NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

Szolgáltatási szabályzat minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz

(HSZSZ-M)

Verziószám	**1.2**
OID szám	**0.2.216.1.200.1100.100.42.3.1.3.1.2**
Hatálybalépés dátuma	**2014.03.15.**
Hatósági nyilvántartásba vétel száma	**EF/50690-12/2013**
Dokumentum besorolása	**Publikus**

NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

Változáskövetés

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2013.08.22.	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

NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban Szolgáltató) szolgáltatásai keretében kibocsájtott minősített tanúsítványokra és minősített időbélyegekre vonatkozó Hitelesítés Szolgáltatási Szabályzat (továbbiakban HSZSZ-M).

A NISZ Zrt. jelen szolgáltatási szabályzata vonatkozásában 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
c. időbélyegzés szolgáltatás

Jelen dokumentum további fejezeteiben a „Szolgáltatások” kifejezés alatt a fenti három szolgáltatás bármelyike, vagy azok tetszőleges kombinációja értendő.

Fenti Szolgáltatások közül Szolgáltató az a) és c) pont szerinti szolgáltatásokat önmagában is nyújtja, míg a b) pont szerinti szolgáltatás csak a hitelesítés-szolgáltatással együtt igényelhető.

Jelen szolgáltatási szabályzat a NISZ Zrt. - mint minősített hitelesítés szolgáltató - fenti Szolgáltatásaira vonatkozó eljárási és működési szabályokat tartalmazza.

A Szolgáltató a Szolgáltatásokat a vele előfizetői szerződéses viszonyban álló Előfizetők részére nyújtja, de egyes szolgáltatási elemeket hozzáférhetővé tesz az elektronikus aláírások és időbélyegek hitelességét ellenőrző Érintett felek részére is. .

1.1. Áttekintés

Jelen szolgáltatási szabályzat a {Sz13} „Hitelesítési Rend nyilvános körben kibocsátott minősített tanúsítványokra (HR-MTT)” (hatósági azonosítója: NI-14020702-HR) hatálya alá tartozó előfizetői tanúsítványokra vonatkozik. Ezen tanúsítványok az alábbiak:

[MTT]	Nyilvános körben kibocsátott, aláírás létrehozó eszköz használatát nem megkövetelő minősített tanúsítványok
[MTT+BALE]	Nyilvános körben kibocsátott, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványok
[NKET]	Nyilvános körben kibocsátott minősített tanúsítványok, melyek a 2004. évi CXL. törvény (KET) és a vonatkozó rendeletei alapján a közigazgatásban nem alkalmazhatók
[KET]	Nyilvános körben kibocsátott minősített tanúsítványok, melyek a 2004. évi CXL. törvény (KET) és a vonatkozó rendeletei a közigazgatásban alkalmazhatóak

Jelen szolgáltatási szabályzatban a különböző tanúsítványtípusokra vonatkozó követelményeket a fent alkalmazott jelölések mutatják. Amennyiben az alkalmazott jelölések nem kerülnek külön feltüntetésre, akkor a követelmények általános szabályként értendők.

Jelen szolgáltatási szabályzat vonatkozik még az {Sz15} Időbélyegzés Szolgáltatási Rend (ISZR) (hatósági azonosítója: NI-14020701-IR) követelményei szerint kiadott minősített időbélyegekre is.

Jelen dokumentum célja, hogy összefogja azokat a szabályokat, adatokat és információkat, melyeket a Szolgáltató Szolgáltatásaival kapcsolatba kerülő feleknek ismerni szükséges vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát és annak megítélését a szolgáltatásokat igénybe vevők számára, hogy az ismertetett szolgáltatási gyakorlat, a kibocsátott tanúsítványok, illetve időbélyegek mennyiben felelnek meg az elvárásaiknak. Jelen dokumentum valamint az egyéb itt hivatkozott publikus dokumentumok, ajánlások, szabványok tartalmának megismerése után, a tanúsítványok felhasználói közösségének egyértelműen meg kell tudni állapítani a tanúsítványok kezelésének módját, az általuk garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat.

1.2. A dokumentum neve és azonosítója

A jelen dokumentum teljes neve: Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz.

Jelen dokumentum rövid neve: HSZSZ-M

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

A dokumentum hatósági nyilvántartásba vételi száma a címlapon található.

A Szolgáltató jelen dokumentum egyedi azonosítója (OID) kapcsán az ISO/IEC {Sz10} és az ITU szabványok által előírt regisztrációs eljárásnak megfelelően jár el.

A HSZSZ-M 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. A Szolgáltató adatai

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

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

Kapcsolat az ügyfelekkel: PKI Ügyfélkapcsolati Iroda

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

A PKI Ügyfélkapcsolati Iroda adatai a következők:

Cím:	1081 Budapest, Csokonai u. 3.
Telefon:	+ 36 1 795-7200, + 36 30 795-7200
Fax:	+36 1 795-0100

E-mail:	info@hiteles.gov.hu
Szolgáltatások internetes honlapjának címe:	http://hiteles.gov.hu

A tanúsítványok felfüggesztésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) biztosít. Az Ügyfélszolgálat elérhető a +36 1 795-7300 és a +36 30 795-7300 telefonszámokon, valamint elektronikus levélben 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, mely 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 közlése, valamint a szolgáltatást támogató informatikai rendszer üzemeltetése.

1.3.2.3. Időbélyegző egység

Az időbélyegző egység (rövidítve: TSA) a hitelesítő szervezet erőforrásaival szorosan együttműködve az időbélyegzés szolgáltatást támogató informatikai rendszer központi erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata az időbélyegek-kérések fogadása, az időbélyegek előállítása, és ezek elküldése a kérelmező felé.

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 felhasználók (Aláírók), akik lehetnek természetes személyek, vagy informatikai eszközök)
c. az Érintett felek

Szolgáltató által kibocsátott időbélyegek felhasználói közössége általában megegyezik a fentiekkel, azzal az értelemszerű kitétellel, hogy időbélyegzés szolgáltatás esetén az időbélyegző egység is a közösség tagja, és a felhasználók nem Aláírók.

1.3.3.1. Előfizető

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

A szerződési feltételeket a {Sz14} „*Általános Szerződési Feltételek a PKI szolgáltatásokhoz*” (továbbiakban: ÁSZF-PKI) tartalmazza.

Az Előfizető lehet jogi személy vagy jogi személyiség nélküli szervezet is..

Az Előfizetőkön belül a közigazgatási szervek az Előfizetők azon csoportja, melyek a Ket. hatálya alá tartoznak [lásd: {J2} Ket. 12. § (3) és (4) bekezdés].

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:

a. bármely természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítványnak megfelelően, a jelen szabályzat 3.2.2 pontjában előírtak szerint igazolta. A HR-MTT {Sz13} illetve a vonatkozó jogszabályi előírás alapján magánszemély a Szolgáltatótól közvetlenül nem igényelhet tanúsítványt

b. bármely természetes személy, aki részére a tanúsítvány azzal a céllal kerül kibocsátásra, hogy jogi személy (szervezet) képviseletében vagy közigazgatási szerv ügyintézőjeként legyen jogosult aláírni, és akinek – a személyazonossága ellenőrzése mellett - a regisztráció során a 3.2.3 pontban meghatározott módon a képviseleti jogosultságot illetve az Előfizetőhöz tartozást is ellenőrizni kell.

c. 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 illetve eszköz tanúsítvány esetében az igényléskor meg kell nevezni azt a természetes személyt, aki az Előfizető részéről eljár a tanúsítvány igényléssel kapcsolatban (pl. az eszköz üzemeltetéséért felelős rendszergazda), és akinek a regisztráció során a személyazonosságát és képviseleti jogosultságát a 3.2 és 3.2.3 pontokban meghatározott módon ellenőrizni kell

1.3.3.3. Érintett fél

Az Érintett fél olyan természetes személy vagy szervezet, aki vagy amely az aláírt és/vagy időbélyegzett elektronikus dokumentum fogadója, és aki vagy amely egy tanúsítvánnyal hitelesített elektronikus aláírásra hagyatkozva jár el az aláírás, és/vagy az időbélyeg hitelességének ellenőrzésekor.

Az Érintett fél egy elektronikusan aláírt dokumentum fogadásakor - az elektronikus aláírás ellenőrzése céljából - az Aláíró nyilvános kulcsához tartozó tanúsítvány érvényességének ellenőrzésére hagyatkozva jár el.

1.3.4. A Közigazgatási Gyökér Hitelesítés-szolgáltató

A Szolgáltató a közigazgatásban alkalmazható tanúsítványok esetében ([KET]) magára nézve kötelezőnek ismeri el a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) által kiadott {J10} hitelesítési rendet és a KGyHSz felügyeleti jogát.

1.4. Tanúsítványhasználat

1.4.1. A szolgáltatások szintje

Szolgáltató az általa nyújtott Szolgáltatások vonatkozásában minősített szolgáltatóként szerepel az {J1} Eat. 19.§.-a szerinti hatósági nyilvántartásokban. Ennek megfelelően, Szolgáltató által a jelen szabályozás keretében kibocsátott tanúsítványok az {J1} Eat. 2.§. 19. pontja szerint minősített tanúsítványok. A HR-MTT {Sz13} illetve a vonatkozó jogszabályi előírás alapján az [MTT] tanúsítványtípussal illetve a kapcsolódó magánkulccsal készített elektronikus aláírást fokozott biztonságú elektronikus aláírásnak kell tekinteni, míg az

[MTT+BALE] tanúsítványtípussal illetve a kapcsolódó magánkulccsal készített elektronikus aláírást minősített elektronikus aláírásnak kell tekinteni.

Hasonlóan, Szolgáltató által jelen szabályozás keretében nyújtott időbélyegzés szolgáltatást minősített szolgáltatóként végzi, így az általa jelen szabályozás keretében kibocsájtott időbélyegeket minősített időbélyegeknek kell tekinteni.

1.4.2. Tanúsítványok alkalmazhatósága

A tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

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

Az időbélyegzéshez kibocsátott szolgáltatói tanúsítványokat, illetve aláíró kulcsokat a Szolgáltató kizárólag időbélyegek hitelesítésére illetve aláírására használja.

Jelen szabályzat hatálya alatt kibocsátott tanúsítványok csak a {Sz14} 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.

1.4.2.1. Engedélyezett tanúsítványhasználat

A kibocsátott előfizetői tanúsítványokhoz tartozó magánkulcsok csak elektronikus állományok aláírására, a publikus kulcsok pedig csak az aláírás ellenőrzésére használhatók fel.

1.4.2.2. Korlátozott alkalmazási lehetőségek

Szolgáltató az {Sz14} ÁSZF-PKI-ban és 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.

1.4.2.3. Tiltott tanúsítványhasználat

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

1.4.3. Időbélyegek alkalmazhatósága

Szolgáltató által kiadott időbélyegek elektronikus aláírásokhoz, elektronikus üzenetekhez, tetszőleges elektronikus dokumentumokhoz vagy állományokhoz kapcsolhatók hozzá igazolva azok létezését az adott időpontban.

1.5. A szolgáltatási szabályzat adminisztrációja

1.5.1. Szabályzat hatálya

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

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

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

1.5.2. Kapcsolattartó személy

A Szolgáltató részéről a kapcsolattartó személy a PKI szolgáltatásokért általánosan felelős vezető. Elérhetőségét a Szolgáltató a PKI Ügyfélkapcsolati Irodán keresztül biztosítja.

1.5.3. Szabályzatra vonatkozó változáskezelés

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoport működik, amely a HSZSZ-M karbantartásáért felelős. A szolgáltatási szabályzat hitelesítési rendeknek való megfeleléséért a Hitelesítési Rend és Szabályozási Csoport, illetve annak vezetője felel. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, az új szabályzat verziókat jóváhagyásra előterjeszti, elektronikus aláírással hitelesíti, a hatályon kívül helyezett szabályzatokat archiválja és 10 évig, illetőleg 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-M módosított verziója a vonatkozó jogszabályok szerint a hatályba lépést megelőzősen 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 HSZSZ-M-el kapcsolatos észrevételek fogadását Szolgáltató a PKI Ügyfélkapcsolati Irodán keresztül biztosítja.

1.5.4. Közzétételi és tájékoztatási elvek

1.5.4.1. A HSZSZ-M-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyeztetik. A Szolgáltató több belső biztonsági és egyéb szabályzattal {Sz16} - {Sz19} rendelkezik, melyeket bizalmasan, üzleti titokként kezel.

1.5.4.2. A HSZSZ-M közzététele

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

1.5.5. Elfogadási eljárások

A jelen HSZSZ-M szerkezetében és tartalmában követi az RFC 3647 szabványt {Sz11}{Sz1} 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-M-et indokolt esetben, de legalább évente felülvizsgálja.

A HSZSZ-M jogszabályoknak való megfelelőségét a Nemzeti Média- és Hírközlési Hatóság (NMHH) is vizsgálja a szabályzat új változatának hatálybalépését megelőzően. Módosítás esetén a Szolgáltató a HSZSZ-M 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 illetve szükség esetén a Közigazgatási Gyökér Hitelesítés-szolgáltatóval a tervezett változtatásairól. A HSZSZ-M új változata hatályba léptetésének feltétele, hogy azt a Nemzeti Média- és Hírközlési Hatóság nyilvántartásba vegye.

A közigazgatásban alkalmazható tanúsítványok kibocsátásának feltétele, hogy a Szolgáltató tanúsítványát a Közigazgatási Gyökér Hitelesítés-szolgáltató felülhitelesítse.

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 elektronikusan aláírt elektronikus dokumentumot megismerő személy (vagy eszköz) az elektronikus aláírás ellenőrzésére használ

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

Aláírás-létrehozó eszköz: olyan hardver vagy szoftver eszköz, amelynek 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, 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.

Biztonságos aláírás-létrehozó eszköz: az {J1} Eat. 1. számú mellékletében foglalt követelményeknek eleget tevő, az Eat. 7. § (5) – (6) bekezdés szerinti tanúsítással rendelkező aláírás-létrehozó eszköz

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 azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat

Elektronikus aláírás ellenőrzése: az elektronikusan aláírt 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 {J1} 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, így különösen 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, (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás-ellenőrző adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató elektronikus aláírás-ellenőrző adatára és annak visszavonására vonatkozó információk), amely alapján megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítványok az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt

Érintett fél: Az a természetes személy vagy szervezet, aki/amely az elektronikusan aláírt és/vagy időbélyegzett dokumentum fogadója, és az adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az aláírás, és/vagy az időbélyeg 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 és/vagy időbélyegeket rendeltetésüknek megfelelően használja.

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

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 {J1} 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 {J1} 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

Időbélyegzés: az a folyamat, melynek során az elektronikus dokumentumhoz olyan igazolás rendelődik, amely tartalmazza a bélyegzés hiteles időpontját, és amely a dokumentumhoz oly módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető

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

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

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 lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés; a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, amelyre alkalmazva a lenyomatképző eljárás eredményeképp az adott lenyomat keletkezik

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 (dokumentum kezelő, 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.

