

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

**Szolgáltatási szabályzat
fokozott biztonságú elektronikus aláírással
kapcsolatos szolgáltatásokhoz
(HSZSZ-F)**

Verziószám	1.2
OID szám	0.2.216.1.200.1100.100.42.3.2.8.1.2
Hatályba lépés dátuma	2014.03.15.
Hatósági nyilvántartásba vétel száma	EF/50690-12/2013
Dokumentum besorolása	Publikus

© Copyright NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. - Minden jog fenntartva

Változáskövetés

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2013.08.18.	Első változat	Lencse Zsolt Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.1	2013.09.02.	Audit észrevételei alapján módosított változat	Kővári Ferenc	Bódi Antal	Ferencz Attila
1.2	2014.02.07.	Hatóság észrevételei alapján módosított változat	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila

Tartalomjegyzék

1.	BEVEZETÉS.....	9
1.1.	ÁTTEKINTÉS	9
1.2.	A DOKUMENTUM NEVE ÉS AZONOSÍTÓJA	9
1.3.	A SZOLGÁLTATÓ ÉS A FELHASZNÁLÓI KÖZÖSSÉG	10
1.3.1.	<i>Szolgáltató adatai és elérhetőségei.....</i>	<i>10</i>
1.3.2.	<i>Regisztrációs és hitelesítő szervezet.....</i>	<i>11</i>
1.3.2.1.	A Szolgáltató regisztrációs szervezete	11
1.3.2.2.	A Szolgáltató hitelesítő szervezete	11
1.3.3.	<i>Felhasználói közösség.....</i>	<i>11</i>
1.3.3.1.	Előfizető	11
1.3.3.2.	Aláíró (alany).....	12
1.3.3.3.	Érintett fél.....	12
1.4.	TANÚSÍTVÁNYHASZNÁLAT	12
1.4.1.	<i>A szolgáltatás szintje.....</i>	<i>12</i>
1.4.2.	<i>Tanúsítványok alkalmazhatósága</i>	<i>12</i>
1.5.	A SZOLGÁLTATÁSI SZABÁLYZAT ADMINISZTRÁCIÓJA	13
1.5.1.	<i>Szabályzat hatálya</i>	<i>13</i>
1.5.2.	<i>Szabályzatra vonatkozó változáskezelés.....</i>	<i>13</i>
1.5.3.	<i>Közzétételi és tájékoztatási elvek</i>	<i>14</i>
1.5.3.1.	A HSZSZ-F-ben nem tárgyalt elemek	14
1.5.3.2.	A HSZSZ-F közzététele.....	14
1.5.4.	<i>Elfogadási eljárások</i>	<i>14</i>
1.6.	MEGHATÁROZÁSOK	14
1.7.	HIVATKOZÁSOK.....	18
1.8.	TANÚSÍTVÁNYOK JELLEMZŐI	19
1.8.1.	<i>Tanúsítványok fajtái.....</i>	<i>20</i>
1.8.1.1.	Előfizetői tanúsítvány	20
1.8.1.2.	Szolgáltatói tanúsítvány.....	20
1.8.1.3.	Teszt tanúsítvány.....	21
1.8.1.4.	„Személyes” tanúsítvány	21
1.8.1.5.	„Munkatársi” tanúsítvány	21
1.8.1.6.	„Szervezeti” vagy eszköz tanúsítvány	21
2.	ÁLTALÁNOS RENDELKEZÉSEK.....	22
2.1.	FELADATOK ÉS HATÁSKÖRÖK.....	22
2.1.1.	<i>A Szolgáltató feladatai és hatásköre</i>	<i>22</i>

2.1.1.1.	A Hitelesítő Szervezet feladatai és hatásköre	23
2.1.1.2.	A Regisztrációs Iroda feladatai és hatásköre	24
2.1.1.3.	Az Ügyfélkapcsolati Iroda feladatai és hatásköre	24
2.1.1.4.	A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre	25
2.1.1.5.	Az Ügyfélszolgálat feladata	25
2.1.2.	<i>Az Előfizető és az Aláíró feladatai és hatásköre</i>	25
2.1.3.	<i>Az Érintett félre vonatkozó ajánlások aláírás ellenőrzése során</i>	25
2.2.	FELELŐSSÉGEK	25
2.2.1.	<i>A Szolgáltató felelőssége</i>	25
2.2.2.	<i>Az Előfizető és az Aláíró felelőssége</i>	26
2.2.3.	<i>Az Érintett fél felelőssége</i>	26
2.3.	ÉRTELMEZÉS ÉS ALKALMAZÁS	27
2.3.1.	<i>Alkalmazott jogszabályok</i>	27
2.3.2.	<i>Hatályosság, megszűnés, értesítések</i>	27
2.3.2.1.	<i>Hatályosság</i>	27
2.3.2.2.	<i>Megszűnés</i>	27
2.3.2.3.	<i>Értesítések</i>	27
2.3.3.	<i>Vitás kérdések kezelése</i>	27
2.4.	KÖZZÉTÉTEL	28
2.4.1.	<i>Adatbázisok</i>	28
2.4.1.1.	<i>Tanúsítványtár</i>	28
2.4.1.2.	<i>Naplók, regisztrációs adatok</i>	28
2.4.1.3.	<i>Az adatbázisok elérésének szabályozása</i>	28
2.4.2.	<i>A tanúsítványokra vonatkozó információk közzététele</i>	28
2.4.3.	<i>A közzététel gyakorisága</i>	28
3.	AZONOSÍTÁSI ELJÁRÁSOK	29
3.1.	MEGNEVEZÉSI KONVENCIÓK	29
3.1.1.	<i>Nevek típusa</i>	29
3.1.2.	<i>Nevek szemantikája</i>	29
3.1.3.	<i>Nevek egyedisége</i>	29
3.1.4.	<i>Név igénylési viták feloldása</i>	30
3.1.5.	<i>Álnevek használata</i>	30
3.1.6.	<i>Védjegyek elismerésének módszere</i>	30
3.2.	REGISZTRÁCIÓ	30
3.2.1.	<i>Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere</i>	30
3.2.2.	<i>Regisztráció „Személyes” tanúsítvány igénylése esetén</i>	31
3.2.3.	<i>Regisztráció „Munkatársi” tanúsítvány igénylése esetén</i>	31
3.2.4.	<i>Regisztráció „Szervezeti vagy eszköz” tanúsítvány igénylése esetén</i>	32
3.2.5.	<i>Adategyeztetés</i>	33
4.	A TANÚSÍTVÁNY-ÉLETCIKLUSRA VONATKOZÓ SZABÁLYOK	33

4.1.	TANÚSÍTVÁNYIGÉNYLÉS	33
4.1.1.	<i>Ki nyújthat be tanúsítványkérelmet.....</i>	33
4.1.2.	<i>A tanúsítványigénylés folyamata és a résztvevők felelőssége</i>	33
4.2.	A TANÚSÍTVÁNY KÉRELEM FELDOLGOZÁSA	34
4.2.1.	<i>Azonosítási funkciók megvalósítása.....</i>	34
4.2.2.	<i>A tanúsítványkérelem jóváhagyása vagy visszautasítása</i>	34
4.2.3.	<i>A tanúsítványigénylések feldolgozásának időtartama.....</i>	34
4.3.	TANÚSÍTVÁNY KIBOCSÁTÁS	34
4.4.	TANÚSÍTVÁNY ELFOGADÁS	35
4.4.1.	<i>Tanúsítvány közzététele a Szolgáltató által</i>	35
4.4.2.	<i>A további szereplők értesítése a tanúsítvány kibocsátásáról</i>	35
4.5.	KULCSPÁR ÉS TANÚSÍTVÁNY HASZNÁLAT	35
4.5.1.	<i>Az Aláíró magánkulcs- és tanúsítvány használata</i>	35
4.5.2.	<i>Az Érintett felek nyilvános kulcs- és tanúsítvány használata</i>	35
4.6.	TANÚSÍTVÁNYOK ÉRVÉNYESSÉGE, MEGÚJÍTÁSA (TANÚSÍTVÁNY FRISSÍTÉSE).....	36
4.6.1.	<i>A tanúsítványok érvényessége.....</i>	36
4.6.2.	<i>A tanúsítványok megújítása.....</i>	36
4.6.3.	<i>Érvénytelen tanúsítványok megőrzése.....</i>	36
4.7.	KULCSCSERE	36
4.8.	TANÚSÍTVÁNY-MÓDOSÍTÁS	37
4.9.	TANÚSÍTVÁNY VISSZAVONÁS ÉS FELFÜGGESZTÉS.....	37
4.9.1.	<i>Visszavonáshoz/felfüggesztéshez vezető körülmények.....</i>	37
4.9.2.	<i>Visszavonás kérelmezése</i>	38
4.9.3.	<i>Visszavonási kérelemre vonatkozó eljárás</i>	39
4.9.4.	<i>A felfüggesztési kérelemre vonatkozó eljárás</i>	39
4.9.4.1.	<i>Ki kérelmezheti a felfüggesztést.....</i>	39
4.9.4.2.	<i>A felfüggesztési eljárás.....</i>	39
4.9.4.3.	<i>A Szolgáltató függeszti fel a tanúsítványt</i>	40
4.9.5.	<i>Kivárási idő visszavonási/felfüggesztési kérelem esetén</i>	40
4.9.5.1.	<i>Kivárási idő felfüggesztési kérelem esetén</i>	40
4.9.5.2.	<i>Kivárási idő visszavonási kérelem esetén</i>	40
4.9.5.3.	<i>A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok</i>	41
4.9.6.	<i>Felfüggesztett állapotra vonatkozó korlátozások, újraérvényesítés</i>	41
4.9.6.1.	<i>A felfüggesztés megengedett időtartama</i>	41
4.9.6.2.	<i>Felfüggesztés megszüntetése.....</i>	41
4.9.7.	<i>A visszavonási információ ellenőrzése az Érintett felek részéről.....</i>	42
4.9.8.	<i>Visszavonási listák (CRL) és kibocsátásuk gyakorisága</i>	42
4.9.9.	<i>A visszavonási lista előállítás és közzététele közötti leghosszabb idő</i>	42
4.9.10.	<i>Visszavonási listák ellenőrzése</i>	42

