



NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

**Bizalmi Szolgáltatási Szabályzat
minősített
elektronikus aláírás és elektronikus bélyegzés
célú tanúsítványokhoz
(BSZ-MTT)**

Verziószám	1.11
OID	0.2.216.1.200.1100.100.42.3.1.18.1.11
Hatályba lépés dátuma	2024.05.08.
Dokumentum besorolása	nyilvános
Jóváhagyó	Adorján István

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0 ¹	2016.12.29	Első, eIDAS megfelelésgértékeléshez elkészített változat	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.1 ²	2017.04.28	Megfelelésgértékelő szervezet észrevételei alapján módosított változat	Polysys Kft. Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.2	2017.05.31.	NMHH észrevételei alapján módosított változat	Papp Eszter	Kővári Ferenc	Ferencz Attila
1.3	2019.03.14	EN szabványok változásainak követése, visszavonás pontosítása, egyéb frissítések	Polysys Kft. Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.4	2019.08.15.	Szolgáltató Ügyfélkapcsolati Irodája címének változása.	Joláthy Dániel	Kővári Ferenc	Ferencz Attila
1.5	2019.11.25.	Új típusú QSCD bevezetése. Ügyvédi kamarai azonosítót tartalmazó tanúsítványok kiadása	Kővári Ferenc	dr. Kovács Ferenc	Ferencz Attila
1.6	2021.03.04.	Új PKI ÜKI tanúsítvány átadó helyszín	Kővári Ferenc	dr. Kovács Ferenc	Adorján István
1.7	2023.04.01	- új algoritmuskészletek bevezetésével kapcsolatos módosítások - kiegészítés tanúsítványmegújítás részleges bevezetéséhez kapcsolódó szabályokkal - kiegészítések a tranzakciós limittel kapcsolatban - azonosítási-hitelesítési, valamint állapotváltozási folyamatokkal kapcsolatos kisebb pontosítások	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.8	2023.11.09	- visszavonással és felfüggesztéssel kapcsolatos szabályok pontosítása - új ECC alapú CA bevezetésével kapcsolatos kiegészítések - alkalmazott QSCD eszközök leírásának pontosítása - egyéb pontosítások	Kővári-Szabó Zoltán	Nagy Benjámin Melo Sándor	Adorján István
1.9	2024.01.02	Székhelyváltozás átvezetése	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.10	2024.04.22	Alkalmazott tanúsítványkiadók (CA) változása	Kővári-Szabó Zoltán	Melo Sándor	Adorján István
1.11	2024.05.08	A 6.3.2 pont kiegészítése a „GovCA Főtanúsítványkiadó”-ra vonatkozó, hiányzó információval	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István

¹ Nem lépett hatályba

² Nem lépett hatályba

Tartalomjegyzék

1	BEVEZETÉS	9
1.1	Áttekintés	9
1.2	Dokumentum neve és azonosítása	10
1.2.1	Hitelesítési rendek	10
1.3	PKI közösség	11
1.3.1	Hitelesítő szervezet	11
1.3.2	Regisztrációs szervezet	13
1.3.3	Előfizetők és Alanyok, Aláírók és Bélyegző Létrehozók	13
1.3.3.1	Előfizető Kapcsolattartója	14
1.3.4	Érintett felek	14
1.3.5	Egyéb felek	14
1.4	A tanúsítvány alkalmazhatósága	14
1.4.1	Engedélyezett tanúsítvány használat	15
1.4.2	Tiltott tanúsítvány használat	16
1.5	Szabályzat adminisztráció	16
1.5.1	Szabályzatot karbantartó szervezet	16
1.5.2	Kapcsolat	16
1.5.3	Szabályzat alkalmasságának meghatározása	17
1.5.4	Szabályzat jóváhagyásának eljárása	17
1.6	Fogalmak, rövidítések és hivatkozások	18
1.6.1	Fogalmak	18
1.6.2	Rövidítések	18
1.6.3	Hivatkozások	19
1.6.3.1	Jogszabályi hivatkozások	19
1.6.3.2	Szabványok és műszaki-technikai specifikációk	19
1.6.3.3	Hivatkozott dokumentumok	20
2	KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR	21
2.1	Tanúsítványtár	21
2.2	A szolgáltatói információ közzététele	21
2.3	A közzététel gyakorisága	21
2.4	Hozzáférés-ellenőrzések	22
3	AZONOSÍTÁS ÉS HITELESÍTÉS	23
3.1	Elnevezések	23
3.1.1	Név típusok	23
3.1.2	Nevek jelentése	23
3.1.2.1	Üzleti tanúsítvány alanyára vonatkozó képzési és igazolási szabályok	23
3.1.2.2	Személyes tanúsítvány alanyára vonatkozó képzési és igazolási szabályok	24
3.1.2.3	Szervezeti tanúsítvány alanyára vonatkozó képzési és igazolási szabályok	25
3.1.2.4	Eszköz tanúsítvány alanyára vonatkozó képzési és igazolási szabályok	26
3.1.3	Előfizetők névtelensége és álnév használata	26
3.1.4	Különbféle név formák megjelenítési szabályai	27
3.1.5	A nevek egyedisége	27
3.1.6	Márkanévek elismerése, hitelesítése és szerepe	27
3.2	Kezdeti azonosítás	27
3.2.1	A magánkulcs birtoklása	28
3.2.2	A szervezeti azonosság hitelesítése	28
3.2.3	A személyazonosság hitelesítése	29
3.2.4	Előfizető nem ellenőrzött adatai	29
3.2.5	Jogosultság ellenőrzése	30
3.2.6	Együttműködési kritériumok	30

3.3	Azonosítás és hitelesítés kulcscsere esetén	30
3.3.1	Azonosítás és hitelesítés érvényes tanúsítvány esetén.....	30
3.3.2	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén.....	30
3.4	Azonosítás és hitelesítés visszavonási vagy felfüggesztési kérelem esetén.....	30
4	A TANÚSÍTVÁNYOK ÉLETCIKLUSA.....	32
4.1	Tanúsítványigénylés.....	32
4.1.1	Ki nyújthat be tanúsítványigénylést	32
4.1.2	Igénylési folyamat és felelősségek	32
4.1.2.1	Regisztráció	33
4.1.2.1.1	Regisztráció [NKET] tanúsítvány esetén	33
4.1.2.1.2	Regisztráció [KET] tanúsítvány esetén.....	33
4.1.2.1.2.1	Személyes regisztráció [ALA+KET] tanúsítvány esetén.....	33
4.1.2.1.2.2	Helyszíni regisztráció [ALA+KET] tanúsítvány esetén.....	34
4.1.2.1.2.3	Ügyintézészt biztosító állami szerv személyzeti nyilvántartásán alapuló regisztráció [ALA+KET] tanúsítvány esetén	34
4.1.2.1.2.4	Regisztráció [BÉLY+KET] tanúsítvány esetén	34
4.2	Tanúsítványigénylés feldolgozása.....	35
4.2.1	Azonosítási és hitelesítési műveletek	35
4.2.2	Tanúsítványigénylés elfogadása vagy visszautasítása.....	35
4.2.3	Tanúsítványigénylés feldolgozás időtartama	36
4.3	Tanúsítvány kibocsátás.....	36
4.3.1	Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek.....	36
4.3.2	Előfizető értesítése a tanúsítvány kibocsátásáról	36
4.3.2.1	Előfizető értesítése az [NKET] tanúsítvány kibocsátásáról	36
4.3.2.2	Előfizető értesítése a [KET] tanúsítvány kibocsátásáról	37
4.3.2.2.1	Előfizető értesítése a személyes regisztrációval kiadott [ALA+KET] tanúsítvány kibocsátásáról	37
4.3.2.2.2	Előfizető értesítése a helyszíni regisztrációval kiadott [ALA+KET] tanúsítvány kibocsátásáról	37
4.3.2.2.3	Előfizető értesítése az ügyintézészt biztosító állami szerv személyzeti nyilvántartásán alapuló regisztrációval kiadott [ALA+KET] tanúsítvány kibocsátásáról.....	38
4.3.2.2.4	Előfizető értesítése a [BÉLY+KET] tanúsítvány kibocsátásáról	38
4.4	Tanúsítvány-elfogadás	39
4.4.1	Tanúsítvány Előfizető általi elfogadása	39
4.4.2	Tanúsítvány közzététele.....	39
4.4.3	További felek értesítése a tanúsítvány kibocsátásáról.....	39
4.5	A kulcspár és a tanúsítvány használata.....	39
4.5.1	Az Előfizető magánkulcs- és tanúsítvány használata	39
4.5.2	Az Érintett felek nyilvános kulcs- és tanúsítvány használata	40
4.6	Tanúsítványok megújítása.....	40
4.6.1	Tanúsítvány megújítás körülményei	40
4.6.2	Ki kérelmezhet tanúsítvány megújítást.....	41
4.6.3	Tanúsítvány megújítási kérelmek feldolgozása	41
4.6.4	Előfizető értesítése a megújított tanúsítvány kibocsátásáról.....	41
4.6.5	Tanúsítvány Előfizető általi elfogadása	41
4.6.6	Megújított tanúsítvány közzététele	41
4.6.7	További felek értesítése tanúsítvány megújításról	41
4.7	Kulcscsere	41
4.7.1	Kulcscsere körülményei	41
4.7.2	Ki kérelmezhet kulcscserét.....	41
4.7.3	Kulcscsere kérelmek feldolgozása	41
4.7.4	Előfizető értesítése az új tanúsítvány kibocsátásáról.....	41
4.7.5	Új tanúsítvány Előfizető általi elfogadása	42

4.7.6	Új tanúsítvány közzététele	42
4.7.7	További felek értesítése az új tanúsítvány kibocsátásáról	42
4.8	Tanúsítvány-módosítás	42
4.8.1	Tanúsítvány-módosítás körülményei	42
4.8.2	Ki kérelmezhet tanúsítvány-módosítást	42
4.8.3	Tanúsítvány-módosítási kérelmek feldolgozása	42
4.8.4	Előfizető értesítése az új tanúsítvány kibocsátásáról	42
4.8.5	Módosított tanúsítvány Előfizető általi elfogadása	42
4.8.6	Módosított tanúsítvány közzététele	42
4.8.7	További felek értesítése a módosított tanúsítvány kibocsátásáról	42
4.9	Tanúsítvány visszavonás és felfüggesztése	43
4.9.1	Visszavonás körülményei	43
4.9.2	Ki kezdeményezheti a visszavonást	43
4.9.3	Visszavonási kérelemre vonatkozó eljárás	44
4.9.4	Kivárási idő visszavonási kérelem esetén	44
4.9.5	Visszavonási kérelem feldolgozásának időbelisége	44
4.9.6	Visszavonás ellenőrzésének ajánlása az Érintett felek számára	45
4.9.7	CRL kibocsátási gyakoriság	45
4.9.8	CRL előállítása és közzététele között leghosszabb idő	45
4.9.9	OCSP szolgáltatás biztosítása	45
4.9.10	OCSP alapú visszavonás ellenőrzés követelményei	45
4.9.11	Visszavonási állapot közlés más formái	45
4.9.12	Különleges követelmények a kulcs kompromittálódása esetére	45
4.9.13	Felfüggesztés körülményei	46
4.9.14	Ki kérelmezhet felfüggesztést	46
4.9.15	Felfüggesztésre vonatkozó eljárás	46
4.9.16	A felfüggesztés megengedett időtartama	46
4.10	Visszavonási állapot szolgáltatások	47
4.10.1	Működési jellemzők	47
4.10.2	Szolgáltatás rendelkezésre állása	48
4.10.3	Opcionális funkciók	48
4.11	Az előfizetés vége	49
4.12	Kulcsletét és visszaállítás	49
4.12.1	Kulcsletét és visszaállítás szabályai	49
4.12.2	Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai	49
5	FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK	50
5.1	Fizikai óvintézkedések	50
5.1.1	Telephely elhelyezése és szerkezeti felépítése	50
5.1.2	Fizikai hozzáférés	50
5.1.3	Áramellátás és légkondicionálás	51
5.1.4	Beázás és elárasztás veszélyeztetettség	51
5.1.5	Tűzmegeelőzés és tűzvédelem	51
5.1.6	Adathordozók tárolása	52
5.1.7	Selejt kezelése és megsemmisítése	52
5.1.8	Fizikailag elkülönítetten őrzött mentési példányok	52
5.2	Eljárásbeli előírások	52
5.2.1	Bizalmi munkakörök	52
5.2.2	Az egyes feladatokhoz szükséges személyzeti létszámok	53
5.2.3	Bizalmi munkakörökben elvárt azonosítás és hitelesítés	53
5.2.4	Egymást kizáró munkakörök	53
5.3	Személyzetre vonatkozó előírások	54
5.3.1	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények	54
5.3.2	Biztonsági háttér ellenőrzés eljárásai	54

5.3.3	Képzési követelmények.....	55
5.3.4	Továbbképzési gyakoriságok és követelmények.....	55
5.3.5	Munkabeosztás körforgásának gyakorisága és sorrendje	56
5.3.6	Felhatalmazás nélküli tevékenységek büntető következményei	56
5.3.7	Szerződéses munkavállalókra vonatkozó követelmények	56
5.3.8	A személyzet számára biztosított dokumentációk	56
5.4	A biztonsági naplózás folyamatai	56
5.4.1	Naplózott esemény típusok	56
5.4.2	Naplóállomány feldolgozásának gyakorisága	57
5.4.3	Naplóállomány megőrzési időtartama	57
5.4.4	Naplóállomány védelme	57
5.4.5	Naplóállomány mentési folyamatai	57
5.4.6	Naplózás gyűjtési rendszere	57
5.4.7	Rendellenes eseményeket kiváltó alanyok értesítése.....	57
5.4.8	Sebezhetőség értékelések	58
5.5	Adatok archiválása	58
5.5.1	A tárolt adatok típusai.....	58
5.5.2	Archívum megőrzési időtartama	58
5.5.3	Archívum védelme	58
5.5.4	Archívum mentési eljárásai	59
5.5.5	Az adatok időbélyegzésére vonatkozó követelmények.....	59
5.5.6	Archívum gyűjtési rendszere	59
5.5.7	Archívum hozzáférés és ellenőrzés eljárásai.....	59
5.6	Kulcs átállítás	59
5.7	Helyreállítás rendkívüli üzemi helyzetek esetén	60
5.7.1	Rendkívüli események és kompromittálódás kezelésének eljárásai	60
5.7.2	Sérült számítási erőforrások, szoftverek és/vagy adatok	61
5.7.3	Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás	61
5.7.4	Üzletmenet folytonosság helyreállítás katasztrófát követően.....	61
5.8	A szolgáltatási tevékenység megszüntetése	61
6	MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	63
6.1	Kulcspár előállítás és telepítés	63
6.1.1	Kulcspár előállítás	63
6.1.1.1	Szolgáltatói kulcspárok előállítása.....	63
6.1.1.2	Előfizetői kulcspárok előállítása.....	63
6.1.2	Magánkulcs eljuttatása a tulajdonoshoz	63
6.1.3	Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz.....	64
6.1.4	A szolgáltatói nyilvános kulcs közzététele	64
6.1.5	Kulcs méretek	64
6.1.6	A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése.....	65
6.1.7	A kulcs használat célja (X.509 v3 kulcs használati mezőnek megfelelően)	65
6.2	Magánkulcs védelme és kriptográfiai modul műszaki szabályozások	66
6.2.1	Kriptográfiai modul szabványok és műszaki szabályozások	66
6.2.2	Több szereplős ("n-ből m") ellenőrzés	67
6.2.3	Magánkulcs letét	67
6.2.4	Magánkulcs visszaállítása	67
6.2.5	Magánkulcs mentése	67
6.2.6	Magánkulcs bejuttatása a kriptográfiai modulba	68
6.2.7	Magánkulcs kriptográfiai modulban történő tárolásának módja	68
6.2.8	Magánkulcs aktiválásának módja	68
6.2.9	Magánkulcs aktív állapotának megszüntetési módja	68
6.2.10	Magánkulcs megsemmisítésének módja	68
6.2.11	Kriptográfiai modul értékelése	69

