a Szolgáltató által

Az Előfizető hozzájárulása esetén a Szolgáltató a kibocsátott tanúsítványokat Tanúsítványtárában teszi közzé.

4.4.2. A további szereplők értesítése a tanúsítvány kibocsátásáról

További szereplőket a Szolgáltató a kibocsátott tanúsítványokról nem értesít.

4.5. Kulcspár és tanúsítvány használat

4.5.1. A Tanúsítványtulajdonos magánkulcs- és tanúsítvány használata

A Tanúsítványtulajdonos magánkulcs- és tanúsítvány használatára az alábbi szabályok érvényesek:

a. A Tanúsítványtulajdonos magánkulcsát és tanúsítványát csak az 1.4.2 pontban leírt korlátozásnak megfelelően használhatja.
b. A Tanúsítványtulajdonos csak a tanúsítvány elfogadása után (lásd 4.4 pont) használhatja magánkulcsát.
c. A Tanúsítványtulajdonos a tanúsítvány lejárta után nem használhatja tovább magánkulcsát.
d. A Tanúsítványtulajdonosnak az adott helyzetben általában elvárható gondosságot kell tanúsítania annak érdekében, hogy megelőzze magánkulcsának illetéktelen felhasználását.
e. A Tanúsítványtulajdonos magánkulcsait csak olyan célokra és olyan alkalmazásokkal használhatja, melyek összhangban vannak a tanúsítványok „kulcshasználat” és „kiterjesztett kulcshasználat” mezőinek tartalmával (lásd még 6.1.6, 7.1.2 és 7.1.3 pontok).

4.5.2. Az Érintett felek nyilvános kulcs- és tanúsítvány használata

Annak érdekében, hogy az Érintett fél megalapozottan hagyatkozhasson a tanúsítvánnyal igazolt kriptográfiai kulcspár használatával működő alkalmazásra, ajánlott a kulcspár megfelelő használatát és a hozzá tartozó tanúsítványt az adott helyzetben tőle általában elvárható gondossággal ellenőriznie:

a. Az Érintett fél csak olyan célokra és olyan alkalmazásokkal fogadhat el nyilvános kulcsokat, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat” és „kiterjesztett kulcshasználat” mezőinek tartalmával.
b. Mielőtt egy tanúsítványba foglalt nyilvános kulcsot felhasználna, az Érintett félnek ajánlott ellenőriznie a tanúsítvány érvényességét, valamint azt, hogy a tanúsítvány nincs felfüggesztve, illetve visszavonva az érvényes visszavonási állapot információ alapján.
c. Amennyiben ésszerű módon egy tanúsítványra kíván hagyatkozni, az Érintett félnek ajánlott figyelembe vennie a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban szerepel.

4.6. Tanúsítványok érvényessége, megújítása (tanúsítvány frissítése)

4.6.1. A tanúsítványok érvényessége

Szolgáltató által kibocsátott Előfizetői tanúsítványok érvényességi ideje alapesetben 2 év, de ettől rövidebb is lehet (pl. 1 év), amelyet az előfizetői szerződésben rögzíteni kell. Az érvényesség kezdete (év, hónap, nap, óra, perc, másodperc) nem lehet korábbi, mint a kibocsátás napja.

Az előfizetői tanúsítványok érvényessége az Előfizető kérésére – a Tanúsítványtulajdonos erre vonatkozó nyilatkozata alapján - az érvényességi idő lejárata előtt legfeljebb egy alkalommal legfeljebb egy évre meghosszabbítható.

4.6.2. A tanúsítványok megújítása

Tanúsítványmegújítás során a Szolgáltató a tanúsítványban a Tanúsítványtulajdonos változatlan nyilvános kulcsát és változatlan egyéb adatait hitelesíti új érvényességi időtartamra.

Tanúsítvány megújítása akkor lehetséges, ha:

a. a tanúsítvány nem szerepel a visszavonási listában
b. a tanúsítványban rögzített adatok érvényességéről és változatlanságáról az Előfizető vagy a Tanúsítványtulajdonos írásban nyilatkozik.

A Szolgáltató az Előfizető vagy a 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 30 nappal értesítést küld a Tanúsítványtulajdonosnak arra az email címre, amelyet a regisztrációs űrlapon megadott.

A megújított tanúsítványt Tanúsítványtulajdonos vagy Előfizető kapcsolattartója a Szolgáltatások internetes honlapján található Tanúsítványtárból töltheti le.

Amennyiben a lejáró tanúsítványhoz aláírás-létrehozó eszközt is igényeltek, a tanúsítvány cseréje az eszközön a Tanúsítványtulajdonos vagy Előfizető kijelölt kapcsolattartójának a feladata, melyhez igény esetén az Ügyfélkapcsolati Iroda támogatást biztosít.

4.6.3. Érvénytelen tanúsítványok megőrzése

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

4.7. Kulcscsere

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

A kulcscsere gyakorlatilag új tanúsítvány kibocsájtását jelenti egy olyan Tanúsítványtulajdonos számára, akinek a Szolgáltató korábban már kibocsájtott egy tanúsítványt, de:

a. a tanúsítvány valamilyen okból visszavonásra került,

b. a tanúsítvány lejárt, vagy lejárathoz közeledik (legfeljebb 30 napig érvényes) és nem megújítható

A kulcscserét az Előfizető kezdeményezheti, az új tanúsítvány igénylésével megegyező módon. A Szolgáltató lefolytatja a 3.2 pontban rögzített regisztrációs eljárást. A tanúsítvány kibocsátása és publikálása megegyezik az új tanúsítványra vonatkozó eljárásokkal.

A kulcscserét Szolgáltató nem támogatja.

4.8. Tanúsítvány-módosítás

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

A tanúsítvány-módosítást Szolgáltató nem támogatja.

4.9. Tanúsítvány visszavonás és felfüggesztés

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatást nyújt. A tanúsítvány visszavonása a tanúsítvány állapotát végérvényesen érvénytelenre állítja. Felfüggesztés esetén a tanúsítvány csak rövid, átmeneti időszakra lesz érvénytelen. A tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam után (lásd: 4.9.6.1 pont) állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni. A visszavonási kérelmeket az Ügyfélkapcsolati Iroda fogadja, nyitvatartási időben.

A felfüggesztési kérelmek fogadását és azoknak a sikeres ellenőrzés utáni végrehajtását a Szolgáltató Ügyfélszolgálatán keresztül biztosítja, a nap 24 órájában, folyamatos rendelkezésre állással.

Visszavont/felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

SSI szerver tanúsítványokra - tekintettel a [21] ajánlásra - jelen szabályzat a fentiektől eltérő különleges szabályokat állapít meg annyiban, hogy SSL szerver tanúsítványok nem lehetnek felfüggesztett állapotban. Ezért SSL szerver tanúsítványokra csak visszavonási kérelmek nyújthatók be illetve teljesíthetők; további különleges szabályokat jelen szabályzat 4.9.3.1 pontja tartalmaz.

4.9.1. Visszavonáshoz/felfüggesztéshez vezető körülmények

A Szolgáltató felfüggeszti a tanúsítványt ha:

a. az Előfizető vagy a Tanúsítványtulajdonos ezt kéri
b. a Szolgáltató a Szolgáltatásokkal kapcsolatos – jogszabályban, jelen szolgáltatási szabályzatban, vagy az általános szerződési feltételeiben meghatározott - rendellenességről szerez tudomást
c. megalapozottan feltételezhető, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy a magánkulcs nem a Tanúsítványtulajdonos kizárólagos birtokában van

A Szolgáltató visszavonja a tanúsítványt ha:

a. az Előfizető vagy a Tanúsítványtulajdonos ezt kéri
b. a Szolgáltató a Szolgáltatásokkal kapcsolatos - jogszabályban, jelen szolgáltatási szabályzatban, vagy az általános szerződési feltételeiben meghatározott - olyan rendellenességről szerez tudomást, amely nem orvosolható

c. tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy a magánkulcs nem a Tanúsítványtulajdonos kizárólagos birtokában van
d. tudomására jut, hogy a tanúsítvánnyal bűncselekményt követtek el
e. tudomására jut, hogy a tanúsítvány használatára Előfizető nem jogosult (ld. még 3.2.6 pont, h) alpontját)
f. a Szolgáltató a tevékenységét befejezte
g. a Szolgáltató és az Előfizető között az előfizetői szerződés megszűnt még a tanúsítvány érvényességének lejáratát megelőzően

Az Előfizető vagy a Tanúsítványtulajdonos bármikor kérheti a tanúsítvány felfüggesztését illetve visszavonását. Ezt különösen a következő körülmények fennállása esetén javasolt megtennie:

a. a magánkulcs kompromittálódása, vagy annak gyanúja
b. az aláírás-létrehozó eszköz elvesztése, eltulajdonítása, vagy annak gyanúja
c. az aláírás-létrehozó eszközt vagy a magánkulcsot védő aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja
d. a tanúsítványban feltűntetett hibás adatok
e. az Előfizető tanúsítványban feltűntetett adatainak megváltozása
f. a Tanúsítványtulajdonos tanúsítványban feltűntetett adatainak megváltozása
g. a tanúsítványban feltűntetett Tanúsítványtulajdonos és szervezet kapcsolatának megváltozása vagy megszűnése.

Fentieken túl az Előfizető vagy a Tanúsítványtulajdonos haladéktalanul köteles kérni a tanúsítvány visszavonását, ha a benne foglalt adatok helytelenek vagy azzá válnak, továbbá, ha felmerül a gyanú vagy alapos okkal feltételezhető, hogy a titkos kulcs kompromittálódott, vagy nem rendeltetésszerűen került felhasználásra. Ezzel egyidejűleg felhagy a tanúsítvány használatával, mind a visszavonásig, mind azt követően.

A Szolgáltató a következő esetekben kezdeményezheti a felfüggesztést vagy visszavonást:

a. a tanúsítvány felfüggesztési ideje lejár
b. az Előfizető és/vagy a Tanúsítványtulajdonos szerződés szegése esetén
c. az Előfizető és/vagy a Tanúsítványtulajdonos kötelezettségeinek be nem tartása
d. az Előfizetői szerződés megszűnése
e. a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról

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

4.9.2. Visszavonás kérelmezése

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

A visszavonási kérelem benyújtható személyesen vagy írásban a Szolgáltató Ügyfélkapcsolati Irodájánál. A visszavonási kérelem teljesítéséhez a következő adatok szükségesek:

a. a tanúsítvány sorszáma, vagy egyéb olyan adatok, amely alapján a Szolgáltató rendszerében a tanúsítvány egyértelműen azonosítható
b. a visszavonást kérő azonosító adatai
c. a visszavonást kérő e-mail címe (ha van)
d. a visszavonás oka, az ahhoz vezető körülmények

Ha a bejelentő a visszavonási igényét akadályoztatása miatt személyesen nem tudja bejelenteni vagy azonnali intézkedés szükséges, akkor a tanúsítvány felfüggesztése telefonon is kérhető az Ügyfélszolgálaton (a Szolgáltató Ügyfélszolgálata a nap 24 órájában, folyamatosan rendelkezésre áll), a felfüggesztési jelszó ismeretében. A felfüggesztési jelszó a tanúsítvány kibocsájtásakor a Tanúsítványtulajdonosnak vagy Előfizető kijelölt kapcsolattartójának átadásra került. A bejelentőnek a felfüggesztett tanúsítvány visszavonására az ettől számított 5 napon belül kell intézkednie.