Minősített elektronikus aláírás: olyan - fokozott biztonságú – elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki

Minősített hitelesítés-szolgáltató: az {J1} Eat. szabályai szerint nyilvántartásba vett, minősített tanúsítványt a nyilvánosság számára kibocsátó hitelesítés szolgáltató

Minősített szolgáltató: a minősített hitelesítés-szolgáltató és az {J1} Eat. 6. § (1) bekezdésének *b)-d)* pontjában meghatározott szolgáltatásokat nyújtó olyan szolgáltató, amely a szolgáltatók nyilvántartásában valamely szolgáltatás tekintetében minősített szolgáltatóként szerepel

Minősített tanúsítvány: az {J1} Eat. 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített szolgáltató bocsátott ki

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 és/vagy időbélyegek 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 nincsen lehetőség

Szolgáltatási szabályzat: az {J1} Eat. 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat

Szolgáltató: elektronikus aláírással kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet

Szolgáltatói kulcspár: a szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs

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

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

Tanúsítvány: hitelesítés-szolgáltató által kibocsátott digitális igazolás, amely a belefoglalt nyilvános kulcsot (aláírás-ellenőrző adatot) az {J1} Eat. 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát.

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

Tanúsítványok típusok: a tanúsítványok alkalmazási célja szerinti megkülönböztetése (pl. biztonságos aláírás létrehozó eszköz használatát nem-megkövetelő minősített tanúsítvány, vagy biztonságos aláírás létrehozó eszköz használatát megkövetelő minősített tanúsítvány)

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

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

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

Visszavonás kezelése: az {J1} 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 vonatkoznak:

{J1} 2001. évi XXXV. törvény az elektronikus aláírásról (a továbbiakban: Eat.)

{J2} 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (a továbbiakban: Ket.)

{J3} 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

{J4} 78/2010. (III.25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól

{J5} 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

{J6} 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

{J7} 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

{J8} 7/2002 (IV. 26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

{J9} 84/2012. (IV.21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

A Szolgáltató által alkalmazott egyéb dokumentumok

{J10} A Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési rendje

{J11} 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 minősített elektronikus aláírással kapcsolatos szolgáltatásaihoz

A Szolgáltató által hivatkozott ajánlások, szabványok:

{Sz1} RFC 3647 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)

{Sz2} RFC 3739 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)

{Sz3} RFC 2459 illetve RFC 3280 (Internet X.509 Nyilvános kulcsú infrastruktúra – Tanúsítvány és Tanúsítvány visszavonási lista profil)

{Sz4} Internet Közösség RFC 2527 ajánlása

{Sz5} ETSI TS 101 862 (Minősített tanúsítvány profil),

{Sz6} RFC – 3161 (Internet X. 509 nyilvános kulcsú infrastruktúra időbélyeg protokoll)

{Sz7} ETSI TS 102 023 (2003. 04) (Időbélyegzés szolgáltatókra vonatkozó követelmények)

{Sz8} IETF RFC 2560 szabvány

{Sz9} Common Criteria (CC, Közös /Informatikai Biztonsági/ Követelmények) az Európai Közösség, az Egyesült Államok és Kanada közös ajánlása az IT termékek biztonsági minősítésének követelményeire

{Sz10} MSZ ISO/IEC 27001 szabvány

A Szolgáltató hivatkozott dokumentumai

{Sz11} A NISZ Zrt. Szervezeti és Működési Szabályzata

{Sz12} A NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai

{Sz13} NISZ Zrt. Hitelesítési Rend nyilvános körben kibocsátott minősített tanúsítványokra (HR-MTT)

{Sz14} NISZ Zrt. Általános Szerződési Feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI)

{Sz15} NISZ Zrt. Időbélyegzés Szolgáltatási Rend (ISZR)

{Sz16} NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája

{Sz17} NISZ Zrt. A PKI szolgáltatások biztonsági szabályzata

{Sz18} NISZ Zrt. A PKI szolgáltatások üzletmenet-folytonossági terve

{Sz19} NISZ Zrt. Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz

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

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

1.8. Tanúsítványok típusok és tanúsítványfajták

A jelen szolgáltatási szabályzat - az 1.1 pontnak megfelelően - alapvetően két minősített tanúsítvány típusra vonatkozik:

[MTT]	Nyilvános körben kibocsátott, aláírás létrehozó eszköz használatát nem megkövetelő minősített tanúsítványok
[MTT+BALE]	Nyilvános körben kibocsátott, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványok

Fenti két típuson belül jelen szabályzatban Szolgáltató leírja azokat a szabályokat is, amelyek az alábbi tanúsítványokra különféleképpen vonatkozik:

[NKET]	Nyilvános körben kibocsátott minősített tanúsítványok, melyek a 2004. évi CXL. törvény {J2} KET) és a vonatkozó rendeletei alapján a közigazgatásban nem alkalmazhatók
[KET]	Nyilvános körben kibocsátott minősített tanúsítványok, melyek a 2004. évi CXL. törvény {J2} KET) és a vonatkozó rendeletei alapján a közigazgatásban alkalmazhatóak

1.8.1. Minősített tanúsítványok jellemzői

Minősített tanúsítvány az {J1} Eat. 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített hitelesítés-szolgáltató bocsátott ki.

A Szolgáltató által jelen szabályzat szerint kibocsátott minősített tanúsítványok tartalmazzák:

- annak megjelölését, hogy a tanúsítvány minősített tanúsítvány,
- annak megjelölését, hogy a minősített tanúsítványhoz biztonságos aláírás-létrehozó eszköz kapcsolódik ([MTT+BALE] tanúsítványok esetén)
- a tanúsítványt kibocsátó Szolgáltató és székhelyének (ország-) azonosítóját

- az aláíró nevét vagy egy álnevet, ennek jelzésével,
- az aláírónak külön jogszabályban, a szolgáltatási szabályzatban vagy 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, valamint azt az időtartamot, ameddig a hitelesítés-szolgáltató az {J1} Eat. 9. § (7) bekezdés szerinti feladatot a tanúsítvány vonatkozásában ellátja,
- a tanúsítvány azonosító kódját
- a Szolgáltató fokozott biztonságú elektronikus aláírását,
- a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
- a tanúsítvány felhasználásának korlátait,
- más személy (szervezet) képviseletére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minőségét és a képviselt személy (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

A Szolgáltató által jelen szabályozás keretében kibocsátott minősített tanúsítványok további jellemzőit az {Sz13} hitelesítési rend írja le, ami a Szolgáltató saját hitelesítési rendje, és amelyhez kapcsolódó tanúsítványtípusok legfontosabb jellemzőit a következő alpontok ismertetik.

1.8.1.1. Nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását nem megkövetelő minősített tanúsítvány (MTT)

Az [MTT] olyan minősített tanúsítvány, amely:

a. megfelel az {J1} Eat. 2. számú mellékletében meghatározott követelményeknek
b. olyan Szolgáltató adta ki, amely teljesíti az {J1} Eat. 3. számú mellékletében meghatározott követelményeket
c. a tanúsítvány használatához illetve a kulcspár előállításához nem kapcsolódik biztonságos aláírás létrehozó eszköz
d. nyilvános körben került kibocsátásra

Az [MTT] tanúsítványtípussal illetve a kapcsolódó magánkulccsal készített elektronikus aláírást **fokozott biztonságú elektronikus aláírásnak** kell tekinteni.

1.8.1.2. Nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványtípus (MTT+BALE)

Az MTT+BALE olyan minősített tanúsítvány, amely:

a. megfelel az Eat. 2. számú mellékletében meghatározott követelményeknek
b. olyan Szolgáltató adta ki, amely teljesíti az {J1} Eat. 3. számú mellékletében meghatározott követelményeket
c. a kulcspár előállításához olyan biztonságos aláírás-létrehozó eszköz került felhasználásra, amely eleget tesz az {J1} Eat. 1. számú mellékletében meghatározott követelményeknek
d. nyilvános körben került kibocsátásra.

Az [MTT+BALE] tanúsítványtípussal illetve a kapcsolódó magánkulccsal készített elektronikus aláírást minősített elektronikus aláírásnak kell tekinteni.

1.8.2. Tanúsítvány fajták és használati jellemzőik

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

1.8.2.1. Előfizetői tanúsítványok

Az előfizetői tanúsítványok a Szolgáltatóval szerződéses viszonyban álló Előfizetők (illetve a vele kapcsolatban álló és őket képviselő Aláírók) számára kerülnek kibocsátásra (végfelhasználói tanúsítványok).

Az előfizetői tanúsítványokhoz kapcsolódó hitelesítési rend ({Sz13} (HR-MTT)) objektum-azonosítója (OID): 0.2.216.1.200.1100.100.42.3.1.1.1.1

1.8.2.2. Szolgáltatói tanúsítványok

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

A saját kiadású Szolgáltatói tanúsítványok hitelesítési rend objektumazonosítója (OID): 0.2.216.1.200.1100.100.42.3.1.5.1

1.8.2.3. Teszt tanúsítványok

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.

1.8.2.4. „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.

Közigazgatásban nem alkalmazható tanúsítványok esetén ([NKET]), ha a tanúsítvány CN mezőjében nem az Aláíró személyazonosító okmányában szereplő név kerül megadásra, úgy ez a név álnévként kerül rögzítésre.
Közigazgatásban alkalmazható tanúsítványok esetén ([KET]) a vonatkozó jogszabály alapján a tanúsítvány CN mezőiben csak valós nevek szerepelhetnek, kivéve a külön jogszabályban {J4} meghatározott pszeudonim azonosítási szinthez kapcsolódó közigazgatási eljárásokhoz igényelt tanúsítványokat, melyekben az álnév használata megengedett.
A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben, Szolgáltató erre vonatkozó dokumentuma ({Sz19}Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz) szerint.

1.8.2.5. „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.

Közigazgatásban nem alkalmazható tanúsítványok esetén ([NKET]), ha a tanúsítvány CN mezőjében nem az Aláíró személyazonosító okmányában szereplő név kerül megadásra, úgy ez a név álnévként kerül rögzítésre.

Közigazgatásban alkalmazható tanúsítványok esetén ([KET]) a vonatkozó jogszabály alapján a tanúsítvány CN mezőiben csak valós nevek szerepelhetnek, kivéve a külön jogszabályban {J4} meghatározott pszeudonim azonosítási szinthez kapcsolódó közigazgatási eljárásokhoz igényelt tanúsítványokat, melyekben az álnév használata megengedett.

A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben Szolgáltató erre vonatkozó dokumentuma ({Sz19}Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz) szerint.

1.8.2.6. „Szervezeti" vagy eszköz tanúsítvány

Szervezeti vagy eszköz tanúsítvány esetében az Aláíró jogi értelemben egy szervezet, akinek a nevében az elektronikus aláírást egy kijelölt személy vagy informatikai eszköz („gépi aláírás" esetén) készíti el technikai értelemben (mint magánkulcs felhasználó).

„Szervezeti" vagy „eszköz" tanúsítványok az Aláíró szervezete, illetve annak szervezeti egységei, vagy informatikai eszközei számára kerülnek kibocsátásra. Az „alany" ebben az esetben ennek megfelelően kerül illetve feltüntetésre a tanúsítványban, azaz mint szervezet, szervezeti egység. vagy informatikai eszköz (pl. web.szerver).

A tanúsítvány „Country" mezőjében a szervezet székhelyének (vagy telephelyének) országkódja, az „Organization" mezőben a szervezet hivatalos 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 ({Sz19}Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz) szerint.

1.9. Időbélyegek jellemzői

Időbélyeget a Szolgáltató a vele szerződéses viszonyban álló Előfizetők illetve a velük kapcsolatban álló végfelhasználók számára bocsát ki a minősített időbélyegekre vonatkozó Időbélyegzés Szolgáltatási Rend ({Sz15}ISZR) szerint.

A Szolgáltató az időbélyegeket az Előfizetők regisztrációja során a számukra kiosztott hozzáférés jogosultság (authentikációs tanúsítvány) vizsgálatát és elfogadását követően bocsátja ki.

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 {Sz13} HR-MTT 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 ([MTT+BALE] tanúsítványok esetén)
2. A Szolgáltató gondoskodik a Szolgáltatásokra vonatkozó valamennyi, a jelen HSZSZ-M-ben részletezett feltétel teljesüléséről, amennyiben azok az adott tanúsítványtípusra vagy időbélyegre 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-M-jét, valamint a kapcsolódó publikus dokumentumokat ({Sz13} HR-MTT és {Sz14} ÁSZF-PKI).
6. A Szolgáltató mindenkor az igénylők illetve Előfizetők által átadott és a regisztrációs szervezet által ellenőrzött adatok alapján bocsátja ki a tanúsítványokat. A Szolgáltató a tanúsítvány kibocsátását követően a tanúsítvány adatait nem változtatja meg.
7. A Szolgáltató a Tanúsítványtárában teszi közzé az általa kibocsátott tanúsítványokat, a visszavonási listákban pedig a felfüggesztett és visszavont tanúsítványokat. A Tanúsítványtár, a visszavonási listák és az időbélyegzés szolgáltatás elérhetőségét a Szolgáltató 99,9%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 3 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 Aláírót 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 nyilvántartásai elérhetőségét, visszavonás kezelési, visszavonási állapot közzétételi és időbélyegzés szolgáltatását minden érdekelt fél számára. Ügyfélszolgálata útján folyamatos felügyeletet biztosít a tanúsítvány visszavonási és felfüggesztési igények fogadására és 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-M, HR-MTT {Sz13}, ÁSZF-PKI {Sz14}). A szabályzatok közzétételét Szolgáltató 99,9 %-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 3 órás időtartamot.
12. A Szolgáltató a lejárat előtti 30 napban értesítést küldhet a lejáró 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 tanúsítványt 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 ellássa 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

A Szolgáltató hitelesítő szervezete, illetve az általa működtetett hitelesítő központok – a {Sz13} HR-MTT követelményeinek megfelelően - biztosítják a tanúsítványok kiadását, a visszavonási listák előállítását valamint közreműködnek ezek közzétételében.

A hitelesítő szervezet feladata az [MTT] tanúsítványok esetén a kapcsolódó kulcspár előállítása is, kivéve, ha Szolgáltató és Előfizető közös megegyezése alapján a kulcspárt Előfizető állítja elő.

A tanúsítványok előállítása során a hitelesítő központok aláírják a tanúsítvány adatokat és kötelesek gondoskodni arról, hogy a kibocsátott tanúsítványokhoz tartozó kulcsok és a tanúsítványokba foglalt nevek egyediek legyenek a szolgáltatás körén belül.

A visszavonási állapot közzétételében való közreműködés keretén belül a hitelesítő központok fogadják a visszavonási kérelmeket, új tanúsítvány visszavonási listát készítenek, és azt aláírásukkal hitelesítik.

Az 1. szintű hitelesítő központ (Főtanúsítvány-kiadó, azaz „Root CA”) alapvető feladata és hatásköre a 2. szintű hitelesítő központ („Produktív CA”) hitelesítése, ezen belül feladatai tételesen a következők:

1. Saját (szolgáltatói) kulcspár generálása és tanúsítvány előállítása önhitelesítéssel, magánkulcsának fokozott biztonságú védelme
2. További szolgáltatói kulcspárok és tanúsítványok előállítása
3. A 2. szintű hitelesítő központok ("Produktív CA”-k) hitelesítési kérelmeinek fogadása és ellenőrzése, részükre tanúsítványok előállítása, hitelesítése
4. A „Produktív CA” tanúsítvány visszavonási és tanúsítvány megújítási kérelmeinek feldolgozása.
5. A „Produktív CA” tanúsítványainak és visszavonási listáinak publikálása.
6. online tanúsítvány-állapot szolgáltatás (OCSP – Online Certificate Status Protocol) nyújtása a „Produktív CA” tanúsítványokra vonatkozóan

A 2. szintű „Produktív CA” alapvető feladata és hatásköre a Regisztrációs Szervezet által regisztrált Előfizetők tanúsítványainak hitelesítése:

1. Saját szolgáltatói kulcspár generálása és magánkulcsának fokozott biztonságú védelme.
2. A Regisztrációs Szervezettől kapott hitelesítési kérelmek fogadása és ellenőrzése.
3. [MTT] tanúsítványok esetén Előfizetői kulcspár generálása (kivéve, ha Szolgáltató és Előfizető közös megegyezése alapján a kulcspárt Előfizető állítja elő).
4. Előfizetői tanúsítványok előállítás és publikálása a Tanúsítványtárban
5. Regisztrációs Irodától érkező tanúsítvány visszavonási, felfüggesztési, újraérvényesítési és tanúsítvány megújítási kérelmek feldolgozása,valamint a tanúsítvány visszavonási listák előállítása és publikálása.