6.3	Kulcspár gondozás egyéb szempontjai	69
6.3.1	Nyilvános kulcs archiválása.....	69
6.3.2	Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama.....	69
6.4	Aktivizáló adatok	70
6.4.1	Aktivizáló adatok előállítása és telepítése	70
6.4.2	Aktivizáló adatok védelme	70
6.4.3	Aktivizáló adatok egyéb szempontjai.....	70
6.5	Informatikai biztonsági óvintézkedések	70
6.5.1	Informatikai biztonsági műszaki követelmények meghatározása	70
6.5.2	Informatikai biztonsági értékelés	71
6.6	Életciklusra vonatkozó műszaki óvintézkedések	71
6.6.1	Rendszerfejlesztési óvintézkedések.....	71
6.6.2	Biztonságkezelési óvintézkedések	71
6.6.3	Életciklus biztonsági óvintézkedések.....	72
6.7	Hálózatbiztonsági óvintézkedések.....	72
6.8	Időforrások	72
7	TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK / CERTIFICATE, CRL, AND OCSP PROFILES	73
7.1	Tanúsítvány profil.....	73
7.1.1	Verziószám	73
7.1.2	Tanúsítvány kiterjesztések	73
7.1.3	Algoritmus azonosítók.....	73
7.1.4	Név formák.....	74
7.1.5	Név megszorítások	74
7.1.6	Hitelesítési rend objektumazonosító.....	74
7.1.7	Szabályzati megszorítások kiterjesztés használata	74
7.1.8	Szabályzat minősítők szintaktikája és szemantikája	74
7.1.9	A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása	74
7.2	CRL profil	74
7.2.1	Verziószám	74
7.2.2	CRL és CRL bejegyzés kiterjesztések.....	74
7.3	OCSP profil	75
7.3.1	Verziószám	75
7.3.2	OCSP kiterjesztések	75
8	MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK	76
8.1	Vizsgálatok gyakorisága és körülményei	76
8.2	Auditor azonosítása és képesítése.....	76
8.3	Auditor függetlensége	77
8.4	Audit során vizsgált területek.....	77
8.5	Hiányosságok esetén végrehajtandó tevékenységek	77
8.6	Eredmény kommunikációja	77
9	EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK	78
9.1	Díjak.....	78
9.1.1	Tanúsítvány kibocsátás díja	78
9.1.2	Tanúsítványhozzáférés díja.....	78
9.1.3	Visszavonási és állapot információ hozzáférés díja.....	78
9.1.4	Egyéb szolgáltatások díja.....	78
9.1.5	Visszatérítési szabályzat	78
9.2	Anyagi felelősség	79
9.2.1	Biztosítási fedezet	79
9.2.2	További követelmények.....	79
9.2.3	Felelősségbiztosítás vagy garancia végfelhasználók számára	79
9.3	Üzleti információk bizalmassága	80
9.3.1	Bizalmasan kezelendő információk köre.....	80

9.3.2	Nem bizalmasnak tekintett információk köre	80
9.3.3	Bizalmas információk védelmének felelőssége.....	80
9.4	Személyes adatok védelme.....	80
9.4.1	Adatvédelmi terv	80
9.4.2	Bizalmasként kezelendő személyes adatok	80
9.4.3	Bizalmasként nem kezelendő személyes adatok.....	80
9.4.4	Személyes adatok védelmének felelőssége	81
9.4.5	Hozzájárulás a személyes adatok felhasználásához	81
9.4.6	Felfedés bírósági vagy polgári peres eljárás keretében.....	81
9.4.7	Egyéb, felfedést eredményező körülmények	81
9.5	Szellemi tulajdonjogok.....	81
9.6	Tevékenységért viselt felelősség és helytállás	82
9.6.1	Szolgáltató felelőssége és helytállása	82
9.6.2	A regisztrációs szervezet felelőssége és helytállása	83
9.6.3	Előfizető felelőssége és helytállása	83
9.6.4	Érintett felek felelőssége és helytállása	85
9.6.5	Egyéb felek felelőssége és helytállása	85
9.7	Helytállás érvénytelenségi köre	85
9.8	Felelősség korlátozása.....	85
9.9	Kártérítések.....	86
9.10	Hatályosság és megszűnés.....	86
9.10.1	Hatályosság	86
9.10.2	Megszűnés.....	86
9.10.3	Megszűnés után is hatályban maradó rendelkezések	86
9.11	Egyéni hirdetések és kommunikáció a résztvevőkkel	87
9.12	Módosítások.....	87
9.12.1	Módosítás eljárása	87
9.12.2	Értesítés módszere és időtartama	87
9.12.3	OID megváltozását előidéző körülmények.....	87
9.13	Vitás kérdések rendezése	87
9.14	Irányadó jog	87
9.15	Hatályos jognak megfelelés.....	88
9.16	Vegyes rendelkezések	88
9.16.1	Teljességi záradék	88
9.16.2	Átruházás.....	88
9.16.3	Részleges érvénytelenség	88
9.16.4	Igényérvényesítés	88
9.16.5	Force Majeure (Vis maior).....	88
9.17	Egyéb rendelkezések.....	88

1 BEVEZETÉS

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban: Szolgáltató) Bizalmi Szolgáltatási Szabályzata, mely a minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokkal kapcsolatos szolgáltatásaira vonatkozik (továbbiakban: BSZ-MTT).

A BR-MTT az alábbi jelöléseket használja:

- a tanúsítvány alanyától függően:
 - BÉLY: a tanúsítvány alanya jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet
 - ALA: a tanúsítvány alanya természetes személy
- attól függően, hogy a tanúsítvány használható-e elektronikus ügyintézési célra, illetve közigazgatási célra:
 - KET: a tanúsítvány a {J9} 137/2016 rendelet szerinti elektronikus ügyintézési célra, illetve közigazgatási célra használható
 - NKET: a tanúsítvány a {J9} 137/2016 rendelet szerint elektronikus ügyintézési célra, illetve közigazgatási célra nem használható
- a tanúsítványhoz kapcsolódó magánkulcsot tároló eszköztől függően:
 - P12: a tanúsítványhoz kapcsolódó magánkulcsot szoftveres (az {Sz14} szabványnak megfelelő) kulcstároló tárolja
 - QSCD: a tanúsítványhoz kapcsolódó magánkulcsot Szolgáltató által forgalmazott QSCD (minősített elektronikus aláírást/bélyegzőt létrehozó eszköz) hozza létre és tárolja

A BR-MTT a Tanúsítványok alábbi típusait különbözteti meg:

BÉLY+KET+P12	elektronikus ügyintézési célra használható, minősített, szoftveres, bélyegzés célú tanúsítvány
BÉLY+KET+QSCD	elektronikus ügyintézési célra használható, minősített, bélyegzés célú tanúsítvány
BÉLY+NKET+P12	minősített, szoftveres, bélyegzés célú tanúsítvány
BÉLY+NKET+QSCD	minősített, bélyegzés célú tanúsítvány
ALA+KET+P12	elektronikus ügyintézési célra használható, minősített, szoftveres, aláírás célú tanúsítvány
ALA+KET+QSCD	elektronikus ügyintézési célra használható, minősített, aláírás célú tanúsítvány
ALA+NKET+P12	minősített, szoftveres, aláírás célú tanúsítvány
ALA+NKET+QSCD	minősített, aláírás célú tanúsítvány

Jelen szolgáltatási szabályzat a kibocsátott tanúsítványok kezelésére (előállítás, kibocsátás, közzététel, megújítás, felfüggesztés, újra-érvényesítés, visszavonás, továbbiakban együttesen: Szolgáltatások) vonatkozó eljárási és működtetési szabályokat tartalmazza.

A Szolgáltató a Szolgáltatásokat a vele szerződéses viszonyban álló ügyfelek részére nyújtja, és egyes szolgáltatási elemeket hozzáférhetővé tesz az elektronikus aláírások és bélyegzők hitelességét ellenőrző Érintett Felek részére is.

1.1 Áttekintés

A szolgáltatási szabályzat célja, hogy összefoglalja mindazokat az információkat, amelyeket 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, tanúsítvány visszavonási listák, valós idejű tanúsítvány-állapot válaszok mennyiben felelnek meg az elvárásaiknak.

Jelen szolgáltatási szabályzat a „Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BR-MTT) hatálya alá tartozó Szolgáltatásokra vonatkozik.

Jelen dokumentum, valamint az 1.6.3 fejezetben hivatkozott jogszabályok, szabványok és műszaki specifikációk, továbbá a Szolgáltató 1.6.3.3 fejezetben felsorolt nyilvános dokumentumainak megismerése után a tanúsítványok, tanúsítvány visszavonási listák, valós idejű tanúsítvány-állapot válaszok használói és elfogadói egyértelműen meg tudják állapítani azok kezelésének módját, az általuk garantált biztonság mértékét, valamint a rájuk vonatkozó technikai, üzleti és pénzügyi garanciákat és jogi felelősségvállalásokat.

Jelen szolgáltatási szabályzat az {Sz1} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában szigorúan követi annak előírásait. Az ott meghatározott felépítés szigorú megtartása érdekében azok a fejezetek is szerepelnek, melyeknél nincs követelmény előírva; ezekben a fejezetekben a „Nincs kikötés” szöveg szerepel.

Szolgáltató a jelen szolgáltatási szabályzat alapján nyújtott Szolgáltatásokat a Bizalmi Felügyeletnek 2017.04.28. napján jelentette be. A Bizalmi Felügyelet erre vonatkozó nyilvántartásának elérhetősége: <http://webpub-ext.nmhh.hu/esign2016/index.jsp>

1.2 Dokumentum neve és azonosítása

Jelen bizalmi szolgáltatási szabályzat teljes neve NISZ Zrt, „Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz”.

A szolgáltatási szabályzat rövid neve: BSZ-MTT.

A szolgáltatási szabályzat objektum azonosítója és verziószáma a címlapon található.

Jelen BSZ-MTT tartalmazza a BR-MTT bizalmi szolgáltatási rend hatálya alatt kiadott tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat. A szolgáltatási szabályzat hatályba lépését és hatályának megszűnését a 9.10 fejezet tartalmazza.

Jelen BSZ-MTT-nek csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.1 Hitelesítési rendek

A BR-MTT bizalmi szolgáltatási rend megfelel az {Sz4} EN 319 411-2 szabvány 5.5 fejezetében meghatározott alábbi hitelesítési rendnek:

BÉLY+KET+P12	QCP-1 itu-t(0) identified-organization(4) etsi(0) qualified-certificate- policies(194112) policy-identifiers(1) qcp-legal (1)
BÉLY+KET+QSCD	QCP-1-qscd itu-t(0) identified-organization(4) etsi(0) qualified-certificate- policies(194112) policy-identifiers(1) qcp-legal-qscd (3)
BÉLY+NKET+P12	QCP-1 itu-t(0) identified-organization(4) etsi(0) qualified-certificate- policies(194112) policy-identifiers(1) qcp-legal (1)

BÉLY+NKET+QSCD	QCP-1-qscd itu-t(0) identified-organization(4) etsi(0) qualified-certificate- policies(194112) policy-identifiers(1) qcp-legal-qscd (3)
ALA+KET+P12	QCP-n itu-t(0) identified-organization(4) etsi(0) qualified-certificate- policies(194112) policy-identifiers(1) qcp-natural (0)
ALA+KET+QSCD	QCP-n-qscd itu-t(0) identified-organization(4) etsi(0) qualified-certificate- policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
ALA+NKET+P12	QCP-n itu-t(0) identified-organization(4) etsi(0) qualified-certificate- policies(194112) policy-identifiers(1) qcp-natural (0)
ALA+NKET+QSCD	QCP-n-qscd itu-t(0) identified-organization(4) etsi(0) qualified-certificate- policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

1.3 PKI közösség

1.3.1 Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítő központokból (CA), a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, az ezt körülvevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll.

A Szolgáltató saját szervezetén kívül más szervezetek nem működnek közre a Szolgáltatások nyújtásában.

RSA Gyökér hitelesítő központok

[KET] Elektronikus ügyintézés célú, illetve közigazgatásban alkalmazható tanúsítványok esetén a gyökér hitelesítő központ a {J9} 137/2016 rendelet szerinti közigazgatási gyökér-hitelesítésszolgáltató (KGYHSZ), amely RSA 2048 bites kulcsával és SHA256 algoritmus felhasználásával szolgáltatói tanúsítványokat bocsát ki az e-ügyintézési célú produktív hitelesítő központok részére. A KGYHSZ közigazgatási gyökértanúsítvány főbb adatai a következők.

Subject (alany): CN= KGYHSZ (Public Administration Root CA – Hungary, C=HU

Issuer (kibocsátó): CN= KGYHSZ (Public Administration Root CA – Hungary, C=HU

A KGYHSZ közigazgatási gyökértanúsítvány SHA1 lenyomata:

1C:93:F6:DF:1D:7E:51:F5:69:2F:B4:0B:E9:83:39:DA:62:94:0E:9F

A KGYHSZ közigazgatási gyökértanúsítvány SHA256 lenyomata:

83:34:92:D7:3A:6C:F4:E3:19:C5:9F:35:8D:37:DF:B5:51:98:ED:38:A9:88:90:FE:47:10:91:F4:E3:DF:27:20

[NKET] A Szolgáltató saját gyökér hitelesítő központja RSA 4096 bites kulcsával és SHA256 algoritmus felhasználásával szolgáltatói tanúsítványokat bocsát ki a Szolgáltató produktív hitelesítő központjai részére. A Szolgáltató saját gyökér tanúsítványának főbb adatai a következők.

Subject (alany): CN=Főtanúsítványkiadó – Kormányzati Hitelesítés Szolgáltató, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=Főtanúsítványkiadó – Kormányzati Hitelesítés Szolgáltató, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

A Szolgáltató saját gyökér tanúsítványának SHA1 lenyomata:

FF:B7:E0:8F:66:E1:D0:C2:58:2F:02:45:C4:97:02:92:A4:6E:88:03

A Szolgáltató saját gyökér tanúsítványának SHA256 lenyomata:

C2:15:73:09:D9:AE:E1:7B:F3:4F:4D:F5:E8:8D:BA:EB:A5:7E:03:61:EB:81:4C:BC:23:9F:4D:54:D3:29:A3:8D

ECC Gyökér hitelesítő központok

[NKET] A Szolgáltató ECC alapú gyökér hitelesítő központja P-384-es görbét alkalmazó ECC kulcsával és SHA384 algoritmus felhasználásával szolgáltatói tanúsítványokat bocsát ki a produktív hitelesítő központok részére. Az ECC gyökér hitelesítő központ főbb adatai a következők.