4.9.11.	Valósídejű tanúsítványállapot-ellenőrzés.....	42
4.9.12.	Visszavonási állapot közlés más formái	42
4.9.13.	Intézkedések magánkulcs kompromittálódás esetén.....	43
4.10.	KULCSLETÉT	43
5.	FIZIKAI, ELJÁRÁSRENDI ÉS HUMÁN BIZTONSÁGI SZABÁLYOZÁSOK.....	43
5.1.	FIZIKAI BIZTONSÁGI SZABÁLYOZÁSOK.....	44
5.2.	HUMÁN SZABÁLYOZÁSOK	44
5.2.1.	Bizalmi munkakörök	44
5.2.2.	Az egyes feladatokhoz szükséges személyzeti létszámok.....	46
5.2.3.	A bizalmi munkakörökben elvart azonosítás és hitelesítés	47
5.2.4.	Egymást kizáró munkakörök.....	47
5.2.5.	Személyzetre vonatkozó előírások.....	47
5.2.6.	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények	48
5.2.7.	Biztonsági háttér ellenőrzésekre vonatkozó eljárások.....	48
5.2.8.	Képzési követelmények.....	49
5.2.9.	A felhatalmazás nélküli tevékenységek büntető következményei	49
5.3.	NAPLÓZÁSI ELJÁRÁSOK.....	50
5.3.1.	Naplózott esemény típusok	50
5.3.2.	Napló adatok védelme.....	50
5.3.3.	A naplók feldolgozásának gyakorisága.....	50
5.3.4.	Napló adatok tárolása.....	50
5.3.5.	A napló fájlok megőrzési időtartama	50
5.4.	ADATOK ARCHIVÁLÁSA	50
5.4.1.	A tárolt adatok típusai.....	50
5.4.2.	Az archívum megőrzési időtartama.....	51
5.4.3.	Az archívum védelme	51
5.4.4.	Az archívum hozzáférését és ellenőrzését végző eljárások	51
5.5.	A SZOLGÁLTATÓ KULCSZERÉJE	51
5.6.	KATASZTRÓFA ELHÁRÍTÁS	51
5.6.1.	A szolgáltatások azonnali felfüggesztése.....	52
5.6.2.	Minimális szolgáltatás rendkívüli üzemeltetési helyzetben.....	52
5.6.3.	Rendkívüli eseményekről történő értesítés.....	52
5.7.	A SZOLGÁLTATÁSI TEVÉKENYSÉG MEGSZÜNTETÉSE	53
6.	MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	53
6.1.	KULCSPÁR ELŐÁLLÍTÁS ÉS TELEPÍTÉS	54
6.1.1.	Kulcspár előállítás.....	54
6.1.2.	Az aláírás-létrehozó eszköz megszemélyesítése	54
6.1.3.	Az aláírás-létrehozó adat eljuttatása az Aláíróhoz (Előfizetőhöz)	54
6.1.4.	Az Aláírók aláírás-ellenőrző adatának eljuttatása az érintett felekhez	54

6.1.5.	<i>A Szolgáltató aláírás-ellenőrző adatainak eljuttatása a felhasználói közösséghez</i>	55
6.1.6.	<i>Kulcsméreteket, használt algoritmusok</i>	55
6.1.7.	<i>Szolgáltatói kulcsgenerálás</i>	55
6.1.8.	<i>Kulcs felhasználási célok</i>	55
6.2.	AZ ALÁÍRÁS-LÉTREHOZÓ ADAT VÉDELME	56
6.2.1.	<i>Az aláírási termékre vonatkozó szabályok</i>	56
6.2.2.	<i>Kriptográfiai modulra vonatkozó szabályok</i>	56
6.2.3.	<i>A többszereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése</i>	56
6.2.4.	<i>Aláírás-létrehozó adat letét, mentés, archiválás</i>	56
6.2.5.	<i>Aláírás-létrehozó adat aktiválása</i>	57
6.2.6.	<i>Aláírás-létrehozó adat deaktiválása</i>	57
6.2.7.	<i>Aláírás-létrehozó adat megsemmisítése</i>	57
6.3.	AZ ELŐFIZETŐI TANÚSÍTVÁNYOK MEGŐRZÉSE	57
6.4.	AKTIVÁLÁSI ADATOK (PIN-KÓDOK)	57
6.5.	INFORMATIKAI BIZTONSÁGI ELŐÍRÁSOK	58
6.5.1.	<i>Számítógép biztonsági követelmények</i>	59
6.5.2.	<i>Az informatikai biztonság értékelése</i>	60
6.6.	ÉLETCIKLUSRA VONATKOZÓ MŰSZAKI ELŐÍRÁSOK	60
6.6.1.	<i>Rendszerfejlesztési szabályok</i>	60
6.6.2.	<i>Biztonságkezelési szabályok</i>	61
6.6.3.	<i>Életciklus biztonsági értékelések</i>	61
6.7.	HÁLÓZATI BIZTONSÁGI SZABÁLYOK	61
6.8.	KRIPTOGRÁFIAI MODUL ELLENŐRZÉSE	61
7.	TANÚSÍTVÁNY ÉS TANÚSÍTVÁNY-VISSZAVONÁSI PROFIL	62
7.1.	TANÚSÍTVÁNY PROFIL	62
7.1.1.	<i>Alap mezők</i>	62
7.1.2.	<i>Tanúsítvány kiterjesztések</i>	63
7.2.	TANÚSÍTVÁNY-VISSZAVONÁSI PROFIL	64
8.	A MEGFELELŐSÉG VIZSGÁLATA	65
8.1.	AZ ELLENŐRZÉSEK GYAKORISÁGA ÉS KÖRÜLMÉNYEI	65
8.2.	AZ AUDITOR ÉS SZÜKSÉGES KÉPESÍTÉSE	65
8.3.	AZ AUDITOR ÉS AZ AUDITÁLT RENDSZERELEM FÜGGETLENSÉGE	66
8.4.	AZ AUDITÁLÁS ÁLTAL LEFEDETT TERÜLETEK	66
8.5.	A HIÁNYOSSÁGOK KEZELÉSE	66
8.6.	AZ EREDMÉNYEK KÖZZÉTÉTELE	66
9.	EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK	67
9.1.	DÍJAK	67
9.1.1.	<i>Tanúsítványkibocsátás és -megújítás</i>	67
9.1.2.	<i>Tanúsítvány hozzáférés</i>	67

9.1.3.	<i>Visszavonás és állapot információ hozzáférés.....</i>	67
9.1.4.	<i>Egyéb szolgáltatásokra vonatkozó díjak</i>	67
9.1.5.	<i>Visszatérítési elvek.....</i>	67
9.2.	ANYAGI FELELŐSSÉG ÉS ANNAK KORLÁTAI	68
9.3.	BIZALMASSÁG - ADATKEZELÉSI SZABÁLYOK.....	68
9.3.1.	<i>Bizalmas információk.....</i>	68
9.3.2.	<i>Nem bizalmas információk</i>	69
9.3.3.	<i>Tanúsítvány visszavonási és felfüggesztési okok felfedése.....</i>	69
9.3.4.	<i>Feltárás törvényi meghatalmazással rendelkezők részére.....</i>	69
9.3.5.	<i>Feltárás bírósági meghatalmazással rendelkezők részére</i>	69
9.3.6.	<i>Feltárás tulajdonos kérésére</i>	70
9.3.7.	<i>Feltárás más esetekben</i>	70
9.4.	A SZEMÉLYES ADATOK VÉDELME	70
9.5.	SZELLEMI TULAJDONHOZ FÜZÖDŐ JOGOK	70
10.	TEVÉKENYSÉGÉRT VISELT FELELŐSSÉG ÉS HELYTÁLLÁS	71
10.1.	A SZOLGÁLTATÓI FELELŐSSÉG ÉS HELYTÁLLÁS.....	71
10.2.	AZ ELŐFIZETŐI FELELŐSSÉG ÉS HELYTÁLLÁS	71
10.3.	AZ ÉRINTETT FÉL FELELŐSSÉGE	71
10.4.	ÉRVÉNYESSÉGI IDŐTARTAM	71
10.5.	IRÁNYADÓ JOG	71

1. Bevezetés

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban Szolgáltató) fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó Hitelesítés Szolgáltatási Szabályzat (továbbiakban HSZSZ-F).

A fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatások (továbbiakban: Szolgáltatások) keretében a NISZ Zrt. a 2001. évi XXXV. számú, elektronikus aláírásról szóló törvényben meghatározott szolgáltatások közül a következőket nyújtja:

- a. elektronikus aláírás hitelesítés-szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás)
- b. aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése

Jelen dokumentum további fejezeteiben a "Szolgáltatások" kifejezés alatt a fenti szolgáltatások közül bármelyik vagy azok értelemszerű kombinációja értendő.