6. online tanúsítvány-állapot szolgáltatás (OCSP – Online Certificate Status Protocol) nyújtása, ennek keretében a szabványos kérések fogadása, ellenőrzése, és a szabványos 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 [MTT+BALE] tanúsítványok esetében az előfizetői kulcspár generálását, és az aláírás-létrehozó adat elhelyezését a biztonságos aláírás-létrehozó eszközön (BALE).

A Regisztrációs Iroda feladatait tételesen a {Sz13} HR-MTT 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 {Sz13} HR-MTT dokumentum tartalmazza.

A fentieken túl – időbélyegzés-szolgáltatás esetén - az Ügyfélkapcsolati Iroda biztosítja az Előfizető részére a szolgáltatáshoz való hozzáférés jogosultságot (jellemzően authentikációs tanúsítványt).

2.1.1.4. A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Rend és Szabályozási Csoport elvégzi a Szolgáltatásokkal kapcsolatos hitelesítési és időbélyegzési rendek, a vonatkozó szolgáltatási szabályzat, valamint a belső szabályzatok kezelését. A Hitelesítési Rend és Szabályozási Csoport feladata a Szolgáltató és 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 és időbélyegzési rend, a szolgáltatási szabályzat, az {Sz14} ÁSZF-PKI, és a belső biztonsági szabályzatok készítése és rendszeres karbantartása.

A Hitelesítési Rend és Szabályozási Csoport feladatai tételesen a {Sz13} HR-MTT dokumentum tartalmazza.

2.1.1.5. Az Ügyfélszolgálat feladata

A tanúsítványokkal kapcsolatos felfüggesztési, illetve visszavonási kérelmeket a Szolgáltató Ügyfélszolgálata telefonon keresztül folyamatosan (napi 24 órában) fogadja, a felfüggesztési kérelmeket végrehajtja, valamint erről telefonon illetve email-ben 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 igénybevétele során.

Az Előfizető és Aláíró feladatait tételesen a {Sz13} HR-MTT dokumentum tartalmazza.

A fentieken túl – időbélyegzés-szolgáltatás esetén – Előfizető és arra feljogosított felhasználói kötelesek:

1. az Előfizető saját érdekében bizalmasan kezelni az időbélyegzés hozzáférés titkos adatait (jellemzően az authentikációs tanúsítvány magánkulcsát),

2. Az időbélyeget felhasználók kötelesek a kért időbélyeg vétele után meggyőződni arról, hogy az időbélyeget a Szolgáltató elektronikusan aláírta, az aláírás az időbélyegzésre szolgáló kulccsal történt-e és a hozzátartozó tanúsítvány érvényes-e.

2.1.3. Érintett félre vonatkozó ajánlások

2.1.3.1. Ajánlás az elektronikus aláírás ellenőrzése során

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

Ezen belül az Érintett félre vonatkozó ajánlásokat tételesen a {Sz13} HR-MTT dokumentum tartalmazza.

2.1.3.2. Ajánlás az időbélyeg ellenőrzése során

Időbélyeg ellenőrzése során ajánlott meggyőződni arról, hogy az időbélyeg valóban a lebélyegzett dokumentumhoz tartozik-e és az időbélyeg aláírása érvényes-e.

Az időbélyeget aláíró kulcs tanúsítványának ellenőrzésére vonatkozóan általában érvényesek a 2.1.3.1 pontban leírt, a tanúsítvány ellenőrzésre vonatkozó szabályok.

2.2. Felelősségek

2.2.1. A Szolgáltató felelőssége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-M szerint kiadott tanúsítványt, időbélyeget,– és ezzel jelzi a felhasználó közösség felé ezen HSZSZ-M használatát – azért vállalja a felelősséget, hogy az igénylők regisztrációja, a tanúsítvány előállítása, kibocsátása, közzététele, visszavonása, a Tanúsítvány Visszavonási Listák (CRL) közzététele, az OCSP tevékenység, valamint az időbélyegzés szolgáltatás a jelen HSZSZ-M-ben előírtaknak teljes mértékben megfelel, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltató maga és az Előfizetők is a jelen HSZSZ-M 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, a vele szerződéses jogviszonyban álló Előfizetővel szemben a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért, ha megszegte a jelen HSZSZ-M-ben, az ÁSZF-PKI-ban {Sz14} vagy az előfizetői szerződésben előírtakat, továbbá az {J1} Eat. 7. § (2) 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 tanúsítványtípusonként maximált összegű, az Előfizetői Szerződés rögzíti, a következők szerint: a 0 Ft tranzakciós limitű tanúsítványokhoz 500 000 Ft, az 1 000 000 Ft tranzakciós limitű tanúsítványokhoz 1000 000 Ft, a 20 000 000 Ft tranzakciós limitű tanúsítványokhoz 5 000 000 Ft, míg a 200 000 000 Ft tranzakciós limitű tanúsítványokhoz 50 000 000 Ft felelősségvállalási összeg tartozik.

A Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott tanúsítvány a {Sz13} HR-MTT dokumentumban vagy jelen HSZSZ-M-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-M-ben tárgyalt – 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 valódiságával kapcsolatban.

Az Előfizetőnek és az Aláírónak kártérítési felelőssége áll fenn a Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket a regisztráció során megadott helytelen adataival, vagy az azokban bekövetkezett változások be nem jelentésével, vagy egyéb kötelezettségeinek be nem tartásával számára okoz. Az Aláíró felelős azért, ha Aláíró magánkulcsát nem a jelen HSZSZ-M-ben, az {Sz14} ÁSZF-PKI-ban és a vonatkozó jogszabályokban meghatározott módon és célra használta. Fentiek alapján az Előfizető vagy az Aláíró köteles azonnal tájékoztatni a Szolgáltatót az aláírás-létrehozó adatnak illetéktelen személy tudomására jutásáról vagy elvesztéséről.

Az Előfizető vagy az Aláíró köteles haladéktalanul tájékoztatni a Szolgáltatót:

a. az azonosításához szükséges személyazonosító adatokról, más személy (szervezet) képviseletében történő aláírásra jogosító elektronikus aláírás esetén a képviseletre, illetőleg aláírásra jogosult személy személyazonosító adatairól, a cégadatokról, továbbá mindezek változásáról;

b. az aláírással vagy az így aláírt elektronikusan aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt - a szolgáltatási szabályzatban meghatározott - rendellenességről;

Az Előfizető illetve az Aláíró felelős az aláírás-létrehozó eszköz átvételét követően annak biztonságos megőrzéséért, az aláírás-létrehozó adat és a PIN-kód valamint az időbélyegzés szolgáltatáshoz kapcsolódó authentikációs tanúsítvány magánkulcsa illetéktelenek tudomására jutásának megakadályozásáért.

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

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

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

2.2.3. Érintett fél felelőssége

Az Érintett fél az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok illetve időbélyegek 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 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 {J1}-{J11}).

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

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

2.3.2. Hatályosság, megszűnés, értesítések

2.3.2.1. Hatályosság

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

Jelen szabályzat a vonatkozó hitelesítési renddel {Sz13} HR-MTT) és az általános szerződési feltételekkel {Sz14} ÁSZF-PKI) kiegészítve a felhasználói közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza. Jelen szabályzat vagy az ÁSZF-PKI {Sz14}egyetlen pontja sem értelmezhető a hitelesítési rendben {Sz13} HR-MTT) foglalt értelmezéstől eltérően.

2.3.2.2. Megszűnés

A HSZSZ-M a Szolgáltató elektronikus aláírással kapcsolatos szolgáltatásainak befejezésével tekintendő megszűntnek.

2.3.2.3. Értesítések

A Szolgáltató az Aláírókat, Előfizetőket és Érintett feleket a Szolgáltatások 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, email-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 {Sz14} ÁSZF-PKI tartalmazza.

2.4. Közzététel

2.4.1. Adatbázisok

2.4.1.1. Tanúsítványtár

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

Az 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), 99,9%-os rendelkezésre állással biztosítja úgy, hogy a Tanúsítványtár szolgáltatás kiesése nem lépheti túl esetenként a 3 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 {Sz17} Szolgáltató biztonsági szabályzata által meghatározott szerepkörű és jogosultságú munkatársai érhetik el.

2.4.2. A tanúsítványokra, időbélyegekre vonatkozó információk közzététele

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

a. a hitelesítési rend (HR-MTT {Sz13}) és az időbélyegzési rend (ISZR {Sz15}), valamint a jelen szolgáltatási szabályzat és a kapcsolódó ÁSZF-PKI {Sz14}
b. a tanúsítványok, illetve az időbélyegek használatára vonatkozó ismertetők, nyomtatványok
c. a kibocsátott előfizetői és szolgáltatói tanúsítványok
d. a felfüggesztett és visszavont előfizetői és szolgáltatói tanúsítványok
e. szolgáltatói közlemények

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

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

2.4.3. A közzététel gyakorisága

A tanúsítványok, kikötések és feltételek nyilvánosságra hozatala tekintetében Szolgáltató a kibocsátott előfizetői tanúsítványokat - az érintett Aláíró, illetve Előfizető hozzájárulása esetén - a Tanúsítványtárban 24 órán belül közzéteszi.

A Szolgáltató az általa működtetett hitelesítő központok szolgáltatói tanúsítványait a Szolgáltatások internetes honlapján 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 az előfizetői tanúsítványokra vonatkozó 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. Azonosítás és hitelesítés

3.1. Megnevezési konvenciók

3.1.1. Nevek típusa

A tanúsítványokban szereplő névmegadás az ITU-T[1] X.500 ajánlásának felel meg: X.500 formátum (ITU-T X.501 /ISO/IEC 9594-2:1997, RFC 2459).

Természetes személy alany esetében a tanúsítványban szereplő név (betű-, szóköz- és ékezet-helyesen) azonos 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=Teljes név=Vezetéknév+Keresztnév), az UTF-8 kódolást használva.

A Szolgáltató a személyazonosság igazolására elfogadott hatósági okmányban foglalt névtől eltérő nevet álnévként kezeli és rögzíti.

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

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

A Szolgáltató fenntartja a jogot az egyes személyeket vagy csoportokat esetlegesen sértő (pl. jóízlést, szemérmet, etnikai hovatartozást sértő) álnevek 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 a Szolgáltató elsődlegesen az Aláíró nevének a „Subject/CommonName" almezőjében, valamint az entitáshoz rendelt egyedi azonosítónak a „Subject/Serialnumber" almezőjében való szerepeltetésével gondoskodik. Az egyedi azonosítót az Ügyfélkapcsolati Iroda munkatársai az általuk használt ügyfélnyilvántartó rendszerben hozzák létre és rögzítik az adott entitáshoz.

3.1.4. Név igénylési viták feloldása

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

A Szolgáltató – lehetőségei szerint – a névkiosztás során ellenőrzi 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

A közigazgatásban nem alkalmazható tanúsítványok esetén ([NKET]) Szolgáltató biztosítja az álnév használatát, Előfizető erre vonatkozó kifejezett igénye alapján.

A közigazgatásban alkalmazható tanúsítványok ([KET]) esetén Szolgáltató csak abban az esetben biztosítja az álnév használatát, ha az igénylésben jelezve lett, hogy a tanúsítványt külön jogszabályban {J4} meghatározott pszeudonim azonosítási szinthez kapcsolódó elektronikus ügyintézéshez kívánják felhasználni.

Az Előfizetőnek álnévre való igényét a regisztrációs űrlapon kell jeleznie.

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

3.1.6. Védjegyek elismerésének és hitelesítésének 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 döntnöki 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 bocsájtott regisztrációs űrlapot, saját kezűleg aláírja, majd aláíratja az Előfizető cégjegyzésre jogosult vezetőivel is, és végül az Ügyfélkapcsolati Iroda részére átadja személyesen, vagy – feltételes regisztráció esetén - 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 (valamint [MTT+BALE] tanúsítvány esetén az aláírás-létrehozó eszköz megszemélyesítéséről),
3. Az előfizetői tanúsítvány elkészültével Szolgáltató értesíti az Aláírót és egyezteti vele a tanúsítvány és az Előfizetői Szerződés átvételének helyét és idejét. Feltételes regisztráció esetén az átvételhez Aláíró személyes megjelenése kötelező

Ha Szolgáltató az aláírás-létrehozó adatot illetve [MTT+BALE] tanúsítvány esetén az aláírás-létrehozó eszközt nem a regisztrációt követően azonnal, ugyanazon a helyszínen helyezi el, illetve adja át az igénylőnek, az aláírás-létrehozó adat illetve az aláírás-létrehozó eszköz átadását megelőzően az ellenőrzést a 3.2.5 és 3.2.9 pontok szerint, a 3.2.5 bekezdés szerinti dokumentálás mellett ismételten el kell végezni.

Ha egy Előfizető csak időbélyegzés szolgáltatást igényel, a regisztráció egyszerűsített eljárással történik a 3.2.6 pont szerint.

3.2.1. Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere

[MTT+BALE] tanúsítványok esetén az Aláíró számára az aláírás-létrehozó adat és az aláírás-ellenőrző adat (kriptográfiai kulcspár) előállítása a Szolgáltatások keretében a Szolgáltató által történik, kiemelt biztonságú környezetben. A kriptográfiai kulcspár biztonságos aláírás-létrehozó eszközön (BALE) áll elő, ezért az aláírás-létrehozó adat és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán az aláírás-létrehozó eszköz átvételének igazolása szükséges. A biztonságos aláírás-létrehozó eszköz személyes átvételénél az Aláíró vagy az Előfizető által kijelölt személy aláírásával igazolja az aláírás-létrehozó eszköz és a kapcsolódó aktivizáló adat (PIN-kód illetve PUK-kód) átvételét.

[MTT] tanúsítványok esetén az Aláíró számára az aláírás-létrehozó adat és az aláírás-ellenőrző adat (kriptográfiai kulcspár) előállítása a Szolgáltatások keretében és – eltérő megállapodás hiányában – a Szolgáltató által történik, kiemelt biztonságú környezetben, tanúsított kriptográfiai modulban (HSM). Erre tekintettel az aláírás-létrehozó adat és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán az aláírás-létrehozó adat és a kapcsolódó tanúsítvány átvételének igazolása szükséges. A aláírás-létrehozó adat átvételénél az Aláíró vagy az Előfizető által kijelölt személy aláírásával igazolja ezek valamint a kapcsolódó aktivizáló adat (PIN kód) átvételét.