4.9.3. Visszavonási kérelemre vonatkozó eljárás

A visszavonási igény bejelentése esetén a Szolgáltató a következők szerint jár el:

a. Személyesen az Ügyfélkapcsolati Irodánál az Iroda munkaidején belül lehet a visszavonási kérelmeket bejelenteni a bejelentő azonosítása-hitelesítése mellett.
b. Írásban történt bejelentés esetén a Szolgáltató Ügyfélkapcsolati Irodája a bejelentő adatai alapján azonosítja és hitelesíti a visszavonás kérelmezőjét. Tanúsítványtulajdonos részéről teljes bizonyító erejű magánokirat, Előfizető részéről cégszerűen aláírt visszavonási kérelem fogadható el.
c. Ha a kérelmező azonosítás-hitelesítése megtörtént, a visszavonási okok megalapozottak, az adatok egyeznek és a kérelmező jogosult a tanúsítvány visszavonását kezdeményezni, vagyis ha a Szolgáltató a visszavonási kérelem jogosságáról meggyőződött, akkor azonnal elvégzi a tanúsítvány visszavonását. Ha a visszavonási kérelmet a Tanúsítványtulajdonos vagy Előfizető terjesztette be, a sikeres azonosítása után a Szolgáltatónak nincs mérlegelési joga a visszavonás tekintetében
d. Ha a kérelmező azonosítás-hitelesítése sikertelen, a visszavonási okok nem megalapozottak, az adatok helytelenek, vagy a kérelmezőnek a Szolgáltató információi alapján nincs joga a tanúsítvány visszavonatására, akkor a Szolgáltató a visszavonási kérelmet visszautasítja.
e. Szolgáltató a visszavonás megtörténtéről vagy annak visszautasításáról értesíti a Tanúsítványtulajdonost, az Előfizetőt és a visszavonás kérelmezőjét.

Telefonon történt bejelentés esetén a Szolgáltató bekéri a felfüggesztési jelszót és lefolytatja a 4.9.4.2. pont szerinti felfüggesztési eljárást. A visszavonási igény elbírálásához felkéri a bejelentőt, hogy jelenjen meg az Ügyfélkapcsolati Irodában személyes azonosítás-hitelesítésre. A bejelentő akadályoztatása esetén a tanúsítvány a felfüggesztés megengedett időtartamára (lásd: 4.9.7.1. pont) felfüggesztési állapotban marad, majd ennek lejártával a Szolgáltató a tanúsítványt visszavonja.

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

4.9.3.1. SSL szerver tanúsítványok visszavonásának különleges szabályai

Amennyiben Szolgáltató Ügyfélszolgálatához SSL szerver tanúsítvány jogtalan felhasználásával vagy visszaélésével kapcsolatos jelzés érkezik (Tanúsítvány Probléma

Bejelentés), akkor az adott szervezet 24 órán belül elkezdi a panasz/észrevétel kivizsgálását. Az Ügyfélszolgálat a Tanúsítvány Probléma Bejelentést haladéktalanul továbbítja a meghatározott kör (a szolgáltatásért általánosan felelős vezető, a szolgáltatásmenedzser, valamint a biztonsági tisztviselő) számára emailen, és telefonon is értesíti őket. A meghatározott kör külön beosztás alapján 7x24 órában rendelkezésre áll és döntést hoz a visszavonásról vagy az egyéb szükséges intézkedésekről (a bejelentőtől, a probléma természetétől, a jelzések, ill. az érintettek számosságától függően, a releváns jogszabályoknak megfelelően).

Szolgáltató haladéktalanul, de legkésőbb 24 órán belül visszavonja az SSL szerver tanúsítványt, ha:

a. ha Előfizető ezt írásban kéri
b. ha Előfizető értesíti a Szolgáltatót, hogy az eredeti igénylés nem volt jogos és visszamenőleg sem tehető jogossá
c. ha Szolgáltató tudomást szerez arról (megalapozott információk alapján), hogy a magánkulcs kompromittálódott, vagy a kulcs hossza illetve a kriptográfiai algoritmus elavulttá vált
d. ha Szolgáltató tudomást szerez arról (megalapozott információk alapján), hogy ha a tanúsítvánnyal visszaéltek
e. ha Szolgáltató tudomást szerez arról, hogy Előfizető nem tartotta be az ÁSZF-PKI-ban vagy az előfizetői szerződésben előírtakat
f. ha Szolgáltató tudomást szerez arról, hogy a kiadott tanúsítványban foglalt domain név használatára Előfizető már nem jogosult (pl. bírósági döntés alapján)
g. ha Szolgáltató tudomást szerez arról, hogy Wildcard-os tanúsítványt csalárd domain hitelesítésére használták
h. ha Szolgáltató tudomást szerez a tanúsítványban foglalt adatok megváltozásáról
i. ha Szolgáltató tudomást szerez arról, hogy egy adott tanúsítvány nem a HR-TET illetve HSZSZ-T előírásai szerint lett kibocsájtva
j. ha Szolgáltató megállapítja, hogy a tanúsítványban foglalt valamely adat félrevezető vagy nem pontos
k. ha Szolgáltató befejezi az SSL tanúsítványok kiadásával kapcsolatos tevékenységét
l. ha Szolgáltatónak megszűnik a jogosultsága vagy az engedélye a tanúsítvány kiadásokra
m. ha Szolgáltató HR-TET vagy HSZSZ-T szabályzatai a fentieken túl ezt előírják
n. ha a tanúsítvánnyal kapcsolatos műszaki paraméterek (pl. bizonyos algoritmusok vagy kulcsméretek) elfogadhatatlan kockázatot jelentenek az Érintett Felek illetve a Szoftverfejlesztők számára

4.9.4. A felfüggesztési kérelemre vonatkozó eljárás

4.9.4.1. Ki kérelmezheti a felfüggesztést

A felfüggesztést kérelmezheti a Tanúsítványtulajdonos vagy az Előfizető illetve annak képviselője; továbbá harmadik fél, ha azt a körülmények indokolják (lásd: 4.9.1. pont).

4.9.4.2. A felfüggesztési eljárás

Tanúsítvány felfüggesztés kérelmezhető írásban vagy személyesen az Ügyfélkapcsolati Irodán. A felfüggesztési kérelemben a visszavonási kérelemmel megegyező adatokat kell megadni.

Tanúsítvány felfüggesztés kérelmezhető telefonon is a Szolgáltató 24 órás Ügyfélszolgálatánál. Telefonos felfüggesztés esetén a személyes adatok mellett a felfüggesztési jelszót kell megadni.

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

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

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

d. Szolgáltató a felfüggesztés megtörténtéről vagy visszautasításáról telefonon és/vagy e-mailben értesíti a Tanúsítványtulajdonost és Előfizetőt illetve a felfüggesztés kérelmezőjét.

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

A felfüggesztett tanúsítványt a Szolgáltató az Előfizető vagy a Tanúsítványtulajdonos kérésére a felfüggesztési időn belül visszaállítja érvényesre (ld. 4.9.6.2 pont).

4.9.4.3. A Szolgáltató függeszti fel a tanúsítványt

A Szolgáltató felfüggeszti a tanúsítványt, ha:

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

b. az Előfizető vagy a Tanúsítványtulajdonos visszavonási kérelme kiegészítésre szorul.

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

4.9.5. Kivárási idő visszavonási/felfüggesztési kérelem esetén

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

4.9.5.1. Kivárási idő felfüggesztési kérelem esetén

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

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

4.9.5.2. Kivárási idő visszavonási kérelem esetén

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

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

b. Ha a Szolgáltató a visszavonási kérelem érvényességéről 3 órán belül nem tud kétséget kizáróan meggyőződni, akkor erről a kérelmezőt értesíti és a tanúsítványt nem visszavonja, hanem 4.9.4.3 pont szerint felfüggeszti. A visszavonást később – a kérelmező hiteles azonosítását követően végzi el.

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

4.9.5.3. A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok

A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig és elfogadásáig az [18] ÁSZF-PKI-nek megfelelően az Előfizető illetve Tanúsítványtulajdonos felelős a felmerülő károkért.

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

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

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

4.9.6. Felfüggesztett állapotra vonatkozó korlátozások, újraérvényesítés

4.9.6.1. A felfüggesztés megengedett időtartama

Tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig lehet.

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 esetén térítésmentesen új tanúsítványt bocsát ki.

Az SSL szerver tanúsítványok esetén a Szolgáltató 1 nap alatt (24 órán belül) dönt a tanúsítvány visszavonásáról.

4.9.6.2. Felfüggesztés megszüntetése

A felfüggesztés megszüntetésének, és ezzel a tanúsítvány újraérvényesítésének feltételei a következők:

a. A felfüggesztés megszüntetése csak a felfüggesztési időszak vége előtt kérhető
b. Az újraérvényesítést csak Tanúsítványtulajdonos, az Előfizető vagy annak a regisztráció során nyilvántartásba vett képviselője kérheti,
c. Az újraérvényesítést kérő személyt azonosítani kell.

Az újraérvényesítés kéréséhez a következő adatokat kell megadni:

a. a felfüggesztett tanúsítvány sorszáma,
b. a felfüggesztés megszüntetését kérő személy azonosító adatai,
c. a felfüggesztés megszüntetésének oka.

Az igényt személyesen az Ügyfélkapcsolati Irodán, vagy írásban, az Előfizető részéről cégszerűen aláírt kérelemben, Tanúsítványtulajdonos részéről teljes bizonyító erejű magánokirati formában lehet benyújtani.

A felfüggesztés megszűntetésének eredménye a tanúsítvány újraérvényesítése vagy visszavonása.

4.9.7. A visszavonási információ ellenőrzése az Érintett felek részéről

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

4.9.8. Visszavonási listák (CRL) és kibocsátásuk gyakorisága

A visszavonási listákban a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A visszavonási listákból a visszavont/felfüggesztett tanúsítványra vonatkozó bejegyzést Szolgáltató a tanúsítvány lejáratának időpontjáig nem törli, de a felfüggesztett tanúsítványok az érvényességi idejük alatt az újraérvényesítés hatására kikerülhetnek a listából. Szolgáltató fenntartja a jogát arra vonatkozóan, hogy a lejárt tanúsítványokat kitörölje a listából.

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

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

4.9.9. A visszavonási lista előállítása és közzététele közötti leghosszabb idő

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

4.9.10. Visszavonási listák ellenőrzése

A visszavonási listák ellenőrzése az Érintett felek felelőssége a tanúsítványok elfogadását megelőzően. A tanúsítványhoz tartozó visszavonási lista elérhetőségét a tanúsítvány tartalmazza. A lista ellenőrzésének arra kell vonatkozni, hogy a kérdéses tanúsítványt a lista tartalmazza-e (és ha igen, milyen időponttól), a lista hiteles és sértetlen, s a kérdéses tranzakció szempontjából időben releváns-e.

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

4.9.11. Valósidejű tanúsítványállapot-ellenőrzés

A Szolgáltató a visszavonási listák közzététele mellett online tanúsítvány-állapot szolgáltatást (OCSP) is nyújt.

Az OCSP szolgáltatás nyújtását illetve a szabványos OCSP kérelmek teljesítését a Szolgáltató hitelesítő szervezete automatikusan végzi:

a. a kérelmet a szolgáltatás igénybe vétele céljából definiált kommunikációs csatornán keresztül, a tanúsítványban szereplő címen fogadja,
b. az OCSP kérés kiszolgálása az RFC 2560 [11] ajánlás szerinti „application/ocsp-request” MIME-TYPE elküldésére valósul meg.
c. az OCSP választ aláíró tanúsítványt ugyanaz a hitelesítő központ („produktív CA”) állatja ki, amely az ellenőrizendő előfizetői tanúsítványt is kiállította
d. az OCSP válasz nem a CRL alapján képződik, hanem a hitelesítő központ adatbázisának egy replikációja alapján
e. Az adatbázisból a visszavont/felfüggesztett tanúsítványra vonatkozó bejegyzést Szolgáltató a tanúsítvány lejáratának időpontjáig nem törli, de a felfüggesztett tanúsítványok az érvényességi idejük alatt az újraérvényesítés hatására kikerülhetnek az adatbázisból

Szolgáltató biztosítja az OCSP válaszban megadott idő 1 másodpercen belüli pontosságát a vonatkozó referenciaadatoz képest (UTC). Az OCSP válaszadó egység órájának pontosságát Szolgáltató folyamatosan ellenőrzi. Szolgáltató a műszaki infrastruktúrája erőforrásainak figyelésével biztosítja azt is, hogy az OCSP válaszadó egység válaszadási ideje 10 másodpercen belül legyen.