Jelen szabályzat a NISZ Zrt. fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó eljárási és működési szabályokat tartalmazza.

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

1.1. Áttekintés

Jelen HSZSZ-F a [17] (Hitelesítési Rend nyilvános körben kibocsátott nem minősített tanúsítványokra (HR-NMT)) hatálya alá tartozó előfizetői tanúsítványokra vonatkozik.

Jelen HSZSZ-F célja, hogy összefogja azokat a szabályokat, adatokat és információkat, melyeket a Szolgáltató fokozott aláírással 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

1.2. A dokumentum neve és azonosítója

Jelen dokumentum teljes neve: Szolgáltatási Szabályzat fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatásokhoz

Jelen dokumentum rövid neve: HSZSZ-F

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

A dokumentum hatósági nyilvántartásba vételi száma 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-F 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 mindenkor 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 a 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 aláírás létrehoz adatok illetve 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 az aláírás-létrehozó adat elhelyezését.

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

1.3.2.2. 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 kulcspárok és tanúsítványok előállítása, a tanúsítványok közzététele, a regisztrációs szervezettől érkező kiadási, megújítási, felfüggesztési, újraérvényesítési és visszavonási igényeknek a végrehajtása, a tanúsítványok állapotára vonatkozó információk előállítása és közzétele, valamint a szolgáltatást 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 Aláírók (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 illetve a képviselőjében eljáró Aláírók 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, az Aláíró(k) pedig jellemzően a szervezet munkatársa(i) vagy informatikai eszköze(i) (ld. következő pont)

1.3.3.2. Aláíró (alany)

Aláíró:

- a) az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja vagy aki a szolgáltató által üzemeltetett aláírás-létrehozó eszközön lévő aláírás-létrehozó adathoz kizárólagosan hozzáfér, és a saját vagy más személy nevében aláírásra jogosult,
- b) a jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, amely az aláírás-létrehozó eszközt birtokolja, és akinek a nevében az őt képviselő természetes személy az elektronikus aláírást az elektronikus dokumentumon elhelyezi, valamint
- c) aki meghatározza, hogy a nevében jogszabályban meghatározott feltételeknek megfelelő informatikai eszköz elektronikus aláírást elektronikus dokumentumon elhelyezzen.

Fentiek alapján Aláíró:

- bármely természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítványnak megfelelően, a jelen szabályzat 3.2 pontjában előírtak szerint igazolta. A HR-NMT [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 (szervezet) képviselőjében legyen jogosult aláírni, és akinek - a személyazonossága ellenőrzése mellett - a regisztráció során a 3.2.3 pontban meghatározott módon a képviselői jogosultságot illetve az Előfizetőhöz 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) az elektronikus aláírást létrehozza, a szervezet által birtokolt illetve a tanúsítványhoz kapcsolódó magánkulccsal. 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 képviselői jogosultságát a 3.2 és 3.2.3 pontokban meghatározott módon ellenőrizni kell

1.3.3.3. Érintett fél

Az Érintett fél (aláírás ellenőrző) olyan természetes személy vagy szervezet, aki vagy amely az aláírt elektronikus dokumentum fogadója, és az Aláíró tanúsítványán alapuló elektronikus aláírásra hagyatkozva jár el az aláírás hitelességének ellenőrzésekor.

1.4. Tanúsítványhasználat

1.4.1. A szolgáltatás szintje

A Szolgáltató Szolgáltatásait jelen szabályozás keretében az [1] Eat. 2.§. 15. pontjában meghatározott fokozott biztonságú elektronikus aláírás hitelesítéséhez nyújtja.

1.4.2. Tanúsítványok alkalmazhatósága

A tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

- A kibocsátott magánkulcsok az elektronikus aláírások megtételére használhatók fel.
- A nyilvános kulcsok a tanúsítványokhoz kapcsolódó aláírások ellenőrzésére használhatók fel.

A Szolgáltató által kibocsátott tanúsítványok (illetve az ezekhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, amelyek támogatják a PKI technológián alapuló elektronikus aláírási és ellenőrzési funkciókat.

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

Jelen szabályzat hatálya alatt kibocsátott tanúsítványok csak a [18] Általános Szerződési Feltételekben, illetve az előfizetői szerződésben rögzített összeghatárok szerinti korlátokkal használhatóak fel.

A tanúsítvány használati lehetőségére vonatkozó fenti információk a tanúsítványban is rögzítésre kerülnek. A tanúsítvány elfogadása, a feltüntetett használati információktól eltérő bármely módú használata az Aláíró és az Érintett fél egyéni felelőssége és kockázata.

Engedélyezett tanúsítványhasználat

A kibocsátott tanúsítványokhoz tartozó privát kulcs csak elektronikus állományok aláírására, a publikus kulcs pedig csak az aláírás ellenőrzésére használható fel, a tanúsítványba foglaltaknak megfelelően.

Korlátozott alkalmazási lehetőségek

Szolgáltató az előfizetői szerződésben felhasználási, területi, pénzügyi stb. korlátozásokat szabhat. A korlátozásokat a kibocsátott előfizetői tanúsítványban is megadja.

Az Előfizető szervezet élhet korlátozásokkal Aláíró és érintett felek tanúsítvány felhasználási tevékenységével kapcsolatosan.

Tiltott tanúsítványhasználat

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

1.5. A szolgáltatási szabályzat adminisztrációja

1.5.1. Szabályzat hatálya

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

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

A HSZSZ-F tárgyi hatálya kiterjed az 1. pontban meghatározott Szolgáltatásokra illetve ezek keretében kibocsátott 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-F karbantartásáért felelős. A szolgáltatási szabályzat hitelesítési rendeknek való megfeleléseért 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 az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal 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 HSZSZ-F módosított verziója a vonatkozó jogszabályok szerint a hatályba lépést megelőzően legalább 30 nappal előzetesen bejelentésre kerül az illetékes hatóság (Nemzeti Média- és Hírközlési Hatóság) részére.

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 HSZSZ-F-el kapcsolatos észrevételek fogadását Szolgáltató a PKI Ügyfélkapcsolati Irodán keresztül biztosítja.

1.5.3. Közzétételi és tájékoztatási elvek

1.5.3.1. A HSZSZ-F-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], operatív szintű előírással rendelkezik [16], [19], melyeket bizalmasan, üzleti titokként kezel.

1.5.3.2. A HSZSZ-F közzététele

A Szolgáltató a HSZSZ-F-t a Szolgáltatások internetes honlapján teszi közzé, nyomtatott formában pedig PKI Ügyfélkapcsolati Irodában biztosít hozzáférést a szabályzathoz.

1.5.4. Elfogadási eljárások

A jelen HSZSZ-F 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 HSZSZ-F-t indokolt esetben, de legalább évente felülvizsgálja.

A HSZSZ-F jogszabályoknak való megfelelését a Nemzeti Média- és Hírközlési Hatóság (NMHH) is vizsgálja a szabályzat új változatának hatálybalépését megelőzően. Módosítás esetén a Szolgáltató a HSZSZ-F változtatásokkal egybeszerkesztett új verziójának tervezetét felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Média- és Hírközlési Hatóság Hivatalának. A Szolgáltató alkalmanként ezt megelőzően is konzultál az NMHH-val a tervezett változtatásairól. A HSZSZ-F új változata hatályba léptetésének feltétele, hogy azt a Nemzeti Média- és Hírközlési Hatóság nyilvántartásba vegye.

1.6. Meghatározások

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

Aláírás-ellenőrző adat: olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), amelyet az elektronikus iratot vagy dokumentumot megismerő személy (vagy eszköz) az elektronikus aláírás ellenőrzésére használ.

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

Aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Aláíró: a) az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja vagy aki a szolgáltató által üzemeltetett aláírás-létrehozó eszközön lévő aláírás-létrehozó adathoz kizárólagosan hozzáfér, és a saját vagy más személy nevében aláírásra jogosult, b) a jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, amely az aláírás-létrehozó eszközt birtokolja vagy aki a szolgáltató által üzemeltetett aláírás-létrehozó eszközön lévő aláírás-létrehozó adathoz kizárólagosan hozzáfér, és akinek a nevében az őt képviselő természetes személy az elektronikus aláírást az elektronikus dokumentumon elhelyezi, valamint c) aki meghatározza, hogy a nevében jogszabályban meghatározott feltételeknek megfelelő informatikai eszköz elektronikus aláírást elektronikus dokumentumon elhelyezzen.

Biztonsági tisztviselő: a hitelesítés-szolgáltatás 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 aláírás felhasználása: elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése

Elektronikus aláírás hitelesítés-szolgáltató: az [1] Eat. 6. § (2) bekezdése szerinti tevékenységet végző személy (szervezet)

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

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

Elektronikus 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.

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.

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 hitelesítés-szolgáltatás hitelesítő kulccsal folytatott tevékenységét 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, az aláírás-létrehozó adat előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezelési szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt 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

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 lenyomattól 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

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.

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 az Aláírókról begyűjt.

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

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

Rendszervizsgáló: a 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 nincs 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.

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.