Azon [MTT] tanúsítványok esetén, amelyeknél a kriptográfiai kulcspárt - a Szolgáltató és Előfizető megállapodása alapján - az Előfizető generálja le, az aláírás-létrehozó adat és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzéséhez Előfizető ún. PKCS10-es kérést kell benyújtson az igénylés keretében, Szolgáltató regisztrációs szervezetéhez. A pkcs10 kérést elektronikus formában (pl. CD adathordozón) base64 kódolással, valamint papír alapon kinyomtatva és Előfizető képviselője által aláírva kell benyújtani. Ez jellemzően a 78/2010. (III.25.) Korm. rendelet 14.§. szerinti hatóság

számítógépes rendszere számára kibocsájtott, gépi aláírás hitelesítésére szolgáló tanúsítványok igénylése esetében lehetséges.

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, azzal a megjegyzéssel, hogy a közigazgatásban alkalmazható ([KET]) és hatósági ügyintézők által használt tanúsítvány esetén a regisztrációt kezdeményezheti:

a) a hatóságot – bemutatott kinevezési okirata, vagy a Magyar Közlönyben megjelent kinevezési döntés alapján – képviselő, a jelen pont illetve a 3.2.5 pont szerint azonosított természetes személy a Szolgáltatónak benyújtott igényléssel, melyet az Ügyfélkapcsolati Iroda munkatársa előtt személyesen ír alá, vagy
b) a hatóságot az a) pont szerint igazoltan képviselő természetes személy, az általa készített, közokiratba foglalt igényléssel.

A regisztrációs űrlap tartalmazza Aláíró aláírását és nyilatkozatát a Szolgáltatások igényléséhez megadott adatainak helyességére, valamint Szolgáltató feltételeinek elfogadására vonatkozóan. Az űrlapot Előfizető képviseletére jogosult vezető tisztségviselőjének is alá kell írnia („cégszerű aláírás").

A munkatársi tanúsítvány igénylésekor az azonosításhoz a következő adatokat kéri az Ügyfélkapcsolati Iroda:

a. az igénylő szervezet neve, székhelye
b. annak a szervezeti egységnek a megnevezése, ahol Aláíró dolgozik
c. az Aláíró természetes azonosítói (név, születési hely és idő, anyja neve)
d. az Aláíró beosztása (az előfizető szervezet és szervezeti egység viszonya az Aláíróhoz) és céges elérhetőségei (telefonszáma)
e. személyazonosítására használt okmány típusa és száma (személyi igazolvány, jogosítvány vagy útlevél szám),
f. az Aláíró e-mail címe
g. az Aláírót megbízó dokumentum cégszerűen aláírva (a dokumentum tartalmazza a megbízó szervezet vagy szervezeti egység nevét, e-mail címét, telefon+fax számát)
h. az előfizető szervezet illetve az Aláíró egyértelmű hozzájárulása ahhoz, hogy:
    - a tanúsítvány kibocsátásra és nyilvánosan közzétételre kerüljön
    - a szervezet vagy szervezeti egysége neve a tanúsítvány tulajdonos-azonosító mezőjében feltüntetésre kerüljön
    - az Aláíró neve a tanúsítvány tulajdonos-azonosító mezőjében feltüntetésre kerüljön

A Szolgáltató a regisztráció során a szervezeti azonosság hitelesítésére elfogad minősített aláírással ellátott elektronikus okiratot is abban az esetben, ha az Előfizetővel ebben

előzetesen megegyezik. Ez esetben az Előfizető szervezeti azonosságának hitelesítése, s a szervezeti adatok felvétele a megegyezés során történik, az elektronikus okirat „már csak" az Előfizető hozzájárulását tartalmazza az Aláíró részére történő tanúsítvány kibocsátásához

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 igénylés során az Előfizető szervezet kötelezettséget vállal arra, hogy:

a. a tanúsítvány kibocsátásával kapcsolatos díjakat megfizeti
b. a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat

A fentieken kívül még a következőket kell megadni:

a. az Aláíró kijelölését engedélyező személy neve és beosztása (az engedélyezőnek minden esetben a szervezet képviseletére jogosult személynek kell lennie és ezt hiteles dokumentumokkal kell igazolni)
b. az adott szervezet nevében aláírásra jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében Aláíró a tanúsítványt használja

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

a. személyazonosítására használt okmány (személyi igazolvány, jogosítvány vagy útlevél), bemutatása személyesen (Aláíró, Kapcsolattartó)
b. cégszerűen aláírt nyilatkozat illetve képviseleti megbízás
c. cégbíróságnál nyilvántartott gazdasági társaságok esetében 30 napnál nem régebbi cégkivonat
d. nem cégbíróságnál nyilvántartott szervezetek esetében a nyilvántartó szervezet igazolása, pl. alapítványok esetében Fővárosi Bíróság, egyéni vállalkozók esetében az illetékes önkormányzat, ügyvédek esetében az Ügyvédi Kamara, könyvvizsgálók esetében a Könyvvizsgálói Kamara,
igazságügyi szakértők esetében az Igazságügyi Minisztérium, stb.,
e. állam-, illetve közigazgatási szervezetek esetében az alapító dokumentum közjegyzővel hitelesített másolata, amelyet a szervezet első számú vezetőjének írásos nyilatkozata kísér,
f. aláírási címpéldány, amely a szervezet aláírásra jogosult vezetőinek nevét és aláírását tartalmazza;
gazdasági társaságok esetében a cégbírósági bejegyzést, más – nem gazdasági – szervezetek esetében a szervezet hivatalos bejegyzését is mellékelni kell a kérelemhez

Az Ügyfélkapcsolati Iroda a bemutatott iratok és okmányok érvényessége és hitelessége, az Aláíró és Előfizető adatainak egyeztetése, valamint az aláírási jogosultság ellenőrzése céljából adategyeztetést végez a hatósági adatbázisokkal (lásd: 3.2.7. pont).

Az Ügyfélkapcsolati Iroda köteles a tanúsítvány kibocsátását megtagadni, ha

a. a bemutatott okmányok személyhez tartozásával, valódiságával vagy érvényességével kapcsolatban kétsége merül fel
b. a csatolt dokumentumok valódiságával vagy érvényességével kapcsolatban kétsége merül fel

c. a cégnyilvántartással végzett adategyeztetés a bemutatott adatoktól eltérő eredményt ad
d. a szervezet kiléte nem állapítható meg minden kétséget kizáróan
e. nem egyértelmű a szervezet felhatalmazása a tanúsítvány kibocsátására
f. nem egyértelmű, hogy Aláíró az adott szervezethez tartozik.

Az Aláírót mint természetes személyt külön is azonosítani kell a 3.2.5. pont szerint.

3.2.4. Regisztráció szervezeti vagy eszköz tanúsítvány 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, azzal a megjegyzéssel, hogy a hatóság számítógépes rendszere számára kibocsátott gépi tanúsítványhoz szükséges regisztrációt kezdeményezheti:

a) a hatóságot – bemutatott kinevezési okirata, vagy a Magyar Közlönyben megjelent kinevezési döntés alapján – képviselő, a 3.2.3 és 3.2.5 pontok szerint azonosított természetes személy a Szolgáltatónak benyújtott igényléssel, melyet az Ügyfélkapcsolati Iroda munkatársa előtt személyesen ír alá, vagy,

b) a hatóságot az a) pont szerint igazoltan képviselő természetes személy, az általa készített, közokiratba foglalt igényléssel.

Szervezeti vagy eszköz tanúsítvány esetében a regisztrációhoz a 3.2.3 pontban jelzett adatokat, dokumentumokat és nyilatkozatokat kéri be az Ügyfélkapcsolati Iroda, az alábbi kiegészítésekkel:

1. Az Aláíró helyett a tanúsítványigénylő (mint kapcsolattartó természetes személy) adatait kell megadni
2. Az űrlapon meg kell adni a tanúsítvány CN mezőjébe kerülő szervezet vagy eszköz pontos megnevezését,
3. Az űrlapon meg kell adni a tanúsítvány SubjectAltname mezőjébe kerülő email címet
4. A 78/2010. (III.25.) Korm. rendelet 14.§. szerinti, hatóság számítógépes rendszere számára kibocsájtott, gépi aláírás hitelesítésére szolgáló tanúsítványok igénylése esetében meg kell adni a regisztrációt kérő hatóság, valamint a gépi aláírást végző eszköz egyértelmű azonosításához szükséges, a tanúsítványban szerepeltetendő adatokat és a hatóságnál a kapcsolattartásért felelős személy elérési adatait
5. Azon [MTT] tanúsítványok esetén, amelyeknél a kriptográfiai kulcspárt - a Szolgáltató és Előfizető megállapodása alapján - az Előfizető generálja le, be kell nyújtani a pkcs10 kérést elektronikus formában (pl. CD adathordozón) base64 kódolással, valamint papír alapon kinyomtatva és Előfizető képviselője által aláírva.
6. A 78/2010. (III.25.) Korm. rendelet 14.§. szerinti, hatóság számítógépes rendszere számára kibocsájtott, gépi aláírás hitelesítésére szolgáló tanúsítványok esetében – amennyiben a kriptográfiai kulcspárt a Szolgáltató állította elő, az aláírás-létrehozó adat elhelyezése a biztonságos aláírás létrehozó eszközre vagy kriptográfiai modulra az Előfizető feladata és hatásköre
7. közigazgatásban alkalmazható, hatósági ügyintéző számára igényelt tanúsítványok esetén [KET], egy közigazgatási szervet képviselő természetes személynek a regisztrációhoz magával kell vinnie egy, az adott közigazgatási szerv által kiállított és

közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a hivatal képviseletében a hitelesítés-szolgáltatónál előforduló ügyekben eljárjon, mely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti

Szervezeti és eszköz tanúsítvány esetében is igazolni kell, hogy az Előfizető részéről az igénylés során eljáró természetes személy valóban az Előfizető szervezetéhez tartozik, illetve hogy jogosult a szervezet nevében az adott tanúsítványt igényelni. Emellett szükség van Előfizető írásos nyilatkozatára a szervezet vagy az eszköz pontos megnevezéséről.

Fentieket az Ügyfélkapcsolati Iroda a 3.2.3 pontban leírtak szerint, az ott felsorolt adatok, dokumentumok és nyilatkozatok bekérésével ellenőrzi, azzal a különbséggel, hogy a 3.2.3 pontban az Aláíróra (mint természetes személyre) vonatkozó ellenőrzéseket a tanúsítványigénylő természetes személyre (a kijelölt kapcsolattartóra) vonatkozóan végzi el.

3.2.5. Természetes személy azonosítása

A természetes személy azonosságának hitelesítését a Szolgáltató a 3.2.2 pontban leírtakon felül a következők szerint biztosítja:

a) A regisztrációhoz az igénylőnek személyesen kell megjelennie a Szolgáltató Ügyfélkapcsolati Irodájában.

b) A regisztráció során az igénylő személyazonosságát a személyazonosság igazolására alkalmas hatósági igazolvány alapján ellenőrizni kell.

c) A regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét az igénylőnek nyilatkozatban, saját kezű aláírásával ellátva kell igazolnia.

d) A b) pont szerinti hatósági igazolvány azonosító adatait, a megadott adatok egyezését és a hatósági igazolvány érvényességét a Szolgáltató Ügyfélkapcsolati Irodája közhiteles nyilvántartásban ellenőrzi.

e) Szolgáltató Ügyfélkapcsolati Irodájának munkatársa aláírásával kell igazolja, hogy a hatósági igazolványon szereplő arckép megfeleltethető az igénylő arcának és az igazolványban szereplő aláírás azonos a c) pont szerinti nyilatkozatot igazoló aláírással.

3.2.6. Időbélyegzés szolgáltatás igénylése

Időbélyegzés szolgáltatást csak jogi személy (szervezet) igényelhet.

Az időbélyegzés szolgáltatás igénybe vétele a Szolgáltató és az Előfizető között megkötött szolgáltatási szerződés keretében lehetséges. Ezen szerződés keretében az Előfizető írásbeli nyilatkozatot ad arra vonatkozóan, hogy a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

Az időbélyegzés szolgáltatás igénybe vételére vonatkozó szerződés megkötése érdekében az Ügyfélkapcsolati Iroda egy cégszerűen aláírt megrendelő bemutatását kéri. Ehhez kapcsolódóan szükség van még az alábbi dokumentumokra:

- az előfizető szervezet 30 napnál nem régebbi cégkivonatára vagy egyéb hivatalos okmányára (pl. alapító okirat),
- az adott szervezet nevében aláírásra jogosult vezető tisztségviselő aláírási címpéldányára
- az adott szervezet részéről eljáró természetes személy részére kiállított meghatalmazásra, hogy a szolgáltatás igénybevételéhez szükséges, Szolgáltató által biztosított authentikációs tanúsítványt és a kapcsolódó magánkulcsot átvegye

Az Ügyfélkapcsolati Iroda az időbélyegzés szolgáltatási szerződés megkötése során megtagadhatja a szerződés megkötését, ha

a. az előfizető részéről eljáró természetes személy által bemutatott személyi okmányok személyhez tartozásával, valódiságával vagy érvényességével kapcsolatban kétsége merül fel

b. a megrendelőből a szervezet kiléte nem állapítható meg minden kétséget kizáróan

Az időbélyegzés szolgáltatás igénybe vételekor a Szolgáltató az igénybe vevőnél biztonságos csatornán keresztüli tanúsítvány alapú kliens azonosítást, vagy egyéb, az előfizető egyértelmű azonosítását lehetővé tevő megoldást alkalmaz.

3.2.7. Feltételes regisztráció

A 78/2010. (III.25) IHM rendelet 11. A § alapján Szolgáltató feltételes regisztrációt is lefolytathat.

Ennek keretében Szolgáltató az igénylő (Előfizető) kérése alapján, az általa megadott adatokkal, a 3.2.8 szerinti közhiteles hatósági nyilvántartásokban történő adatellenőrzést követően előzetesen előállítja a tanúsítványt, a kapcsolódó aláírás-létrehozó adatot illetve aláírás-ellenőrző adatot, az ezekhez tartozó aktivizáló adatot (valamint [MTT+BALE] tanúsítvány esetén megszemélyesíti a biztonságos aláírás létrehozó eszközt).

Feltételes regisztráció keretében az előre elkészített aláírás-létrehozó adat illetve aláírás-ellenőrző adat, az ezekhez tartozó aktivizáló adat (valamint [MTT+BALE] tanúsítvány esetén a megszemélyesített biztonságos aláírás létrehozó eszköz) a tanúsítvánnyal együtt kizárólag személyesen az Aláírónak adható át, Szolgáltató Ügyfélkapcsolati Irodájában, vagy (külön megállapodás alapján) az igénylő (Előfizető) által megjelölt külső helyszínen, az Ügyfélkapcsolati Iroda munkatársa által. Az átadott tanúsítvány illetve magánkulcs az átadást követően aktiválható.

3.2.8. Hatóság humánpolitikai szervezet által elvégzett regisztráció

[KET] Közigazgatásban alkalmazható, hatósági ügyintézők által használt aláíráshoz tartozó tanúsítvány esetén a regisztráció és ennek keretében a személyazonosság megállapítása - a vonatkozó jogszabály (78/2010. Kormányrendelet 12§ 2). bekezdés) alapján, a Szolgáltató és az illetékes hatóság erre vonatkozó előzetes megállapodását követően – az illetékes hatóság humánpolitikai szervezete által is elvégezhető, a saját személyzeti nyilvántartására alapozva.