Subject (alany): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

A gyökér tanúsítvány SHA1 lenyomata:

49:47:e8:6b:02:1f:f2:e3:94:b3:dd:d4:fd:0f:da:65:78:e6:49:7f

A gyökér tanúsítvány SHA256 lenyomata:

B1:ED:0B:29:D0:54:2B:2A:13:71:D9:66:F5:8E:42:0B:9E:BD:9C:A1:9F:B9:B2:AF:81:E6:DE:1E:99:D5:E0:8A

RSA Produktív hitelesítő központok

[NKET] „**Minősített Tanúsítványkiadó v2 – GOV CA**”: a Szolgáltató saját gyökér hitelesítő központja által felülhitelesített produktív hitelesítő központ RSA 2048 bites kulcsával és SHA256 algoritmus felhasználásával végtanúsítványokat bocsát ki az Előfizetők, illetve a velük kapcsolatban álló Aláírók és Bélyegző Létrehozók részére. A Szolgáltató ezen produktív hitelesítő központja tanúsítványának főbb adatai a következők.

Subject (alany): CN=Minősített Tanúsítványkiadó v2 – GOV CA, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=Főtanúsítványkiadó – Kormányzati Hitelesítés Szolgáltató, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

ECC Produktív hitelesítő központok

[KET] „**GovCA Minősített Közigazgatási Tanúsítványkiadó**”: a {J9} 137/2016 rendelet szerinti közigazgatási gyökér-hitelesítésszolgáltató (KGYHSZ) által felülhitelesített produktív hitelesítő központ P-384-es görbét alkalmazó ECC kulcsával és SHA384 algoritmus felhasználásával végtanúsítványokat bocsát ki az Előfizetők, illetve a velük kapcsolatban álló Aláírók és Bélyegző Létrehozók részére, közigazgatási, illetve elektronikus ügyintézési – kiadmányozási felhasználás céljára. A Szolgáltató ezen produktív hitelesítő központja tanúsítványának főbb adatai a következők.

Subject (alany): CN= GovCA Minősített Közigazgatási Tanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=KGYHSZ (Public Administration Root CA – Hungary), C=HU

[NKET] A Szolgáltató ECC alapú produktív hitelesítő központjai P-384-es görbét alkalmazó ECC kulcsával és SHA384 algoritmus felhasználásával ECC és RSA alapú végtanúsítványokat

bocsátanak ki az Előfizetők, illetve a velük kapcsolatban álló Alanyok részére. Az ECC produktív hitelesítő központok főbb adatai a következők:

1. E-mailek aláírására nem alkalmas végtanúsítványokat hitelesítő CA

Subject (alany): CN= GovCA Minősített Tanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

2. E-mailek aláírására is alkalmas végtanúsítványokat hitelesítő CA

Subject (alany): CN= GovCA Minősített Tanúsítványkiadó 2024, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

1.3.2 Regisztrációs szervezet

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

Az Ügyfélkapcsolati Iroda végzi az ügyfelekkel való kapcsolattartást, az előfizetők és tanúsítvány alanyok adatainak felvételét, az előfizetők és tanúsítvány alanyok azonosítását, a tanúsítvány kérelmek összeállítását, az elkészült tanúsítványok szétosztását, valamint gondoskodik a szolgáltatási szerződésben foglaltak teljesítéséről.

A Regisztrációs Iroda végzi az előfizetők és tanúsítvány alanyok technikai regisztrációját, a tanúsítványok előállításának, felfüggesztésének és visszavonásának jóváhagyását és kezelését, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat lát el.

A Szolgáltató saját szervezetén kívüli regisztrációs szervezettel jelenleg nem működik közre a Szolgáltatások nyújtásában.

1.3.3 Előfizetők és Alanyok, Aláírók és Bélyegző Létrehozók

Előfizető az {D1} ÁSZF-GOVCA szerinti feltételeknek megfelelő, a Szolgáltatóval szerződéses viszonyban álló jogi személy vagy közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet, amely megrendeli a Szolgáltatótól a Szolgáltatásokat, jellemzően tanúsítvány kibocsátását az általa megnevezett tanúsítvány alanyok számára.

A tanúsítvány alanya (továbbiakban: Alany):

- [ALA] természetes személy: az Előfizetővel kapcsolatban álló személy, aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hoz létre;
- [BÉLY] jogi személy: az Előfizető szervezete, vagy annak valamely szervezeti egysége, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hoz létre;
- [BÉLY] eszköz: az Előfizető által vagy nevében működtetett informatikai eszköz vagy rendszer, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hoz létre.

[ALA] Az a) pont szerinti természetes személy Alany megnevezésére jelen dokumentumban a továbbiakban az „Aláíró” kifejezés is használt.

[BÉLY] A b) és c) pont szerinti, nem természetes személy Alany megnevezésére jelen dokumentumban a továbbiakban a „Bélyegző Létrehozó” kifejezés is használt. A Bélyegző Létrehozó kifejezés alatt – különösen a felelőségek és kötelezettségek vonatkozásában – Előfizető szervezetét, mint jogi személyt vagy közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezetet is érteni kell.

1.3.3.1 Előfizető Kapcsolattartója

A Szolgáltatási Szerződés megkötése során az Előfizető kapcsolattartó személyt jelölhet meg, akit a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) felhatalmaz, illetve feljogosít a tanúsítványokkal kapcsolatos ügyekben Előfizető szervezete nevében eljárni, akár meghatározott esetekre kiterjedő aláírási joggal is. Szolgáltató a későbbiekben – a képviseletre jogosult személy(ek)en felül – ezen személy aláírását fogadja el a tanúsítványokkal kapcsolatos ügyekben, különösen a tanúsítvány igénylési folyamatban, vagy a tanúsítvány visszavonási folyamatban, az ezekhez kapcsolódó kérelmekben. Kapcsolattartó kijelölésének hiányában Szolgáltató csak a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) aláírását fogadja el a tanúsítványokkal kapcsolatos ügyekben. Bélyegzés célú tanúsítvány esetén Kapcsolattartó kijelölése kötelező.

Jelen dokumentumban a továbbiakban az Előfizető Kapcsolattartója kifejezés a fentiek szerint kijelölt személyt, illetve kijelölés hiányában a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személyt jelenti.

1.3.4 Érintett felek

Érintett Fél: a tanúsítványon alapuló elektronikus aláírással vagy bélyegzővel ellátott elektronikus dokumentumot fogadó természetes vagy jogi személy, aki/amely az elektronikus aláírásra vagy bélyegzőre hagyatkozva jár el a dokumentum hitelességének ellenőrzésekor.

1.3.5 Egyéb felek

Bizalmi Felügyelet

A Bizalmi Felügyelet ellátja a Szolgáltató és az általa nyújtott bizalmi szolgáltatások felügyeletét, ellenőrzi a szolgáltatások jogszabályi megfelelőségét. Többek között, figyelemmel kíséri a bizalmi szolgáltatásokkal kapcsolatos technológia és kriptográfiai algoritmusok fejlődését és határozatba foglalja a bizalmi szolgáltatók által a szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket, továbbá jogerős és végrehajtható határozatában elrendelheti a bizalmi szolgáltatások keretében kibocsátott tanúsítványok felfüggesztését vagy visszavonását.

1.4 A tanúsítvány alkalmazhatósága

A BR-MTT hatálya alatt kiadott tanúsítványok a {J1} eIDAS szerinti minősített tanúsítványok, melyek típusai az {Sz3} EN 319 411-1 szerint az alábbiak lehetnek:

- a) [ALA] üzleti tanúsítvány: a tanúsítvány Alanya az Előfizetővel kapcsolatban álló természetes személy (képviseleti joggal rendelkező vagy cégjegyzésre jogosult személy, vagy Előfizető szervezete által foglalkoztatott személy, akinek Előfizetővel való kapcsolata igazolásra és a

tanúsítványban megjelölésre került), aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hozhat létre;

- b) [ALA] személyes tanúsítvány: a tanúsítvány Alanya az Előfizetővel kapcsolatban álló természetes személy (akinek Előfizetővel való kapcsolata a tanúsítványban megjelölésre nem került), aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hozhat létre;
- c) [BÉLY] szervezeti tanúsítvány: a tanúsítvány Alanya az Előfizető szervezet, vagy annak valamely szervezeti egysége, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hozhat létre;
- d) [BÉLY] eszköz tanúsítvány: a tanúsítvány Alanya az Előfizető által vagy nevében működtetett informatikai eszköz vagy rendszer, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hozhat létre.

[ALA+QSCD] Az üzleti és személyes tanúsítványok a {J1} eIDAS 25. cikke szerinti minősített elektronikus aláírás létrehozására és ellenőrzésére használhatók.

[ALA+P12] Az üzleti és személyes tanúsítványok minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás létrehozására és ellenőrzésére használhatók.

[BÉLY+QSCD] A szervezeti és eszköz tanúsítványok a {J2} eIDAS 35. cikke szerint minősített elektronikus bélyegző létrehozására és ellenőrzésére használhatók.

[BÉLY+P12] A szervezeti és eszköz tanúsítványok minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzők létrehozására használhatók.

[QSCD] A minősített elektronikus aláírások és bélyegzők joghatását a {J4} Pp. 325. § f) pontja határozza meg. E szerint a minősített elektronikus aláírással vagy bélyegzővel hitelesített dokumentum teljes bizonyító erejű magánokirat.

[P12] A minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírások és bélyegzők joghatását a {J4} Pp. 325. § f) pontja határozza meg. E szerint a minősített tanúsítványon alapuló elektronikus aláírással vagy bélyegzővel hitelesített dokumentum teljes bizonyító erejű magánokirat.

Teszt tanúsítványok

A Szolgáltató – egyrészt saját rendszerének tesztelése céljából, másrészt azért, hogy harmadik felek a Szolgáltatásokat kipróbálhassák – teszt tanúsítványokat is kibocsát. A Szolgáltató semmilyen felelősséget nem vállal a teszt tanúsítványok kibocsátásáért, felhasználásukért, a hozzájuk kapcsolódó szolgáltatások rendelkezésre állásáért.

Szolgáltató az éles szolgáltatást nyújtó gyökér hitelesítő központ hierarchiájában nem bocsát ki teszt tanúsítványt. A teszt tanúsítványok a külön az erre a célra létesített teszt gyökér hitelesítő központ hierarchiájában kerülnek kiadásra.

A teszt tanúsítványok megjelölése olyan módon történik, hogy a tanúsítványban feltüntetett hitelesítési rend objektumazonosító: 0.2.216.1.200.1100.100.42.3.999.

A teszt tanúsítványokhoz és azon alapuló elektronikus aláírásokhoz vagy bélyegzőkhöz semmilyen joghatás nem kapcsolódik.

1.4.1 Engedélyezett tanúsítvány használat

[ALA] A kibocsátott üzleti vagy személyes tanúsítványhoz kapcsolódó magánkulcs kizárólag elektronikus aláírások létrehozására, a tanúsítvánnyal hitelesített nyilvános kulcs kizárólag az elektronikus aláírások érvényesítésére használható.

[BÉLY] A kibocsátott szervezeti vagy eszköz tanúsítványhoz kapcsolódó magánkulcsok kizárólag elektronikus bélyegzők létrehozására, a tanúsítvánnyal hitelesített nyilvános kulcsok kizárólag az elektronikus bélyegzők érvényesítésére használhatók.

[ALA+QSCD] A kibocsátott üzleti vagy személyes tanúsítványok minősített elektronikus aláírást létrehozó eszköz (QSCD) használatát megkövetelő tanúsítványok.

[BÉLY+QSCD] A kibocsátott szervezeti vagy eszköz tanúsítványok minősített elektronikus bélyegzőt létrehozó eszköz (QSCD) használatát megkövetelő tanúsítványok.

A személyes tanúsítványokat az Alanyok csak és kizárólag az Előfizetőhöz kapcsolódó tevékenységükhöz (munkaviszonyukból fakadó feladataik elvégzéséhez) használhatják fel.

A fentieken túl, a kibocsátott tanúsítványok és kapcsolódó kulcspárok csak a {D1} Általános Szerződési Feltételekben, illetve a {D2} Szolgáltatási Szerződésben rögzített feltételekkel használhatók fel.

1.4.2 Tiltott tanúsítvány használat

Tilos a tanúsítványt, illetve a hozzá kapcsolódó kulcspárt felhasználni titkosításra vagy visszafejtésre, azonosításra, más tanúsítványok aláírására vagy bármilyen – Szolgáltatóval nem egyeztetett – bizalmi szolgáltatás nyújtásához.

Mind a személyes, mind pedig az üzleti, szervezeti és eszköz tanúsítványokat az Aláírók illetve Bélyegző létrehozók csak az Előfizetőhöz kapcsolódó tevékenységükhöz használhatják fel; a tanúsítványok bármilyen személyes célra történő felhasználása tilos.

1.5 Szabályzat adminisztráció

1.5.1 Szabályzatot karbantartó szervezet

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoportot működtet, amely többek között jelen bizalmi szolgáltatási szabályzat karbantartásáért is felelős.

1.5.2 Kapcsolat

Szolgáltató adatai

Cégjegyzék szám:	01-10-041633
Székhely:	1149 Budapest, Róna utca 52-80.
Levélcím:	1389 Budapest, Pf.: 133.
Telefon:	+36 1 459-4200
Fax:	+36 1 303-1000
Internetes honlap címe:	www.nisz.hu
Adatvédelmi és adatbiztonsági szabályzat:	A http://hiteles.gov.hu/szabalyzatok oldalon, az „Adatkezelési tájékoztató kormányzati hitelesítés-szolgáltatásokhoz” címen érhető el.

Ügyfélkapcsolati Iroda

Az ügyfelekkel való kapcsolattartás érdekében a Szolgáltató Ügyfélkapcsolati Irodát tart fenn, mely egyben a Szolgáltatásokért illetékes szervezeti egység, és amelyet az ügyfelek előzetes időpont-

egyeztetést követően személyesen, illetve telefonon a nyitvatartási időkben kereshetnek fel. A mindenkor nyitvatartási időket a Szolgáltató a Szolgáltatások internetes honlapján teszi közzé.

Cím: 1097 Budapest, Vaskapu utca 30/b.
Telefon: +36 1 795-7200
Email: info@hiteles.gov.hu
Szolgáltatások internetes honlapja: <http://hiteles.gov.hu>

Az elkészült tanúsítványok átadását és az ehhez kapcsolódó személyes azonosítást az Ügyfélkapcsolati Iroda a fenti cím mellett egy másik helyszínen, a 1054 Budapest, Kálmán Imre utca 2-4. címen is biztosítja (NISZ Pont).

Telefonos HelpDesk

A tanúsítványok felfüggesztésére és a Szolgáltatások nyújtásához felhasznált rendszerrel kapcsolatos műszaki hibák bejelentésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk) biztosít.

Telefon: +36 1 795-7300
Email: helpdesk@nisz.hu

Illetékes fogyasztóvédelmi felügyelőség

Budapest Főváros Kormányhivatala, Fogyasztóvédelmi Főosztály
Cím: 1051 Budapest, Sas u. 19.
Telefon: +36 1 450-2598
Email: fogyved_kmf_budapest@bfkh.gov.hu

Illetékes békéltető testület

Budapesti Békéltető Testület
Cím: 1016 Budapest, Krisztina krt. 99. I., em. 111.
Levelezési cím: 1253 Budapest, Pf.: 10.
Telefon: +36 1 488 2131
Email: bekelteto.testulet@bkik.hu

1.5.3 Szabályzat alkalmasságának meghatározása

A Szolgáltató legalább évente egyszer megvizsgálja a bizalmi szolgáltatási rend, illetve a szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit változtatási igényként figyelembe veszi.