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. Aláírónak), valamint a tanúsítvány elérhetővé tétele a tanúsítványtárban

Tanúsítványtár: X. 509 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: az [1] Eat. 14. §-ban 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 tevékenységeért 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 nyilvános körben kibocsátott nem-minősített tanúsítványokra (HR-NMT)
- [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

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

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

1.8. Tanúsítványok jellemzői

Jelen HSZSZ-F az aláírás létrehozó eszköz használatát nem megkövetelő, közigazgatásban nem alkalmazható, nyilvános körben kibocsátott nem-minősített, azaz fokozott biztonságú elektronikus aláíráshoz kapcsolódó tanúsítványokra vonatkozik.

Ezen tanúsítványok jellemzőit a Szolgáltató [17] Hitelesítési Rend nyilvános körben kibocsátott nem minősített tanúsítványokra (HR-NMT) dokumentumának 1.5.2 pontja írja le.

A nem-minősített tanúsítvány a CWA 14167-1:2001 [12] szerint az Európai Unió 1999/93. direktívájának (a továbbiakban: direktíva) 5.2 cikkelyével összhangban az aláíró és nyilvános kulcsának összetartozását tanúsítja. A direktíva 5.2 cikkelye kimondja, hogy az Európai Unió tagállamainak biztosítani kell, hogy egy elektronikus aláírás jogi eljárásban nem utasítható vissza, mint törvénytelenen hatályos és elfogadható bizonyíték csupán azon az alapon, mert az

- elektronikus formában létezik, vagy mert az
- nem minősített tanúsítványra alapozott, vagy mert az
- nem egy akkreditált hitelesítés-szolgáltató által kibocsátott minősített tanúsítványra alapozott, vagy mert azt
- nem ún. biztonságos aláírás-létrehozó eszközzel (BALE) hozták létre.

A Szolgáltató által kibocsátott tanúsítványok megfelelnek az Eat. előírásainak, nyilvános körben kerülnek kibocsátásra és olyan Szolgáltató adta ki, amely szerepel az NMHH nyilvántartásában.

A tanúsítványok tartalmazzák:

- annak megjelölését, hogy a tanúsítvány fokozott biztonságú aláíráshoz lett kiadva
- a tanúsítványt kibocsátó Szolgáltató és székhelyének (ország-) azonosítóját
- az Aláíró nevét (vagy álnevét, ennek jelzésével)
- az Aláírónak külön jogszabályban, a szolgáltatási szabályzatban, az általános szerződési feltételekben vagy az előfizetői szerződésben meghatározott speciális jellemzőit, a tanúsítvány szándékolt felhasználásától függően,
- azt az aláírás-ellenőrző adatot (publikus kulcsot), amely az Aláíró által birtokolt aláírás-létrehozó adathoz kapcsolódik,
- a tanúsítvány érvényességi idejének kezdetét és végét,
- a tanúsítvány azonosító kódját
- a Szolgáltató fokozott biztonságú elektronikus aláírását,
- a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
- szervezet képviselőjére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minőségét és a képviselt szervezet adatait.

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

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 Aláírók) számára kibocsátott tanúsítvány (végfelhasználói tanúsítvány).

Az előfizetői tanúsítványokhoz kapcsolódó hitelesítési rend ([17] Hitelesítési Rend nyilvános körben kibocsátott nem minősített tanúsítványokra (HR-NMT)) objektum-azonosítója (OID): 0.2.216.1.200.1100.100.42.3.2.7.1.1

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 aláírást létrehozó adatok az Aláírók által semmilyen olyan célra nem használhatók, amelynél az átvitt adatok hitelességének vagy sértetlenségének sérüléséből vagy elvesztéséből, az aláírás-létrehozó adat vagy eszköz illetéktelen kezekbe történő jutásából az Aláírónak 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 „Common Name” (CN) vagy valamelyik másik mezőjében megtalálható a ’teszt’ vagy ’Teszt’ szövegrészlet.

1.8.1.4. „Személyes” tanúsítvány

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

A tanúsítvány „Country” és „Locality” mezőjében az Aláíró lakóhelyének országkódja és helységneve, a „Common Name” (CN) mezőben az Aláíró 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 az Aláíró 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 az Aláíró olyan természetes személy, aki egy szervezethez tartozik és azt képviseli valamilyen minőségben (jellemzően Előfizető munkavállalójaként), és ennek megfelelően kerül regisztrálásra illetve feltüntetésre a tanúsítványban.

„Munkatársi” tanúsítványok jogi személy vagy jogi személyiség nélküli szervezet munkatársai, tisztségviselői számára kerülnek kibocsátásra. Az Előfizető ebben az esetben a jogi személy vagy szervezet, az Aláíró 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 (Aláíró) 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 (Aláíró) e-mail címe szerepel.

Ha a tanúsítvány CN mezőjében nem az Aláíró 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 az Aláíró 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.

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-NMT követelményeinek megfelelően:
 - regisztráció
 - tanúsítvány előállítás
 - tanúsítvány kiadás és szétosztás
 - visszavonás kezelés (ebben felfüggesztés és újraérvényesítés biztosítása)
 - visszavonási állapot közzététele
 - aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése
2. A Szolgáltató gondoskodik a Szolgáltatásokra vonatkozó valamennyi, a jelen HSZSZ-F-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-F-jét valamint a kapcsolódó publikus dokumentumokat ([17] HR-NMT 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 Tanúsítványtárban 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 Aláírókat 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. Ügyfélszolgálat 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-F, HR-NMT [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 küldhet a lejárat tanúsítványokról az Előfizető vagy Aláíró részére.
13. Szolgáltató a tanúsítványban feltünteti az előfizetői szerződésben vagy más szabályozásban rögzített, a tanúsítvány felhasználhatóságával kapcsolatos 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 az elektronikus aláírással vagy az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.
16. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről legalább hatvan nappal korábban értesíti az Előfizetőket és a Nemzeti Média- és Hírközlési Hatóságot. 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, valamint ellátja a hatályos jogszabályokban foglalt feladatokat. A Szolgáltató a visszavont tanúsítványokkal kapcsolatos minden adatot - beleértve a személyes adatokat is – átadja ezen szolgáltatónak.
19. Ha a Szolgáltató ellen felszámolási vagy végelszámolási eljárás indult, a Szolgáltató haladéktalanul tájékoztatja a hatóságot (NMHH) e tényről, megnevezve az eljárást lefolytató szervezetet.
20. 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-NMT követelményeinek megfelelően - biztosítják a tanúsítványok illetve az aláírás-

létrehozó adatok 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 („Produkív 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 („Produkív CA”) hitelesítési kérelmeinek fogadása és ellenőrzése, részére tanúsítványok előállítása, hitelesítése
4. A „Produkív CA” tanúsítvány visszavonási és tanúsítvány megújítási kérelmeinek feldolgozása.
5. A „Produkív CA” tanúsítványainak és visszavonási listáinak publikálása
6. online tanúsítvány-állapot szolgáltatás (OCSP – Online Certificate Status Protocol) nyújtása a „Produkív CA” tanúsítványokra vonatkozóan

A 2. szintű „Produkív 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

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 az aláírás-létrehozó adat elhelyezését.

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

2.1.1.5. Az Ügyfélszolgálat feladata

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

2.1.2. Az Előfizető és az Aláíró feladatai és hatásköre

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

2.1.3. Az Érintett félre vonatkozó ajánlások aláírás ellenőrzése során

Az Érintett félnek ajánlott a Szolgáltató szabályzataiban leírtaknak megfelelően a legnagyobb gondossággal eljárni az elektronikus aláírás és a tanúsítvány elbírálásakor.

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

2.2. Felelősségek

2.2.1. A Szolgáltató felelőssége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-F szerint kiadott tanúsítványt – és ezzel jelzi a felhasználó közösség és az érintett felek felé ezen HSZSZ-F használatát – azért vállalja a felelősséget, hogy az igénylők regisztrációja, a tanúsítvány előállítás, kibocsátása, közzététele, visszavonása, a Tanúsítvány Visszavonási Lista (CRL) közzététele valamint az OSCP tevékenységek a jelen HSZSZ-F-ben előírtaknak teljes mértékben megfelelnek, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltató maga és az Előfizetők is a jelen HSZSZ-F előírásainak megfelelően járjanak el.

A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a Magyar Köztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény 339. §-a szerint, az Előfizetővel szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért, ha megszegte a szolgáltatási szabályzatban (HSZSZ-F), az általános szerződési feltételekben ([18] ÁSZF-PKI) vagy az Előfizetői Szerződésben előírtakat, továbbá az [1] Eat. 7. § (5) bekezdésében, a 9-11. §-okban vagy a 14.§-ban foglaltakat. E szabályok megtartását kétség esetén a Szolgáltatónak kell bizonyítania.

A Szolgáltató általi felelősségvállalás mértékét, mely tanúsítvány típusonként maximált összegű, az Előfizetői Szerződés rögzíti, a következők szerint: a 0 Ft tranzakciós limitű tanúsítványokhoz 100 000 Ft, az 1 000 000 Ft tranzakciós limitű tanúsítványokhoz 500 000

Ft, míg a 10 000 000 Ft tranzakciós limitű tanúsítványokhoz 4 000 000 Ft felelősségvállalási összeg tartozik.

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

A Szolgáltató felelősséget vállal minden – jelen HSZSZ-F-ben tárgyal – elektronikus aláírással kapcsolatos szolgáltatásért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki.

2.2.2. Az Előfizető és az Aláíró felelőssége

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

Az Előfizetőnek és az Aláírónak kártérítési felelőssége áll fenn a Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket a regisztráció során megadott helytelen adataival, vagy az azokban bekövetkezett változások be nem jelentésével, vagy egyéb kötelezettségeinek be nem tartásával számára okoz. Az Előfizető felelős azért, ha Aláíró a magánkulcsát nem a HSZSZ-F-ben, az ÁSZF-PKI-ben [18] és a vonatkozó jogszabályban ([1]) meghatározott módon és célra használta.