4.9.12. Visszavonási állapot közlés más formái

A Szolgáltató a tanúsítvány visszavonási listán (CRL) valamint az OCSP szolgáltatáson túl nem alkalmaz más nyilvános visszavonási állapot közlő eljárást.

4.9.13. Intézkedések magánkulcs kompromittálódás esetén

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

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

4.10. Kulcsletét

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 letétbe elhelyezett kulcsokat Szolgáltató kizárólag a jogosultaknak adja át (Előfizető meghatalmazott kapcsolattartója vagy Tanúsítványtulajdonos), akiket átadás előtt a 3. fejezet szerint azonosít és ellenőrzi a jogosultságukat.

A letétben őrzött kulcsokat Szolgáltató a tanúsítvány lejártáig köteles őrizni, azt követően jogosult törölni a kulcsletét adatbázisából.

5. Fizikai, eljárásrendi és humán biztonsági szabályozások

A Szolgáltató a Szolgáltatások nyújtása során az elfogadott szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza.

A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására. A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetősége hagy jóvá.

A biztonságkezelési szabályokat a Szolgáltató PKI szintű informatikai biztonságpolitikája [15] tartalmazza. Ez a szabályzat biztonsági okokból nem nyilvános. A Szolgáltató informatikai rendszere vonatkozásában a PKI szolgáltatások biztonsági szabályzata [16] érvényesül. Ez a szabályzat szervezeti egység szinten és munkakörökre lebontva rögzíti a biztonságkezeléssel összefüggő feladatokat, felelősségeket és szabályokat, így többek között a bizalmi munkakörök felsorolását, a kinevezési feltételeket és az összeférhetetlenségi kritériumokat.

A Szolgáltató megvalósította és folyamatosan fenntartja a Szolgáltatásokat nyújtó eszközök, rendszerek biztonsági ellenőrzéseit és üzemeltetési eljárásait.

A Szolgáltató rendszeres belső ellenőrzései és külső auditjai ezen eljárásokat, a vonatkozó dokumentumokat és a dokumentumokban a Szolgáltatásokra vonatkozó előírások teljesülését a szolgáltatás évente esedékes ellenőrzései során vizsgálja.

Fenti eljárásokat Szolgáltató a 3/2005. (III. 18) IHM rendelet 20.§-21.§-nak megfelelő, megbízható és szakértő üzemeltető személyzete biztosítja.

A Szolgáltató gondoskodik arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek. A Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit az elvégzett kockázatelemzéssel összhangban osztályokba sorolja és minősíti.

A Szolgáltatásokat támogató informatikai rendszer, annak személyi és fizikai környezete megfelel a 2/2002 MeHVM irányelvben rögzített követelményeknek, amely egyértelműen meghatározza a Hitelesítő Szervezet és a Regisztrációs Szervezet informatikai rendszereinek, a szolgáltatás személyi és fizikai környezetének biztonsági követelményeit.

Szolgáltató gondoskodik az informatikai biztonság fenntartásáról azokban az esetekben is, amikor Szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez kerül kiadásra.

5.1. Fizikai biztonsági szabályozások

A hitelesítő központok a Szolgáltató legmagasabb védelmi szintet képező objektumában (központi géptermében) helyezkednek el, mivel biztonsági szempontból a legkritikusabb hardver/szoftver egységeket tartalmazzák. Itt történik a kulcspárok és a tanúsítványok előállítása, a visszavonási listák generálása és publikálása, a kulcsletétek őrzése, valamint az OCSP kérések fogadása és a válaszok kiadása.

Hasonlóan kiemelt védelmi szintet képező objektumban történik a kulcspárok elhelyezése az aláírás-létrehozó eszközre és az aláírás-létrehozó eszközök megszemélyesítése is, valamint a napi üzemeltetési feladatok ellátása is, csakúgy, mint a rendkívüli üzemeltetési helyzet esetére biztosított másodlagos szolgáltatói rendszer üzemeltetése, az ennek helyet adó objektumban.

A Szolgáltató ezen fizikai biztonsági körletek kapcsán olyan óvintézkedéseket valósít meg, amelyekkel megakadályozza, hogy a Szolgáltatásokkal kapcsolatos berendezéseket, információkat, adathordozókat vagy szoftvereket jogosulatlanul elvigyék, megrongálják, vagy azokhoz jogosulatlanul hozzáférjenek[9].

A Szolgáltató fentiekhez kapcsolódó eljárásrendi szabályait három szabályzat tartalmazza:

a. a [14] Szolgáltató Szervezeti és Működési Szabályzata, amely meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes szervezetekhez kapcsolt feladat-, felelősség és hatásköröket,

a. a jelen szolgáltatási szabályzat,

b. a [16] PKI szolgáltatások biztonsági szabályzata, amely részletesen szabályozza az adatokhoz és az informatikai rendszerekhez, valamint a személyi és a fizikai környezethez kapcsolódó biztonsági szabályokat.

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

5.2. Humán szabályozások

5.2.1. Bizalmi munkakörök

A Szolgáltató biztosítja a Szolgáltatásokhoz a 3/2005. (III. 18.) IHM rendeletben és a HR-TET hitelesítési rendjében előírt bizalmi munkaköröket, úgymint:

a. a Szolgáltató informatikai rendszeréért általánosan felelős vezető,
b. biztonsági tisztségviselő,
c. rendszeradminisztrátor,
d. rendszerüzemeltető,
e. független rendszervizsgáló,
f. regisztrációs felelős.

Az alábbi táblázatban a Szolgáltatásokhoz kapcsolódó bizalmi munkakörök, azok feladat-, felelősség és hatáskörei kerülnek összefoglalásra.

MUNKAKÖR	FELADATKÖR	FELELŐSSÉG	HATÁSKÖR
Szolgáltatásokért általánosan felelős vezető	A PKI szolgáltatások irányítása és általános felügyelete, a szolgáltatások vezetői szintű ellenőrzése. Változási kérelmek és szabályzatok jóváhagyása	A PKI szolgáltatásokhoz kapcsolódó általános felelősség, a jogszabályi és egyéb informatikai illetve biztonsági előírásoknak való megfelelőség biztosítása	Felügyeleti, irányítási, javaslattételi és véleményezési hatáskör a társaság PKI szolgáltatásaiban érintett szervezetei és munkatársai felé a külső/belső előírások és szabályzatok betartása érdekében
PKI biztonsági tisztviselő I.	A PKI szolgáltatások biztonságának általános felügyelete. A PKI szolgáltatások információbiztonsági tevékenységének irányítása és ellenőrzése. Operatív biztonsági beállítások rendszeres és eseti ellenőrzése.	A PKI szolgáltatásokra vonatkozó általános, fizikai biztonsági, IT biztonsági illetve adatvédelmi szabályok és előírások betartásának kontrollja A társasági szintű és a PKI biztonsági szabályzatok összhangjának biztosítása	A PKI szolgáltatások teljes területe, beleértve az operatív biztonsági ellenőrzést az informatikai és adatvédelmi területen, valamint az előfizetői adatok kezelésének területén
PKI biztonsági tisztviselő II.	A PKI géptermek és helyiségek biztonságtechnikai rendszereinek felügyelete, a beléptetési jogosultságok kezelése, a bizalmi munkakörökbe belépő munkatársak ellenőrzése, kilépők jogosultságának megvonása	A PKI szolgáltatások fizikai környezetére és személyzeti biztonságra vonatkozó előírások megfelelőségének biztosítása	A PKI szolgáltatások fizikai környezetére és személyzeti biztonságra vonatkozó hatáskör társaságon belül

MUNKAKÖR	FELADATKÖR	FELELŐSSÉG	HATÁSKÖR
PKI Rendszervizsgáló .	PKI naplófájlok elemzése és ellenőrzése. Biztonsági hiányosságok, visszaélések felfedése, jelentése. Archivált adatállomány, mentések ellenőrzése. Funkcionális és biztonsági hiányosságok, visszaélések felfedése, jelentése	A PKI rendszer naplózási követelményei megfelelőségének biztosítása. A fentiek mellett a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzése, a meglévő eljárások vizsgálata és felügyelete.	A PKI szolgáltatások teljes informatikai eszközparkja és infrastruktúrája, a keletkezett biztonsági és audit naplók. A PKI szolgáltatások teljes informatikai eszközparkja és infrastruktúrája, a keletkezett biztonsági és audit naplók. A PKI szolgáltatások belső eljárásai és folyamatai.
Regisztrációs felelős (Registration Officer /RO/)	Tanúsítvány elállítás és státuszváltoztatás. Aláírás létrehozó eszköz megszemélyesítés, aktiváló adatok és ügyféladatok szabályszerű kezelése. Adminisztráció.	A PKI szolgáltatások keretében az előfizetői tanúsítványok előállításának és sátusz-változásainak végrehajtása, jóváhagyása	A PKI szolgátlatások keretében megrendelt tanúsítványok kezelésével, a kapcsolódó eszközök megszemélyesítésével kapcsolatos tevékenység
PKI Rendszerüzemeltető I. PKI Rendszerüzemeltető II.	A PKI rendszerben levő tűzfalak, hálózati határvédelmi eszközök üzemeltetése, napi karbantartása, hibaelhárítása A PKI rendszerben levő szerverek, adatbázis gépek, üzemeltetése, napi karbantartása, hibaelhárítása	A PKI rendszerben levő kiszolgáló gépek, adatbázis gépek, tűzfalak és hálózati illetve határvédelmi eszközök üzemeltetése a vonatkozó előírásoknak megfelelően	A PKI rendszerben levő kiszolgálók, adatbázis gépek, tűzfalak és hálózati illetve határvédelmi eszközök üzemeltetése, operatív intézkedések ezen eszközökre vonatkozóan
PKI Rendszerüzemeltető III.	A PKI rendszerben levő MS Windows alapú gépek üzemeltetése, mentése, napi karbantartása, hibaelhárítása illetve helyreállítása	A PKI rendszerben levő MS Windows alapú gépek folyamatos üzemeltetése a vonatkozó előírásoknak megfelelően	A PKI rendszerben levő MS Windows alapú gépek üzemeltetési tevékenysége
PKI Rendszerüzemeltető IV	A PKI rendszerben levő Vmware gépek és Nagios rendszerek üzemeltetése, mentése, napi karbantartása, hibaelhárítása illetve helyreállítása	A PKI rendszerben levő Vmware gépek és Nagios rendszerek folyamatos üzemeltetése a vonatkozó előírásoknak megfelelően	A PKI rendszerben levő Vmware gépek és Nagios rendszerek üzemeltetése, operatív intézkedések ezen eszközökre

MUNKAKÖR	FELADATKÖR	FELELŐSSÉG	HATÁSKÖR
PKI rendszeradminisztrátor	PKI rendszer alkalmazói szoftvereinek telepítése, konfiguráció, karbantartás. HSM modulok telepítése, biztonsági beállítások és környezet létrehozása. Rendeltetésszerű működés biztosítása.	A PKI rendszert alkotó gépek telepítésének, konfigurálásának, karbantartásának elvégzése során a jogszabályok és szakmai előírásoknak való megfelelőség biztosítása	A teljes PKI rendszer alkalmazás szinten, beleértve az ügyfélkapcsolati irodai (ÜKI) alkalmazást is

A táblázatban jelzett bizalmi munkakörökön túl Szolgáltató ún. bizalmi szerepköröket is meghatároz a Szolgáltatások nyújtásához. A bizalmi szerepköröket Szolgáltató belső, nem publikus dokumentuma tartalmazza.

Bizalmi munkakörökbe és szerepkörökbe a Szolgáltató felső vezetősége nevezi ki a kijelölt munkatársakat.

A bizalmi munkakört és szerepkört betöltő személyek munkaviszonyban állnak a Szolgáltatóval.