A változtatási igényeket a Hitelesítési Rend és Szabályozási Csoport gyűjti, a módosításokat legalább évente egyszer elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

1.5.4 Szabályzat jóváhagyásának eljárása

Az ellenőrzésre, illetve jóváhagyásra a Szolgáltató belső szervezete, illetve a Szolgáltatásokért felelős vezetője rendelkezik hatáskörrel és felelősséggel.

A jóváhagyás előtt a Szolgáltató megvizsgálja a szolgáltatási szabályzat bizalmi szolgáltatási rendnek való megfelelését.

A szolgáltatási szabályzat jogszabályoknak való megfelelőségét a Bizalmi Felügyelet is ellenőrzi.

A jóváhagyott szolgáltatási szabályzat a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával kerül hitelesítésre.

A jóváhagyott szolgáltatási szabályzatot Szolgáltató vezetése lépteti hatályba. A hatályba lépés napját a dokumentum címlapja tartalmazza.

A szolgáltatási szabályzat új verziója mindig új verziószámmal kerül nyilvánosságra és közzétételre Szolgáltató internetes honlapján.

Az új verzió kötelező érvényű az összes Előfizetőre, továbbá az abban foglalt változásokat javasolt figyelembe vennie az összes, a bizalmi szolgáltatási rend előző verzióinak hatálya alatt kibocsátott tanúsítványokat használó Érintett Félnek.

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

A jelen szabályzatban használt fogalmak értelmezése megegyezik a Szolgáltatásokra vonatkozó jogszabályokban (1.6.3.1 fejezet) szereplő meghatározásokkal.

Az ezen felül alkalmazott fogalmak meghatározását a BR-MTT szabályzat 1.6.1 fejezete tartalmazza.

1.6.2 Rövidítések

CA	Certification Authority	hitelesítő központ
CRL	Certificate Revocation List	tanúsítvány visszavonási lista
CP	Certificate Policy	Hitelesítési Rend
CPS	Certification Practice Statement	Hitelesítési Szolgáltatás Szabályzat
ECC	Elliptic Curve Cryptography	elliptikus görbe alapú aláíró algoritmus
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
QSCD	Qualified Signature/Seal Creation Device	a {J1} eIDAS II. mellékletének megfelelő, minősített aláírást/bélyegzőt létrehozó eszköz
P12	PKCS#12	az {Sz14} szabványnak megfelelő, szoftveres kulcstároló
RA	Registration Authority	regisztrációs szervezet
RSA	Rivest–Shamir–Adleman	aláíró algoritmus
SHA	Secure Hash Algorithm	lenyomatképző algoritmus
UTC	Coordinated Universal Time	koordinált univerzális idő

1.6.3 Hivatkozások

1.6.3.1 *Jogszabályi hivatkozások*

- {J1} 910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (röviden: eIDAS)
- {J2} 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (továbbiakban: E-ügyintézési tv.)
- {J3} 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról (továbbiakban: Nytv.)
- {J4} 2016. évi CXXX. törvény a polgári perrendtartásról (röviden: Pp.)
- {J5} 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.)
- {J6} 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- {J7} 84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
- {J8} 24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- {J9} 137/2016 (VI. 13.) Korm. rendelet az elektronikus ügyintézés céljára felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről
- {J10} 679/2016/EU Európai Parlament és Tanács rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (továbbiakban: GDPR)

1.6.3.2 *Szabványok és műszaki-technikai specifikációk*

- | | | |
|-------|--------------|---|
| {Sz1} | RFC 3647 | Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework |
| {Sz2} | EN 319 401 | General policy requirements for Trust Service Providers |
| {Sz3} | EN 319 411-1 | Policy and security requirements for Trust Service Providers issuing Certificates; Part 1: General requirements |
| {Sz4} | EN 319 411-2 | Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates |
| {Sz5} | EN 319 412-1 | Certificate Profiles; Part 1: Overview and common data structures |
| {Sz6} | EN 319 412-2 | Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons |

{Sz7}	EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issues to legal persons
{Sz8}	EN 319 412-5	Certificate Profiles; Part 5: QCStatements
{Sz9}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz10}	ITU-T X.520	Information technology – Open Systems Interconnection – The Directory: Selected attribute types
{Sz11}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz12}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz13}	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
{Sz14}	PKCS#12	Personal Information Exchange Syntax Standard
{Sz15}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz16}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz17}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules

1.6.3.3 Hivatkozott dokumentumok

{D1}	ÁSZF-GOVCA	Általános Szerződési Feltételek a NISZ Zrt. kormányzati hitelesítés szolgáltatásaihoz
{D2}	SZSZ	Szolgáltatási Szerződés
{D3}		NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}		NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}		NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}		NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}		NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}		Tanúsítvány profilok a NISZ eIDAS rendelet szerinti bizalmi szolgáltatásaihoz
{D9}		Tanúsítvány megrendelő és regisztrációs űrlap
{D10}		Visszavonási kérelem űrlap

2 KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR

2.1 Tanúsítványtár

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott végfelhasználói és szolgáltatói tanúsítványok, a tanúsítványokkal kapcsolatos szabályzatok, a tanúsítványok visszavonási állapotára vonatkozó információk, valamint az egyéb közérdekű szolgáltatói információk az Előfizetők és Érintett Felek részére folyamatosan rendelkezésre álljanak. Szolgáltató az információk elérhetőségét az év minden napján, napi 24 órában, 99,9 %-os rendelkezésre állással biztosítja, úgy, hogy a kiesés nem lépheti túl esetenként a 3 órás időtartamot.

A Szolgáltató nem hozza nyilvánosságra azokat az érzékeny és/vagy bizalmas információkat tartalmazó dokumentációkat, melyek biztonsági intézkedéseket, eljárási szabályokat és belső biztonsági szabályzatokat tartalmaznak.

2.2 A szolgáltatói információ közzététele

A Szolgáltató a szolgáltatói tanúsítványokat, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat a Szolgáltatások internetes honlapján (<https://hiteles.gov.hu>) teszi közzé.

A Szolgáltató a végfelhasználói tanúsítványokat belső tanúsítványtárában tárolja, a kiadott tanúsítványt az Előfizető számára rendelkezésre bocsátja. A szolgáltató a végfelhasználói tanúsítványt a tanúsítvány alanya – szervezeti vagy eszköz tanúsítvány esetén az Előfizető – hozzájárulásával közzé teszi internetes honlapján nyilvánosan elérhető, kereshető tanúsítványtárában.

A Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítja. A visszavonási állapot információk közzétételével kapcsolatos információkat a 4.10 fejezet tartalmazza.

2.3 A közzététel gyakorisága

Szolgáltató a szolgáltatói tanúsítványokat legkésőbb azok éles üzembe helyezését megelőző 24 órán belül teszi közzé.

Szolgáltató a végfelhasználói tanúsítványokat a nyilvánosan kereshető tanúsítványtárban a tanúsítvány alany – szervezeti vagy eszköz tanúsítvány esetén az Előfizető- hozzájárulása esetén a kibocsátást követő 24 órán belül teszi közzé.

Szolgáltató a tanúsítványokkal kapcsolatos szabályzatokat azok változása esetén közzé teszi legalább 30 nappal a változás hatályba lépését megelőzően.

Szolgáltató a CRL-t legalább 24 óránként frissíti, azaz két egymást követő CRL kibocsátási között idő nem haladja meg a 24 órát. Amennyiben egy tanúsítvány állapota megváltozik, a Szolgáltató a változást követően haladéktalanul, de legfeljebb 1 órán belül új CRL-t állít elő és tesz közzé.

Szolgáltató az OCSP szolgáltatása keretében minden OCSP kérésre friss választ állít elő és ad vissza.

2.4 Hozzáférés-ellenőrzések

Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a szolgáltatói tanúsítványokhoz, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokhoz, a tanúsítványokkal kapcsolatos visszavonási információkhoz.

A végfelhasználói tanúsítványokkal kapcsolatban biztosítja a nyilvános tanúsítványtár kereshetőségét a tanúsítványban tárolt adatok alapján.

Szolgáltató biztonsági intézkedésekkel és eljárási szabályokkal gondoskodik az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.

A kibocsátott tanúsítványokkal kapcsolatos szabályzatoknak csak az elektronikus, aláírással vagy bélyegzővel ellátott formája tekinthető hitelesnek, a dokumentumok nyomtatott változatai semmilyen formában nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

3 AZONOSÍTÁS ÉS HITELESÍTÉS

3.1 Elnevezések

3.1.1 Név típusok

A tanúsítványban szereplő nevek megadása megfelel az {Sz10} ITU-T X.520 szabványnak. Ezen túl:

A tanúsítvány alanya (*Subject*) mező tartalma megfelel:

- üzleti vagy személyes tanúsítvány esetén: az {Sz6} EN 319 412-2 szabvány 4.2.4 fejezetében foglalt előírásoknak;
- szervezeti vagy eszköz tanúsítvány esetén: az {Sz7} EN 319 412-3 szabvány 4.2.1 fejezetében foglalt előírásoknak.

A tanúsítvány kibocsátója (*Issuer*) mező tartalma megfelel:

- az {Sz6} EN 319 412-2 szabvány 4.2.3.1 fejezetében foglalt előírásoknak.

3.1.2 Nevek jelentése

A tanúsítványban szereplő név attribútumok jelentése megegyezik az {Sz10} ITU-T X.520 szerintivel.

Ezen felül, az 1.4 fejezet szerinti tanúsítványtípusok *Subject* mezőjében szereplő név-attribútumokra a következő alfejezetekben megadott képzési és igazolási szabályok érvényesek.

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

3.1.2.1 Üzleti tanúsítvány alanyára vonatkozó képzési és igazolási szabályok

Üzleti tanúsítvány esetén mind az Aláíróra, mind az Előfizető szervezetére vonatkozó, a tanúsítványban feltüntetésre kerülő név-attribútumokat ellenőrizni és igazolni kell.

név-attribútum	leírás	igazolás / ellenőrzés módja
surname	Az Alany vezetéknéve, betű szerint azonos a személy azonosítására használt okmányban feltüntetett vezetéknévvel, amely egy vagy több családi nevet és egy vagy több előtagot (pl. „dr.” jelzést) tartalmazhat, egymástól szóköz karakterrel elválasztva. Nem álneves tanúsítványban kötelezően szerepel, álneves tanúsítványban nem szerepel.	Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolványban szereplő adat, közhiteles nyilvántartásban az egyezőség ellenőrzésével igazolt adat (*).
givenName	Az Alany utónéve, betű szerint azonos a személy azonosítására használt okmányban feltüntetett viselt utónévvel, amely egy vagy több keresztnévet tartalmazhat, egymástól szóköz karakterrel elválasztva. Nem álneves tanúsítványban kötelezően szerepel, álneves tanúsítványban nem szerepel.	Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolványban szereplő adat, közhiteles nyilvántartásban az egyezőség ellenőrzésével igazolt adat (*).
pseudonym	Az Alany álneve, ha annak megjelölésére az Alany igényt tart és azt számára Előfizető engedélyezte. Nem álneves tanúsítványban nem szerepel.	A tanúsítvány igénylésben megjelölt, a {D9} úrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.
commonName	Nem álneves tanúsítvány esetén a surname és givenName egymás után fűzése, egymástól szóköz karakterrel elválasztva.	Nem álneves tanúsítvány esetén az Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolványban

	Álneves tanúsítvány esetén az álnevet '~' (tilde) karakterekkel határolva tartalmazza.	szereplő, közhiteles nyilvántartásban az egyezőség ellenőrzésével igazolt adat (*). Álneves tanúsítvány esetén a tanúsítványigénylésben megjelölt, a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.
serialNumber	Szolgáltató által képzett, egyértelműséget biztosító, az Előfizetőhöz és/vagy az Alanyhoz rendelt egyedi azonosító, Szolgáltató ügyfélaazonosító rendszere által automatikusan képzett adat. Minden tanúsítványban kötelezően szerepel.	
title	Az Alany szervezetben viselt beosztása, ügyvédi illetve jogtanácsosi tanúsítvány esetén ezen titulus feltüntetése a kamarai azonosító számmal (KASZ) kiegészítve. Opcionális mező, akkor kerül feltüntetésre a tanúsítványban, ha Előfizető azt kérte.	Hivatalos szervezeti dokumentum (pl. cégkivonat) alapján ellenőrzött, vagy a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat. KASZ esetén a Magyar Ügyvédi Kamara közhiteles nyilvántartásában az egyezőség ellenőrzésével igazolt adat.
countryName	A szervezet székhelyének ország kódja. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött és igazolt adat.
localityName	A szervezet székhelyének helység neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött és igazolt adat.
organizationName	A szervezet hivatalos (teljes vagy rövid) neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött és igazolt adat.
organizationalUnitName	Szervezeti egység megjelölése, amelyhez az Alany tartozik. Opcionális, akkor kerül feltüntetésre a tanúsítványban, ha Előfizető azt megjelölni kérte.	A {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.
organizationIdentifier	A szervezet nyilvántartott azonosítója (adószáma). Kötelező.	Cégkivonat vagy ennek megfelelő okirat (pl. törzskönyvi kivonat) alapján igazolt adat.

(*): [KET] tanúsítvány esetén, ha a regisztráció az e-ügyintézkést biztosító állami szerv személyzeti nyilvántartásán alapulva történik (4.1.2.1.2.3 fejezet), akkor az adatok egyezőségének ellenőrzése a közhiteles nyilvántartásban a Szolgáltató feladata, kivéve, ha az Előfizetővel ezirányú szerződést kötöttek, és az ellenőrzés elvégzését Előfizető igazolni tudja.

Az Alany email címét a tanúsítvány `SubjectAlternativeName` kiterjesztése tartalmazza. Kötelező mező, a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.