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

- a. az azonosításához szükséges személyazonosító adatokról, más személy (szervezet) képviselőjében történő aláírásra jogosító elektronikus aláírás esetén a képviselőre, illetőleg aláírásra jogosult személy személyazonosító adatairól, a cégekről, továbbá mindezek változásáról;
- b. az aláírással vagy az így aláírt elektronikus aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt - a szolgáltatási szabályzatban meghatározott - rendellenességről;

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

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

Az Előfizető illetve Aláíró 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.

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

2.2.3. Az Érintett fél felelőssége

Az Érintett fél az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok elfogadása során a tőle elvárható gondossággal jár el és az adott helyzetben általában elvárható magatartást tanúsítja. Az Érintett Félnek e tekintetben javasolt megismernie a jelen szolgáltatási szabályzatban (HSZSZ-F) rá 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.

Ezekon túlmenően a Szolgáltatónak az üzleti titkok vonatkozásában a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény szerint, a személyes adatok vonatkozásában 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-NMT) 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-NMT) foglalt értelmezéstől eltérően.

2.3.2.2. Megszűnés

Jelen szabályzat a Szolgáltató fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatásainak befejezésével tekintendő megszüntnek.

2.3.2.3. Értesítések

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

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

2.3.3. Vitás kérdések kezelése

Bármely vitás kérdés felmerülése esetén az Aláírónak 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 Tanúsítványtárban helyezi el.

Az Aláíró 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-NMT), valamint a jelen szolgáltatási szabályzat és a kapcsolódó ÁSZF-PKI
- b. a tanúsítványok használatára vonatkozó ismertető, 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.

2.4.3. A közzététel gyakorisága

Szolgáltató a kibocsátott előfizetői tanúsítványokat - az érintett Aláíró, 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.

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-T¹ X.500 ajánlásának felel meg: X.500 formátum (ITU-T X.501 /ISO/IEC 9594-2:1997, RFC 2459).

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.

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

A tanúsítvány „SubjectAltname” mezőjében az alanyhoz kapcsolódó elektronikus levelezési cím szerepel, melynek struktúrája megfelel az RFC 822 előírásainak.

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 az Aláíró nevének a „Subject/CommonName” almezőjében, valamint az entitáshoz rendelt egyedi azonosítónak a

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

„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 az Aláíró 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 nem kötelessége a védjegyek jogos használatának ellenőrzése, és nem vállal közvetítő vagy döntő szerepet ilyen jellegű viták feloldásában. Szolgáltató nem garantálja Előfizetők számára védjegyeik feltüntetését a tanúsítványban.

3.2. Regisztráció

A regisztrációs folyamat lépései általánosságban a következők:

1. Az igénylő (Aláíró vagy Előfizető kapcsolattartója) kitölti a Szolgáltató által rendelkezésre bocsátott regisztrációs űrlapot, saját kezűleg aláírja, majd aláírja az Előfizető cégjegyzésre jogosult vezetőivel is, és végül az Ügyfélkapcsolati Iroda részére átadja személyesen vagy megküldi (elektronikus) levélben, a Szolgáltató által 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 az Aláírót és egyeztet vele a tanúsítvány és az Előfizetői Szerződés átvételének módját.

3.2.1. Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere

A Szolgáltató az Aláíró kriptográfiai kulcspárját a Szolgáltatások keretében maga állítja elő, vagy ún. kriptográfiai modulban (HSM), vagy pedig biztonságos aláírás létrehozó eszközön, kiemelt biztonságú környezetben, ezért az aláírás-létrehozó adat és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán az aláírás-létrehozó adat 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 az Aláíró vagy az Előfizető kijelölt kapcsolattartója személyesen kell jelen legyen és aláírásával igazolja az aláírás-létrehozó adat illetve eszköz valamint a kapcsolódó PIN-kód átvételét.

Amennyiben Aláíró természetes személy és az átvételnél nem ő jelenik meg személyesen, Szolgáltató kérheti, hogy az Előfizető kapcsolattartója rendelkezzen Aláíró általi meghatalmazással az átvételre vonatkozóan.

3.2.2. Regisztráció „Személyes” tanúsítvány igénylése esetén

Személyes tanúsítvány esetén az Aláíró olyan természetes személy, aki magánszemélyként kerül regisztrálásra és ennek megfelelően kerül feltüntetésre a tanúsítványban,

Magánszemély a Szolgáltatótól közvetlenül nem igényelhet tanúsítványt.

3.2.3. Regisztráció „Munkatársi” tanúsítvány igénylése esetén

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

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, tranzakciós limitre, és az 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 képviselőjére jogosult személy(ek) neve, beosztása
3. Az Aláíró (tanúsítványigénylő) tekintetében:
 - 3.1. annak a szervezeti egységnek a megnevezése, ahol az Aláíró dolgozik,
 - 3.2. annak a szervezeti egységnek a telephelye, ahol az Aláíró dolgozik
 - 3.3. Aláíró neve
 - 3.4. Aláíró álneve, ha annak megjelölésére az Aláíró igényt tart és azt számára az Előfizető engedélyezte
 - 3.5. az Aláíró anyja neve
 - 3.6. Aláíró születési helye és ideje,
 - 3.7. Aláíró állampolgársága és neme
 - 3.8. az Aláíró beosztása, telefonszáma, email címe
 - 3.9. az Aláíró 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 Aláíró nyilatkozatát a Szolgáltatások igényléséhez megadott adatainak helyességére, valamint Szolgáltató feltételeinek elfogadására vonatkozóan. Hasonlóan, a regisztrációs űrlap tartalmazza az Előfizető képviselőjére jogosult személy nyilatkozatát arról, hogy Aláíró a szervezethez tartozik, és a tanúsítványt használhatja és a szervezet képviselőjében 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 képviselőjére jogosult személy képviselői 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.

Az Aláíró(k) személyazonosításához nincs szükség személyes megjelenésre; az ellenőrzést a regisztrációs űrlapon megadott személyazonosító adatok alapján végzi el az Ügyfélkapcsolati Iroda. Ilyen esetben viszont Aláíró meghatalmazottat kell megjelölni Szolgáltató részére, aki az elkészült tanúsítványt és az aláírás létrehozó adatot (a kapcsolódó eszközzel és/vagy aktivizáló adattal együtt) átveszi. Ilyenkor a meghatalmazás mellé Szolgáltató bekéri Aláíró írásos nyilatkozatát is a tanúsítvány használatával kapcsolatos kikötések és szabályok elfogadására vonatkozóan.

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, az Aláíró(k) személyazonosságának megállapítása, valamint az aláírási jogosultság ellenőrzése céljából adategyeztetést végez (lásd: 3.2.5. pont).

A Szolgáltató megtagadja a tanúsítvány kibocsátását, ha az Aláíró(k) személyazonosító adatokkal, az okmányok személyhez tartozásával, eredetiségével, valóságával 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, valóságával vagy érvényességével kapcsolatban kétség merül fel.

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

A Szolgáltató a fentiekben leírtak alapján eltekint a személyes megjelenéstől és az Aláíró 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 (Aláírónak vagy meghatalmazottjának) került-e átadásra.

3.2.4. Regisztráció „Szervezeti vagy eszköz” tanúsítvány igénylése esetén

Szervezeti vagy eszköz tanúsítvány esetében az Aláíró nem természetes személy, hanem egy szervezet. Ennek megfelelően a tanúsítvány igénylésekor eljáró természetes személy Előfizető kapcsolattartójaként értelmezendő, és jellemzően ő fogja használni vagy telepíteni 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 Aláíró helyett a tanúsítványigénylő (természetes személy) adatait kell megadni

2. Az űrlapon meg kell adni a tanúsítvány CN mezőjébe kerülő szervezet, szervezeti egység, szerepkör, vagy eszköz megnevezését,
3. Az űrlapon meg kell adni a tanúsítvány SubjectAltname mezőjébe kerülő email címet.

Az Ügyfélkapcsolati Iroda a 3.2.3 pontban leírt - Aláíróra 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 az Aláíró (természetes személy) vagy Előfizető képviselője (szervezeti vagy eszköz tanúsítvány esetén) személyazonosságát a személyazonosításra alkalmas okmánya alapján. A Szolgáltató a regisztráció során 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.

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.-3.2.5. pontok).

A Szolgáltató azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatja az Előfizetőt illetve az Aláíró a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről. Ez alapesetben a Szolgáltatások internetes honlapján közzétett Tájékoztatóval 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 bocsátott 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 az Aláíró aláírásával igazolja azt is, hogy:

- a. vállalja az aláírás-létrehozó adat 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 Aláírónak (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 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 az Aláíró 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, az Aláíró vagy annak meghatalmazottja (aki előfizető kijelölt kapcsolattartója is lehet egyben) személyesen átveszi az Ügyfélkapcsolati Irodán, az aláírás-létrehozó adattal illetve aláírás-létrehozó eszközzel és a kapcsolódó PIN-kóddal együtt, vagy
- b. az Előfizető kapcsolattartója vagy az Aláíró letölti a Szolgáltató nyilvános Tanúsítványtárából

A tanúsítvány valamint az aláírás-létrehozó adat (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 pontoknak megfelelően.

4.4. Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető illetve az Aláíró részéről az átvétellel történik meg.