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

A PKI rendszerben minden rendszer-telepítési, hardver-konfigurálást és szoftver-frissítést igénylő beavatkozást csak két bizalmi munkakört betöltő munkatárs egyidejű jelenlétében lehet elvégezni. A műveletek sikerességét a biztonsági tisztviselő(k) ellenőrzi(k).

A Szolgáltató vezetője által kijelölt bizottság jelenlétében, előre megtervezett módon, kulcsceremónia keretében, ellenőrzötten és jegyzőkönyvezett végezhetők az alábbi feladatok:

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

Továbbá legalább két, bizalmi munkakört betöltő munkatárs (aki egyben kulcsőr szerepkört is betölt) együttesen végezheti - fizikailag védett környezetben, más személyek jelenlétét kizárva - az alábbi feladatokat:

a. a szolgáltatói magánkulcsok biztonsági mentése
b. a szolgáltatói magánkulcsok mentésből történő visszaállítása
c. a szolgáltatói magánkulcsok (és másodpéldányainak) megsemmisítése
d. az RO-kat azonosító adminisztratív kulcspárok generálása, cseréje és megsemmisítése.
e. kulcsletétbe elhelyezett kulcs kivétele

5.2.3. A bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkakört betöltő munkatársak a PKI alkalmazásokba erős azonosítási eljárással, pl. tokenes tanúsítvánnyal illetve az azt aktivizáló PIN-kód megadásával lépnek be.

5.2.4. Egymást kizáró munkakörök

Szolgáltató a bizalmi munkakörök közötti személyi átfedésekre a jogszabályban előírtak alapján az alábbi korlátozásokat alkalmazza:

a. a biztonsági tisztviselő és a regisztrációs felelős nem töltheti be a független rendszervizsgáló munkakört,
b. a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgáló munkakört,
c. az informatikai rendszerért általánosan felelős vezető nem töltheti be a biztonsági tisztviselő és a független rendszervizsgáló munkakört,
d. Szolgáltató törekszik a bizalmi munkakörök teljes személyi elválasztására, ugyanazon személy nem tölt be két bizalmi munkakört akkor sem, ha az jogszabályban egyébként megengedett.

5.2.5. Személyzetre vonatkozó előírások

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

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

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

A Szolgáltató munkatársai a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaköri leírásokkal rendelkeznek. A munkaköri leírásokhoz kapcsolódó részletes feladatleírásokat a belső biztonsági szabályzat tartalmazza.

5.2.6. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

A Szolgáltató informatikai rendszeréért általánosan felelős vezető kinevezéséhez szakirányú felsőfokú végzettség és legalább egy év, az informatikai biztonsággal összefüggésben szerzett gyakorlat szükséges.
A biztonsági tisztviselők és rendszervizsgáló esetén szakirányú közép vagy felsőfokú végzettség, középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.
A regisztrációs tisztviselők esetén középfokú szakirányú végzettség,és legalább egy év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.
A rendszerüzemeltető és rendszeradminisztrátor esetén középfokú szakirányú végzettség, valamint legalább egy év, hasonló munkakörben szerzett szakmai gyakorlat szükséges.

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

5.2.7. Biztonsági háttér ellenőrzésekre vonatkozó eljárások

Az alább meghatározott bizalmi munkakörök illetve szerepkörök betöltését az átlagosnál magasabb szintű biztonsági ellenőrzés előzi meg:

a. A PKI szolgáltatásokért általánosan felelős vezető
b. Az Ügyfélkapcsolati Iroda vezetője
c. A Szolgáltató biztonsági tisztviselője
d. Kulcsőrök
e. Regisztrációs felelős (Registration Officer /RO/)
f. rendszervizsgáló
g. PKI rendszerüzemeltetők

A Szolgáltató által meghatározott munkakörökhöz illetve szerepkörökhöz csak fokozott biztonsági ellenőrzéssel lehet személyt rendelni, amelyhez szükséges a szerepkörre kijelölt személy hozzájárulása, ugyanakkor a fokozott ellenőrzés a szerepkör betöltésének alapfeltétele. Nem tölthet be bizalmi munkakört az a személy, akinél a biztonsági ellenőrzés kockázatot tár fel.

A bizalmi munkakörhöz történő hozzárendeléskor:

a. pontos és írásos munkaköri leírást kell átvennie a fölérendelt vezetőtől vagy Szolgáltató humán szervezetétől,
b. titoktartási nyilatkozatot kell a kijelölt személlyel aláíratni, amelyben 3 év titoktartási kötelezettség szerepel a Szolgáltatótól történő kilépés utáni időponttól számítva.
c. a szükséges mértékű oktatásban kell a kijelölt személyt részesíteni, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

a. A kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságait azonnal meg kell szüntetni. A kilépő ezután csak az biztonsági tisztviselő kíséretében léphet be a Szolgáltatásokkal kapcsolatos körletekbe.
b. A kilépő személy számítógépes tevékenységét legalább két hétre visszamenőlegesen le kell ellenőrizni.
c. Vissza kell venni az aláírás-létrehozó eszközét, azonnal és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítvány(oka)t azonnal vissza kell vonni.
d. Minden a Szolgáltatásokra vonatkozó, a kilépőnél levő dokumentációt és ügyiratot vissza kell venni. A visszaadott anyagokról tételes átvételi jegyzőkönyvet kell felvenni.

5.2.8. Képzési követelmények

A Hitelesítő Szervezet, a Regisztrációs Iroda, az Ügyfélkapcsolati Iroda és az Ügyfélszolgálat területén dolgozó valamennyi munkatárs felvételét követően, illetve a Szolgáltatások indítását megelőzően, a saját bizalmi munkakörének illetve szerepkörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt.

Az érintett személyek részére a képzést vagy annak elemeit Szolgáltató megismétli minden lényeges változtatás után.

Abban az esetben, amikor a szolgáltatásokban jelentős változás[10] következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.[11]

Kisebb változások[12] bekövetkezése előtt a munkatársak írásos tájékoztatást kapnak a változásokról..

5.2.9. A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs a munkaköri kinevezéssel tájékoztatást kap jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról, valamint a titoktartással kapcsolatos szabályokról. A munkatársak belső munkaköri leírása tartalmazza az őket érintő biztonsági feladatokat is.

Mindezeken túl a Szolgáltató társasági szintű dokumentumai tartalmazzák azokat a munkajogi vagy büntető következményeket, melyek a különböző fegyelmi, munkaköri kötelezettségek be nem tartását, illetve a törvénysértést szankcionálják.

5.3. Naplózási eljárások

5.3.1. Naplózott esemény típusok

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

A Szolgáltató által végzett műveletek naplózásra kerülnek. A naplóbejegyzések többek között a regisztráció, kulcspárok generálása, az aláírás-létrehozó eszköz megszemélyesítése, a tanúsítvány létrehozása, kibocsátása és kezelése, kulcsletét valamint egyéb Szolgáltatói tevékenységek során készülnek.

A naplózott adatállományok tartalmazzák a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

5.3.2. Napló adatok védelme

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

A Szolgáltató biztosítja naplóállományok bizalmasságát és sértetlenségét.

---

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

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

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

5.3.3. A naplók feldolgozásának gyakorisága

A Szolgáltató a hitelesítő központok (CA-k) naplóit naponta, az egyéb napló fájlokat a [16] biztonsági szabályzatában rögzített gyakorisággal dolgozza fel.

A PKI alkalmazás, és az operációs rendszerek biztonsági esemény és audit naplóinak operatív ellenőrzését csak a rendszervizsgálók végezhetik és csak olvasási jogosultsággal. A rendszervizsgálók feladata az alkalmazásokon és operációs rendszereken kívüli, de a PKI rendszer részét képző szoftver elemek (hálózat, tűzfalak, betörés detektor) naplóinak ellenőrzése is.

5.3.4. Napló adatok tárolása

A napló adatok rendszeresen archiválásra kerülnek ellenőrzés, szükségessé váló visszakeresés és esetleges újbóli használat céljából (ld. 5.4 pont).

5.3.5. A napló fájlok megőrzési időtartama

Lásd: 5.4 Adatok archiválása c. fejezetet.

5.4. Adatok archiválása

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

Az archivált adathordozók első példányai a Szolgáltató archívumában, a biztonsági példányai a PKI Dokumentumtárban kerülnek elhelyezésre.

5.4.1. A tárolt adatok típusai

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

a. az Előfizető illetve a tanúsítványt igénylő természetes személy által benyújtott igény, valamint a regisztráció során megadott adatok
b. az Előfizető illetve a tanúsítványt igénylő természetes személy által benyújtott igazolványok és dokumentumok típusa, egyedi azonosító adatai (például a személyazonosító igazolvány száma)
c. az Előfizetői Szerződés másolata
d. a regisztrációs kérelmet elfogadó regisztrációs felelős (RO) azonosítója
e. a tanúsítvány, valamint a magánkulcs illetve az aláírás-létrehozó eszköz átadás-átvételére vonatkozó feljegyzés
f. az Előfizetővel kötött megállapodás esetleges egyedi választásai
g. Az 5.3.1 pontban felsorolt összes esemény, illetve napló típus.

5.4.2. Az archívum megőrzési időtartama

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

5.4.3. Az archívum védelme

A Szolgáltató archívumában olyan fizikai védelmet biztosít, amely fenntartja az archivált adatok bizalmasságát és sértetlenségét. A Szolgáltató az archivált adatokat fokozott biztonságú elektronikus aláírással és időbélyegzővel látja el.

5.4.4. Az archívum hozzáférését és ellenőrzését végző eljárások

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

a. A Szolgáltató biztosítja, hogy mindaddig, amíg az archivált adatokat őrzi, az arra jogosult személyek számára hozzáférhetők és értelmezhetők lesznek.
b. A tanúsítványokra vonatkozó adatokat rendelkezésre bocsátja, ha azokra jogi eljárásokban bizonyíték nyújtása céljából szükség van.
c. Az Tanúsítványtulajdonosnak, illetve az adatvédelmi követelmények korlátozásain belül az Előfizetőnek hozzáférést biztosít a Tanúsítványtulajdonosra vonatkozó regisztrációs és egyéb információkhoz.

5.5. A Szolgáltató kulcscseréje

A Szolgáltató szolgáltatói kulcsának tervezett cseréje előtt legalább 30 nappal tájékoztatja az Előfizetőket, Tanúsítványtulajdonosokat és az Érintett Feleket a honlapján történő értesítéssel.

5.6. Katasztrófa elhárítás

A Szolgáltató olyan megbízható rendszert működtet, amely a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatások elérhetőségét.

A Szolgáltató gondoskodik arról, hogy rendkívüli üzemeltetési helyzet esetén (pl.: súlyos üzemzavar vagy katasztrófa, beleértve a saját aláírás-létrehozó magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is) a rendszerüzemeltetés a lehető legrövidebb időn belül helyreálljon.

Rendkívüli üzemeltetési helyzet esetére a Szolgáltató rendelkezik minimális szolgáltatásokat biztosító tartalék rendszerrel: a Szolgáltató rendkívüli üzemeltetési helyzet esetén is gondoskodik tanúsítványtára és nyilvános szabályzatai elérhetőségéről, a tanúsítvány felfüggesztés/visszavonás kezelésről és a tanúsítvány visszavonási listák közzétételéről.

A rendkívüli üzemeltetési helyzetek kezelésére a Szolgáltató rendelkezik biztonsági mentésekkel, tartalékolt műszaki megoldásokkal és eljárásokkal. A megelőzésre és rendkívüli üzemeltetési helyzetekre érvényes intézkedéseket a Szolgáltató üzletmenet-folytonossági terve tartalmazza.

A rendkívüli üzemeltetési helyzetekben a Szolgáltató eseménynaplót vezet.

5.6.1. A szolgáltatások azonnali felfüggesztése

A szolgáltató köteles a rendkívüli üzemeltetési helyzetről és annak hatásáról közvetlenül, illetve elektronikus levél formájában értesíteni a Szolgáltatásokat igénybe vevő mindazon személyeket, akiket a rendkívüli üzemeltetési helyzet érint, valamint az erről szóló tájékoztatást az interneten elérhetővé tenni.