Ez esetben nem szükséges az Eat. 12. § szerinti – 3.2.9 pontban részletezett - ellenőrzés elvégzése, és Szolgáltató elfogadja az így elvégzett regisztrációt.

A regisztrációs folyamat lépései – részben - megegyeznek a 3.2 pontban leírtakkal, a következő értelemszerű különbségekkel:

- Szolgáltató előzetes megállapodást köt az illetékes hatósággal, melyben többek között rögzíti a hatóság kijelölt kapcsolattartójának nevét és személyes adatait, valamint a felek jogait és kötelességeit, különös tekintettel a regisztrációval és az aláírás létrehozó adatok illetve aláírás-létrehozó eszközök és aktivizáló adatok szétosztásával kapcsolatos tevékenység- és felelősség megosztásra
- Szolgáltató egyedi regisztrációs űrlapot készít a regisztrációhoz és oktatásban részesíti az illetékes hatóság humánpolitikai szervezete részéről kijelölt kapcsolattartót a kitöltéssel és adatellenőrzéssel kapcsolatos tudnivalókról

- Szolgáltató a hatóság kijelölt kapcsolattartójától átvett és hitelesített űrlapok alapján végzi el a tanúsítványok előállítását, de adategyeztetést nem végez
- Szolgáltató a tanúsítványokat illetve a kapcsolódó előfizetői kulcspárt és PIN-kódot (valamint [MTT+BALE] tanúsítvány esetén a megszemélyesített biztonságos aláírás létrehozó eszközt) a hatóság kijelölt kapcsolattartójának adja át személyesen
- a hatóság kijelölt kapcsolattartójának azonosítása során a 3.2.5 pontban leírtakat alkalmazza (kivéve a d) pont szerinti adategyeztetést)
- Szolgáltató feltételeinek elfogadását a Szolgáltatásokra vonatkozóan az illetékes hatóság humánpolitikai szervezete fogadtatja el az Aláírókkal, erre rendszeresített nyilatkozat (pl. Tanúsítvány átvételi elismervény) aláírásával, melyeket Szolgáltató ellenőrizhet és bekérhet az illetékes hatóság humánpolitikai szervezetétől

3.2.9. Hatósági adategyeztetés

A Szolgáltató jogosult megállapítani az igénylések során eljáró természetes személyek személyazonosságát a személyazonosításra alkalmas okmányaik alapján. A Szolgáltató a regisztráció során a személyazonosság 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.
Nem magyar állampolgár adatait útlevele vagy más, jogszabály által a személyének azonosítására alkalmasnak minősített okmány alapján ellenőrzi a Szolgáltató. Ha a természetes személy az idegenrendészeti nyilvántartásban szerepel, akkor az adatait Szolgáltató a központi idegenrendészeti nyilvántartásban is ellenőrizheti,

3.2.10. Együttműködési képességek

A Szolgáltató eleget tesz a {J10} hitelesítési rend 3.2.6. a) pontjában rögzített együttműködési képességre vonatkozó követelménynek.
A Szolgáltató az együttműködő partnerek részére teszt célokat szolgáló tanúsítványokat és nyilvános körben hozzáférhető szolgáltatásaihoz teszt célú hozzáférést is biztosíthat. A tesztek során felmerülő kérdések tisztázására a Szolgáltató partnereivel együttműködik.
Az együttműködés eredményéről a Szolgáltató a szolgáltatások internetes honlapján esetenként tájékoztatást tehet közzé.

3.2.11. Viszontazonosítás. Hatóság kérésére történő adategyeztetés

Szolgáltató nem végez viszontazonosítást.

A Szolgáltató az elektronikus aláírás alkalmazásával elektronikus ügyintézést végző közigazgatási szerv megkeresésére - az aláírást alkalmazó személy (Aláíró) azonosító adatainak ellenőrzése céljából - adategyeztetést végez és az adatok egyezéséről, vagy az eltérés tényéről a megkereső hatóságot tájékoztatja. A közigazgatási szerv a megkeresést a Szolgáltató Ügyfélkapcsolati Irodájának kell beküldje írásban, megadva az Aláíró tanúsítványának azonosítóját (sorozatszámát) valamint Aláíró természetes azonosító adatait.

Az Ügyfélkapcsolati Iroda ellenőrzi az Aláíróról a saját nyilvántartásában szereplő azonosító adatokat, és ezt követően elektronikusan aláírt emailben értesíti a megkereső hatóságot az egyezőség vagy az eltérés tényéről.

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 egy, az adott szervezet képviselő személy lehet, aki személyazonosságát a regisztráció során hitelt érdemlően igazolta (lásd: 3.2. pont)

A Szolgáltató azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatja az Előfizetőt illetve az Aláírót a tanúsítvány és/vagy az időbélyeg szolgáltatás 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 bocsájtott regisztrációs űrlapot és le kell folytatni a 3.2 pontban meghatározott regisztrációs eljárást. Az űrlap nyomtatott vagy elektronikus formában igényelhető az Ügyfélkapcsolati Irodánál, vagy elektronikus formában letölthető a Szolgáltató internetes honlapjáról.

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

Az 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 és hitelesítési 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 Aláíró vagy meghatalmazottja - illetve ha Aláíró nem természetes személy, az Előfizető kapcsolattartója - személyesen átveszi az Ügyfélkapcsolati Irodán. Meghatalmazott részére történő átadás csak akkor megengedett, ha előzőleg - a regisztráció során - az Aláíró személyes ellenőrzése megtörtént a regisztrációs szervezet által.

b. [KET] közigazgatásban alkalmazható, hatóságok által használt aláíráshoz tartozó tanúsítvány esetén Szolgáltató az aláírás létrehozó adatot illetve aláírás létrehozó eszközt - a vonatkozó jogszabály ({J4} 78/2010. Kormányrendelet 12§ 2). bekezdés) alapján, erre vonatkozó előzetes megállapodást követően - a hatóság humánpolitikai szervezete kijelölt munkatársának (Előfizető által kijelölt kapcsolattartónak) is átadhatja, aki gondoskodik a továbbiakban az Aláíróknak történő személyes átadásról

c. 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 pontnak 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 egyen egyben a {Sz13} hitelesítési rend, a jelen szolgáltatási szabályzat és {Sz14} az általános szerződési feltételek elfogadását is jelenti.

4.4.1. Tanúsítvány közzététele a Szolgáltató által

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

4.4.2. A további szereplők értesítése a tanúsítvány kibocsátásáról

A közigazgatásban alkalmazható tanúsítványok ([KET]) esetében, ha a hivatali aláíráshoz tartozó tanúsítvány kibocsátását megelőző regisztrációt a hatóságot képviselő természetes személy kezdeményezte, továbbá a hatóság számítógépes rendszere számára kibocsátott gépi tanúsítvány esetén a Szolgáltató köteles az érintett hatóságot a tanúsítvány kibocsátásának, és az aláírás-létrehozó adat előállításának tényéről írásban értesíteni. Az aláírás-létrehozó adat és a tanúsítvány átvételét a hatóságnak ugyancsak írásban kell igazolnia. Az átvétel vagy a visszaigazolás elmaradása esetén a hatóságot az átvételre, illetve annak igazolására ismételten fel kell hívni.

További szereplőket a Szolgáltató a kibocsátott tanúsítványokról nem értesít. Időbélyeg kiadásáról Szolgáltató nem küld külön értesítést.

4.5. Kulcspár és tanúsítvány illetve időbélyeg használat

4.5.1. Az alany magánkulcs- és tanúsítvány használata

Az Aláíró (alany) 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 7.1.2 pont).
f. Időbélyeget Előfizető az 1.4.3 pontban megadott célokra használhat fel.

4.5.2. Az Érintett felek nyilvános kulcs- és tanúsítvány használata

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

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 ellenőrizni 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.

d. Amennyiben az Érintett fél ésszerű módon egy időbélyegre kíván hagyatkozni, ajánlott azt ellenőriznie, a 2.1.3 pont szerint.

4.6. Tanúsítványok érvényessége, megújítása

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 lejárata 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 lejárat előtt 30 nappal értesítést küld az Aláírónak arra az email címére, amelyet a regisztrációs űrlapon megadott.

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

Biztonságos aláírás-létrehozó eszközhöz kapcsolódó tanúsítvány ([MTT+BALE]) esetén 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 minősített archiválási szolgáltató igénybevételével is eleget tehet.

4.7. Kulcscsere

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

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

a. a tanúsítvány valamilyen okból visszavonásra került,
b. a tanúsítvány lejárt, vagy lejárathoz közeledik (legfeljebb 30 napig érvényes) és nem megújítható
c. a magánkulcsot tartalmazó biztonságos aláírás-létrehozó eszköz megsérült és nem használható ([MTT+BALE] tanúsítványok esetén)

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. Tanúsítványok visszavonása és felfüggesztése

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 (lásd 4.9.7.1 pont) után 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 vagy 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 (Nemzeti Média- és Hírközlési Hatóság) 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 adatot illetve az aláírás létrehozó eszközt védő aktivizáló adat (PIN-kód) kompromittálódása, vagy annak gyanúja
d. a tanúsítványban feltűntetett hibás adatok
e. az Előfizető tanúsítványban feltűntetett adatainak megváltozása
f. az Aláíró tanúsítványban feltűntetett adatainak megváltozása
g. a tanúsítványban feltűntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszűnése[2].

A Szolgáltató a következő esetekben kezdeményezheti a felfüggesztést vagy visszavonást:

a. a tanúsítvány felfüggesztési ideje lejárt
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 valótlanságáról

[2] {J1} Eat. 10. § (3)

f.

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

4.9.2. Visszavonás kérelmezése

Tanúsítvány visszavonását az előző pontban feltüntetett körülmények alapján 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 feltűntetett esetekben a visszavonás azonnali kezdeményezése.

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

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

Ha a bejelentő a visszavonási igényét akadályoztatása miatt személyesen nem tudja bejelenteni vagy azonnali intézkedés szükséges, akkor a tanúsítvány felfüggesztése telefonon is kérhető az Ügyfélszolgálaton (a Szolgáltató Ügyfélszolgálata a nap 24 órájában, folyamatosan rendelkezésre áll), a felfüggesztési jelszó ismeretében. A felfüggesztési jelszó a tanúsítvány kibocsájtásakor 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 visszavonatására, akkor a Szolgáltató a visszavonási kérelmet visszautasítja.

e. Szolgáltató a visszavonás megtörténtéről vagy annak visszautasításáról értesíti az Aláírót, 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 azonosítás 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 Aláírót 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 valótlanságáról,

b. az Előfizető vagy az Aláíró visszavonási kérelme kiegészítésre szorul.

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

4.9.5. Kivárási idő visszavonási/felfüggesztési kérelem esetén

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

4.9.5.1. Kivárási idő felfüggesztési kérelem esetén

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

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

4.9.5.2. Kivárási idő visszavonási kérelem esetén

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

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

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

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

4.9.6. A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok

A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig és elfogadásáig az {Sz14} 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.

4.9.7. Felfüggesztett állapotra vonatkozó korlátozások, újraérvényesítés

4.9.7.1. 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 estén részére térítésmentesen új tanúsítványt bocsát ki.

4.9.7.2. A felfüggesztés megszüntetése

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

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

Az újraérvényesítés kéréséhez a következő adatokat kell megadni:

d. a felfüggesztett tanúsítvány sorszáma,
e. a felfüggesztés megszüntetését kérő személy azonosító adatai,
f. 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 megszűntetésének eredménye a tanúsítvány újraérvényesítése vagy visszavonása.

4.9.8. A visszavonási információ ellenőrzése az Érintett felek részéről

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

Időbélyeg esetén értelemszerűen az időbélyeget aláíró szolgáltatói tanúsítványra vonatkozó visszavonási listát ajánlott ellenőrizni.

4.9.9. Visszavonási lista (CRL) és kibocsátásának gyakorisága

A visszavonási listában 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, előfizetői tanúsítványokra vonatkozó 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 haladéktalanul új visszavonási listát tesz közzé.

4.9.10. A visszavonási lista előállítása és közzététele közötti leghosszabb idő

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

4.9.11. A visszavonási listák ellenőrzése

A visszavonási listákat az Érintett feleknek ajánlott ellenőrizni - saját felelősségükre - a tanúsítványok elfogadását megelőzően. A tanúsítványhoz tartozó visszavonási lista elérhetőségét a tanúsítvány tartalmazza. A lista ellenőrzése abból áll, hogy a kérdéses tanúsítványt a lista tartalmazza-e (és ha igen, milyen időponttól), a lista hiteles és sértetlen-e, s a kérdéses tranzakció szempontjából időben releváns-e.

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

4.9.12. Visszavonási állapot közlés más formái

A Szolgáltató a visszavonási listák közzététele mellett online tanúsítvány-állapot szolgáltatást (OCSP) is nyújt (ld. 4.11 pont).

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.

4.11. Valósidejű tanúsítványállapot-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 {Sz8} 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 referenciaadatoz képest (UTC). Az OCSP válaszadó egység órájának pontosságát Szolgáltató folyamatosan ellenőrzi.

4.12. Időbélyegzés

4.12.1. Az időbélyegzés szolgáltatás igénylése

Időbélyegzés szolgáltatás igénylése esetén az Szolgáltató Ügyfélkapcsolati Irodája tájékoztatja az Igénylőt az időbélyeg használat módjáról, az azzal járó kötelezettségekről és felelősségről.

Az Igénylő azonosítását a 3.2.6 pontban leírt egyszerűsített eljárással kell elvégezni.

Az időbélyegzés szolgáltatást az Előfizető részére a szerződéskötést követő 30 napon belül biztosítja a Szolgáltató.

4.12.2. Az időbélyegzés szolgáltatás szintje

Az időbélyegzés szolgáltatás elérhetőségét a Szolgáltató 99,9%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 3 órás időtartamot.

Az időbélyegben megadott idő 1 másodpercen belüli pontosságot biztosít az UTC[3] időalaphoz viszonyítva. Az időbélyegző egység órájának pontossága folyamatos ellenőrzés alatt áll. Ha ez túllépné a pontossági határt, akkor az ellenőrző program leállítja az időbélyegzés szolgáltatást, és minden további kérésre a hiba kijavításáig hibaüzenetet küld a felhasználók felé. A szolgáltatás akkor indul újra, ha az időszinkron helyreállt és az egy másodperces pontossági határ teljesül. Az időszinkron helyreállítását a Szolgáltató húsz percen belül biztosítja.

4.12.3. Az időbélyegzés kérelmek teljesítése

Időbélyegzés iránti kérelmet (időbélyeg kérést) Előfizető erre feljogosított[4] felhasználói nyújthatnak be, amennyiben Előfizető a Szolgáltatóval előzetesen szerződéses kapcsolatot létesített.

Az időbélyeg kérést az Előfizető erre feljogosított felhasználója az RFC 3161 {Sz6}szerinti szabványos formában kell elküldjön Szolgáltató időbélyegző egységének elektronikus úton, a Szolgáltató által megadott URL címre. Ehhez Előfizetőnek rendelkeznie kell megfelelő (az RFC 3161 {Sz6} szerinti kérés összeállítására alkalmas) számítógépes alkalmazással, mely kezeli a tanúsítvány alapú authentikációt.

Időbélyeg kérés esetén a kérelem jóváhagyása vagy visszautasítása az ellenőrzést követően automatikusan történik.