A tanúsítvány illetve az aláírás-létrehozó adat használatba vétele előtt az Előfizető kijelölt kapcsolattartójának illetve az Aláírónak kötelessége ellenőrizni a tanúsítványban feltüntetett adatainak helyességét és visszaigazolni a tanúsítvány átvételét. Amennyiben bármilyen rendellenességet talál, az aláírás-létrehozó adatot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonására.

A 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 Tanúsítványtárban teszi közzé.

4.4.2. A további szereplők értesítése a tanúsítvány kibocsátásáról

További szereplőket a Szolgáltató a kibocsátott tanúsítványokról nem értesít.

4.5. Kulcspár és tanúsítvány használat

4.5.1. Az Aláíró magánkulcs- és tanúsítvány használata

Az Aláíró magánkulcs- és tanúsítvány használatára az alábbi szabályok érvényesek:

- a. Az Aláíró magánkulcsát és tanúsítványát csak az előfizetői szerződésben rögzített korlátozásnak megfelelően használhatja.
- b. Az Aláíró csak a tanúsítvány elfogadása után (lásd 4.4 pont) használhatja magánkulcsát.
- c. Az Aláíró a tanúsítvány lejárta után nem használhatja tovább magánkulcsát.
- d. Az Aláírónak az adott helyzetben általában elvárható gondosságot kell tanúsítania annak érdekében, hogy megelőzze magánkulcsának illetéktelen felhasználását.
- e. Az Aláíró 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 hagyatkozhatson 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 – az Aláíró erre vonatkozó nyilatkozata alapján - az érvényességi idő lejáratára előtt legfeljebb egy alkalommal legfeljebb egy évre meghosszabbítható.

4.6.2. A tanúsítványok megújítása

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

Tanúsítvány megújítása akkor lehetséges, ha:

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

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

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

A Szolgáltató a tanúsítvány megújítás lehetőségéről a lejárattól 30 nappal értesítést küld az Aláírónak arra az email címre, amelyet a regisztrációs űrlapon megadott.

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

Amennyiben a lejárt tanúsítványhoz aláírás-létrehozó eszközt is igényeltek, a tanúsítvány cseréje az eszközön az Aláíró 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 tanúsítványhoz tartozó privát kulccsal elektronikusan aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi. A Szolgáltató ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható. E megőrzési kötelezettségnek a Szolgáltató 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 kibocsátását jelenti egy olyan Aláíró számára, akinek a Szolgáltató korábban már kibocsátott egy tanúsítványt, de:

- a. a tanúsítvány valamilyen okból visszavonásra került,
- b. a tanúsítvány lejárt, vagy lejáráthoz 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.

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.

4.9.1. Visszavonáshoz/felfüggesztéshez vezető körülmények

A Szolgáltató felfüggeszti a tanúsítványt ha:

- a. az Előfizető vagy az Aláíró 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 az aláírás-létrehozó adat nem az Aláíró kizárólagos birtokában van
- d. az illetékes hatóság (NMHH) jogerős és végrehajtható határozatában így rendelkezik

A Szolgáltató visszavonja a tanúsítványt ha:

- a. az Előfizető vagy az Aláíró 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 az aláírás-létrehozó adat nem az Aláíró kizárólagos birtokában van
- d. az illetékes hatóság (NMHH) jogerős és végrehajtható határozatában így rendelkezik
- e. a Szolgáltató a tevékenységét befejezte
- f. a Szolgáltató és az Előfizető között az előfizetői szerződés megszűnt még a tanúsítvány érvényességének lejáratát megelőzően
- g. a tanúsítvány érvényességi ideje lejár

Az Előfizető vagy az Aláíró 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 védő aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja
- d. a tanúsítványban feltüntetett hibás adatok
- e. az Előfizető tanúsítványban feltüntetett adatainak megváltozása
- f. az Aláíró tanúsítványban feltüntetett adatainak megváltozása
- g. a tanúsítványban feltüntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszűnése².

A Szolgáltató a következő esetekben kezdeményezheti a felfüggesztést vagy visszavonást:

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

A fentiekén 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 az Aláíró, az Előfizető vagy azok képviselője, a Szolgáltató, az illetékes hatóság (Nemzeti Média- és Hírközlési Hatóság) vagy más harmadik fél kezdeményezheti. Az Előfizetőnek illetve Aláírónak és a Szolgáltatónak kötelessége, harmadik félnek joga az előző (4.9.1) pontban feltüntetett 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

² Eat. 10. § (3)

- 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 Ügyfélszolgálat a nap 24 órájában, folyamatosan rendelkezésre áll), a felfüggesztési jelszó ismeretében. A felfüggesztési jelszó a tanúsítvány kibocsájtásakor az Aláírónak 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. Aláíró 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 az Aláíró 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 visszavonására, akkor a Szolgáltató a visszavonási kérelmet visszautasítja.
- e. Szolgáltató a visszavonás megtörténtéről vagy annak visszautasításáról értesíti az Aláíró, 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.

4.9.4. A felfüggesztési kérelemre vonatkozó eljárás

4.9.4.1. Ki kérelmezheti a felfüggesztést

A felfüggesztést kérelmezheti az Aláíró vagy az Előfizető illetve annak képviselője; 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 az Aláíró 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 emailben értesíti az Aláíró 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 az Aláíró 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 valótlanosságáról,
- b. az Előfizető vagy az Aláíró visszavonási kérelme kiegészítésre szorul.

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

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

4.9.6.2. Felfüggesztés megszüntetése

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

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

Az újraérvényesítés kéréséhez a következő adatokat kell megadni:

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

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

A felfüggesztés megszüntetésének 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 felfüggesztett tanúsítványok az újraérvényesítés hatására kerülhetnek ki a listából. Szolgáltató fenntartja a jogát arra vonatkozóan, hogy a lejárt tanúsítványokat kitörölje a listából.

A Szolgáltató által kezelt visszavonási 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 előállítás 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 bármilyen kár Érintett felet terheli.

4.9.11. Valós idejű tanúsítvány állapot-ellenőrzés

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

OCSP szolgáltatás igénylése esetén a felhasználói közösséget Szolgáltató Ügyfélkapcsolati Irodája telefonon illetve személyesen tájékoztatja a használat módjáról, az azzal járó kötelezettségekről és felelősségről.

Az 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 válasz nem a CRL alapján képződik, hanem a hitelesítő központ adatbázisának egy replikációja alapján

Szolgáltató biztosítja az OCSP válaszban megadott idő 1 másodpercen belüli pontosságát a vonatkozó referenciaadatok képest (UTC). Az OCSP válaszadó egység órájának pontosságát Szolgáltató folyamatosan ellenőrzi.

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

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

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

4.10. Kulcsletét

A Szolgáltató kulcsletétet nem szolgáltat.

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 bármilyen 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, felelőségeket 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 az elektronikus aláírással kapcsolatos 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 géptermben) helyezkednek el, mivel biztonsági szempontból a legkritikusabb hardver/szoftver egységeket tartalmazzák. Itt történik a kulcspárok és a tanúsítványok előállítás, a visszavonási listák generálása és publikálása, 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 fokozott biztonságú elektronikus aláírás-hitelesítéssel kapcsolatos szolgáltatásaihoz szükséges berendezéseket, információkat, adathordozókat vagy szoftvereket jogosulatlanul elvigyék, megrongálják, vagy azokhoz jogosulatlanul hozzáférjenek³.

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.

5.2. Humán szabályozások

5.2.1. Bizalmi munkakörök

A Szolgáltató biztosítja a Szolgáltatásokhoz a vonatkozó jogszabályban (3/2005. (III. 18.) IHM rendelet) és 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.

³ A biztonsági körletben egyéb funkciók is támogathatók, a hozzáférések jogosult személyzetre való korlátozás biztosításával.

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 megfelelés biztosítása	Felügyeleti, irányítási, javaslattevési 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 géptermekek 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 megfelelésének biztosítása	A PKI szolgáltatások fizikai környezetére és személyzeti biztonságra vonatkozó hatáskör társaságon belül
PKI Rendszervizsgáló I.	PKI naplófájlok elemzése és ellenőrzése. Biztonsági hiányosságok, visszaélések felfedése, jelentése.	A PKI rendszer naplózási követelményei megfelelésének biztosítása.	A PKI szolgáltatások teljes informatikai eszközparkja és infrastruktúrája, a keletkezett biztonsági és audit naplók.
PKI Rendszer-vizsgáló II.	PKI naplófájlok elemzése és ellenőrzése. Archivált adatállomány, mentések ellenőrzése. Funkcionális és biztonsági hiányosságok, visszaélések felfedése, jelentése	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 belső eljárásai és folyamatai.

MUNKAKÖR	FELADATKÖR	FELELŐSSÉG	HATÁSKÖR
Regisztrációs felelős (Registration Officer (RO/))	Tanúsítvány elállítás és státuszváltoztatás. Aláírás létrehozó eszköz megszemélyesítés, aktiváló adatok és ügyfeladatok szabályszerű kezelése. Adminisztráció.	A PKI szolgáltatások keretében az előfizetői tanúsítványok előállításának és státusz- változásainak végrehajtása, jövőhagyása	A PKI szolgáltatások 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 helyreállítás	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 rendszeradminisztrát or	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) ellenőrző(k).

A Szolgáltató vezetője által kijelölt bizottság jelenlétében, előre megtervezett módon, kulcsceremónia keretében, ellenőrzöten és jegyzőkönyvezett végezhető 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.