3.1.2.2 Személyes tanúsítvány alanyára vonatkozó képzési és igazolási szabályok

Amennyiben az Előfizető a tanúsítvány megrendelésekor és/vagy a Szolgáltatási Szerződésben a szervezetére vonatkozó név-attribútumok tanúsítványba foglalását mellőzni kérte és Szolgáltató ezt elfogadta, akkor az Előfizetővel kapcsolatban álló természetes személy, mint Alany számára személyes tanúsítvány adható ki. A személyes tanúsítvány Előfizető szervezetére vonatkozó név-attribútumokat nem tartalmaz. A személyes tanúsítvány esetén az Aláíróra vonatkozó, a tanúsítványban feltüntetésre kerülő név-attribútumokat ellenőrizni és igazolni kell.

névattribútum	leírás	igazolás / ellenőrzés módja
surname	Az Alany vezetéknéve, betű szerint azonos a személy azonosítására használt okmányban feltüntetett vezetéknévvel, amely egy vagy	Nyvtv. szerinti személyazonosság igazolására alkalmas hatósági igazolványban szereplő adat,

	több családi neve és egy vagy több előtagot (pl. „dr.” jelzést) tartalmazhat, egymástól szóköz karakterrel elválasztva. Nem álneves tanúsítványban kötelezően szerepel, álneves tanúsítványban nem szerepel.	közhiteles nyilvántartásban az egyezőség ellenőrzésével igazolt adat.
givenName	Az Alany utóneve, betű szerint azonos a személy azonosítására használt okmányban feltüntetett viselt utónévvel, amely egy vagy több keresztnév és egy vagy több előtagot (pl. „dr.” jelzést) tartalmazhat, egymástól szóköz karakterrel elválasztva. Nem álneves tanúsítványban kötelezően szerepel, álneves tanúsítványban nem szerepel.	Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolványban szereplő adat, közhiteles nyilvántartásban az egyezőség ellenőrzésével igazolt adat.
pseudonym	Az Alany álneve, ha annak megjelölésére az Alany igényt tart és azt számára Előfizető engedélyezte. Nem álneves tanúsítványban nem szerepel.	A tanúsítvány igénylésben megjelölt, a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.
commonName	Nem álneves tanúsítvány esetén a surname és givenName egymás után fűzése, egymástól szóköz karakterrel elválasztva. Álneves tanúsítvány esetén az álnevet „~” (tilde) karakterekkel határolva tartalmazza.	Nem álneves tanúsítvány esetén az Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolványban szereplő, közhiteles nyilvántartásban az egyezőség ellenőrzésével igazolt adat. Álneves tanúsítvány esetén a tanúsítványigénylésben megjelölt, a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.
serialNumber	Szolgáltató által képzett, egyértelműséget biztosító, az Előfizetőhöz és/vagy az Alanyhoz rendelt egyedi azonosító, Szolgáltató ügyfélazonosító rendszere által automatikusan képzett adat. Minden tanúsítványban kötelezően szerepel.	
countryName	A személy lakcímének ország kódja. Kötelező.	Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolványban szereplő, közhiteles nyilvántartásban az egyezőség ellenőrzésével igazolt adat.
localityName	A személy lakcímének helység neve. Kötelező.	Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolványban szereplő, közhiteles nyilvántartásban az egyezőség ellenőrzésével igazolt adat.

Az Alany email címét a tanúsítvány SubjectAlternativeName kiterjesztése tartalmazza. Kötelező mező, a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.

3.1.2.3 Szervezeti tanúsítvány alanyára vonatkozó képzési és igazolási szabályok

Szervezeti tanúsítvány esetén az Előfizető szervezetére vonatkozó, a tanúsítványban feltüntetésre kerülő névtribútumokat ellenőrizni és igazolni kell.

névtribútum	leírás	igazolás / ellenőrzés módja
commonName	A szervezet hivatalos (teljes vagy rövid) neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött, igazolt adat.
serialNumber	Szolgáltató által képzett, egyértelműséget biztosító, az Előfizetőhöz és/vagy az Alanyhoz rendelt egyedi azonosító, Szolgáltató ügyfélazonosító rendszere által automatikusan képzett adat. Minden tanúsítványban kötelezően szerepel.	

countryName	A szervezet székhelyének ország kódja. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött, igazolt adat.
localityName	A szervezet székhelyének helység neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött, igazolt adat.
organizationName	A szervezet hivatalos (teljes vagy rövid) neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött, igazolt adat.
organizationalUnitName	A szervezeten belüli szervezeti egység megjelölése. Opcionális, akkor kerül feltüntetésre a tanúsítványban, ha Előfizető azt megjelölni kérte.	Igénylőlap írásos nyilatkozata alapján igazolt, nem ellenőrzött adat.
organizationIdentifier	A szervezet nyilvántartott azonosítója (adószáma). Kötelező.	Cégkivonat vagy ennek megfelelő okirat (pl. törzskönyvi kivonat) alapján igazolt adat.

Az Alany email címét a tanúsítvány `SubjectAlternativeName` kiterjesztése tartalmazza. Kötelező mező, a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.

3.1.2.4 **Eszköz tanúsítvány alanyára vonatkozó képzési és igazolási szabályok**

Eszköz tanúsítvány esetén az Előfizető szervezetére vonatkozó, a tanúsítványban feltüntetésre kerülő névattribútumokat ellenőrizni és igazolni kell.

névattribútum	leírás	igazolás / ellenőrzés módja
commonName	Előfizető által vagy nevében működtetett informatikai rendszer vagy eszköz megnevezése. Kötelező.	Igénylőlap írásos nyilatkozata alapján igazolt, nem ellenőrzött adat.
serialNumber	Szolgáltató által képzett, egyértelműséget biztosító, az Előfizetőhöz és/vagy az Alanyhoz rendelt egyedi azonosító, Szolgáltató ügyfélazonosító rendszere által automatikusan képzett adat. Minden tanúsítványban kötelezően szerepel.	
countryName	A szervezet székhelyének ország kódja. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött, igazolt adat.
localityName	A szervezet székhelyének helység neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött, igazolt adat.
organizationName	A szervezet hivatalos (teljes vagy rövid) neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat, cégkivonat) alapján ellenőrzött, igazolt adat.
organizationalUnitName	A szervezeten belüli szervezeti egység megjelölése. Opcionális, akkor kerül feltüntetésre a tanúsítványban, ha Előfizető azt megjelölni kérte.	Igénylőlap írásos nyilatkozata alapján igazolt adat.
organizationIdentifier	A szervezet nyilvántartott azonosítója (adószáma). Kötelező.	Cégkivonat vagy ennek megfelelő okirat (pl. törzskönyvi kivonat) alapján igazolt adat.

Az Alany email címét a tanúsítvány `SubjectAlternativeName` kiterjesztése tartalmazza. Kötelező mező, a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.

3.1.3 **Előfizetők névtelensége és álnév használata**

Az Előfizetők névtelensége nem megengedett.

A természetes személy Alanyok (Aláírók) számára kiadott tanúsítványokban Előfizető ezirányú rendelkezése esetén az álnév használata megengedett.

Az álneves tanúsítványok felismerhetőségére vonatkozó szabályok:

- az álnév a tanúsítvány `Subject / pseudonym` mezőjében szerepel; és
- a `Subject / commonName` mező az álnevet „~” (tilde) karakterekkel határolva tartalmazza.

3.1.4 Különböző név formák megjelenítési szabályai

A tanúsítványba foglalt megkülönböztető nevek (`Distinguished Name`) ASN.1 szintaxisa az {Sz8} RFC 5280 szerinti, megjelenítési szabályait az {Sz11} RFC 4514 adja meg.

3.1.5 A nevek egyedisége

A tanúsítvány alanyának (Aláíró vagy a Bélyegző Létrehozó) megkülönböztető nevét Szolgáltató úgy biztosítja, hogy tanúsítvány `Subject / serialNumber` mezőbe befoglal egy, az ügyfélszolgálati rendszere által automatikusan képzett – Előfizetőt és Alanyt azonosító – egyedi karaktersorozatot.

3.1.6 Márkanevek elismerése, hitelesítése és szerepe

A tanúsítvány megrendelésével, illetve a regisztrálással Előfizető kifejezi, hogy a tanúsítványba foglalt nevek, márkanév és védjegyek, egyéb adatok nem sértik harmadik fél jogait.

Szolgáltatónak nem kötelessége a márkanév és védjegyek jogos használatának ellenőrzése, nem vállal közvetítő vagy döntő szerepet az ilyen jellegű viták feloldásában.

Szolgáltató nem garantálja Előfizetők számára a védjegyek feltüntetését a tanúsítványban.

3.2 Kezdeti azonosítás

Szolgáltató a vonatkozó jogszabályoknak megfelelően végzi el Előfizető szervezeti azonosságának, a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személy képviseleti jogának, valamint Előfizető Kapcsolattartója és a természetes személy alanyok személyazonosságának ellenőrzését és igazolását.

A szervezeti azonosság igazolásához megfelelő hivatalos dokumentum (pl. hatályos létesítő okirat, törzskönyvi kivonat, 30 napnál nem régebbi cégkivonat) és aláírási címpéldány, aláírás minta elektronikus másolatának Szolgáltató részére történő eljuttatása, valamint az eredeti dokumentumok bemutatása szükséges.

Az Előfizető által kijelölt Kapcsolattartó azonosítását a személyazonosításra alkalmas hatósági igazolvány személyes bemutatásával kell elvégezni.

Szolgáltató a {J1} eIDAS 24. cikk rendelkezéseinek megfelelően, közvetlenül vagy harmadik fél révén, a nemzeti jogszabályokkal összhangban (vö. E-ügyintézési tv. 82. § (2) bekezdés) ellenőrzi annak a természetes vagy jogi személynek az azonosságát és – adott esetben – egyedi jellemzőit, akinek vagy amelynek a részére a tanúsítványt kibocsátja:

- a természetes személynek vagy a jogi személy képviseletre jogosult képviselőjének a személyes jelenléte útján; vagy
- távrol, olyan elektronikus azonosító eszköz használatával, amely tekintetében a minősített tanúsítvány kibocsátása előtt biztosították a természetes személynek vagy a jogi személy képviseletre jogosult képviselőjének személyes jelenlétét, és amely megfelel a 8. cikkben a „jelentős”, illetve a „magas” biztonsági szintre vonatkozóan meghatározott követelményeknek; vagy
- minősített elektronikus aláírás vagy minősített elektronikus bélyegző a) vagy b) ponttal összhangban kibocsátott tanúsítványával; vagy

- d) személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerek alkalmazásával. A biztonság egyenértékűségét megfelelőségértékelő szervezetnek kell igazolnia.

Megjegyzés: A c) pont esetében Szolgáltató csak az általa kiadott minősített tanúsítvány alapján tudja elvégezni az azonosítást.

[NKET] tanúsítványok esetében Szolgáltató a fenti eljárások közül az a) és c) pontokat alkalmazza a gyakorlatban.

[KET] E-ügyintézés célú tanúsítványok esetén Szolgáltató a fenti eljárások közül ugyancsak az a) és c) pontokat alkalmazza a gyakorlatban, de a {J9} 137/2016 rendelet előírásait is figyelembe véve:

- a) a 9. § szerint az igénylő személyesen megjelenik a regisztrációt végző szervezet előtt; vagy
- b) a 10. § szerint külső helyszíni ellenőrzéssel; vagy
- c) a 13. § szerint az ügyintézészt biztosító állami szerv személyzeti nyilvántartására alapozva; vagy
- d) ügyintézési célú bélyegző tanúsítvány esetén a 15. § szerint, az elektronikus ügyintézészt biztosító szerv nevében eljáró személy (Előfizető Kapcsolattartója) személyes jelenléte útján, illetve a közokiratba foglalt igénylés alapján.

Megjegyzés: Szolgáltató a {J9} 137/2016 rendelet 11. §-a szerinti feltételes regisztrációt nem alkalmazza.

3.2.1 A magánkulcs birtoklása

Szolgáltató meggyőződik arról, hogy az Alany (Aláíró vagy a Bélyegző Létrehozó) a tanúsítványhoz kapcsolódó magánkulcsot birtokolja:

- a) Amennyiben az igényelt tanúsítványhoz kapcsolódó kulcspárt Szolgáltató állította elő, akkor a magánkulcs a szoftveres kulcstároló eszköz vagy az aláírás- vagy bélyegző létrehozó eszköz és az ahhoz tartozó aktivizáló adat (PIN kód) átadásával kerül az Aláírónak vagy a Bélyegző Létrehozójának a birtokába.
- b) Amennyiben Előfizető az általa biztosított kulcspárhoz kéri a tanúsítvány kibocsátását, akkor a PKCS#10 formátumban kell közölnie Szolgáltatóval a magánkulcshoz tartozó, tanúsítványba foglalandó nyilvános kulcsot. Ez esetben Szolgáltató a PKCS#10 formátumú tanúsítványkérelemnél levő digitális aláírás ellenőrzésével győződik meg arról, hogy az Alany birtokolja a magánkulcsot.

3.2.2 A szervezeti azonosság hitelesítése

Az 1.4 fejezetben ismertetett üzleti-, szervezeti- és eszköz tanúsítványok kibocsátása előtt Szolgáltató ellenőrzi Előfizető szervezetének teljes nevét és egyedi azonosító adatát (adószámát vagy cégjegyzékszámát) valamint címadatait. Az adatok valóságát és hatályosságát közhiteles nyilvántartás alapján, vagy ha ilyen közhiteles nyilvántartás nincsen, az igényléshez bekért hivatalos dokumentum (pl. 30 napnál nem régebbi cégkivonat, létesítő okirat) alapján ellenőrzi.

A tanúsítvány kibocsátása előtt Szolgáltató ellenőrzi és igazolja a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személy képviseleti jogának fennállását, a tanúsítványba foglalt jogviszony meglétét, illetve adott esetben a Magyar Ügyvédi Kamaránál fennálló tagságot igazoló azonosító szám (KASZ) megfelelőségét, jogszabály, közhiteles nyilvántartás, létesítő okirat, vagy ezek hiányában meghatalmazás alapján. Szolgáltató rögzíti az ellenőrzés eredményét nyilvántartásában.

3.2.3 A személyazonosság hitelesítése

[NKET] Az 1.4 fejezetben ismertetett üzleti- vagy személyes tanúsítvány megrendelését megelőzően, a tanúsítvány alanya, mint természetes személy a {D9} tanúsítvány megrendelő és regisztrációs űrlapon megadott, a regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét az űrlapon saját kezű aláírásával vagy minősített elektronikus aláírásával igazolja.

[NKET] Szolgáltató a természetes személy alany, valamint a nem természetes személy alany (szervezet) kapcsolattartója személyazonosságát az Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolványa alapján ellenőrzi, és az igazolvány érvényességét, valamint az igazolványban foglalt adatok egyezését a megfelelő közhiteles hatósági nyilvántartásban is ellenőrzi. Amennyiben a természetes személy alany külföldi állampolgár és nem rendelkezik az Nytv. szerinti személyazonosító igazolvánnyal, akkor a Szolgáltató a külföldi útlevelének másolata alapján ellenőrzi az adatokat.

[KET] E-ügyintézés célú tanúsítványok esetén Szolgáltató a természetes személy alany személyazonosságának ellenőrzésekor az alábbiak szerint jár el:

- a) a {J9} 137/2016 rendelet 9. §-a szerint: az igénylő személyesen megjelenik a regisztrációt végző szervezet előtt, bemutatja a személyazonosság igazolására alkalmas hatósági igazolványát, Szolgáltató közhiteles hatósági nyilvántartásban ellenőrzi az igazolvány érvényességét és az igazolványban foglalt adatok egyezését; vagy
- b) a {J9} 137/2016 rendelet 10. §-a szerint: Szolgáltató az a) pont szerinti regisztrációt külső helyszínen folytatja le, azzal a megjegyzéssel, hogy a közhiteles hatósági nyilvántartásban való ellenőrzést Szolgáltató legkésőbb az aláírást létrehozó eszköz átadásáig lefolytatja; vagy
- c) a {J9} 137/2016 rendelet 13. §-a szerint: Szolgáltató ezirányú rendelkezést is tartalmazó szolgáltatási szerződést köt az e-ügyintézészt biztosító állami szervvel, és a regisztrációt az ügyintézészt biztosító állami szerv a saját személyzeti nyilvántartására alapozva folytatja le. Az adatok egyezőségének ellenőrzése a közhiteles nyilvántartásban a Szolgáltató feladata, kivéve, ha Előfizetővel ezirányú szerződést kötöttek, és az ellenőrzés elvégzését Előfizető igazolni tudja.