5.6.2. Minimális szolgáltatás rendkívüli üzemeltetési helyzetben

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

A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását megelőzi.

Rendkívüli üzemeltetési helyzetben a Szolgáltató minden egyéb szolgáltatás elemet szüneteltet.

5.6.3. Rendkívüli eseményekről történő értesítés

A rendkívüli üzemeltetési eseményekről Szolgáltató a Szolgáltatások internetes honlapján tesz közzé értesítést. Amennyiben ez nem lehetséges, úgy a társasági honlapján értesíti a felhasználói közösség tagjait.

A Szolgáltatásokat támogató informatikai rendszerre, annak fizikai és személyi környezetére kiható súlyos üzemzavari és katasztrófa események megelőzéséről, kezeléséről, az érintettek értesítéséről és a rendszer visszaállításáról részletesen a Szolgáltató [19] Üzletmenet-folytonossági Terve intézkedik. Az Üzletmenet-folytonossági Tervben az üzletmenetet veszélyeztető, sértő, illetve azt leállító események súlyossági osztályokba vannak sorolva. A Terv részletes intézkedési forgatókönyveket tartalmaz a súlyos üzemzavari, illetve katasztrófa események kezelésére és részletesen szabályozza a Hitelesítő Központok szolgáltatói kulcsainak kompromittálódása esetén elvégzendő teendőket is. Ez a dokumentum biztonsági okokból nem nyilvános.

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

5.7. A szolgáltatási tevékenység megszüntetése

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezdhet más szolgáltatókkal a Szolgáltatások átvételéről. A tárgyalások eredményéről Előfizetőit tájékoztatja.

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

Ennek érdekében a Szolgáltató mielőtt szolgáltatási tevékenységét leállítja:

a. legalább 60 nappal korábban értesíti illetve a Szolgáltatások internetes honlapján tájékoztatja a felhasználói közösség tagjait
b. megszűnteti a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások összes felhatalmazását
c. megteszi a szükséges lépéseket, hogy a regisztrációs adatok és az eseménynapló archívumok fenntartására vonatkozó adatokat átruházza (amennyiben erre vonatkozó megállapodás megszületett)

A bejelentéssel egyidejűleg a Szolgáltató leállítja:

a. a tanúsítvány előállítás és kibocsátás szolgáltatást (nem ad ki sem új, sem megújított tanúsítványokat)
b. az aláírás-létrehozó eszközön a magánkulcs elhelyezése szolgáltatást.

Szolgáltató a tervezett megszűnés előtt intézkedik az előfizetői tanúsítványok és szolgáltatói tanúsítványai visszavonásáról. Ezzel egyidejűleg leállítja a visszavonás kezelési szolgáltatását.

Eljárás külső regisztrációs szervezet megszűnése esetén:

a. A regisztrációs szervezet megszűnése előtt 60 nappal értesíti azon Előfizetőket, akik a megszűnő regisztrációs szervezetnél kötöttek szerződést és a Szolgáltató által kibocsátott érvényes tanúsítvánnyal rendelkeznek.

b. A regisztrációs szervezet megszűnéséről a felhasználói közösség tagjait Szolgáltató a web oldalain történő közzététel útján tájékoztatja

6. Műszaki biztonsági óvintézkedések

Szolgáltató különböző adminisztratív biztonsági óvintézkedéseket alkalmaz a szolgáltatói tevékenysége során. A hibák (különösen a telepítési és karbantartási hibák) elkerülése érdekében rendszer-telepítési, hardver-konfigurálást és szoftver-frissítést igénylő beavatkozást csak két munkatárs egyidejű jelenlétében lehet elvégezni. A műveletek sikerességét auditorok ellenőrizik és hitelesítik.

A Szolgáltató megbízható, biztonságtechnikailag értékelt és minősített elektronikus aláírási terméket használ Szolgáltatásai nyújtásához.

A Szolgáltató által használt kriptográfiai modulok (HSM) az alábbiak:

HSM modul neve:	nShield F3 500
Hardware verzió:	nC4033P-500
Firmware verzió:	2.33.60-3
Tanúsításának száma:	HUNG-T-068-2014
Érvényességi ideje:	2017. 12. 15.

HSM modul neve:	nShield F3 500e
Hardware verzió:	nC4033E-500
Firmware verzió:	2.50.16-3
Tanúsításának száma:	HUNG-T-067-2014
Érvényességi ideje:	2017. 11. 11.

HSM modul neve:	nShield F3 6000e
Hardware verzió:	nC4033E-6K0
Firmware verzió:	2.50.16-3
Tanúsításának száma:	HUNG-T-067-2014
Érvényességi ideje:	2017. 11. 11.

A Szolgáltató önkéntes akkreditációs rendszer keretében még nem lett tanúsítva.

6.1. Kulcspár előállítás és telepítés

6.1.1. Kulcspár előállítás

A Szolgáltató maga generálja a szolgáltatói kriptográfiai kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben, erre szolgáló kriptográfiai modulban (HSM), kettős ellenőrzés mellett.

A kriptográfiai modul rendelkezik a vonatkozó jogszabály által előírt tanúsítással, és szerepel a Nemzeti Média- és Hírközlési Hatóság nyilvántartásában. A kulcspárok generálását Szolgáltató olyan algoritmussal valósítja meg, végzi, amely szerepel a Nemzeti Média- és Hírközlési Hatóság 2011. szeptemberében kiadott, algoritmusokra vonatkozó határozatának 1. sz. mellékletében.

A magánkulcs elhelyezése aláírás-létrehozó eszközön szolgáltatás keretében a kulcspár előállításra Szolgáltató csak tanúsítvány kibocsátással együtt vállalkozik.

6.1.2. Az aláírás-létrehozó eszköz megszemélyesítése

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

A megszemélyesítés szolgáltatáshoz chipkártya esetén vizuális megjelenítés is kapcsolódik (egy oldali nyomással történő grafikus megszemélyesítés, Tanúsítványtulajdonos és Előfizető nevének kártyára nyomtatása, vagy egyéb, az Előfizetői Szerződésben meghatározott adattartalommal).

A Szolgáltató a magánkulcs aktivizálásához PIN-kódot biztosít. A PIN-kódot fizikailag védett környezetben állítja elő és a kódot tartalmazó PIN-borítékot az aláírás-létrehozó eszköztől elkülönítve tárolja.

6.1.3. A magánkulcs eljuttatása a Tanúsítványtulajdonoshoz (Előfizetőhöz)

A Szolgáltató a magánkulcsot illetve a megszemélyesített aláírás-létrehozó eszközt (a rajta lévő kulcsokkal és tanúsítvánnyal) az átvételig biztonságos módon tárolja, fizikailag védett környezetben, és biztosítja, hogy a magánkulcs titkossága ne sérüljön.

A Szolgáltató a magánkulcsot illetve az aláírás-létrehozó eszközt az Előfizetőnek vagy a Tanúsítványtulajdonosnak úgy adja át, hogy a magánkulcs titkossága ne sérüljön.
A Szolgáltató a magánkulcs illetve az aláírás-létrehozó eszköz aktivizálási adatát (PIN-kódját) biztonságos módon, kriptográfiai modulban állítja elő, és PIN borítékban rögzíti el és tárolja.
Az átvételre jogosult személynek (Tanúsítványtulajdonosnak, meghatalmazottjának illetve Előfizető kapcsolattartójának) a magánkulcsot illetve az aláírás létrehozó eszközt valamint a kapcsolódó PIN-kódot tartalmazó borítékot személyesen, az átvétel írásos elismerésével kell átvennie. Az átadás-átvételt megelőzően az átvételre jogosultságot a regisztrációnál leírt eljárásnak megfelelően kell igazolni.

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

6.1.4. A Tanúsítványtulajdonosok publikus kulcsának eljuttatása az érintett felekhez

A Szolgáltató a Tanúsítványtulajdonosok nyilvános kulcsát Tanúsítványtárában teszi mindenki számára elérhetővé. A Tanúsítványtulajdonosok publikus kulcsa az előfizetői tanúsítványba van foglalva.

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

A Szolgáltató a hitelesítő központok (Root CA, Produktív CA) tanúsítványait és ezen keresztül aláírás-ellenőrző adatait (nyilvános kulcsait) a Szolgáltatások internetes honlapján keresztül teszi mindenki számára elérhetővé.

A szolgáltatói tanúsítványok letölthetők és a felhasználók kliens-alkalmazásaiba installálhatók.

6.1.6. Kulcsméretek, használt algoritmusok

A Szolgáltató a Nemzeti Média- és Hírközlési Hatóság 2011. szeptemberi, algoritmusokra vonatkozó határozatának megfelelően az SHA256-with-RSA algoritmuskészletet használja fel a szolgáltatási tevékenysége során, mind a Tanúsítványtulajdonosok, mind a szolgáltatói tanúsítványok, visszavonási listák és OCSP válaszok aláírásához.

A legfelső szintű hitelesítő központ aláíró kulcsának mérete: 4096 bit

A közbenső szintű hitelesítő központ aláíró kulcsainak mérete: 2048 bit

Az OCSP választ aláíró kulcs mérete: 2048 bit

Az Tanúsítványtulajdonosok (Előfizetők) aláíró kulcsainak mérete: 2048 bit

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

6.1.7. Szolgáltatói kulcsgenerálás

A szolgáltatói tanúsítványokhoz a kulcsgenerálás a vonatkozó jogszabályban előírt tanúsítással rendelkező kriptográfiai modulban (HSM-ben) történik, védett környezetben, megfelelő személyi felügyelet mellett.

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

6.1.8. Kulcs felhasználási célok

A Szolgáltató Előfizetők részére nem aláírás célú tanúsítványokat (és kulcspárt) bocsát ki.

Ennek érdekében a Szolgáltató az Előfizetői tanúsítványok kulcshasználati mezőit a felhasználási területnek és célnak megfelelően állítja be.

A kulcspár kizárólag arra a célra használható, amelyre a Szolgáltató kibocsátotta, jelen szabályzatnak és a HR-TET szabályzatnak megfelelően.

A szolgáltatói magánkulcsok használati célja kizárólag tanúsítványok, visszavonási listák, illetve OSCP válaszadó tanúsítványok aláírása. Ennek megfelelően a Szolgáltató szervezeti egységei esetében a „Key Usage” mezők lehetséges (egyúttal kötelezően kitöltendő) értékeit a következő táblázat mutatja.

Kulcs megnevezése	Kulcs használati mező („Key Usage”) értéke	Kritikus/Nem kritikus
Hitelesítő Központ (CA) aláíró kulcsa	KeyCertSign, CRLSign	K
OCSP válasz egység aláíró kulcsa	DigitalSign, DataEncipherment, KeyEncipherment	K
	Az „Extended Key Usage” mezőbe: OCSP signing	NK

A Szolgáltató Főtanúsítványának aláírás-létrehozó adata – a 2.1.1.1 fejezettel összhangban, valamint a szakmai ajánlásoknak ([21]) megfelelően – csak az alábbi tanúsítványok kiállítására és aláírására használható:

a. a Főtanúsítvány önaláírására
b. másodlagos hitelesítő központok („produktív CA-k”) tanúsítványának aláírása
c. kereszthitelesítések esetén a kapcsolódó hitelesítő központok tanúsítványának aláírása
d. Szolgáltató hitelesítő szervezetéhez kapcsolódó (infrastruktúra) tanúsítványok aláírása (pl. naplóadatok aláírásához használt tanúsítványok, vagy OCSP válaszok aláírásához használt tanúsítványok)

6.2. A magánkulcsok védelme

6.2.1. A magánkulcsokra vonatkozó szabályok

A tanúsítványokhoz tartozó magánkulcsot a Szolgáltató PIN-kóddal védve bocsátja ki és adja át a Tanúsítványtulajdonosnak vagy arra jogosult átvevőnek. A magánkulcs átvétele után a Tanúsítványtulajdonos felelős a magánkulcs, valamint a PIN-kód védelméért.