Az időbélyegzés kérelmek teljesítését (az időbélyeg válasz összeállítását) a Szolgáltató időbélyegző egysége automatikusan és haladéktalanul végzi:

a. a kérelmet egy olyan, a szolgáltatás igénybe vétele céljából megkötött szerződésben definiált kommunikációs csatornán keresztül fogadja, amelyen keresztül az időbélyeg kérőt a Szolgáltató rendszere azonosítani tudja,

---

[3] **UTC:** Coordinated Universal Time, az ITU-R TF.460-5 ajánlás szerint definiált, másodperc felbontású időalap

[4] Feljogosítás általában a felhasználók gépére telepített authentikációs tanúsítványt jelent, melyet Szolgáltató biztosít Előfizető részére

b. Időbélyeg kiadása az időbélyegző egység által az RFC 3161 {Sz6} szerinti időbélyeg válasz elküldésével valósul meg

Időbélyeg fogadásához Előfizetőnek (illetve felhasználóinak) olyan alkalmazással kell rendelkezniük, mely az RFC 3161 {Sz6} szerinti időbélyeg választ fogadni és értelmezni képes.

4.12.4. Az időbélyeg érvényességének ellenőrzése

Az időbélyeg érvényességének ellenőrzése az időbélyeget aláíró szolgáltatói tanúsítvány érvényességének ellenőrzését, illetve az időbélyeget aláíró szolgáltatói tanúsítványra vonatkozó visszavonási lista ellenőrzését jelenti, a jelen szabályzat 2.1.3.2 pontja szerint.

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

A biztonságkezelési szabályokat a Szolgáltató PKI szintű biztonságpolitikája {Sz16} tartalmazza. Ez a szabályzat biztonsági okokból nem nyilvános. A Szolgáltató informatikai rendszere vonatkozásában a PKI szolgáltatások biztonsági szabályzata {Sz17} érvényesül. Ez a szabályzat szervezeti egység szinten és munkakörökre lebontva rögzíti a biztonságkezeléssel összefüggő feladatokat, felelősségeket és szabályokat, így többek között a bizalmi munkakörök felsorolását, a kinevezési feltételeket és az összeférhetetlenségi kritériumokat.

A Szolgáltató megvalósította és folyamatosan fenntartja a Szolgáltatásokat nyújtó eszközök, rendszerek biztonsági ellenőrzéseit és üzemeltetési eljárásait.
A Szolgáltató rendszeres belső ellenőrzései és külső auditjai ezen eljárásokat, a vonatkozó dokumentumokat és a dokumentumokban a Szolgáltatásokra vonatkozó előírások teljesülését a szolgáltatás évente esedékes ellenőrzései során vizsgálja.

Fenti eljárásokat Szolgáltató a {J3} 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 {J11} 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.

A Szolgáltató gondoskodik az informatikai biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással, időbélyegzéssel szolgáltatással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősségek más szervezethez kerülnek kiadásra.

5.1. Fizikai biztonsági szabályozások

5.1.1. Hitelesítő Központok

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

5.1.2. Regisztrációs Iroda

Szintén kiemelt védelmi szintet képező objektumban került kialakításra a Szolgáltató regisztrációs irodája, ahol a regisztrációs munkahelyek és munkaállomások kapnak helyet, és ahol a tanúsítvány kiállítási (visszavonási stb.). kérelmek előállítása, az aktivizáló adatok kezelése, valamint – [MTT+BALE] tanúsítvány esetén - a kulcspároknak a biztonságos aláírás-létrehozó eszközön való generálása és az eszköz megszemélyesítése is történik.

5.1.3. Egyéb körletek

Hasonlóan kiemelt védelmi szintet képező objektumban kap helyet a napi üzemeltetési feladatok ellátása is, csakúgy, mint a rendkívüli üzemeltetési helyzet esetére biztosított másodlagos szolgáltatói rendszer üzemeltetése.

A Szolgáltató ezen fizikai biztonsági körletek kapcsán olyan óvintézkedéseket valósít meg, amelyekkel megakadályozza, hogy a minősített Szolgáltatásaihoz szükséges berendezéseket, információkat, adathordozókat vagy szoftvereket jogosulatlanul elvigyék, megrongálják, vagy azokhoz jogosulatlanul hozzáférjenek.

5.2. Eljárásrendi szabályozások

A Szolgáltató fizikai, eljárásrendi és humán biztonsági szabályait a következő szabályzatok tartalmazzák:

a. a Szolgáltató Szervezeti és Működési Szabályzata {Sz11}, amely meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes szervezetekhez kapcsolt feladat-, felelősség és hatásköröket,

b. a jelen szolgáltatási szabályzat, mely a Szolgáltató és a felhasználói közösség (előfizetők, aláírók, érintett felek stb.) viszonyát szabályozza,

c. a PKI szolgáltatások biztonsági szabályzata {Sz17}, amely részletesen szabályozza az adatokhoz és az informatikai rendszerekhez, valamint a személyi és a fizikai környezethez kapcsolódó biztonsági szabályokat.

5.3. Humán szabályozások

5.3.1. Bizalmi munkakörök

A Szolgáltató biztosítja a Szolgáltatásokhoz a vonatkozó jogszabályban ({J3} 3/2005. (III. 18.) IHM rendelet) és a hitelesítési rendjében {Sz13} 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.

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.

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

PKI biztonsági tisztviselő II.	A PKI géptermek és helyiségek biztonságtechnikai rendszereinek felügyelete, a beléptetési jogosultságok kezelése, a bizalmi munkakörökbe belépő munkatársak ellenőrzése, kilépők jogosultságának megvonása	A PKI szolgáltatások fizikai környzetére és személyzeti biztonságra vonatkozó előírások megfelelőségének biztosítása	A PKI szolgáltatások fizikai környzetére és személyzeti biztonságra vonatkozó hatáskör társaságon belül
PKI Rendszervizsgáló I. PKI Rendszer-vizsgáló II.	PKI naplófájlok elemzése és ellenőrzése. Biztonsági hiányosságok, visszaélések felfedése, jelentése. PKI naplófájlok elemzése és ellenőrzése. Archivált adatállomány, mentések ellenőrzése. Funkcionális és biztonsági hiányosságok, visszaélések felfedése, jelentése	A PKI rendszer naplózási követelményei megfelelőségének biztosítása. A fentiek mellett a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzése, a meglévő eljárások vizsgálata és felügyelete.	A PKI szolgáltatások teljes informatikai eszközparkja és infrastruktúrája, a keletkezett biztonsági és audit naplók. A PKI szolgáltatások teljes informatikai eszközparkja és infrastruktúrája, a keletkezett biztonsági és audit naplók. A PKI szolgáltatások belső eljárásai és folyamatai.
Regisztrációs felelős (Registration Officer /RO/)	Tanúsítvány elállítás és státuszváltoztatás. Aláírás létrehozó eszköz megszemélyesítés, aktiváló adatok és ügyféladatok szabályszerű kezelése. Adminisztráció.	A PKI szolgáltatások keretében az előfizetői tanúsítványok előállításának és státusz-változásainak végrehajtása, jóváhagyása	A PKI szolgátlatások keretében megrendelt tanúsítványok kezelésével, a kapcsolódó eszközök megszemélyesítésével kapcsolatos tevékenység
PKI Rendszerüzemeltető I. PKI Rendszerüzemeltető II.	A PKI rendszerben levő tűzfalak, hálózati határvédelmi eszközök üzemeltetése, napi karbantartása, hibaelhárítása A PKI rendszerben levő szerverek, adatbázis gépek, üzemeltetése, napi karbantartása, hibaelhárítása	A PKI rendszerben levő kiszolgáló gépek, adatbázis gépek, tűzfalak és hálózati illetve határvédelmi eszközök üzemeltetése a vonatkozó előírásoknak megfelelően	A PKI rendszerben levő kiszolgálók, adatbázis gépek, tűzfalak és hálózati illetve határvédelmi eszközök üzemeltetése, operatív intézkedések ezen eszközökre vonatkozóan
PKI Rendszerüzemeltető III.	A PKI rendszerben levő MS Windows alapú gépek üzemeltetése, mentése, napi karbantartása, hibaelhárítása illetve helyreállítása	A PKI rendszerben levő MS Windows alapú gépek folyamatos üzemeltetése a vonatkozó előírásoknak megfelelően	A PKI rendszerben levő MS Windows alapú gépek üzemeltetési tevékenysége
PKI rendszeradminisztrátor	PKI rendszer alkalmazói szoftvereinek telepítése, konfiguráció, karbantartás. HSM modulok telepítése, biztonsági beállítások és környezet létrehozása.	A PKI rendszert alkotó gépek telepítésének, konfigurálásának, karbantartásának elvégzése során a jogszabályok és szakmai előírásoknak való	A teljes PKI rendszer alkalmazás szinten, beleértve az ügyfélkapcsolati irodai (ÜKI) alkalmazást is

	Rendeltetésszerű működés biztosítása.	megfelelőség biztosítása	

5.3.2. Az egyes feladatokhoz szükséges személyzeti létszámok

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

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

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

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.

5.3.3. 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.

5.3.4. 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.

5.3.5. 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 hitelesítés-szolgáltató tevékenységeinek semlegességét.

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

5.3.6. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

A Szolgáltató informatikai rendszeréért általánosan felelős vezető kinevezéséhez szakirányú felsőfokú végzettség és három 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 felelős 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 szolgáltatásokhoz kapcsolódó technológia terén, ismeri a biztonsági felelősséggel tartozó munkatársakra vonatkozó biztonsági eljárásokat, valamint gyakorlattal rendelkezik az informatika biztonság és a kockázat elemzés területein.

5.3.7. Biztonsági háttér ellenőrzésekre vonatkozó eljárások

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

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

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

A bizalmi munkakörhöz történő hozzárendeléskor:

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

Kilépéskor:

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

5.3.8. 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 munkakörének illetve szerepkörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt.

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

Abban az esetben, amikor a szolgáltatásokban jelentős változás[5] következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.[6]

---

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

[6] 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.

Kisebb változások[7] bekövetkezése előtt a munkatársak írásos tájékoztatást kapnak a változásokról.

5.3.9. A felhatalmazás nélküli tevékenységek büntető következményei

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

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

5.3.10. A szerződéses alkalmazottakra vonatkozó követelmények

Az egyéb feladatok ellátására, vállalkozási vagy megbízásos szerződésben foglalkoztatott személyeket a Szolgáltató csak az „ellenőrzött beszállítók" listájáról választ. Az ellenőrzött beszállítókkal a Szolgáltató írásos megállapodást köt, amelyben rögzíti a biztonsági szabályokat.

Valamennyi szerződő fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során birtokába kerülő üzleti titkokat és bizalmas információkat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is.

5.4. Naplózási eljárások

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványokra valamint a kiadott időbélyegekre 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. A pontos időt a Szolgáltató időbélyegző egysége biztosítja.

5.4.1. Naplózott esemény típusok

A hitelesítés szolgáltatással kapcsolatosan a Szolgáltató naplóz minden a rendszerrel és a szolgáltatás nyújtásával kapcsolatos eseményt, különösen:

a. a szolgáltatói tanúsítványok életciklusával kapcsolatos összes eseményt
b. az előfizetői tanúsítványokat aláíró infrastruktúrális és ellenőrző kulcsok tanúsítványainak életciklusával kapcsolatos összes eseményt, ezen belül különösen

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

az előfizetői tanúsítványok előállítási és megújítási igény-benyújtási időpontját, valamint az igények teljesítésének időpontját

Az Előfizetők biztonságos aláírás-létrehozó eszközzel való ellátásával kapcsolatosan a Szolgáltató naplóz minden általa gondozott kulcs életciklusával kapcsolatos eseményt és a biztonságos aláírás-létrehozó eszközök megszemélyesítésével kapcsolatos valamennyi eseményt.

A visszavonás kezeléssel kapcsolatosan a Szolgáltató gondoskodik a kérések, valamint az ezek következtében előállt tevékenységek naplózásáról.

Az időbélyegzéssel kapcsolatosan naplóz minden a rendszerrel és a szolgáltatás nyújtásával kapcsolatos eseményt, különösen:

a. az időbélyegzés szolgáltatás fő lépései, a kérelemtől az időbélyeg válasz elküldésig
b. az időbélyeget aláíró kulcsok életciklusában bekövetkező eseményeket (generálás, használat, visszavonás, megsemmisítés)
c. az időbélyeget aláíró kulcsok tanúsítványa életciklusában bekövetkező eseményeket (kiadás, használat, visszavonás)

A hitelesítés-szolgáltatást támogató informatikai rendszer biztonságával kapcsolatosan naplózza:

a. a naplózási funkció elindításával és leállításával
b. a naplózási paraméterek megváltoztatásával
c. a naplózás tárolásával kapcsolatos hibákkal
d. a napló adatok integritásának megsértésével
e. a hitelesítés-szolgáltatást támogató informatikai rendszerhez történő bármely hozzáférési kísérlettel kapcsolatos eseményeket

A hitelesítés szolgáltatást támogató informatikai rendszer operációs rendszerére, illetve a rendszer többi elemére vonatkozóan a biztonsági szabályzatban meghatározott események kerülnek naplózásra.

5.4.2. Naplóadatok védelme

A Szolgáltató a naplóadatokat 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.

5.4.3. Naplók feldolgozásának gyakorisága

A Szolgáltató a hitelesítő központok (CA-k) naplóit naponta, az egyéb napló fájlokat a {Sz17} biztonsági szabályzatában rögzített gyakorisággal dolgozza fel.

A PKI alkalmazás, az időbélyegzés 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.

5.4.4. Napló adatok tárolása

A napló adatok rendszeresen archiválásra kerülnek ellenőrzés, szükségessé váló visszakeresés és esetleges újbóli használat céljából (lásd: 5.5 pont).

5.4.5. A napló fájlok megőrzési időtartama

Lásd: 5.5 Adatok archiválása c. fejezetet.

5.5. Adatok archiválása

A Szolgáltató gondoskodik arról, hogy az általa kibocsájtott tanúsítványokra és az időbélyegzésre 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.

5.5.1. 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 dokumentum(ok) 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 a biztonságos aláírás-létrehozó eszköz átadás-átvételére vonatkozó feljegyzés
f. az Előfizetővel kötött megállapodás esetleges egyedi választásai
g. Az 5.4.1 pontban felsorolt összes esemény, illetve napló típus.

5.5.2. Az archívum megőrzési időtartama

A Szolgáltató az 5.4.1 pontban megnevezett naplókat az {J1} Eat. 9. § (7) bekezdése alapján és a {J3} 3/2005. (III. 18) IHM rendelettel összhangban a keletkezésüktől számított 10 évig, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig megőrzi.

5.5.3. Az archívum védelme

A Szolgáltató az archívumában és a PKI Dokumentumtárban olyan fizikai védelmet biztosít, amely fenntartja a tanúsítványokra és az időbélyegzésre vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét. A Szolgáltató az archivált adatokat legalább fokozott biztonságú elektronikus aláírással és időbélyegzővel látja el.

5.5.4. 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.

5.6. Felülhitelesítés

A Szolgáltató közigazgatásban alkalmazható tanúsítványok ([KET]) esetében a kibocsátó produktív hitelesítő központját (CA-t) a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) felülhitelesíti.