Megjegyzés: Szolgáltató a fenti a) és b) alpontok eljárásait együttesen is alkalmazhatja: az Előfizetővel megkötött Szolgáltatási Szerződés alapján az igénylő a személyes adatait (beleértve a személyazonosság igazolására alkalmas hatósági igazolvány típusát és számát) a {D9} tanúsítvány megrendelő és regisztrációs űrlap kitöltésével és aláírásával megküldi Szolgáltatónak, aki a közhiteles hatósági nyilvántartásban ellenőrzi az igénylő személyazonosságát, az igazolvány érvényességét és az igazolványban foglalt adatok egyezését; megfelelőség esetén elkészíti a tanúsítványt, illetve az elektronikus aláírást létrehozó eszközt. Ezt követően egyeztetett időpontban Szolgáltató elvégzi az igénylő személyes megjelenés alapú regisztrációját, vagy az a) pont szerint a saját Ügyfélkapcsolati Irodájában, vagy a b) pont szerint külső helyszínen (az e-ügyintézészt biztosító szerv telephelyén). Mindkét esetben a tanúsítvány, illetve az elektronikus aláírást létrehozó eszköz csak akkor kerül átadásra az igénylő részére, ha a személyazonosságát és adatait egyezőségét a Szolgáltató megállapította.

Amennyiben a természetes személy, valamint a nem természetes személy alany (szervezet) kapcsolattartója nem esik az Nytv. hatálya alá, így nem rendelkezik az Nytv. szerinti személyazonosításra alkalmas okmánnal, vagy azt jogszabály alapján nem használhatja fel ilyen esetben, abban az esetben a Szolgáltató személyazonosságát úti okmány alapján ellenőrizni.

3.2.4 Előfizető nem ellenőrzött adatai

Szolgáltató ellenőrzi és igazol minden, a tanúsítvány alany mezőjébe (Subject) kerülő adatot.

Az ellenőrzés és igazolás módszere:

- üzleti tanúsítvány esetén a 3.1.2.1 fejezetben;
- személyes tanúsítvány esetén a 3.1.2.2 fejezetben;
- szervezeti tanúsítvány esetén a 3.1.2.3 fejezetben;
- eszköz tanúsítvány esetén a 3.1.2.4 fejezetben

került ismertetésre.

A tanúsítvány egyéb mezőibe és kiterjesztésébe kerülő adatok tekintetében azok valódiságáról Előfizető Kapcsolattartója – üzleti és személyes tanúsítvány esetén a természetes személy alany is – írásban nyilatkozott a {D9} tanúsítvány megrendelő és regisztrációs űrlap kitöltésével és aláírásával.

3.2.5 Jogosultság ellenőrzése

Szolgáltató ellenőrzi, hogy a {D9} tanúsítvány megrendelő és regisztrációs űrlapot az arra jogosult személy – Előfizető Kapcsolattartója – írta alá.

Az egyes tanúsítvány alanyok tanúsítványra való jogosultságának elbírálása és ellenőrzése Előfizető döntésköre és felelőssége.

3.2.6 Együttműködési kritériumok

Szolgáltató a Szolgáltatások nyújtása során nem működik együtt más bizalmi szolgáltatókkal.

3.3 Azonosítás és hitelesítés kulcscsere esetén

A kulcscsere az a folyamat, melynek során az eredeti tanúsítványba foglalt változatlan adatokhoz, megegyező érvényességi időtartammal új nyilvános kulcs kerül hitelesítésre.

A Szolgáltató nem nyújt kulcscsere szolgáltatást.

A tanúsítvány kulcsának cseréjéhez Előfizető új tanúsítványt kell igényeljen, melynek eljárásrendjét a 4.1 fejezet ismerteti.

3.3.1 Azonosítás és hitelesítés érvényes tanúsítvány esetén

Nincs kikötés.

3.3.2 Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Nincs kikötés.

3.4 Azonosítás és hitelesítés visszavonási vagy felfüggesztési kérelem esetén

Visszavonási kérelem esetén

Visszavonási igényt az Ügyfélkapcsolati Iroda számára személyesen, papír alapon saját kezű aláírással ellátva, vagy legalább nem minősített (fokozott biztonságú) elektronikus aláírással ellátott dokumentumon lehet benyújtani az Előfizető Kapcsolattartója – vagy aláírás célú tanúsítvány esetén – az Aláíró által.

A minősített elektronikus aláírással ellátott dokumentum abban az esetben fogadható el, amennyiben az aláíró tanúsítvány a Szolgáltató által került kiadásra, illetve a visszavonás körülményei (oka) nem állnak összefüggésben a tanúsítvány megbízhatóságával (pl. kulcskompromittálódás, kriptográfiai paraméterek vagy a tanúsítvány egyéb műszaki tartalmának nem megfelelőse, vö. 4.9.1 Visszavonás körülményei).

Felfüggesztési kérelem esetén

Felfüggesztési kérelmet kizárólag telefonon keresztül fogad be a Szolgáltató, a Telefonos HelpDesk 1.5.2 fejezetben megadott elérhetőségén.

Az üzleti vagy személyes tanúsítvány felfüggesztését az Aláíró vagy Előfizető Kapcsolattartója kérheti.

A szervezeti- vagy eszköz tanúsítvány felfüggesztését Előfizető Kapcsolattartója kérheti.

A fentiek szerint, az Aláírónak vagy Előfizető Kapcsolattartójának azonosításához a hívás során be kell mondania személyes adatait, a felfüggesztendő tanúsítványnak a sorozatszámát, vagy a típusát, illetve kiadásának hónapját, majd a jogosultságának ellenőrzéséhez meg kell adnia a felfüggesztési jelszót.

4 A TANÚSÍTVÁNYOK ÉLETCIKLUSA

4.1 Tanúsítványigénylés

4.1.1 Ki nyújthat be tanúsítványigénylést

A tanúsítványigénylési kérelmeket Előfizető Kapcsolattartója nyújthatja be Szolgáltató részére.

4.1.2 Igénylési folyamat és felelősségek

A tanúsítványigénylés folyamata az alábbi:

- 1) Mielőtt Szolgáltató és Előfizető Szolgáltatási Szerződést kötnének a Szolgáltatások igénybe vételére, Szolgáltató tájékoztatja Előfizetőt az alábbiakról:
 - a) az elektronikus aláírás/bélyegző használati lehetőségeiről és jogszabályi feltételeiről;
 - b) az elektronikus aláírást/bélyegzőt létrehozó eszköz használatáról;
 - c) az elektronikus aláírás/bélyegző létrehozásához használt adat (magánkulcs) használatával kapcsolatos intézkedésekről, a magánkulcs védelméhez szükséges biztonsági intézkedésekről;
 - d) az Aláíró, a Bélyegző Létrehozó, és az aláírást/bélyegzőt ellenőrizni kívánó felek felelősségéről és kötelezettségeiről;
 - e) a tanúsítványok felfüggesztésének és visszavonásának lehetőségéről;
 - f) a tanúsítványok kibocsátásának körülményeiről;
 - g) a tanúsítvány érvényességéről, érvényességi idejének lejártáról;
 - h) a tanúsítvánnyal kapcsolatos tárgyi, időbeni, földrajzi vagy egyéb korlátozásokról;
 - i) a szolgáltatói nyilvános kulcsról;
 - j) a szolgáltatási szabályzat elérhetőségéről és tartalmáról.
- 2) Szerződéskötés előkészítése
 - a) Szolgáltató emailben megküldi Előfizető részére az igényléshez szükséges információkat és űrlapokat (pl. {D9}, Kapcsolattartó kijelölésére szolgáló meghatalmazás);
 - b) Előfizető előzetesen kitöltheti és aláírhatja az űrlapokat, és megküldheti Szolgáltató részére, a szükséges csatolmányokkal; ez történhet a szolgáltatási szerződés megkötését követően is
 - c) Szolgáltató elkészíti a szerződéstervezetet és megküldi Előfizető részére.
- 3) Szolgáltatási Szerződés megkötése
 - a) Szolgáltató és Előfizető írásbeli szerződést köt egymással;
 - b) Előfizető kapcsolattartót jelölhet meg, aki jogosult eljárni és aláírási joggal is rendelkezhet a tanúsítványokkal kapcsolatos ügyekben. Kijelölés esetén Előfizető a kapcsolattartó számára meghatalmazást állít ki, amely tartalmazza a kapcsolattartó személyes adatait és személyazonosításra alkalmas hatósági igazolványának számát, és amelyet cégszerű aláírásával lát el.
 - c) Előfizető – vagy a felek ezirányú megállapodása esetén Szolgáltató – tájékoztatja a leendő Aláírókat vagy Bélyegző Létrehozókat az 1) pontban felsoroltakról.

- 4) Regisztrációs eljárás lefolytatása a 4.1.2.1 fejezetben leírtak szerint
- 5) A sikeres regisztrációt követően az Ügyfélkapcsolati Iroda intézkedik a tanúsítványkérelem előállításáról és annak feldolgozásáról.

A Felek igénylési folyamattal kapcsolatos felelősségeit a 9.6 fejezet és annak alfejezetei tartalmazzák.

4.1.2.1 Regisztráció

4.1.2.1.1 Regisztráció [NKET] tanúsítvány esetén

- 1) Minden egyes tanúsítványhoz külön-külön kitöltésre és Előfizető Kapcsolattartója által aláírásra kerül egy {D9} tanúsítvány megrendelő és regisztrációs űrlap:
 - a) Az űrlap benyújtható papíralapon, személyesen az Ügyfélkapcsolati Irodában vagy postai úton az Szolgáltatónak címezve, Előfizető Kapcsolattartójának és az üzleti- vagy személyes tanúsítvány leendő alanyának saját kezű aláírásával ellátva. Az űrlapok aláírt és beszkenelt másolatát Előfizető Kapcsolattartója emailben is megküldheti Szolgáltató részére, a szerződés előkészítési fázisban. Ilyenkor az eredeti papír alapú példányok a későbbiekben (legkésőbb a tanúsítványok átadását megelőzően) kerülnek átadásra Szolgáltató részére.
 - b) Amennyiben az igényelt tanúsítvány típusa szervezeti vagy eszköz tanúsítvány, és Előfizető Kapcsolattartója már rendelkezik Szolgáltató által kiadott, minősített üzleti tanúsítvánnyal, vagy más bizalmi szolgáltatótól származó minősített tanúsítvánnyal, akkor az űrlapok elektronikus formában is benyújthatók az Ügyfélkapcsolati Iroda email címére címezve, Előfizető Kapcsolattartójának elektronikus aláírásával hitelesítve.
 - c) az űrlap kitöltésével és aláírásával Előfizető Kapcsolattartója, továbbá üzleti- és személyes tanúsítvány esetén a természetes személy alany is:
 - nyilatkozik az űrlapon megadott adatok valóságáról;
 - nyilatkozik a {D1} Általános Szerződési Feltételek, valamint a szolgáltatási szabályzat elfogadásáról;
 - hozzájárul ahhoz, hogy személyes adatait Szolgáltató kezelje;
 - hozzájárul ahhoz, hogy Szolgáltató a kibocsátott tanúsítványt a nyilvános tanúsítványtárban közzé tegye.
- 2) A kitöltött {D9} regisztrációs űrlapot, valamint csatolmányait (pl. létesítő okirat, aláírási címpéldány) a Szolgáltató Ügyfélkapcsolati Irodája ellenőrzi és szükség esetén hiánypótlást kér.

Hiánytalan igénylés esetén az Ügyfélkapcsolati Iroda a 3.2 fejezetben leírt módon és eljárásokkal elvégzi a szervezeti azonosság, illetve a személyazonosság ellenőrzését és igazolását, azzal, a kiegészítéssel, hogy amennyiben a természetes személy azonosításának megállapítására Szolgáltató az {J1} eIDAS 24. cikk 1) bekezdés a) pontját alkalmazza, akkor ezt legkésőbb tanúsítvány, illetve az aláírást létrehozó eszköz átadását megelőzően folytatja le.

4.1.2.1.2 Regisztráció [KET] tanúsítvány esetén

4.1.2.1.2.1 Személyes regisztráció [ALA+KET] tanúsítvány esetén

A {J9} 137/2016 rendelet 9. §-a szerint, az igénylő személyesen megjelenik az Ügyfélkapcsolati Irodán, bemutatja a személyazonosság igazolására alkalmas hatósági igazolványát. Szolgáltató közhiteles hatósági nyilvántartásban ellenőrzi az igazolvány érvényességét és az igazolványban foglalt adatok egyezőségét. A tanúsítvány csak akkor adható ki, ha az ellenőrzés eredményes volt.

Az Ügyfélkapcsolati Iroda munkatársa és/vagy az igénylő kitölti a {D9} tanúsítvány megrendelő és regisztrációs űrlapot az ellenőrzött adatokkal. A regisztráció és a személyazonosság ellenőrzése

alapjául szolgáló, rögzítendő adatok helyességét az igénylő nyilatkozatban, saját kezű aláírásával ellátva igazolja. Az Ügyfélkapcsolati Iroda munkatársa aláírásával igazolja, hogy a hatósági igazolványon szereplő arckép megfeleltethető az igénylő arcának és az igazolványban szereplő aláírás azonos a nyilatkozatot igazoló aláírásával.

Ha az aláírás létrehozásához használt adat vagy az aláírást létrehozó eszköz átadása nem a regisztrációt követően azonnal, ugyanazon helyszínen történik, akkor az adatok közhiteles nyilvántartással való egyezősége az átadást megelőzően ismételt ellenőrzésre kerül.

4.1.2.1.2.2 Helyszíni regisztráció [ALA+KET] tanúsítvány esetén

A {J9} 137/2016 rendelet 10. §-a szerint, az igénylő külső helyszínen (jellemzően az e-ügyintézt biztosító szerv telephelyén) jelenik meg az Ügyfélkapcsolati Iroda munkatársa előtt, bemutatja a személyazonosság igazolására alkalmas hatósági igazolványát.

Az Ügyfélkapcsolati Iroda munkatársa és/vagy az igénylő kitölti a {D9} tanúsítvány megrendelő és regisztrációs űrlapot. A regisztráció és a személyazonosság ellenőrzése alapjául szolgáló adatok helyességét az igénylő nyilatkozatban, saját kezű aláírásával ellátva igazolja. Az Ügyfélkapcsolati Iroda munkatársa aláírásával igazolja, hogy a hatósági igazolványban szereplő arckép megfeleltethető az igénylő arcának és az igazolványban szereplő aláírás azonos a nyilatkozatot igazoló aláírásával.

Az igazolvány érvényességének és az igazolványban foglalt adatok egyezőségének ellenőrzését az Ügyfélkapcsolati Iroda munkatársa a tanúsítvány kiadását megelőzően végzi el.

4.1.2.1.2.3 Ügyintézt biztosító állami szerv személyzeti nyilvántartásán alapuló regisztráció [ALA+KET] tanúsítvány esetén

A {J9} 137/2016 rendelet 13. §-a szerint, az ügyintézésben közreműködő személyek elektronikus aláíráshoz szükséges adatokkal, valamint eszközökkel történő ellátásához a regisztráció az ügyintézt biztosító állami szerv által, az ügyintézt biztosító szerv személyzeti nyilvántartására alapozva is lefolytatható. A személyazonosító adatok egyezőségének a közhiteles nyilvántartásban való ellenőrzése a Szolgáltató feladata, kivéve, ha Előfizetővel ezirányú szerződést kötöttek, és az ellenőrzés elvégzését Előfizető igazolni tudja.