A Szolgáltató a magánkulcsot a szolgáltatás nyújtása során visszafejtésre alkalmas formában nem tárolja, illetve adott esetben az aláírás-létrehozó eszközre helyezést követően pedig biztosítja, hogy a magánkulcsról semmilyen másolat ne kerüljön tárolásra.

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

A Szolgáltató az aláíró eszközökhöz kapcsolódó tanúsítványok esetében az Előfizetők magánkulcsának előállítására olyan eszközt használ, amely teljesíti a CC EAL4 követelményeket, rendelkezik a jogszabály által előírt, Európai Unió tagállamában nyilvántartásba vett, eszköztanúsításra jogosult szervezet által erre a célra kiadott tanúsítvánnyal[13] (CERTIFICAT ANSSI-CC-2012/76, keltezés: 2012. Dec, 3). Az eszköz gyártója és típusa: a Gemalto S.A. által gyártott, Gemalto IDClassic 340 intelligens kártya, melynek neve és verziója (a tanúsítási jelentés szerint) IAS Classic v3 alkalmazás Java Card platformon, nyílt konfigurációban, MultiApp ID V2.1 chipkártyán P5CC081V1A komponensen, MPH117 V2.2 szűrővel.

6.2.2. Kriptográfiai modulra vonatkozó szabályok

A Szolgáltató saját szolgáltatói magánkulcsainak tárolására illetve használatára olyan kriptográfiai modult (HSM) alkalmaz, amely teljesíti a vonatkozó ([1] Eat. 7. § (5)-(6) bekezdéseiben foglalt) feltételeket, azaz rendelkezik az NMHH által regisztrált, illetve az Európai Unió valamely tagállamában nyilvántartásba vett tanúsításra jogosult szervezetek által erre a célra kiadott igazolással (Lásd: 6. pont bevezető fejezet).

6.2.3. A többszereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése

A Szolgáltatónál egyedül a hitelesítő központokban alkalmazzák az „n-ből m” ellenőrzést.

6.2.4. 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.

Az egyéb nem aláírás célú tanúsítványok esetében Szolgáltató nem nyújt kulcsletét szolgáltatást. Szolgáltató az Előfizető magánkulcsát semmilyen formában nem menti vagy archiválja; annak előállítására, visszafejtésére alkalmas programot, adatot nem tárol.

[13] A tanúsítvány valamint a kapcsolódó tanúsítási jelentés eredeti, francia nyelvű változata elérhető a https://hiteles.gov.hu honlap „Termékek” menüpontjában, ahol a tanúsítási jelentés magyar nyelvű fordítása is megtalálható

A Szolgáltatónál a hitelesítő központok aláíró magánkulcsai[14] biztonsági okokból duplikálásra kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik

6.2.5. Magánkulcsok 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.

6.2.6. 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.

6.2.7. Magánkulcs megsemmisítése

Az előfizetői tanúsítvány lejárta után a magánkulcs fizikai megsemmisítését az Előfizetőnek illetve a Tanúsítványtulajdonosnak saját felelősségi körében úgy kell elvégezni, hogy az semmilyen körülmények között ne legyen újra felhasználható.

A szolgáltatói aláírás-létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3. Az előfizetői tanúsítványok megőrzése

Az előfizetői tanúsítványokat a Szolgáltató megőrzi az érvényesség lejáratától számított 10 évig, illetve a tanúsítvánnyal kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig. A Szolgáltató ugyanezen határidőig olyan eszközt biztosít, amellyel a kibocsátott tanúsítvány tartalma megállapítható. E megőrzési kötelezettségnek a Szolgáltató archiválási szolgáltató igénybevételével is eleget tehet.

6.4. Aktiválási adatok (PIN-kódok)

A magánkulcsok illetve az aláírás-létrehozó eszközök aktivizáló adatait (PIN-kódjait) a Szolgáltató által használt tanúsított kriptográfiai modul (HSM) állítja elő, a beépített véletlenszám-generátor segítségével.

A Szolgáltató a PIN-kódokat műszaki és szervezési intézkedésekkel védi és csak az arra jogosult személy részére adja át. Az átvételt követően a Tanúsítványtulajdonosnak illetve az Előfizető kijelölt kapcsolattartójának saját felelősségi körében kell biztosítania a PIN-kód kizárólagos birtoklását.

Az Tanúsítványtulajdonos bármikor megváltoztathatja a PIN-kódját.

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

Az aktiváló adat elvesztése, elfelejtése vagy illetéktelen kezekbe történő jutása esetén minden esetben új aktiválási adatot kell előállítani, amely esetenként új aláírás létrehozó adat illetve tanúsítvány előállítását is feltételezi.

[14] A kriptográfiai hardver modul (tanúsítványokat, illetve visszavonási listákat aláíró) magánkulcsai.

6.5. Informatikai biztonsági előírások

Szolgáltató a számítógép biztonság technikai követelményeit a MeH ITB 12. ajánlás szerinti fokozott biztonsági osztályba sorolással határozza meg.

A Szolgáltató gondoskodik arról, hogy az informatikai rendszeréhez a hozzáférés és azok védelme a vonatkozó jogszabályi és szakmai előírásoknak megfelelően szabályozva legyen. Különösképpen:

1. A Szolgáltató védi rendszerei és információi sértetlenségét vírusok, káros és engedély nélküli szoftverek ellen.
2. A Szolgáltató biztonságosan kezeli adathordozó eszközeit a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.
3. A Szolgáltató gondoskodik a felhasználói[15] hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.
4. A Szolgáltató gondoskodik arról, hogy az információhoz és az alkalmazói rendszer funkciókhoz történő hozzáférés, a hozzáférés ellenőrzési szabályzatnak megfelelően korlátozott legyen, és hogy a szolgáltatói rendszere megfelelő számítógép-biztonsági ellenőrzéseket nyújtson a jelen szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében, beleértve a biztonsági adminisztrátori és üzemeltetési funkció elkülönítését. Különösképpen a rendszer szolgáltatási programok használatát korlátozza és ellenőrzi szigorúan.
5. A Szolgáltató gondoskodik arról, hogy személyzetét sikeresen azonosítsák és hitelesítsék, mielőtt a tanúsítvány gondozásával kapcsolatos kritikus alkalmazásokat használhatnák.
6. A Szolgáltató eljárásokat dolgoztat ki és hajtat végre valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására.
7. A Szolgáltató műszaki óvintézkedéseket juttat érvényre (például tűzfalak[16] segítségével), hogy a hitelesítés-szolgáltató belső hálózati tartományai védettek legyenek a harmadik felek számára elérhető külső hálózati tartományoktól.
8. A Szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.
9. A Szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni és regisztrálni az erőforrásaihoz való jogosulatlan és/vagy szabálytalan hozzáférési kísérleteket, valamint képes legyen ezekre időben reagálni[17].
10. A Szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.

---

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

[16] A tűzfalakat úgy konfigurálják, hogy azok a Szolgáltató működéséhez nem szükséges protokollokat és hozzáféréseket kiiktassák.

[17]A Szolgáltató erre használhat egy behatolás észlelő rendszert, vagy hozzáférés ellenőrzést felügyelő és riasztási eszközöket.

11. A Szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ (hálózatról történő) módosítására vonatkozóan.
12. A Szolgáltató gondoskodik arról, hogy az érzékeny adatokat[18] megvédjék az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.
13. A Szolgáltató biztosítja a személyzet tevékenységéért való felelősségre vonhatóságát.[19]

6.5.1. Számítógép biztonsági követelmények

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

a. operációs rendszer,
b. PKI alkalmazás,
c. kriptográfiai modulok,
d. tűzfalak, határvédelmi eszközök.

Az operációs rendszerek által megvalósított biztonsági funkciók az alábbiak:

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

A PKI alkalmazás által megvalósított biztonsági funkciók az alábbiak:

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

A kriptográfiai modulok által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás,
b. kriptográfiai támogatás (kriptográfiai kulcsok generálása, védelme és megsemmisítése; bizalmasságot, sértetlenséget, hitelességet és letagadhatatlanságot biztosító kriptográfiai eljárások megvalósítása),
c. a felhasználói adatok védelme (hozzáférés ellenőrzési szabályok érvényre juttatása),
d. azonosítás és hitelesítés,

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

[19] Például az eseménynapló megőrzésén keresztül.

e. biztonságkezelés (a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
f. a biztonsági funkciók megbízható védelme (a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása),
g. megbízható út/csatorna (megbízható útvonal kiépítése a magát hitelesítő felhasználóval, mely alkalmas az átvitt adatok illetéktelen felfedésének és módosításának megakadályozására).

A tűzfal és a határvédelmi eszközök által megvalósított biztonsági funkciók az alábbiak:

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

Az OCSP szolgáltatásra vonatkozóan megvalósított biztonsági funkciók az alábbiak:

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

6.5.2. Az informatikai biztonság értékelése

Szolgáltató által alkalmazott informatikai biztonsági értékelések rendszerét az alábbi táblázat mutatja.

BIZTONSÁGI ELLENŐRZÉS TÍPUSA		VÉGZI	RENDSZERESSÉG
Operatív	PKI alkalmazás	Rendszer vizsgáló	Naponta
	IT infrastruktúra	Rendszerüzemeltető operátorok	Naponta
Belső ellenőrzés	IT infrastruktúra és PKI alkalmazás	Informatikai biztonsági tisztviselő	Évente egyszer
	PKI szabályozási dokumentumok	Hitelesítési Rend és Szabályozási Csoport	Évente egyszer

6.6. Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési szabályok

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató belső informatikai szabályzatai tartalmazzák, amelyek meghatározzák az előkészítés, a projekt, a működtetés, a menedzselés és az újratervezés ciklus időszakok feladatait és az alkalmazott módszertanokat.

6.6.2. Biztonságkezelési szabályok

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

A biztonságkezelési szabályokat a Szolgáltató PKI informatikai biztonságpolitikája [15] illetve a biztonsági szabályzata [16] tartalmazzák.

6.6.3. Életciklus biztonsági értékelések

A Szolgáltató által alkalmazott megbízható informatikai rendszerek megfelelnek a 2/2002 MeHVM irányelvben rögzített követelményeknek.

6.7. Hálózati biztonsági szabályok

A hálózati védelmi intézkedések a 2/2002 MeHVM ajánlásnak felelnek meg.

Szolgáltató a regisztrációs adatok vonatkozásában biztosítja ezek bizalmasságát és sértetlenségét mind az Előfizetővel/Tanúsítványtulajdonossal folytatott külső, mind pedig a Szolgáltató egyes komponensei (regisztrációs iroda és a hitelesítő központ) közötti belső adatcsere során.

A Szolgáltató gondoskodik arról, hogy a regisztrációs adatokat csak általa elismert, azonosságában hitelesített adatbázisokban ellenőrizze.

A tanúsítvány előállítással és visszavonás kezeléssel kapcsolatosan Szolgáltató gondoskodik arról, hogy a helyi hálózati komponensek fizikailag biztonságos környezetben legyenek és konfigurációikat időszakonként ellenőrizzék. A Szolgáltató folyamatos felügyelő és riasztó eszközöket üzemeltet, hogy képes legyen felismerni és regisztrálni az erőforrásaihoz a hálózatról történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre.

A Szolgáltató a Szolgáltatásokat támogató informatikai rendszerénél a védett belső és a külső hálózatok biztonságos elválasztását tűzfal és határvédelmi eszközök (behatolás érzékelő rendszer (IDS)) révén biztosítja.

A hitelesítő központok nem folytatnak közvetlen külső kommunikációt az Előfizetőkkel, vagy Tanúsítványtulajdonosokkal sem pedig az Érintett Felekkel vagy egyéb külső felhasználóval.