A KGyHSz tanúsítvány kiadásával igazolja a Szolgáltató és a szolgáltatói nyilvános kulcsok összetartozását, illetve a Szolgáltató a felültanúsított szolgáltatói tanúsítvány elfogadásával magára nézve kötelezőnek ismeri el a KGyHSz által kiadott szabályzatokat és a KGyHSz felügyeleti, ellenőrzési jogát.

A Nemzeti Média- és Hírközlési Hatóság a nyilvántartásba vételi eljárás keretében és azt követően – a jogszabályban előírt hatáskörrel – felügyeli többek között a jelen szolgáltatási szabályzat előírásainak a {J10} hitelesítési rendnek való megfelelőségét.

5.7. 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.

A Szolgáltató a közigazgatásban alkalmazható tanúsítványokat aláíró szolgáltatói kulcsának tervezett cseréje előtt fél évvel köteles tájékoztatni a Közigazgatási Gyökér Hitelesítés-szolgáltatót és vele egyeztetni a szükséges feladatokról.

A szolgáltatói kulcs kompromittálódása esetén az 5.8 pontban előírtak szerint kell eljárni.

5.8. A folyamatos üzemmenet biztosítása

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 kezelésről és a tanúsítvány visszavonási listák közzétételéről, valamint az időbélyegzés szolgáltatás fenntartásáról.

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 {Sz18} üzletmenet-folytonossági terve tartalmazza.

A rendkívüli üzemeltetési helyzetekben a Szolgáltató eseménynaplót vezet.

5.8.1. 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.

5.8.2. Biztonsági képesség rendkívüli üzemeltetési helyzetben

Rendkívüli üzemeltetési helyzetben a Szolgáltató életbe lépteti {Sz18} üzletmenet-folytonossági tervében megtervezett eljárásait annak érdekében, hogy az üzemeltetés helyreálljon az üzletmenet-folytonossági tervben megjelölt időn belül.

A visszaállítási időt alapvetően az esemény súlyossága, azaz az {Sz18} üzletmenet-folytonossági terv szerint értelmezett osztályba sorolása határozza meg. A súlyos üzemzavari és a katasztrófa esetet – többek között – az különbözteti meg egymástól, hogy katasztrófa esetén nagy valószínűséggel nem csak az informatikai rendszer, hanem annak fizikai környezete is megsemmisül részben vagy egészben. Ez utóbbi esetben az üzletmenet-folytonossági tervben meghatározott módon egy válságstáb intézkedik a tartalék helyszínre történő áttelepülésről és az informatikai rendszer szükséges mértékű visszaállításáról a tartalék helyszínen korábban elhelyezett mentések segítségével.

5.8.3. 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 {Sz18} Szolgáltató üzletmenet-folytonossági terve intézkedik. Az üzletmenet-folytonossági tervben az üzletmenetet veszélyeztető, sértő, illetve azt leállító események súlyossági osztályokba vannak sorolva. A terv részletesen szabályozza a hitelesítő központok saját aláírás-létrehozó adatainak, aktiváló adatainak és az időbélyegek aláíró kulcsának kompromittálódása esetén elvégzendő teendőket.

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

5.8.4. Minimális szolgáltatás rendkívüli üzemeltetési helyzetben

A Szolgáltató rendkívüli üzemeltetési helyzetben is biztosítja az időbélyegzés szolgáltatást, 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.

5.8.5. Üzletmenet-folytonossági terv

A Szolgáltató rendelkezik üzletmenet-folytonossági tervvel {Sz18}), amely részletes intézkedési forgatókönyveket tartalmaz a súlyos üzemzavarok vagy katasztrófa események kezelésére. Ez a dokumentum biztonsági okokból nem nyilvános.

5.9. A szolgáltatási tevékenység megszüntetése

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más szolgáltatókkal a szolgáltatások átvételéről. A tárgyalások eredményéről tájékoztatja a felhasználói közösséget.

A Szolgáltató gondoskodik a szolgáltatásainak megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról. Különösképpen gondoskodik az időbélyegzés, a tanúsítvány visszavonás kezelés és közzététel szolgáltatások folyamatos fenntartásáról.

Ennek érdekében a Szolgáltató mielőtt szolgáltatási tevékenységét leállítja:

a. legalább 60 nappal korábban értesíti a Nemzeti Média- és Hírközlési Hatóságot és a Szolgáltatások internetes honlapján tájékoztatja a felhasználói közösség tagjait

b. megszűnteti a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások összes felhatalmazását

c. megteszi a szükséges lépéseket, hogy a regisztrációs adatok és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket átruházza

A bejelentéssel egyidejűleg a Szolgáltató leállítja:

a. a tanúsítvány előállítás és kibocsátás szolgáltatást (nem ad ki sem új, sem megújított tanúsítványokat)

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

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

6. Műszaki biztonsági óvintézkedések

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

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. Kriptográfiai kulcspár előállítás és aláírás-létrehozó eszköz megszemélyesítés

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 végzi, amely szerepel a Nemzeti Média- és Hírközlési Hatóság 2011. szeptemberében kiadott, algoritmusokra vonatkozó. határozatának 1. sz. mellékletében.

Az időbélyeget aláíró szolgáltatói kulcsot az időbélyegző egység szerves részét képező, tanúsított kriptográfiai modul (HSM) generálja és tárolja. Az aláíró kulcs teljes életciklusa alatt ezen eszközben marad.

[MTT] tanúsítványok esetén – ezzel ellentétes megegyezés hiányában a Szolgáltató maga generálja az előfizetői kriptográfiai kulcspárokat tanúsított kriptográfiai modulban. Bizonyos esetekben – erre vonatkozó megegyezés alapján - Szolgáltató elfogadhat Előfizető által generált kulcspárt is, de ez esetben Előfizetőnek nyilatkoznia kell, hogy ezt fizikailag védett környezetben, kriptográfiai modulban (HSM) hajtotta végre.

MTT+BALE] tanúsítványok esetén az előfizetői kulcspárokhoz a Szolgáltató kizárólag biztonságos aláírás-létrehozó eszközt (BALE) alkalmaz, a kriptográfiai kulcspárt a Szolgáltató PKI alkalmazása magán a biztonságos aláírás-létrehozó eszközön generálja. Az aláíró kulcs teljes életciklusa alatt ezen eszközben marad. A biztonságos aláírás létrehozó eszköz megfelel az {J1} Eat. 1. sz. mellékletében foglalt követelményeknek, azaz rendelkezik a 9/2005. (VII. 21.) IHM rendelet {J5} szerint kijelölt szervezet vagy ezzel egyenértékű

Európai Uniós szervezet által kiadott tanúsítással, illetve szerepel a Nemzeti Média- és Hírközlési Hatóság által nyilvántartott minősített elektronikus aláírási termékek listájában.

6.1.2. Az aláírás-létrehozó eszköz megszemélyesítése

[MTT+BALE] tanúsítványok esetén a biztonságos aláírás-létrehozó eszköz (chipkártya 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).

[MTT+BALE] tanúsítványok esetén a Szolgáltató az aláírás-létrehozó adat aktivizálásához PIN-kódot (valamint a blokkolt kártyák feloldásához PUK-kódot) biztosít. A PIN és PUK-kódot fizikailag védett környezetben állítja elő és a kódokat tartalmazó borítékot a biztonságos aláírás-létrehozó eszköztől elkülönítve tárolja.

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

A Szolgáltató az aláírás-létrehozó adatot, illetve - [MTT+BALE] tanúsítványok esetén a megszemélyesített biztonságos 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 ([MTT] tanúsítvány esetén) illetve a biztonságos aláírás-létrehozó eszközt ([MTT+BALE] tanúsítvány esetén) és a kapcsolódó PIN-kódot tartalmazó borítékot személyesen adja át az Aláírónak, Előfizetőnek, vagy az általuk feljogosított személynek.

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 a biztonságos 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 a biztonságos 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) az előfizetői tanúsítványokon keresztül 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) valamint az időbélyegző egységek 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. Kulcs méretek, algoritmusok

A Szolgáltató a Nemzeti Média- és Hírközlési Hatóság 2011. szeptemberi, algoritmusokra vonatkozó határozatának megfelelően az SHA256-with-RSA[8] 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 kulcsának mérete:	2048 bit
Az OCSP választ aláíró kulcs mérete:	2048 bit
Az időbélyegző egység aláíró kulcsának 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 a kulcshosszak növeléséről.

6.1.7. Előfizetői aláírás-ellenőrző adat előállításához használt paraméterek előállítása

Az előfizetői aláírás-ellenőrző adat előállításához a Szolgáltató által használt algoritmusokat az előző pont tartalmazza..

6.1.8. 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 és az időbélyeget aláíró kulcsok tanúsítványait a Szolgáltató 1. szintű hitelesítő központja (Root CA-ja) hitelesíti.

A közigazgatásban alkalmazható tanúsítványokat kibocsátó produktív hitelesítő központ aláíró kulcsa tanúsítványát a KGYHSZ (felül) hitelesíti.

6.1.9. Kulcs felhasználási célok

A Szolgáltató Előfizetők részére tanúsítványt (kulcspárt) kizárólag elektronikus aláírási célra bocsát ki.

---

[8] RSA Rsagen1 IETF RFC 3447 (2003) “PKCS #1: RSA Cryptography Specifications Version 2.1”

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 OSCP válaszadó tanúsítványok aláírása. Ennek megfelelően a Szolgáltató szervezeti egységei esetében a „Key Usage" mezők lehetséges (egyúttal kötelezően kitöltendő) értékeit a következő táblázat mutatja.

Kulcs megnevezése	Kulcs használati („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. 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 Szolgáltató az [MTT+BALE] tanúsítványok esetében az Előfizetők aláírás-létrehozó adatának előállítására olyan eszközt használ, amely teljesíti a CC EAL4 {Sz9} 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 megfelelőségi 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. A kriptográfiai modulra vonatkozó szabályok

A Szolgáltató saját szolgáltatói magánkulcsainak tárolására illetve használatára olyan biztonságos kriptográfiai modult (HSM) alkalmaz, amely teljesíti a vonatkozó {J1} 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 kiadott igazolással.

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

A Szolgáltatónál a hitelesítő központokban alkalmazzák az „n-ből m” ellenőrzést a Root CA kulcsgondozási funkcióinak aktivizálásánál.

6.2.4. Aláírás-létrehozó adat letét, mentés, archiválás

A Szolgáltató nem nyújt magánkulcs letétszolgáltatást. Szolgáltató az Előfizetői aláírás-létrehozó adatát, semmilyen formában nem menti vagy archiválja, annak előállítására, visszafejtésére alkalmas programot, adatot nem tárol.

A Szolgáltatónál a hitelesítő központok aláíró magánkulcsai[9] biztonsági okokból duplikálásra kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik.

6.2.5. Aláírás-létrehozó adat védelme

[MTT+BALE] tanúsítványok esetén az előfizetői kulcspárokat a Szolgáltató kizárólag a biztonságos aláírás-létrehozó eszközön generálja, így a magánkulcsok semmilyen körülmények között nem hagyják el azokat. A biztonságos aláírás-létrehozó eszközt a Szolgáltató PIN-kóddal védve adja át. [MTT] tanúsítványok esetén az előfizetői kulcspárokat a Szolgáltató tanúsított kriptográfiai modulban állítja elő, és szintén PIN-kóddal védve adja át az arra jogosult személynek.

A Szolgáltató munkatársai számára a PKI rendszeradminisztrátor a biztonsági tisztviselő és a kulcsőr jelenlétében generálja a kulcspárokat a kijelölt kulcshordozó eszközön, így a magánkulcsok semmilyen körülmények között nem hagyják el azokat. Az aláírás-létrehozó adatot illetve eszközt a Szolgáltató PIN-kóddal védve adja át munkatársainak.

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

6.2.6. Aláírás-létrehozó adat aktiválása

Az előfizetői aláírás-létrehozó adat aktiválása az Aláíró által történik a Szolgáltatótól kapott (és a későbbiekben módosított) PIN-kód megadásával.

[MTT+BALE] tanúsítványok esetén az aláírás-létrehozó adat az aktiváláskor sem hagyja el az eszközt, azt onnan leolvasni nem lehet.

6.2.7. Aláírás-létrehozó adat deaktiválása

Az előfizetői aláírás-létrehozó adatok deaktiválását az Aláíró alkalmazása végzi kijelentkezéskor vagy - [MTT+BALE] tanúsítványok esetén - amikor az Aláíró a biztonságos aláírás-létrehozó eszközt (chipkártyát) eltávolítja az olvasóból.

---

9 A kriptográfiai hardver modul (tanúsítványokat, illetve visszavonási listákat aláíró) magánkulcsai.

6.2.8. Aláírás-létrehozó adat megsemmisítése

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

A szolgáltatói aláírás-létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3. Kulcspár kezelés egyéb aspektusai

6.3.1. Aláírás-ellenőrző adat (az előfizetői tanúsítványok) megőrzése

Az aláírás-ellenőrző adatokat a tanúsítványok tartalmazzák. A Szolgáltató minden általa előállított és kibocsátott tanúsítványt megőriz az érvényesség lejártától 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 minősített archiválási szolgáltató igénybevételével is eleget tehet.

Az archiválás biztonsági okokból 2 példányban történik.

6.3.2. Aláírás-létrehozó és aláírás-ellenőrző adatok felhasználási ideje

Az aláírás-létrehozó adat (aláíró kulcs) és az aláírás-ellenőrző adat (nyilvános kulcs) érvényességi ideje megegyezik a kulcsok hitelességét igazoló tanúsítvány érvényességi idejével:

Root CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 20 év
Időbélyegző egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
Produktív CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 15 év
OCSP egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 30 nap
Előfizetői aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 2 év

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

6.4. Aktiválási adatok

6.4.1. Aktiválási adatok generálása és installációja

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

A Szolgáltató az Aláíró hozzáférési jogosultságát ellenőrző adatot (PIN-kódot) csak abból a célból rögzítheti, hogy azt az Aláíró vagy a feljogosított személy számára - másolat megőrzése nélkül - átadhassa[10].

6.4.2. Aktiválási adatok védelme

A Szolgáltató az aláírás-létrehozó adatok vagy aláírás létrehozó eszközök PIN-kódjait védi a létrehozástól kezdve az Aláírónak vagy a feljogosított személynek történő átadásig.

A PIN-kódokat Szolgáltató tanúsított kriptográfiai modulban vagy tanúsított biztonságos aláírás-létrehozó eszközön állítja elő, és erre szolgáló PIN-borítékban nyomtatja ki.

A Szolgáltató a PIN-kódot tartalmazó borítékot az aláírás-létrehozó adattól illetve a biztonságos aláírás-létrehozó eszköztől elkülönítve adja át.

Az átvételt követően Aláírónak saját felelősségi körében kell biztosítania PIN-kódja kizárólagos birtoklását.

Az Aláírónak rendelkeznie kell megfelelő PIN-kód módosító kliens alkalmazással, amelyet - [MTT+BALE] tanúsítványok esetén - a Szolgáltató biztosít számára.

A biztonságos aláírás-létrehozó eszköz első használatakor –- jellemzően az Aláíró saját munkaállomásán –- az alkalmazás kikényszeríti a PIN-kód megváltoztatását.

Az Aláíró a későbbiekben is bármikor megváltoztathatja a PIN-kódját.