Ekkor Szolgáltató és az ügyintézt biztosító állami szerv (Előfizető) a Szolgáltatási Szerződésben rögzítik a felek jogait és kötelezettségeit, különös tekintettel a regisztrációval és az aláírás létrehozásához használt adatok vagy az aláírás létrehozó eszközök és az aktivizáló adatok szétosztásával kapcsolatos tevékenység- és felelősség megosztására.

Az e-ügyintézt biztosító állami szerv és Szolgáltató ezirányú megállapodása esetén Szolgáltató egyedi űrlapot készít a regisztrációhoz és oktatásban részesíti Előfizető Kapcsolattartóját a kitöltéssel és az adategyeztetéssel kapcsolatos tudnivalókról.

Szolgáltató az Előfizető Kapcsolattartójáról átvett és hitelesített űrlapok alapján veszi nyilvántartásba a tanúsítványba foglalandó adatokat. A folyamat során Szolgáltató Előfizető Kapcsolattartójának személyazonosságát személyes jelenlét útján, a személyazonosság igazolására alkalmas igazolvány bemutatása alapján ellenőrzi.

4.1.2.1.2.4 Regisztráció [BÉLY+KET] tanúsítvány esetén

- 1) A regisztrációs eljárás során Előfizető Kapcsolattartója személyesen kell eljárjon. Szolgáltató az Előfizető Kapcsolattartójának személyazonosságát a személyazonosság igazolására alkalmas igazolvány bemutatása alapján ellenőrzi, valamint közhiteles nyilvántartásban ellenőrzi az igazolvány érvényességét és az igazolványban foglalt adatok egyezőségét.
- 2) Minden egyes tanúsítványhoz külön-külön kitöltésre és Előfizető Kapcsolattartója által aláírásra kerül egy {D9} tanúsítvány megrendelő és regisztrációs űrlap:

- a) az űrlap papíralapon, személyesen az Ügyfélkapcsolati Irodában nyújtható be, Előfizető Kapcsolattartójának az Ügyfélkapcsolati Iroda munkatársa előtt tett, saját kezű aláírásával ellátva;
- b) az űrlap kitöltésével és aláírásával Előfizető Kapcsolattartója:
- nyilatkozik az űrlapon megadott adatok helyességéről és valóságáról;
 - nyilatkozik a {D1} Általános Szerződési Feltételek, valamint a szolgáltatási szabályzat elfogadásáról;
 - hozzájárul ahhoz, hogy személyes adatait Szolgáltató kezelje;
 - hozzájárul ahhoz, hogy Szolgáltató a kibocsátott tanúsítványt a nyilvános tanúsítványtárban közzé tegye.
- c) az űrlapon az Ügyfélkapcsolati Iroda munkatársa aláírásával igazolja, hogy:
- az 1) pont szerinti ellenőrzés eredményes volt;
 - a hatósági igazolványon szereplő arckép megfeleltethető az igénylő (Előfizető Kapcsolattartója) arcának és igazolványban szereplő aláírás azonos a 2) a) pontban említett aláírással.
- 3) A kitöltött {D9} regisztrációs űrlapot, valamint csatolmányait (pl. létesítő okirat, aláírási címpéldány) a Szolgáltató Ügyfélkapcsolati Irodája ellenőrzi és szükség esetén hiánypótlást kér.
- Hiánytalan igénylés esetén az Ügyfélkapcsolati Iroda a 3.2 fejezetben leírt módon és eljárásokkal elvégzi a szervezeti azonosság ellenőrzését és igazolását.

4.2 Tanúsítványigénylés feldolgozása

4.2.1 Azonosítási és hitelesítési műveletek

A tanúsítványigénylés elfogadása előtt Szolgáltató a 3.2 fejezetben – továbbá a 4.1.2.1 vonatkozó alfejezeteiben – leírt módon elvégzi Előfizető Kapcsolattartójának, valamint a tanúsítvány alanyának azonosítását és hitelesítését, a kitöltött tanúsítvány megrendelő űrlap és csatolmányainak (pl. cégkivonat, létesítő okirat, törzskönyvi kivonat, aláírási címpéldány) a felhasználásával.

4.2.2 Tanúsítványigénylés elfogadása vagy visszautasítása

Szolgáltató elfogadja a tanúsítványigénylést akkor, ha az űrlapon megadott, illetve a tanúsítvány alanyának megkülönböztető nevébe (Subject) kerülő valamennyi adat ellenőrzése és igazolása sikeres volt.

Az ellenőrzés és igazolás módszere:

- üzleti tanúsítvány esetén a 3.1.2.1 fejezetben;
- személyes tanúsítvány esetén a 3.1.2.2 fejezetben;
- szervezeti tanúsítvány esetén a 3.1.2.3 fejezetben;
- eszköz tanúsítvány esetén a 3.1.2.4 fejezetben

került ismertetésre.

Elfogadás esetén a Szolgáltató és az Előfizető Szolgáltatási Szerződést köt.

Szolgáltató visszautasítja a tanúsítványigénylés elfogadását:

- hiányos vagy nem megfelelően kitöltött űrlap esetén;

- ha úgy ítéli meg, hogy az igényelt tanúsítvány valamely jogszabály (különösen a {J6} 451/2016 és {J7} 84/2012) vonatkozó rendelkezése miatt nem adható ki;
- ha a személyazonosító adatokkal, az okmányok személyhez tartozásával, eredetiségével, valódiságával kapcsolatban kétség merül fel;
- ha a szervezeti azonosság, a képviseleti jog, a szervezethez való tartozás igazolására bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel;
- az esetlegesen kért álnév egyes személyeket vagy csoportokat esetlegesen sért (pl. jó ízlést, szemérmét, etnikai hovatartozást).

4.2.3 Tanúsítványigénylés feldolgozás időtartama

Szolgáltató a tanúsítványigényléseket a benyújtást követően a Szolgáltatási Szerződésben rögzített időtartamon belül, ennek hiányában a {D1} Általános Szerződési Feltételekben jelzett 15 naptári napon belül dönt a 4.2.2.-ben foglaltakról.

4.3 Tanúsítvány kibocsátás

4.3.1 Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

Szolgáltatási Szerződés megléte esetén, illetve megkötését követően az Ügyfélkapcsolati Iroda továbbítja az elfogadott tanúsítványigénylésen alapuló kérelmet a Regisztrációs Irodának.

A Regisztrációs Iroda:

- ha Előfizető az általa biztosított kulcspárhoz kéri a tanúsítvány kibocsátását, akkor ellenőrzi a PKCS#10 formátumú tanúsítványkérelem olvashatóságát és feldolgozhatóságát, az azon elhelyezett digitális aláírást, valamint azt, hogy a kulcspár hossza és algoritmusai megfelelő-e (6.1.5 és 6.1.6 fejezet);
- a Szolgáltatásokat támogató informatikai rendszerben elindítja a tanúsítvány létrehozását, melynek során – abban az esetben, ha Előfizető kulcspárját Szolgáltató kell előállítsa – a kulcspár generálása a 6.1.6 fejezetben leírt módon történik meg;
- értesíti az Ügyfélkapcsolati Irodát a tanúsítvány elkészültéről.

4.3.2 Előfizető értesítése a tanúsítvány kibocsátásáról

4.3.2.1 Előfizető értesítése az [NKET] tanúsítvány kibocsátásáról

A Regisztrációs Iroda emailben vagy telefonon értesíti Előfizető Kapcsolattartóját – és/vagy aláírás célú tanúsítvány esetén az Aláíró – a tanúsítvány elkészültéről, és egyeztetnek az elkészült tanúsítvány átvételének módjáról és időpontjáról.

Az átvétel történhet az Ügyfélkapcsolati Iroda helyszínén, vagy az Előfizető helyszínén.

Az aláírás célú tanúsítvány esetén az Aláíró, a bélyegzés célú tanúsítvány esetén az Előfizető Kapcsolattartója az átvétel során átveszi:

- a {D9} Tanúsítvány megrendelő és regisztrációs űrlap Szolgáltató ügyfélkapcsolati munkatársa által aláírt példányát, kivéve, ha az eredetileg elektronikusan került aláírásra és beküldésre az Ügyfélkapcsolati Iroda számára;
- a tanúsítványt;
- a felfüggesztési jelszót tartalmazó lezárt borítékot;

- opcionálisan a megrendelt aláírás- vagy bélyegző létrehozó eszközt és az ahhoz tartozó PIN és PUK kódot tartalmazó lezárt borítékot; vagy a tanúsítványt és magánkulcsot tartalmazó PKCS#12 formátumnak megfelelő (szoftveres) kulcstárolót (CD adathordozón) és az ahhoz tartozó PIN kódot tartalmazó lezárt borítékot.

Az átvételről „Átvételi elismervény és tanúsítvány elfogadás” bizonylat készül, melynek aláírásával az átvevő személy elismeri a tanúsítvány átvételét és elfogadását, valamint az ahhoz kapcsolódó, fent részletezett borítékok és eszközök átvételét. Az Ügyfélkapcsolati Iroda munkatársa aláírásával igazolja, hogy az átvevő személyazonosságát ellenőrizte és az átvételre való jogosultságot megállapította. Szolgáltató naplózza, hogy az elektronikus aláírás vagy bélyegző létrehozásához használt adatot mikor adta át az arra jogosultnak.

4.3.2.2 Előfizető értesítése a [KET] tanúsítvány kibocsátásáról

4.3.2.2.1 Előfizető értesítése a személyes regisztrációval kiadott [ALA+KET] tanúsítvány kibocsátásáról

Az ügyfélkapcsolati Iroda emailben vagy telefonon értesíti az Aláíró, illetve Előfizető Kapcsolattartóját a tanúsítvány elkészültéről és egyeztetnek az elkészült tanúsítvány átvételének módjáról és időpontjáról.

Az átvétel történhet az Ügyfélkapcsolati Iroda helyszínén vagy az Előfizető helyszínén.

Az Aláíró vagy meghatalmazottja az átvétel során átveszi:

- a {D9} Tanúsítvány megrendelő és regisztrációs űrlap Szolgáltató ügyfélkapcsolati munkatársa által aláírt példányát;
- a tanúsítványt;
- a felfüggesztési jelszót tartalmazó lezárt borítékot;
- amennyiben a tanúsítványhoz kapcsolódó kulcspárt Szolgáltató állította elő, akkor:
 - a megrendelt aláírás- vagy bélyegző létrehozó eszközt és az ahhoz tartozó PIN és PUK kódot tartalmazó lezárt borítékot; vagy
 - a tanúsítványt és magánkulcsot tartalmazó PKCS#12 formátumnak megfelelő (szoftveres) kulcstárolót (CD adathordozón) és az ahhoz tartozó PIN kódot tartalmazó lezárt borítékot.

Ha az átvevő nem Aláíró személyesen, hanem annak meghatalmazottja, akkor az Ügyfélkapcsolati Iroda munkatársa az átvevő személyazonosságát az általa bemutatott hatósági igazolvány alapján ellenőrzi, továbbá közhiteles nyilvántartásban ellenőrzi az igazolvány érvényességét és az igazolványban foglalt adatok egyezőségét.

Az átvételről „Átvételi elismervény és tanúsítvány elfogadás” bizonylat készül, melynek aláírásával az átvevő személy elismeri a tanúsítvány átvételét és elfogadását, valamint az ahhoz kapcsolódó, fent részletezett borítékok és eszközök átvételét. Az Ügyfélkapcsolati Iroda munkatársa aláírásával igazolja, hogy az átvevő személyazonosságát ellenőrizte és az átvételre való jogosultságot megállapította. Szolgáltató naplózza, hogy az elektronikus aláírás létrehozásához használt adatot mikor adta át az arra jogosultnak.

4.3.2.2.2 Előfizető értesítése a helyszíni regisztrációval kiadott [ALA+KET] tanúsítvány kibocsátásáról

Az eljárás azonos a 4.3.2.2.1 fejezetben leírtakkal, azzal a különbséggel, hogy az Ügyfélkapcsolati Iroda munkatársa az Aláíró hatósági igazolványának közhiteles nyilvántartásban való ellenőrzését az aláírás létrehozásához használt adat vagy aláírás létrehozó eszköz átadását megelőzően végzi el.

4.3.2.2.3 Előfizető értesítése az ügyintézését biztosító állami szerv személyzeti nyilvántartásán alapuló regisztrációval kiadott [ALA+KET] tanúsítvány kibocsátásáról

Az Ügyfélkapcsolati Iroda írásban (emailben) értesíti Előfizető Kapcsolattartóját a tanúsítvány elkészültéről, és egyeztetni az elkészült tanúsítványok átvételének módját és időpontját.

Az átvétel történhet az Ügyfélkapcsolati Iroda helyszínén, vagy az Előfizető helyszínén.

Az átvétel előtt az Ügyfélkapcsolati Iroda munkatársa az átvevő (Előfizető Kapcsolattartója) személyazonosságát az általa bemutatott hatósági igazolvány alapján ellenőrzi.

Az Előfizető Kapcsolattartója az átvétel során átveszi:

- a tanúsítványt;
- a felfüggesztési jelszót tartalmazó lezárt borítékot;
- amennyiben a tanúsítványhoz kapcsolódó kulcspárt Szolgáltató állította elő, akkor:
 - a megrendelt aláírás- vagy bélyegző létrehozó eszközt és az ahhoz tartozó PIN és PUK kódot tartalmazó lezárt borítékot; vagy
 - a tanúsítványt és magánkulcsot tartalmazó PKCS#12 formátumnak megfelelő (szoftveres) kulcstárolót (CD adathordozón) és az ahhoz tartozó PIN kódot tartalmazó lezárt borítékot.

Az átvételről „Átvételi elismervény és tanúsítvány elfogadás” bizonylat készül, melynek aláírásával az átvevő személy elismeri a tanúsítvány átvételét és elfogadását, valamint az ahhoz kapcsolódó, fent részletezett borítékok és eszközök átvételét. Az Ügyfélkapcsolati Iroda munkatársa aláírásával igazolja, hogy az átvevő személyazonosságát ellenőrizte és az átvételre való jogosultságot megállapította. Szolgáltató naplózza, hogy az elektronikus aláírás létrehozásához használt adatot mikor adta át az arra jogosultnak.

Az átvétel elmaradása esetén az ügyintézését biztosító szervet ismételten fel kell hívni az átvételre. Ha a kézbesítés a felhívást követő 30 napon belül nem történik meg, akkor Szolgáltató a tanúsítványokat visszavonja.

4.3.2.2.4 Előfizető értesítése a [BÉLY+KET] tanúsítvány kibocsátásáról

Az Ügyfélkapcsolati Iroda írásban (emailben) értesíti Előfizető Kapcsolattartóját a tanúsítvány elkészültéről, és egyeztetni az elkészült tanúsítványok átvételének módját és időpontját.

Az átvétel történhet az Ügyfélkapcsolati Iroda helyszínén vagy az Előfizető helyszínén.

Az átvétel előtt az Ügyfélkapcsolati Iroda munkatársa az átvevő (Előfizető Kapcsolattartója) személyazonosságát az általa bemutatott hatósági igazolvány alapján ellenőrzi.

Az Előfizető Kapcsolattartója az átvétel során átveszi:

- a tanúsítványt;
- a felfüggesztési jelszót tartalmazó lezárt borítékot;
- amennyiben a tanúsítványhoz kapcsolódó kulcspárt Szolgáltató állította elő, akkor:
 - a megrendelt aláírás- vagy bélyegző létrehozó eszközt és az ahhoz tartozó PIN és PUK kódot tartalmazó lezárt borítékot; vagy
 - a tanúsítványt és magánkulcsot tartalmazó PKCS#12 formátumnak megfelelő (szoftveres) kulcstárolót (CD adathordozón) és az ahhoz tartozó PIN kódot tartalmazó lezárt borítékot.