6.8. Kriptográfiai modul ellenőrzése

A Szolgáltató gondoskodik a kriptográfiai modul védelméről és biztonságos használatáról annak teljes élettartama alatt. Különösképpen gondoskodik arról, hogy:

a. a kriptográfiai modult ne manipulálhassák sem szállítás, sem pedig tárolás közben,
b. a Szolgáltató aláíró kulcsainak kriptográfiai modulban történő installálása, aktivizálása, mentése és visszaállítása legalább két bizalmi munkakört betöltő személy együttes jelenlétét kívánja meg,
c. a kriptográfiai modult a gyártási dokumentációnak megfelelően helyesen üzemeltesse,
d. a kriptográfiai modulban tárolt szolgáltatói magánkulcsok a modul visszavonásakor megsemmisítésre kerüljenek
e. a kriptográfiai modul folyamatosan rendelkezzen a jogszabály szerinti érvényes tanúsítással.

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

a. a memóriájában levő magánkulcsot törli
b. a modul saját tanúsítványa is törlésre kerül és ezzel a modul használhatatlanná válik

7. Tanúsítvány és tanúsítvány-visszavonási profil

7.1. Tanúsítvány profil

7.1.1. Alap mezők

A Szolgáltató az RFC 3280 ajánlásnak megfelelő tanúsítványokat bocsát ki.

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

Mezőnév	Szabály
Verzió Version	Szolgáltató az RFC 2459-nek megfelelő tanúsítványokat bocsát ki. Az Előfizető és Érintett fél által alkalmazott eljárásoknak és alkalmazásoknak támogatnia kell az ilyen típusú tanúsítványok helyes kezelését. Szolgáltató a kibocsátott tanúsítványok „Version” mezőjébe V3 értéket ír.
Sorozatszám Serial Number	A kibocsátó hitelesítő szervezeten belül egyedi véletlen szám.
Algoritmus azonosító Signature Algorithm Identifier	Szolgáltató tanúsítványt hitelesítő elektronikus aláírásának algoritmus azonosítója (sha256RSA)
Aláírás Signature	Szolgáltató tanúsítványt hitelesítő elektronikus aláírása az RFC 2459 szerint generálva és kódolva.
Kibocsátó Issuer	A tanúsítványt kibocsátó hitelesítő szervezet és egység egyedi azonosítója egyedi X.500 név formátum szerint, UTF8String formátumban. Az SSL szerver tanúsítványokat Szolgáltató egy csak erre a célra használt „produktív CA-ból” bocsájtja ki. Szolgáltató „Kibocsátó” azonosítója a CN, O, L és C almezőkből állnak össze. Az egyéb nem aláírás célú tanúsítványokat Szolgáltató egy másik (a fentitől eltérő) „produktív CA-ból” bocsájtja ki, melyben a „Kibocsátó” azonosítója szintén a CN, O, L és C almezőkből állnak össze, de a CN értelemszerűen eltérő.
Érvényesség Valid From & Valid To	A tanúsítvány érvényességének kezdete és vége. UCT szerinti érték, az RFC 2459 szerinti kódolással.
Tulajdonosazonosító	A Tulajdonos egyedi neve egyedi X.500 név

Mezőnév	Szabály
Subject	formátum szerint, UTF8String formátumban.
Tulajdonos nyilvános kulcsának algoritmus azonosítója Subject Public Key Algorithm Identifier	A Tulajdonos nyilvános kulcs algoritmusának azonosítója.
Tulajdonos nyilvános kulcsa Subject Public Key Value	A Tulajdonos nyilvános kulcsa.
Kibocsátó egyedi azonosító Issuer Unique Identifier	Nem kitöltött.
Tulajdonos egyedi azonosítója Subject Unique Identifier	Nem kitöltött.

A mezők kitöltésének további részleteit a Szolgáltató Tanúsítványprofilok [20] a PKI szolgáltatásokhoz című dokumentuma tartalmazza.

7.1.2. Tanúsítvány kiterjesztések

A Szolgáltató az ITU X.509 szabvány 3. változatának megfelelő tanúsítvány kiterjesztéseket támogatja.

Mezőnév	Szabály	Kritikus
Kibocsátó kulcsazonosítója IssuerKeyIdentifier	Kibocsájtó kulcsazonosítója	Nem
Tulajdonos kulcsazonosítója SubjectKeyIdentifier	Kibocsájtó által generált adat	Nem
Tanúsítvány-irányelv Certificate Policies	PolicyIdentifier PolicyQualifier UserNotice A pontos értékeket Szolgáltató profildokumentuma tartalmazza ([20])	Nem
Alapvető megkötések Basic Constraints	Subject type = End Entity Path Length Constraint = None	Igen
Kulcshasználat Key Usage	A kulcshasználat értékeit az 1.4.2 fejezetben leírtaknak megfelelően Szolgáltató profildokumentuma tartalmazza ([20])	Igen
Kulcshasználat kiterjesztés ExtendedKey Usage	Ezen mező értékeit az 1.4.2 fejezetben leírtaknak megfelelően Szolgáltató profildokumentuma tartalmazza ([20])	Nem
Tulajdonos alternatív neve	Ezen mező értékeit az 1.4.2 fejezetben leírtaknak megfelelően Szolgáltató profildokumentuma tartalmazza ([20])	

Mezőnév	Szabály	Kritikus
SubjectAltName		
CRL szétosztási pont CRL Distribution Points	CRL elérési helye (URL megadásával)	Nem
Hozzáférés a kiállítói információkhoz Authority Information Acces	Hozzáférési mód=A tanúsítványkiadói tanúsítvány hozzáférésének URL-je [2] Hozzáférési mód=online tanúsítványállapot-protokoll URL-je	IGEN

A mezők kitöltésének további szabályait a Szolgáltató Tanúsítványprofilok [20] a PKI szolgáltatásokhoz című dokumentuma tartalmazza.

A kiterjesztési mezők feldolgozásáért az Előfizető és Érintett fél alkalmazása és eljárása felelős. A Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztés, vagy a szabályzatokban foglaltak figyelmen kívül hagyása, téves értelmezése miatt.

7.2. Tanúsítvány-visszavonási profil

A Szolgáltató által kibocsátott tanúsítványok visszavonási listák megfelelnek az RFC 3280 ajánlásban leírt X.509 2-es verziójú tanúsítvány visszavonási listáknak.

A Szolgáltató által kibocsátott visszavonási listák alap mezői a következők:

Mezőnév	Érték vagy szabály
Verzió Version	A visszavonási lista a ITU X.509 ajánlás 2. verziójának felel meg.
Algoritmus azonosító Signature Algorithm Identifier	Szolgáltató visszavonási listát hitelesítő elektronikus aláírásának algoritmus azonosítója (sha256RSA)
Aláírás Signature	Szolgáltató visszavonási listát hitelesítő elektronikus aláírása, RFC 2459 szerint generálva és kódolva.
Kibocsátó Issuer	A visszavonási listát kibocsátó hitelesítő szervezet egyedi azonosítója (az SSL szerver tanúsítványokat Szolgáltató egy csak erre a célra használt „produktív CA-ból” állítja ki; az egyéb nem aláírás célú tanúsítványokat pedig egy másik „produktív CA-ból”)
Hatályba lépés Effective Date	A visszavonási lista hatályba lépésének kezdete. A jelen szabályzat szerinti Szolgáltatások esetében ez megegyezik a lista kibocsátási idejével. UCT szerinti érték, RFC 2459 szerinti kódolással.
Következő kibocsátás Next Update	A következő visszavonási lista kibocsátásának ideje. UCT szerinti érték, RFC 2459 szerinti kódolással.
Visszavont tanúsítványok Revoked Certificates	A visszavont tanúsítványok listája a tanúsítvány sorozatszámával és a visszavonás idejével.

A Szolgáltató által használt visszavonás bejegyzési kiterjesztések a következők lehetnek:

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

A Szolgáltató a kiterjesztéseket nem köteles kitölteni.

A Szolgáltató által kitöltött visszavonási lista kiterjesztések a következők:

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

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

8. 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

A jelen szabályzatban leírt Szolgáltatások személyi, tárgyi és egyéb környezete lényegében megegyezik Szolgáltató elektronikus aláírással kapcsolatos szolgáltatói környezetével. Mivel ez utóbbit az illetékes hatóság (NMHH) évente ellenőrzi, az ellenőrzések közvetett módon a jelen szabályzatban leírt Szolgáltatásokat is érintik.

A hatósági ellenőrzéseken túl Szolgáltató külső és belső vizsgáltatokat végez illetve végeztet annak érdekében, hogy a Szolgáltatásaival kapcsolatos folyamatai, eszközei, személyzete és környezete megfeleljenek a vonatkozó jogszabályi és szakmai követelményeknek.

Szabályzatainak megfelelőségét Szolgáltató saját szervezete részéről a Hitelesítési Rend és Szabályozási Csoport vizsgálja meg. A Szolgáltatások megfelelőségének vizsgálatára Szolgáltató saját belső ellenőrzéseket hajt végre.

A jelen dokumentumban definiált Szolgáltatásokhoz kapcsolódó szolgáltatói szabályzatokat és Szolgáltató tevékenységét külső auditor is megvizsgálja a CA Browser Fórum ([21]) követelményei szerinti megfelelőség szempontjából, tekintettel arra, hogy az SSL szerver tanúsítványokra vonatkozóan Szolgáltató tevékenysége meg kell feleljen a CAB fórum Basic Requirements követelményeinek is, valamint az erre vonatkozó audit követelményeknek is.

A Szolgáltató egyéb (pl. az Eat. 8/b § szerinti) önkéntes akkreditációs rendszer keretében nem lett tanúsítva.

8.1. Az ellenőrzések gyakorisága és körülményei

A megfelelőségi ellenőrzéseket évente meg kell ismételni. Ezek az ellenőrzések lehetnek mind külső, mind pedig belső auditok. Az Szolgáltató érintett szervezetei és munkatársai kötelesek együttműködni az ellenőrzések során a Szolgáltató részéről kijelölt auditorral, és biztosítani az ellenőrzéshez szükséges feltételeket.

8.2. Az auditor és szükséges képesítése

Szolgáltató biztosítja, hogy a külső és belső auditálást illetve ellenőrzéseket csak megfelelő szakmai ismeretek birtokában lévő, tapasztalt szakemberek végezzék.

8.3. Az auditor és az auditált rendszerelem függetlensége

A belső vizsgálatokat illetve ellenőrzéseket a Szolgáltatások nyújtásáért illetékes szervezeti egységétől független munkatársak végzik, valamint külső auditorok esetén olyan személyek illetve szervezetek, amelyek függetlenek Szolgáltatótól illetve az általuk ellenőrzött rendszertől, területtől.

8.4. Az auditálás által lefedett területek

A [17] HR-TET követelményeivel összhangban Szolgáltató megfelelőségi vizsgálatai az alábbi területekre vonatkoznak:

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

Az auditorok illetve a belső munkatársak két fő területet, a Szolgáltatások és az informatikai biztonság területét vizsgálják, abból a szempontból, hogy Szolgáltató tanúsítványkiadói és biztonsági rendszere, annak személyi és fizikai környezete megfelel-e a mindenkori hatályos szakmai és jogszabályi előírásoknak, valamint a Szolgáltató folyamatai és tevékenységei, valamint ezek dokumentációja megfelelnek-e a vonatkozó hitelesítési rendnek, a szolgáltatási szabályzatnak, és a biztonsági szabályzatoknak.

8.5. A hiányosságok kezelése

Az auditor illetve a belső munkatárs a vizsgálati jelentést a Szolgáltató szervezetén belül a Szolgáltatásokért általánosan felelős vezetőnek nyújtja be, valamint tájékoztatásul a saját szervezeti vezetőjének.

A jelentésben megállapított hiányosságok kezelése az alábbiak mentén történik.

Amennyiben a hiányosságok nem sértik alapvetően a Szolgáltató tevékenységébe vetett bizalmat, vagy az informatikai biztonságot, úgy a Szolgáltató változatlan formában folytatja tevékenységét, de köteles a hiányosságokat ésszerű határidőn belül megszüntetnie.