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. törekedni kell a bizalmi munkakörök teljes személyi elválasztására.

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

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

A Szolgáltató munkatársai a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaköri leírásokkal rendelkeznek. A munkaköri

leírásokhoz kapcsolódó részletes feladatléírásokat a belső biztonsági szabályzat tartalmazza.

5.2.6. Képzettségre, gyakoratra 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. Kulcsörök
- 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 változás⁴ következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.⁵

Kisebbségi változások⁶ 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.

Mindezeket 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.

⁴ Jelentős változásnak minősül a szervezeti biztonságpolitika módosulása, a szoftver vagy hardver rendszer változása (upgrade), valamint a kulcs kezelés és biztonság kezelési óvintézkedések változásai.

⁵ 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.

⁶ Kisebbségi változásnak minősül, pl. egy új, kevés tapasztalattal rendelkező munkatárs munkába állása, mely a vele dolgozóktól átmenetileg nagyobb figyelmet és óvatosságot igényel.

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, az aláírás-létrehozó és ellenőrző kulcspár generálása, az aláírás-létrehozó eszköz megszemélyesítése, a tanúsítvány létrehozása, kibocsátása és kezelése, 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.

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 az aláírás-létrehozó adat 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 legalább 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 Aláírónak, illetve az adatvédelmi követelmények korlátozásain belül az Előfizetőnek hozzáférést biztosít az Aláíróra vonatkozó regisztrációs és egyéb információkhoz.

5.5. A Szolgáltató kulcscseréje

A Szolgáltató szolgáltatói kulcsának tervezett cseréje előtt legalább 60 nappal köteles tájékoztatni a Nemzeti Média- és Hírközlési Hatóságot és vele egyeztetni a szükséges feladatokról.

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 a jogszabályban előírt minimális szolgáltatásokat biztosító tartalék rendszerrel: a Szolgáltató rendkívüli üzemeltetési helyzet esetén is gondoskodik tanúsítványtára és nyilvános szabályzatai elérhetőségéről, a tanúsítvány felfüggesztés/visszavonás kezeléséről 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

Rendkívüli üzemeltetési helyzet határidőn túli fennállása esetén a Szolgáltató haladéktalanul értesíti a Nemzeti Média- és Hírközlési Hatóságot a rendkívüli üzemeltetési helyzet bekövetkezéséről, annak hatásáról, várható időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről. 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 üzletmenet 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 kezd 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:

- legalább 60 nappal korábban értesíti a Nemzeti Média- és Hírközlési Hatóságot és a Szolgáltatások internetes honlapján tájékoztatja a felhasználói közösség tagjait
- megszünteti a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások összes felhatalmazását
- megteszi a szükséges lépéseket, hogy a regisztrációs adatok és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket átruhazza

A bejelentéssel egyidejűleg a Szolgáltató leállítja:

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

Szolgáltató a tervezett megszűnés előtt 20 nappal intézkedik az előfizetői tanúsítványok és szolgáltatói tanúsítványai visszavonásáról. Ezzel egyidejűleg leállítja a visszavonás kezelési szolgáltatását.

Szolgáltató nem biztosít a szokásosnál és a jogszabályokban előírtnál nagyobb mértékű adatszolgáltatást a megszűnéskor.

Eljárás külső regisztrációs szervezet megszűnése esetén:

- 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.
- 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 ellenőrzik és hitelesítik.

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

A Szolgáltató által használt kriptográfiai modul (HSM) neve: nCipher nShield 500 F3

Hardware verzió:	nC4033P-500
Firmware verzió:	2.33.60-3
Tanúsításának száma:	HUNG-T-059-2011
Érvényességi ideje:	2014. 12. 15.

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 jogszabály által előírt tanúsítással, és szerepel a Nemzeti Média- és Hírközlési Hatóság vonatkozó 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.

Az aláírás-létrehozó adat 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, Aláíró és Előfizető nevének kártyára nyomtatása, vagy egyéb, az Előfizetői Szerződésben meghatározott adattartalommal).

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

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

A Szolgáltató az aláírás-létrehozó adatot illetve az aláírás-létrehozó eszközt az Előfizetőnek vagy az Aláírónak úgy adja át, hogy az aláírás-létrehozó adat (magánkulcs) titkossága ne sérüljön.

A Szolgáltató az aláírás-létrehozó adat illetve a biztonságos aláírás-létrehozó eszköz aktivizálási adatát (PIN-kódját) biztonságos módon, kriptográfiai modulban állítja elő, és PIN borítékban rögzíti el és tárolja.

Az átvételre jogosult személynek (Aláírónak, meghatalmazottjának illetve Előfizető kapcsolattartójának) az aláírás-létrehozó adatot 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.

Az aláírás-létrehozó adat illetve az aláírás-létrehozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

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

A Szolgáltató az Aláírók aláírás-ellenőrző adatát (nyilvános kulcsát) Tanúsítványtárában teszi mindenki számára elérhetővé. Az Aláírók aláírás-ellenőrző adata 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 az Aláírók, 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 Aláírók (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 tanúsítványt (és kulcspárt) elektronikus aláírási célra 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 az Előfizetői Szerződés feltételeinek megfelelően.

A szolgáltatói magánkulcsok használati célja kizárólag tanúsítványok, visszavonási listák, illetve OCSP 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 („Key Usage”) mező értéke	Kritikus/Nem kritikus
Hitelesítő Központ (CA) aláíró kulcsa	KeyCertSign, CRLSign	K
OCSP válasz egység aláíró kulcsa	DigitalSign, DataEncipherment, KeyEncipherment	K

	Az „Extended Key Usage” mezőbe: OCSP signing	NK
--	---	----

6.2. Az aláírás-létrehozó adat védelme

6.2.1. Az aláírási termékre vonatkozó szabályok

Az aláírás-létrehozó adatot a Szolgáltató PIN-kóddal védve bocsátja ki és adja át az Aláírónak vagy arra jogosult átvevőnek. Az aláírás-létrehozó adat átvétele után az Aláíró felelős az aláírás-létrehozó adat, valamint a PIN-kód védelméért.

A Szolgáltató az aláírás-létrehozó adatot a szolgáltatás nyújtása során visszafejtésre alkalmas formában nem tárolja, illetve adott esetben az aláírás-létrehozó eszközre helyezést követően pedig biztosítja, hogy az aláírás-létrehozó adatról 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 aláírás-létrehozó eszközhöz kapcsolódó tanúsítványok esetében Előfizetők aláírás-létrehozó adatának előállítására olyan eszközt használ, amely teljesíti a CC EAL4 követelményeket, rendelkezik a jogszabály által előírt, eszköztanúsításra jogosult szervezet által erre a célra kiadott tanúsítvánnyal (E-MS12T_TAN.BALE, érvényes: 2015.05.21.), és szerepel a Nemzeti Média- és Hírközlési Hatóság vonatkozó nyilvántartásában. A Szolgáltató által az Előfizetők aláírás-létrehozó adatának előállítására használt biztonságos aláírás létrehozó termék a Gemalto S.A. által gyártott, Classic TPC IM CC v3 intelligens kártya, melynek neve és verziója (a tanúsítvány szerint) MultiApp ID Citizen 72K (Általános konfiguráció, IAS Classic v3.0 elektronikus aláírási programot támogató JC/GP MultiApp 1.1 platformmal maszkolt S3CC91C komponens, intelligens kártya).

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. Aláírás-létrehozó adat letét, mentés, archiválás

Szolgáltató nem nyújt aláírás-létrehozó adat letét szolgáltatást. Szolgáltató az Előfizető aláírás-létrehozó adatát semmilyen formában nem menti vagy archiválja; annak előállítására, visszafejtésére alkalmas programot, adatot nem tárol.

A Szolgáltatónál a hitelesítő központok aláíró magánkulcsai⁷ biztonsági okokból duplikálásra kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik

6.2.5. Aláírás-létrehozó adat aktiválása

Az előfizetői aláírás-létrehozó adat aktiválása a felhasználó által történik a Szolgáltatótól kapott (és a későbbiekben módosított) PIN-kód megadásával, azokban az esetekben, amikor az aláírás-létrehozó adat használatára szükség van.

6.2.6. Aláírás-létrehozó adat deaktiválása

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

6.2.7. Aláírás-létrehozó adat megsemmisítése

Az előfizetői tanúsítvány lejártá után az aláírás-létrehozó adat fizikai megsemmisítését az Előfizetőnek illetve az Aláírónak saját felelősségi körében úgy kell elvégezni, hogy az semmilyen körülmények között ne legyen újra felhasználható.

A szolgáltatói aláírás-létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3. Az előfizetői tanúsítványok megőrzése

Az előfizetői tanúsítványokat a Szolgáltató megőrzi az érvényesség lejáratától számított 10 évig, illetve a tanúsítványhoz kapcsolódó privát kulccsal elektronikusan aláírt elektronikus dokumentummal 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 igénybevételeivel is eleget tehet.

6.4. Aktiválási adatok (PIN-kódok)

Az aláírás-létrehozó adatok 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 az arra jogosult személy részére az aláírás-létrehozó adattól illetve az aláírás-létrehozó eszköztől elkülönítve adja át. Az átvételt követően az Aláírónak illetve az Előfizető kijelölt kapcsolattartójának saját felelősségi körében kell biztosítani a PIN-kód kizárólagos birtoklását.

Az Aláíró 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.