Az Előfizető és Aláíró személye „munkatársi” tanúsítvány esetén jellemzően szétválik, de az aláírás-létrehozó adat felhasználása az Aláíró felelőssége. Mivel az aláírás-létrehozó adat felhasználása szempontjából a PIN-kód kritikus biztonsági elem, ezért a PIN-kódokat Szolgáltató az Aláírónak adja át. Előfizetői szempontból az aláírás-létrehozó adatnak az Aláíró által történő kizárólagos birtoklása az alapvető feltétel az elektronikusan aláírt adat, dokumentum hitelességének biztosítására. Emiatt az Előfizetőnek saját felelősségi körében kell biztosítania azt, hogy az aktivizáló adatot kizárólag az Aláíró birtokolja. Amennyiben a PIN-kód sérül vagy elveszik, illetve ennek alapos gyanúja fennáll, akkor az Aláírónak ezt haladéktalanul jelentenie kell az Ügyfélkapcsolati Irodánál, amely azonnal intézkedik a tanúsítvány felfüggesztéséről.

A PIN-kódot a Szolgáltató nem tárolja és nem állítja újra elő sem az Aláíró, 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.

6.4.3. Aktiválási adatok egyéb aspektusai

Az aláírás-létrehozó eszközök aktiválási adatait Szolgáltató nem tárolja, és nem állítja újra elő az Aláíró, Előfizető, harmadik fél, vagy hatóság kifejezett kérése esetén sem.

Az aktiváló adat elvesztése, elfelejtése vagy illetéktelen kezekbe történő jutása esetén minden esetben új kulcspárt és aktiválási adatot kell előállítani.

[10] 3/2005. (III. 18.) IHM rendelet {J3} 40. §, 4. bek. szerint.

6.5. Az időszinkronizálás megvalósítása

A Szolgáltató által adott időbélyeg felépítése megfelel az RFC 3161 {Sz6} szabványnak és a {Sz15} Szolgáltató Időbélyegzés Szolgáltatási Rendjében (ISZR) meghatározott további követelményeknek.

A Szolgáltató a Nemzeti Távközlési Gerinchálózat időforrását használja.

A Szolgáltató által alkalmazott referencia időforrások:

server ntp.gov.hu

server ntp2.gov.hu

A referencia időforrások pontossága századmásodpercen belül van.

6.6. Számítógép biztonsági szabályok

6.6.1. Számítógép biztonság technikai követelményei

A Számítógép biztonság technikai követelményeit a {J11} 2/2002 MeHVM ajánlás határozza meg.

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

a. operációs rendszer,
b. PKI alkalmazás, időbélyegzés 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).

Az időbélyegzésre szolgáltatásra vonatkozó biztonsági funkciók az alábbiak:

a. Az időbélyeget aláíró kulcsok tárolása a tanúsítással rendelkező HSM egységekben. Az időbélyegző szerverek külön biztonsági zónában történő üzemeltetése.

b. Az időbélyegző szerverek belső órájának pontossága folyamatos ellenőrzés alatt áll. A pontossági tartományból történő kilépés esetén az időbélyegző szolgáltatás leáll és a hiba kijavításáig minden további kérésre hibaüzenet kerül kiküldésre.
c. A szinkronizáló órajelek hitelességét az időbélyegző informatikai rendszer indításakor az illetékes személyek ellenőrizték.
d. biztonsági naplózás,
e. Az időbélyeget választ kibocsátó szervereket többszörös tűzfal rendszer védi a külső hálózatokról érkező fenyegetésektől.
f. Az időbélyegzés szolgáltatás rendelkezésre állási szintje 99,9%. Ez a szint többszörösen redundáns kialakítással illetve meleg tartalékolt időbélyegző szerver architektúrával, és a szervereknek a hitelesítés szolgáltató informatikai rendszer magas rendelkezésre állást felügyelő és vezérlő rendszerébe történő integrálásával biztosított

A kriptográfiai modulok (HSM) 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,
e. biztonságkezelés (a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása), több-szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése
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.

Biztonsági rezsimintézkedések által megvalósított funkcióként Szolgáltató gondoskodik arról, hogy a használatból kivonandó informatikai eszközökről minden a Szolgáltatásokkal

összefüggő adat biztonságos módon, megfelelő ellenőrzés mellett és jegyzőkönyvezetten kerüljön törlésre.

6.6.2. Számítógép biztonsági értékelések

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

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

6.7. Életciklus technikai szabályok

6.7.1. Rendszerfejlesztési szabályok

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

6.7.2. 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 {Sz16} illetve a biztonsági szabályzata {Sz17} tartalmazzák.

6.7.3. Életciklus biztonsági értékelések

A Szolgáltató által alkalmazott megbízható informatikai rendszerek megfelelnek a 2/2002 MeHVM {J11} ajánlásban rögzített követelményeknek,

6.8. Hálózati biztonsági szabályok

A hálózati védelmi intézkedések a {J11} 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, azonosságában hitelesített adatbázisokban ellenőrizze.

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

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

A hitelesítő központok nem folytatnak közvetlen külső kommunikációt a végfelhasználókkal.

6.9. Kriptográfiai (HSM) 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

A Szolgáltató által kibocsátott minősített tanúsítvány profilok és tanúsítvány-visszavonási profilok megfelelnek a {J11} 2/2002 (IV.26.) MeHVM irányelvnek, az {Sz6} ITU-T X.509 szabvány 3. változatának, az EU {Sz5} ETSI TS 101 862 (Minősített tanúsítvány profil) szabványnak és az {Sz2} RFC 3739 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil) Internet szabványnak. Az alkalmazott minősített tanúsítványtípus mezői és azok értelmezése e szabványokat követi.

7.1. Tanúsítvány profil

7.1.1. Alap mezők

A Szolgáltató az RFC 3280 {Sz3} 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 {Sz3} 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 {Sz3} 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 Subject Unique Identifier	Nem kitöltött.

A mezők kitöltésének további részleteit a Szolgáltató Tanúsítványprofilok {Sz19} a PKI szolgáltatásokhoz című dokumentuma tartalmazza.

7.1.2. Tanúsítvány kiterjesztések

A Szolgáltató az {Sz6} ITU X.509 szabvány 3. változatának, az {Sz5} EU ETSI TS 101 862 és az {Sz2} RFC 3739 szabványoknak megfelelő tanúsítvány kiterjesztéseket támogatja.

Mezőnév	Szabály	Kritikus
Kibocsátó kulcsazonosítója IssuerKeyIdentifier	Kibocsájtó kulcsazonosítója	Nem
Tulajdonos kulcsazonosítója SubjectKeyIdentifier	Kibocsájtó által generált adat	Nem
Tanúsítvány-irányelv Certificate Policies	PolicyIdentifier PolicyQualifier UserNotice	Nem
Alapvető megkötések Basic Constraints	Subject type = End Entity Path Length Constraint = None	Igen
Kulcshasználat Key Usage	Letagadhatatlanság	Igen
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 hozzáférésének URL-je [2] Hozzáférési mód=online tanúsítványállapot-protokoll URL-je	IGEN
Tanúsítványminősítési nyugta QcStatements	A minősített tanúsítványok minősítésére vonatkozó bejegyzések. A biztonságos aláírás-létrehozó eszköz jelzése [MTT+BALE] tanúsítványok esetén	

A mezők kitöltésének további részleteit a Szolgáltató Tanúsítványprofilok {Sz19} 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.

7.1.3. Közigazgatásban alkalmazható tanúsítványok

A közigazgatásban alkalmazható tanúsítványok ([KET]) esetében Szolgáltató a következő kibocsátó azonosítót alkalmazza:

Kibocsátó	
Common Name	Minősített Közigazgatási Tanúsítványkiadó – Kormányzati Hitelesítés Szolgáltató
Organisation	NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
Locality	Budapest
Country	HU

A közigazgatásban nem alkalmazható tanúsítványok ([NKET]) esetében Szolgáltató a fentitől eltérő kibocsátó azonosítót alkalmaz, a megkülönböztethetőség érdekében.

7.2. Tanúsítvány-visszavonási profil

A Szolgáltató által kibocsátott tanúsítványok visszavonási listák megfelelnek az RFC 3280 {Sz3} 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 {Sz3} 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 {Sz3} szerinti kódolással.
Következő kibocsátás Next Update	A következő visszavonási lista kibocsátásának ideje. UCT szerinti érték, RFC 2459 {Sz3} szerinti kódolással.
Visszavont tanúsítványok Revoked Certificates	A visszavont tanúsítványok listája a tanúsítvány sorozatszámával és a visszavonás idejével.

A Szolgáltató által használt visszavonás bejegyzési kiterjesztések a következők lehetnek:

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

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

A Szolgáltató által kitöltött visszavonási lista kiterjesztések a következők:

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

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

7.3. Időbélyeg profil

A Szolgáltató által kibocsátott időbélyegek szerkezete követi az {Sz6} RFC 3161 szabványt és az {Sz7} ETSI ET 102 023 szabvány 7.3.1 pontjában előírtakat.

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 a minősített hitelesítés-szolgáltatók nyilvántartásába 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 minősített hitelesítés-szolgáltatásához és a minősített időbélyegzés szolgáltatásához olyan biztonságos aláírás létrehozó eszközt és kriptográfiai modult használ, amely rendelkezik a 9/2005. (VII. 21.) IHM rendelet {J5} szerint kijelölt szervezet vagy ezzel egyenértékű Európai Uniós szervezet által kiadott tanúsítással, illetve szerepel a Nemzeti Média- és Hírközlési Hatóság „Tanúsított elektronikus aláírási termékek” listáján.

Szolgáltató külső és belső vizsgáltatokat végez illetve végeztet annak érdekében, hogy a Szolgáltatásaival kapcsolatos folyamatai, eszközei, személyzete és e 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.

Szolgáltató rendelkezik minőségbiztosítási rendszerrel és információbiztonsági irányítási rendszerrel, melyek ellenőrzését külső fél végzi.

Szolgáltató az {J1} Eat. 8/b § szerint önkéntes akkreditációs rendszer keretében nem lett tanúsítva.

8.1.1. Vizsgálatok gyakorisága

A Szolgáltató által használt kriptográfiai modul vizsgálatára a használatba vételt megelőzően került sor; a tanúsítás érvényességét (és az ezzel kapcsolatos esetleges változásokat) a Szolgáltató negyedévente ellenőrzi.

A Szolgáltató által az Előfizetők számára biztosított biztonságos aláírás-létrehozó eszköz (BALE) vizsgálatára a Szolgáltatások megkezdését megelőzően került sor; a tanúsítás érvényességét (és az ezzel kapcsolatos esetleges változásokat) Szolgáltató negyedévente ellenőrzi.

A Nemzeti Média- és Hírközlési Hatóság a jogszabályoknak megfelelően évente átfogó helyszíni ellenőrzést végez.

A Szolgáltató a külső, illetve a saját ellenőrző szervezete által végzett belső vizsgálatokat a {Sz17} PKI szolgáltatások biztonsági szabályzatában megjelölt rendszerességgel – évente legalább egyszer - biztosítja.

8.1.2. Az átvizsgáló szervezet megnevezése/jellemzői

A Szolgáltató tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket a Szolgáltató biztonsági szervezete végzi, az ott dolgozó biztonsági tisztviselők bevonásával. A külső auditot a Szolgáltató olyan, széles körben ismert szakértővel illetve auditor céggel végezteti el, amely szakértelmét bizonyítani tudja a nyilvános kulcsú infrastruktúra és informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában (pl. CISA minősítéssel).

A vizsgálatokat illetve ellenőrzéseket végző munkatársak, valamint külső auditorok olyan személyek illetve szervezetek, amelyek függetlenek Szolgáltatótól illetve az általuk ellenőrzött rendszertől, területtől.

8.1.3. Hiányosságok kezelése

Az üzemszerű ellenőrzések, a belső és külső auditok, valamint a szakértői elemzések során feltárt hiányosságok, hibás gyakorlatok esetén a Szolgáltató intézkedési tervet készít és a hiányosságokat késlekedés nélkül megszünteti, intézkedéseit dokumentálja illetve ellenőrzi.

A Nemzeti Média- és Hírközlési Hatóság által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató késlekedés nélkül megszünteti a vizsgálatot végző Nemzeti Média- és Hírközlési Hatóságtól kapott információk és ajánlások alapján.

8.1.4. Eredmény kommunikációja

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, de a hiányosságok felszámolásáról a Szolgáltató Nemzeti Média- és Hírközlési Hatóságot az éves ellenőrzések keretében tájékoztatni kell.

A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni.

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. Tanúsítványhozzáférés

Szolgáltató a közzétett tanúsítványok eléréséért nem számol fel díjat.

9.1.3. Visszavonási és állapot információ hozzáférés

A Szolgáltató a közzétett visszavonási lista eléréséért nem számol fel díjat.

9.1.4. Időbélyegzés

A Szolgáltató az időbélyegek kibocsátásáért az erre vonatkozó szerződés keretében meghatározott díjat számol fel.

9.1.5. Egyéb szolgáltatásokra vonatkozó díjak

[MTT+BALE] tanúsítványok esetén Szolgáltató az aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatásért 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.

Az igénylők személyes regisztrációjáért – amennyiben Előfizető kérésére ezt Szolgáltató helyszíni kiszállás keretében, az Előfizető megjelölt telephelyén végzi el – mobil regisztrációs díjat számol fel Szolgáltató az Előfizető felé, az előfizetői szerződésben rögzítettek szerint.

9.1.6. Visszatérítési elvek

Az Előfizető a számára kibocsátott tanúsítvány éves fenntartási díjának visszatérítésére 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. [MTT+BALE] tanúsítványok esetén a kibocsátott aláírás-létrehozó eszközön szereplő adatok a Szolgáltató hibájából fakadóan nem megfelelők (pl. a kártyára festett név hibás),
d. [MTT+BALE] tanúsítványok esetén 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 számára a megjelölt bankszámlaszámra 20 naptári napon belül visszautalja, 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.

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

9.2. Anyagi felelősség és annak korlátai

A Szolgáltató anyagi felelősségéről és annak korlátairól a {Sz14} 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 csak az Aláírótól közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjthet személyes adatokat és csak olyan mértékben, ami a tanúsítvány kiadásához szükséges.

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, tényt, információt, tervet vagy dokumentumot a másik fél előzetes írásbeli hozzájárulása nélkül harmadik személynek átadni. A felek az üzleti titok megsértésével okozott kárért a polgári jog általános szabályai szerint felelnek.

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

Ennek keretén belül:

a. a fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól
b. megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénysértő kezelése ellen
c. csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához
d. gondoskodik az Előfizetőre és 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 űrlapon 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 {J1} 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 Aláírót nem tájékoztathatja.

9.3.5. Információszolgáltatás polgári eljárás keretében

A Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az Aláíró személyazonosságát igazoló adatokat átadhatja az ellenérdekű peres félnek vagy képviselőjének feltárhat bizalmas felhasználói információkat, illetőleg azt közölheti a megkereső bírósággal az {J1} Eat. 11.§ paragrafusa alapján.

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

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 nyilvántartásait, a bizalmas adatokkal együtt, át kell adnia más - vele azonos besorolású – szolgáltató részére az {J1} Eat. 16. § (2.) bekezdése szerint.

9.4. 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
b. a Szolgáltató által az Aláíró részére kibocsátott egyedi azonosító
c. a Szolgáltató szabályzatai, szerződéses feltételei
d. 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 {Sz14} 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 {Sz14} 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 a Magyarország törvényei az irányadók. Az alkalmazott jogszabályokat a 2.3.1 pont tartalmazza.