Ha a hiányosságok alapvetően érintik a Szolgáltató egyes tevékenységeit, vagy az informatikai biztonság egyes területeit, a Szolgáltatónak fel kell függesztenie a hiányosságok által érintett tevékenységeit a hiányosságok megszüntetéséig. Amennyiben ez a magánkulcsok, az aláírás-létrehozó eszközök biztonságát vagy a tanúsítványok, visszavonási listák hitelességét veszélyezteti, akkor ezen tevékenységet és a kibocsátott tanúsítványokat fel kell függeszteni.

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

Ha a CA Browser fórum követelményeinek ([21]) teljesítése valamilyen jogszabályba ütközik, akkor Szolgáltató a követelmény lehető legkisebb módosításával köteles módosítani a tevékenységét úgy, hogy megfeleljen a jogszabálynak, és erről értesítenie kell a CA Browser fórumot.

8.6. Az eredmények közzététele

A külső és belső ellenőrzéseket végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a Szolgáltató bizalmas üzleti információi, ezért azokat a társaság titokvédelmi előírásai szerint kell kezelni.

A Szolgáltató a vizsgálati jelentést belső használatra szolgáló anyagként kezeli, a jelentést a vizsgálat szempontjából érintett szervezeti egységek vezetői kaphatják meg. A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni, de azok alapot adhatnak a Szolgáltató kötelezettségszegésének bizonyítására.

A CA Browser Fórum ([21]) követelményeinek betartására vonatkozó audit publikus riportját a Szolgáltató a Szolgáltatások internetes honlapján is közzéteszi.

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató a Szolgáltatások internetes honlapján közzéteheti, vagy egyedi ajánlatot küldhet az érdeklődők számára. A Szolgáltató jogosult az árlistát egyoldalúan módosítani.

Az Előfizetőkre vonatkozó hatályos szolgáltatási díjak az előfizetői szerződésben kerülnek rögzítésre.

A Szolgáltató a következő pontokban ismertetett díjtípusokat alkalmazza a Szolgáltatások nyújtásakor.

9.1.1. Tanúsítványkibocsájtás és -megújítás

Szolgáltató a kibocsátott illetőleg megújított tanúsítványokért éves fenntartási díjat számol fel az Előfizető felé, amely tartalmazza:

a. a tanúsítványok kibocsátásának illetőleg megújításának díját,
b. a tanúsítványtárban történő közzététel díját az érvényesség időtartamára,
c. a tanúsítvány felfüggesztésének, újraérvényesítésének illetve visszavonásának díját (amennyiben ilyen tevékenységre sor kerül),
d. a tanúsítványok lejárat utáni archiválásának a díját.

9.1.2. Tanúsítvány hozzáférés

Szolgáltató a közzétett tanúsítványok eléréséért nem számol fel díjat.

9.1.3. Visszavonás és állapot információ hozzáférés

Szolgáltató a közzétett visszavonási információ eléréséért nem számol fel díjat.

9.1.4. Egyéb szolgáltatásokra vonatkozó díjak

Szolgáltató a magánkulcs elhelyezése aláírás-létrehozó eszközön szolgáltatásért - amennyiben ezt Előfizető megrendelte - egyszeri díjat számol az Előfizető felé, amely tartalmazza az adott eszköz (chipkártya vagy USB-token), valamint a Szolgáltató általi megszemélyesítés díját.

A chipkártyákhoz megrendelt kártyaolvasó esetében Szolgáltató egyszeri díjat számol fel Előfizető felé a kártyaolvasóra vonatkozóan.

Amennyiben az igény emelt szintű regisztrációra vonatkozik, Szolgáltató a személyes ellenőrzésihez egyszeri díjat számít fel. Amennyiben a személyes megjelenésre és ellenőrzésre Előfizető igénye alapján az által megjelölt helyszínen kerül sor („kihelyezett regisztrációs"), ezért Szolgáltató kiszállási díjat számít fel.

Kulcsletét szolgáltatás keretében a letétbe helyezett kulcsok kivételéért és átadásáért Szolgáltató alkalmankénti eljárási díjat számít fel.

9.1.5. Visszatérítési elvek

Az Előfizető a számára kibocsátott tanúsítvány éves fenntartási díjának visszakérésére a következő esetekben jogosult:

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

A díj visszatérítésére vonatkozó igényt Előfizetőnek a tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon belül az Ügyfélkapcsolati Irodánál kell írásban jeleznie a Szolgáltató részére. Az igényt a Szolgáltató 15 naptári napon belül köteles elbírálni. Az igény pozitív elbírálása esetén a Szolgáltató a tanúsítványt visszavonja és a fenntartási díjat az Előfizető által megjelölt bankszámlaszámra 20 naptári napon belül átutalja, vagy részére új tanúsítványt bocsát ki.

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

Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

9.2. Anyagi felelősség és annak korlátai

A Szolgáltató anyagi felelősségéről és annak korlátairól a jelen szabályzat 2.2.1 pontja valamint a [18] Általános Szerződési Feltételek (ÁSZF-PKI) rendelkezik.

9.3. Bizalmasság - adatkezelési szabályok

9.3.1. Bizalmas információk

A Szolgáltató tevékenysége során a következő bizalmas adatköröket kezeli:

a. a Szolgáltató által kezelt személyes adatok és szolgáltatói adatok
b. a Szolgáltató üzleti titkai
c. az Előfizető által a Szolgáltatónak átadott üzleti titkok

A legmagasabb érzékenységi szintet bizalmasság szempontjából a Tanúsítványtulajdonosok és a Szolgáltató magánkulcsai képezik, ezen belül a legérzékenyebb a szolgáltatói aláírás-létrehozó adat, mert kompromittálódása a Szolgáltató tevékenységének azonnali felfüggesztésével jár. Ezért ezeket az adatokat, valamint az ezeket hordozó eszközöket fokozott biztonsággal tárolja, aktivizáló adatokkal védi, és az átadást illetve a hozzáférést csak az arra jogosult személyeknek biztosítja.

A Szolgáltató által kezelt személyes adatok egy része a nyilvános kulcs tulajdonosának azonosítása céljából a tanúsítványba foglalva a Szolgáltató tanúsítványtárán keresztül – Tanúsítványtulajdonos és Szolgáltató ilyen irányú megállapodása esetén - nyilvánosságra kerül, másik részét a Szolgáltató védett módon tárolja a Tanúsítványtulajdonos azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

Szolgáltató nyilvántartásba veszi az Előfizetővel aláírt szerződést, beleértve a Tanúsítványtulajdonos hozzájárulását az alábbiakhoz:

a. hozzájárulás a szolgáltatások során felhasznált adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához
b. hozzájárulás a nyilvántartásba vett adatok harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén
c. hozzájárulás a tanúsítvány közzétételéhez

Az Előfizető és a Tanúsítványtulajdonos a fenti hozzájárulást a tanúsítvány igénylésekor a regisztrációs űrlap kitöltésével és aláírásával, illetve az előfizetői szerződés aláírásával teszi meg.

Az üzleti titkok kezelésére a Polgári Törvénykönyvről szóló 2013. évi V. törvény és Szolgáltató titokvédelmi előírásai a mérvadóak. Így például egyik szerződő fél sem jogosult az előfizetői szerződés teljesítése kapcsán tudomására jutott bármely adatot, tényt, információt, tervet vagy dokumentumot a másik fél előzetes írásbeli hozzájárulása nélkül harmadik személynek átadni. A felek az üzleti titok megsértésével okozott kárért a polgári jog általános szabályai szerint felelnek.

A Szolgáltató gondoskodik a fentiekhez kapcsolódó adatvédelem és az adatbiztonság területén a jogok, kötelezettségek és felelősségek meghatározásáról, valamint a jogszabályoknak megfelelő szabályszerű működésről.

Ennek keretén belül:

a. a fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól
b. megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénysértő kezelése ellen
c. csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához
d. gondoskodik az Előfizetőre és a Tanúsítványtulajdonosra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,
e. védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az Előfizetővel folytatott adatcsere során is
f. gondoskodik arról, hogy a regisztrációs eljárás során az adatvédelmi jogszabályok követelményei érvényesüljenek,

9.3.2. Nem bizalmas információk

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

9.3.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

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

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

9.3.4. Feltárás törvényi meghatalmazással rendelkezők részére

A Szolgáltató a tanúsítványok felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az érintett személyazonosságát igazoló adatok tekintetében adatokat továbbíthat a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak, amennyiben erre irányuló hivatalos írásbeli megkeresést kap.

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

9.3.5. Feltárás bírósági meghatalmazással rendelkezők részére

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.

A Szolgáltató rögzíti az információszolgáltatás tényét és arról tájékoztatja az Előfizetőt.

9.3.6. Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson túl az Előfizetők és a Tanúsítványtulajdonosok nem nyilvános személyes adatait – beleértve az álneves tanúsítvány esetén a Tanúsítványtulajdonos valódi nevét - csak az Előfizető illetve a Tanúsítványtulajdonos írásos beleegyezése alapján tárhatja fel harmadik fél részére.

9.3.7. Feltárás más esetekben

Szolgáltatónak tevékenysége befejezésekor az [1] Eat. 16. § (2.) bekezdés szerinti nyilvántartásait, a bizalmas adatokkal együtt átadhatja egy másik szolgáltató részére.

9.4. A személyes adatok védelme

A Szolgáltató működése és szabályzatai megfelelnek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény követelményeinek.

A Szolgáltató csak a Tanúsítványtulajdonostól közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjthet személyes adatokat és csak olyan mértékben, ami a tanúsítvány kiadásához szükséges. A Szolgáltató az Előfizetők képviselőinek és a Tanúsítványtulajdonosoknak a személyes adatait csak az előfizetői szerződéssel összhangban levő célokra használhatja fel, harmadik félnek azokat az Előfizetők és a Tanúsítványtulajdonosok írásos hozzájárulása nélkül nem adhatja át, kivéve a 9.3.4 és a 9.3.5 pontban meghatározott eseteket.

9.5. 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 Szolgáltató tulajdonát képezik:

a. a visszavonási információk
a. a Szolgáltató által a Tanúsítványtulajdonos részére kibocsátott egyedi azonosító
b. a Szolgáltató szabályzatai, szerződéses feltételei
c. a tanúsítványban szereplő hitelesítő azonosító

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

A tanúsítványban szereplő megkülönböztető név használatára a megnevezett Tanúsítványtulajdonos jogosult.

10. Tevékenységért viselt felelősség és helytállás

10.1. A szolgáltatói felelősség és helytállás

A Szolgáltató felelősségét a jelen szolgáltatási szabályzat 2.2.1 fejezete, helytállására vonatkozó kötelezettségeit a [18] Általános Szerződési Feltételek (ÁSZF-PKI) tartalmazza.

10.2. Az előfizetői felelősség és helytállás

Az előfizetői felelősség és helytállás mértékére a jelen szolgáltatási szabályzat 2.2.2 fejezete, az előfizetői szerződés és a [18] Általános Szerződési Feltételek (ÁSZF-PKI) előírásai érvényesek.

10.3. Az Érintett fél felelőssége

Az Érintett fél felelősségét a jelen szolgáltatási szabályzat 2.2.3 fejezete tartalmazza

10.4. Érvényességi időtartam

Jelen szolgáltatási szabályzat érvényességét az 1.5.1 pont írja le.

10.5. Irányadó jog

A Szolgáltató működésére Magyarország törvényei az irányadók. Az alkalmazott jogszabályokat a 2.3.1 pont tartalmazza.

Ferencz Attila József

Digitálisan aláírta: Ferencz Attila József
DN: c=HU, l=Budapest, o=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., title=igazgató, serialNumber=DO20130917-1DO27, cn=Ferencz Attila József, postalCode=1081, street=Csokonai u. 3.
Dátum: 2015.06.12 15:04:39 +02'00'