7 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 osztálybasorolással 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 felhasználói⁸ hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.
4. A Szolgáltató gondoskodik arról, hogy az információhoz és az alkalmazói rendszer funkciókhoz történő hozzáférés, a hozzáférés ellenőrzési szabályzatnak megfelelően korlátozott legyen, és hogy a hitelesítés-szolgáltató rendszere megfelelő számítógép-biztonsági ellenőrzéseket nyújtson a hitelesítés-szolgáltató szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében, beleértve a biztonsági adminisztrátori és üzemeltetési funkció elkülönítését. Különösképpen a rendszer szolgáltatási programok használatát korlátozza és ellenőrzi szigorúan.
5. A Szolgáltató gondoskodik arról, hogy személyzetét sikeresen azonosítsák és hitelesítsék, mielőtt a tanúsítvány gondozásával kapcsolatos kritikus alkalmazásokat használhatnák.
6. A Szolgáltató eljárásokat dolgoztat ki és hajtat végre valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására.
7. A Szolgáltató műszaki óvintézkedéseket juttat érvényre (például tűzfalak⁹ 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 reagálni¹⁰.
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.

⁸ A felhasználó fogalma itt felöleli a rendszer operátorokat, rendszer adminisztrátorokat és bármely olyan felhasználót, akinek közvetlen hozzáférése van a rendszerhez.

⁹ A tűzfalakat úgy konfigurálják, hogy azok a Szolgáltató működéséhez nem szükséges protokollokat és hozzáféréseket kiiktassák.

¹⁰A 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 adatokat¹¹ 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.¹²

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,

¹¹ Az érzékeny adatok közé tartoznak a regisztrációs információk is.

¹² 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/Aláíróval 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, azonosságban hitelesített adatbázisokban ellenőrizze.

A tanúsítvány előállításával és visszavonás kezelésével 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 Aláírókkal 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.
Érvényesség Valid From & Valid To	A tanúsítvány érvényességének kezdete és vége. UCT szerinti érték, az RFC 2459 szerinti kódolással.
Tulajdonosazonosító Subject	A Tulajdonos egyedi neve egyedi X.500 név 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	Nem kitöltött.

Mezőnév	Szabály
Subject Unique Identifier	

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	Kibocsátó kulcsazonosítója	Nem
Tulajdonos kulcsazonosítója SubjectKeyIdentifier	Kibocsátó által generált adat	Nem
Tanúsítvány-irányelv Certificate Policies	PolicyIdentifier PolicyQualifier UserNotice	Nem
Alapvető megkötések Basic Constraints	Subject type = End Entity Path Length Constraint = None	Igen
Kulcshasználat Key Usage	Letagadhatatlanság, Digitális aláírás	Igen
Kulcshasználat kiterjesztés ExtendedKey Usage	Ügyfél hitelestés, Biztonságos email	Nem
Tulajdonos alternatív neve SubjectAltName	RFC822Name (email cím)	
CRL szétosztási pont CRL Distribution Points	CRL elérési helye (URL megadásával)	Nem
Hozzáférés a kiállítói információkhoz Authority Information Acces	Hozzáférési mód=A tanúsítványkiadói tanúsítvány hozzáférése 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
Aláírás Signature	Szolgáltató visszavonási listát hitelesítő elektronikus aláírása, RFC 2459 szerint generálva és kódolva.
Kibocsátó Issuer	A visszavonási listát kibocsátó hitelesítő szervezet egyedi azonosítója.
Hatályba lépés Effective Date	A visszavonási lista hatályba lépésének kezdete. A Szolgáltató által kibocsátott tanúsítványok esetében ez megegyezik a kibocsátás idejével. UCT szerinti érték, RFC 2459 szerinti kódolással.
Következő kibocsátás Next Update	A következő visszavonási lista kibocsátásának ideje. UCT szerinti érték, RFC 2459 szerinti kódolással.
Visszavont tanúsítványok Revoked Certificates	A visszavont tanúsítványok listája a tanúsítvány sorszámával 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 sorszám CRL number	A visszavonási lista egyesével növekvő sorszámával	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

A Szolgáltató a vonatkozó jogszabályok alapján bejelentette a Szolgáltatások nyújtására vonatkozó szándékát a Nemzeti Média- és Hírközlési Hatóság számára, és kérte a hatósági nyilvántartásba vételét 2013. szeptember 2-án. A Szolgáltató nyilvántartásba vételére a hatóság (NMHH) erről szóló, 2013.11.04-i keltezésű határozata szerint a jogerőre emelkedés napjával, 2013.11.23-án került sor.

Amennyiben a Szolgáltató működésében a hatósági nyilvántartásba vételi eljáráshoz kapcsolódó bejelentéshez képest változás következik be, azt a vonatkozó jogszabályi előírás alapján 30 nappal a változás bevezetése előtt bejelenti a Hatóságnak.

A Szolgáltató a Szolgáltatásaihoz olyan biztonságos aláírás létrehozó eszközt és kriptográfiai modult használ, amely rendelkezik a 9/2005. (VII. 21.) IHM rendelet szerint kijelölt szervezet vagy ezzel egyenértékű Európai Uniói szervezet által kiadott tanúsítással, illetve szerepel a Nemzeti Média- és Hírközlési Hatóság „Tanúsított elektronikus aláírási termékek” listáján.

A Szolgáltató külső és belső vizsgálatokat 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 Szolgáltató nyilvános szabályzatait a Nemzeti Média- és Hírközlési Hatóság is megvizsgálja a Szolgáltató nyilvántartásba vételi eljárása során, valamint a szabályzatok módosításakor, és megfelelőség esetén nyilvántartásba veszi. A hatóság a vonatkozó jogszabályok alapján a Szolgáltató tevékenységét is rendszeresen ellenőrizheti.

A Szolgáltató az Eat. 8/b § szerint 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 Szolgáltató hitelesítés szolgáltatásért 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-NMT 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 hitelesítő és biztonsági rendszere, annak személyi és fizikai környezete megfelel-e a mindenkor hatályos törvényi 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 létrehozandó aláírás-létrehozó adatok, 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.

A Szolgáltató a vizsgálati jelentést belső használatra szolgáló anyagként kezeli, a jelentést a Szolgáltató Szervezeti és Működési Szabályzatban [14] meghatározott érintett szervezeti egységek vezetői kaphatják meg. A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni, de azok alapot adhatnak a Szolgáltató kötelezettségszegésének bizonyítására.

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.

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató a Szolgáltatások internetes honlapján keresztül teszi közzé, vagy tájékoztatót 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. Tanúsítványkibocsátás 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 az aláírás-létrehozó adat 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.

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 [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 az Aláírók és a Szolgáltató aláírás-létrehozó adatai képezik, ezen belül a legérzékenyebb a szolgáltatói aláírás-létrehozó adat, mert kompromittálódása a Szolgáltató tevékenységének azonnali felfüggesztésével jár. Ezért ezeket az adatokat, 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 – Aláíró és Szolgáltató ilyen irányú megállapodása esetén - nyilvánosságra kerül, másik részét a Szolgáltató védett módon tárolja az Aláíró azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

Szolgáltató nyilvántartásba veszi az Előfizetővel aláírt szerződést, beleértve az Aláíró 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 az Aláíró a fenti hozzájárulást a tanúsítvány igénylésekor a regisztrációs űrlap kitöltésével és aláírásával, illetve az előfizetői szerződés aláírásával teszi meg.

Az üzleti titkok kezelésére a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény és Szolgáltató titokvédelmi előírásai a mérvadóak. Így például egyik szerződő fél sem jogosult az előfizetői szerződés teljesítése kapcsán tudomására jutott bármely adatot, tény, 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 elvesztéstől, 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 az Aláíróra 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 az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az érintett személyazonosságát igazoló adatok tekintetében – az [1] Eat. 11.§ paragrafusa alapján adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak, díjmentesen. Az adattovábbítást a vonatkozó jogszabály alapján haladéktalanul köteles megtenni, azt nem kötheti egyéb feltételekhez, így különösen az adatszolgáltatás költségeiben való megállapodáshoz vagy a költségek előlegezéséhez.

Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató sem az Előfizetőt, sem az Aláírókat 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 - az Aláíró személyazonosságát igazoló adatokat

átadhatja az ellenérdekű peres félnek vagy képviselőjének, feltárhat bizalmas felhasználói információkat, illetőleg azt közölheti a megkereső bírósággal az [1] Eat. 11.§ paragrafusa alapján.

A Szolgáltató rögzíti az információs szolgáltatás tényét és arról tájékoztatja az Előfizetőt.

9.3.6. Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson túl az Előfizetők és az Aláírók nem nyilvános személyes adatait – beleértve az álneves tanúsítvány esetén az Aláíró valódi nevét - csak az Előfizető illetve az Aláíró 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, át kell adnia 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 az Aláírótól közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjthet személyes adatokat és csak olyan mértékben, ami a tanúsítvány kiadásához szükséges. A Szolgáltató az Előfizetők képviselőinek és az Aláíróknak a személyes adatait csak az előfizetői szerződéssel összhangban levő célokra használhatja fel, harmadik félnek azokat az Előfizetők és az Aláírók 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 az Aláíró, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

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

A Szolgáltató tulajdonát képezik:

- a. a visszavonási információk
- c. a Szolgáltató által az Aláíró részére kibocsátott egyedi azonosító
- d. a Szolgáltató szabályzatai, szerződéses feltételei
- e. a tanúsítványban szereplő hitelesítő azonosító

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

A tanúsítványban szereplő megkülönböztető név használatára a megnevezett Aláíró 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.