Az átvételről „Átvételi elismervény és tanúsítvány elfogadás” bizonylat készül, melynek aláírásával az átvevő személy elismeri a tanúsítvány átvételét és elfogadását, valamint az ahhoz kapcsolódó, fent részletezett borítékok és eszközök átvételét. Az Ügyfélkapcsolati Iroda munkatársa aláírásával igazolja, hogy az átvevő személyazonosságát ellenőrizte és az átvételre való jogosultságot megállapította. Szolgáltató naplózza, hogy az elektronikus bélyegző létrehozásához használt adatot mikor adta át az arra jogosultnak.

Az átvétel elmaradása esetén az ügyintézészt biztosító szervet ismételtten fel kell hívni az átvételre, ennek eredménytelensége esetén Szolgáltató a tanúsítványt visszavonja.

4.4 Tanúsítvány-elfogadás

4.4.1 Tanúsítvány Előfizető általi elfogadása

A 4.3.2 megfelelő alfejezeteiben említett „Átvételi elismervény és tanúsítvány elfogadás” bizonylat kinyomtatva tartalmazza a kibocsátott tanúsítvány adatait és a tanúsítványba foglalt adatokat.

A tanúsítványt átvevő személy (bélyegző tanúsítvány esetén Előfizető Kapcsolattartója, aláírás célú tanúsítvány esetén az Aláíró vagy [KET] esetén a meghatalmazott) ez alapján ellenőrzi és aláírásával igazolja, hogy a tanúsítványba foglalt adatok megegyeznek a tanúsítvány megrendelő és regisztrációs űrlapon szereplő adatokkal, a kibocsátott tanúsítványt elfogadja. Ezen felül, az Alany (az Aláírónak vagy a Bélyegző Létrehozójának) kötelezettsége, hogy a tanúsítványhoz kapcsolódó magánkulcs első használatát megelőzően, a tanúsítványba foglalt adatokat ellenőrizze, eltérés esetén haladéktalanul intézkedjen a tanúsítvány visszavonásáról.

Ha a kiadott tanúsítványban szereplő adatok nem egyeznek meg {D9} Tanúsítvány megrendelő és regisztrációs űrlapon szereplő adatokkal vagy nem felelnek meg a valóságnak, akkor a tanúsítvány nem kerül átadásra, és a Szolgáltató a tanúsítványt haladéktalanul visszavonja.

Ha a tanúsítvány átvételére nem került sor a Regisztrációs Iroda általi automatikus értesítéstől számított 60 napon belül, akkor Szolgáltató a tanúsítványt visszavonja.

4.4.2 Tanúsítvány közzététele

Az Előfizető – valamint az üzleti- és személyes tanúsítványok esetén az Aláíró – írásos hozzájárulása esetén Szolgáltató a kibocsátott tanúsítványt haladéktalanul közzé teszi a Szolgáltatások internetes honlapján elérhető nyilvános tanúsítványtárban.

4.4.3 További felek értesítése a tanúsítvány kibocsátásáról

Nincs kikötés.

4.5 A kulcspár és a tanúsítvány használata

4.5.1 Az Előfizető magánkulcs- és tanúsítvány használata

Az Alany (az Aláíró vagy a Bélyegző Létrehozó) csak azt követően használhatja a tanúsítványt és a kapcsolódó magánkulcsot, hogy a tanúsítványban foglalt adatok helyességéről meggyőződött.

Az Alany csak az 1.4.1 fejezetben ismertetett célokra és módon használhatja a magánkulcsot és a tanúsítványt.

Az Alany a magánkulcs és tanúsítvány használata során be kell tartania a 9.6.3 fejezetben ismertetett kötelezettségeit, különösen gondoskodnia kell az aláírás- vagy bélyegző létrehozó eszköz és az aktivizáló adat (PIN kód) illetéktelen hozzáférés elleni védelméről.

4.5.2 Az Érintett felek nyilvános kulcs- és tanúsítvány használata

A jelen szabályzat hatálya alatt kibocsátott tanúsítványon alapuló elektronikus aláírás vagy bélyegző elfogadása során szükséges, hogy az Érintett Fél megfelelő körültekintéssel és gondossággal járjon el, melyhez javasolt betartania az alábbi ajánlásokat:

- a tanúsítványok, valamint az elektronikus aláírások vagy bélyegzők ellenőrzését olyan megbízható alkalmazással végezze, amely megfelel a jelen szolgáltatási szabályzat 1.6.3.1 fejezetében felsorolt jogszabályoknak és amely képes az 1.6.3.2 fejezetben megadott műszaki szabványok támogatására és azokat helyesen valósítja meg;
- az előző pontban említett aláírás / bélyegző ellenőrző alkalmazást megbízható, vírusmentes környezetben használja, továbbá az alkalmazás beállítási lehetőségei helyesen legyenek konfigurálva;
- a tanúsítványokat csak olyan alkalmazásokban fogadja el, melyek összhangban vannak a tanúsítvány „kulcshasználat” (`KeyUsage`) és „kiterjesztett kulcshasználat” (`ExtendedKeyUsage`) kiterjesztésének tartalmával;
- végezze el a tanúsítványra az {Sz9} RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítést, valamint visszavonás ellenőrzést, a tanúsítványt, illetve az ezen alapuló elektronikus aláírást vagy bélyegzőt csak ezen ellenőrzések pozitív eredménye esetén fogadja el;
- vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítvány által hivatkozott szabályzatokban szerepel, különös tekintettel a tanúsítvánnyal egy alkalommal vállalható kötelezettségvállalás mértékére (tranzakciós limit, azaz a `QcStatements` kiterjesztésben a `QcLimitValue` mező értéke), mivel az ezen összehatárt meghaladó ügyletekben létrehozott és aláírt vagy bélyegzett elektronikus dokumentumokból származó követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.

Szolgáltató nem vállal felelősséget azokért a károkért, melyek abból adódnak, hogy az Érintett Fél nem a fenti ajánlásokban leírtak szerint jár el.

4.6 Tanúsítványok megújítása

Az irányadó szabvány ({Sz1} RFC 3647) szerint tanúsítványmegújítás az a folyamat, amikor az eredeti tanúsítványba foglalt változatlan adatokhoz új érvényességi időtartamra kerül hitelesítésre az Aláíró vagy Bélyegző Létrehozó változatlan nyilvános kulcsa.

A Szolgáltató nem nyújt tanúsítványmegújítás szolgáltatást, kivéve azon eseteket, amelyről a Szolgáltató külön megállapodott az Előfizetővel

Egyéb esetben ha a tanúsítvány lejár, de a szolgáltatásra továbbra is szükség van, Előfizető új tanúsítványt kell igényeljen, melynek eljárásrendjét a 4.1 fejezet ismerteti. Szolgáltató a lejárat előtt 30 nappal értesítést küld Előfizetőnek, a {D9} tanúsítvány megrendelő és regisztrációs űrlapon megadott email címre.

4.6.1 Tanúsítvány megújítás körülményei

Tanúsítványmegújítás akkor kezdeményezhető, ha

- a Szolgáltató erről külön megállapodott az Előfizetővel
- a megújítandó tanúsítvány érvényes
- a megújítandó tanúsítvány érvényességi idejéből kevesebb mint 60 nap van hátra
- a megújítandó tanúsítvány alanyadatai nem változtak.

4.6.2 Ki kérelmezhet tanúsítvány megújítást

Lásd 4.1.1, egyéb kikötés nincs.

4.6.3 Tanúsítvány megújítási kérelmek feldolgozása

Lásd 4.2, egyéb kikötés nincs.

4.6.4 Előfizető értesítése a megújított tanúsítvány kibocsátásáról

Lásd 4.3.2, egyéb kikötés nincs.

4.6.5 Tanúsítvány Előfizető általi elfogadása

Lásd 4.4, egyéb kikötés nincs.

4.6.6 Megújított tanúsítvány közzététele

Lásd 4.4.2, egyéb kikötés nincs.

4.6.7 További felek értesítése tanúsítvány megújításról

Lásd 4.4.3, egyéb kikötés nincs.

4.7 Kulcscsere

A kulcscsere az a folyamat, melynek során az eredeti tanúsítványba foglalt változatlan adatokhoz, megegyező érvényességi időtartammal új nyilvános kulcs kerül hitelesítésre.

A Szolgáltató nem nyújt kulcscsere szolgáltatást.

A tanúsítvány kulcsának cseréjéhez Előfizető új tanúsítványt kell igényeljen, melynek eljárásrendjét a 4.1 fejezet ismerteti.

4.7.1 Kulcscsere körülményei

Nincs kikötés.

4.7.2 Ki kérelmezhet kulcscserét

Nincs kikötés.

4.7.3 Kulcscsere kérelmek feldolgozása

Nincs kikötés.

4.7.4 Előfizető értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.7.5 Új tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.7.6 Új tanúsítvány közzététele

Nincs kikötés.

4.7.7 További felek értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.8 Tanúsítvány-módosítás

A tanúsítvány módosítása az a folyamat, melynek során az eredeti tanúsítvánnyal hitelesített nyilvános kulcshoz, de megváltozott (pl. név, szervezeti egység) adatokkal új tanúsítvány kerül kiadásra.

A Szolgáltató nem nyújt tanúsítvány-módosítás szolgáltatást.

A tanúsítványba foglalt adatok változása esetén Előfizetőnek új tanúsítványt kell igényelnie (4.1 fejezet) és intézkednie kell a meglévő tanúsítvány visszavonásáról.

4.8.1 Tanúsítvány-módosítás körülményei

Nincs kikötés.

4.8.2 Ki kérelmezhet tanúsítvány-módosítást

Nincs kikötés.

4.8.3 Tanúsítvány-módosítási kérelmek feldolgozása

Nincs kikötés.

4.8.4 Előfizető értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.8.5 Módosított tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.8.6 Módosított tanúsítvány közzététele

Nincs kikötés.

4.8.7 További felek értesítése a módosított tanúsítvány kibocsátásáról

Nincs kikötés.

4.9 Tanúsítvány visszavonás és felfüggesztése

A tanúsítvány visszavonása a tanúsítvány érvényességének a tervezett érvényességi idő lejárat előtti megszüntetését jelenti. A visszavonás végleges és visszafordíthatatlan állapot.

Felfüggesztés esetén a tanúsítvány csak rövid, átmeneti időszakra lesz érvénytelen. A tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam után (4.9.16) állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni.

A visszavont / felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

A visszavont tanúsítványhoz tartozó magánkulcs használatát azonnal be kell szüntetni. A visszavonási kérelemnek a Szolgáltatóhoz történő megérkezéséig az Aláíró / Bélyegző Létrehozó felelős a felmerült károkért. A visszavonási kérelem elfogadásától, a visszavonás tényének közzétételéig a Szolgáltató felelős a felmerülő károkért. Ez alól kivételt képez a bizonyíthatóan csalárd szándékkal történt visszavonás kérés, amely esetben a felmerült károkért a Szolgáltató nem vállal felelősséget. A visszavonás tényének közzététele után az Érintett Fél felelős a felmerülő károkért.

Az Érintett Feleknek javasolt ellenőrizniük a tanúsítvány visszavonási állapotát a tanúsítványon alapuló elektronikus aláírás vagy bélyegző elfogadása előtt.

4.9.1 Visszavonás körülményei

Szolgáltató visszavonja a tanúsítványt, ha:

- Előfizető Kapcsolattartója vagy Aláíró ezt kéri;
 - fennáll az a lehetőség vagy gyanú, hogy a tanúsítványhoz tartozó magánkulcs kompromittálódott;
 - adatváltozás vagy egyéb ok miatt.
- a felfüggesztett tanúsítvány újra-érvényesítése nem történik meg 4.9.16 fejezet szerinti, felfüggesztésre megengedett időtartamon belül;
- a tanúsítvány átvételére nem került sor a Regisztrációs Iroda általi értesítéstől számított 60 napon belül;
- Szolgáltató a Szolgáltatásokkal kapcsolatos rendellenességről szerez tudomást;
- Szolgáltató tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak – illetve a bizalmi szolgáltatási rendnek, amely hatálya alatt a tanúsítvány kibocsátásra került -, vagy a tanúsítványt jogellenesen használták, vagy a Szolgáltató által biztosított aláírás / bélyegző létrehozó eszközt jogosulatlan személy használhatta;
- a Bizalmi Felügyelet jogerős és végrehajtható határozatában elrendeli a visszavonást;
- a visszavonást jogszabály kötelezővé teszi;
- Szolgáltató a tevékenységét befejezi;
- a tanúsítvány formátuma vagy műszaki tartalma (pl. kriptográfiai algoritmus vagy kulcsméret már nem biztonságos) elfogadhatatlan kockázatot jelent az Érintett Felek részére;
- a tanúsítványban felhasznált kriptográfiai algoritmus, kulcshossz, azok paraméterei már nem biztosítják az Alany és a nyilvános kulcs hiteles összekapcsolását a tanúsítvány érvényességének hátralevő időszakára.

4.9.2 Ki kezdeményezheti a visszavonást

Visszavonást kezdeményezheti a 4.9.1 fejezetben megjelölt esetekben:

- Előfizető Kapcsolattartója vagy Aláíró;
- Szolgáltató (ide értve azt az esetet is, amikor a visszavonás a Bizalmi Felügyelet határozata vagy jogszabályi előírás miatt történik).

4.9.3 Visszavonási kérelemre vonatkozó eljárás

A visszavonási kérelem érvényes, minősített, vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírással ellátott dokumentum esetén e-mailben; vagy kézi aláírással ellátott dokumentum esetén személyesen illetve postai úton nyújtható be a Szolgáltató Ügyfélkapcsolati Irodájához, az erre a célra rendszeresített űrlap – {D10} Visszavonási kérelem – kitöltésével és aláírásával.

A visszavonási kérelem kitöltéséhez, illetve teljesítéséhez a következő adatok szükségesek:

- a tanúsítvány alanyának neve (CN érték),
- a tanúsítvány sorozatszáma,
- visszavonást kérő személy azonosító adatai;
- visszavonás oka, az ahhoz vezető körülmények.

Az Aláíró abban az esetben kérheti tanúsítványának visszavonását elektronikus aláírt {D10} Visszavonási kérelmen, amennyiben a visszavonás indoka nem az adott magánkulcs kompromitálódására vezethető vissza.

Szolgáltató azonosítja a visszavonást kérő személyét és elbírálja, hogy jogosult-e a tanúsítvány visszavonását kérni, továbbá megvizsgálja a beérkezett kérelmet alaki-formai, illetve tartalmi szempontból. Amennyiben a Szolgáltató az előzőekben felsoroltak valamelyikében nem megfelelőséget talál, abban az esetben a visszavonást nem végzi el és ennek tényéről, illetve a felmerült hibákról, a kérelem beérkezését követő huszonnégy (24) órán belül értesíti a kérelmet beküldő felet. Amennyiben a {D10} Visszavonási kérelem megfelel a Szolgáltató által elvártaknak, abban az esetben a Szolgáltató, a kérelem beérkezését követő huszonnégy (24) órán belül elvégzi a tanúsítvány visszavonását – lásd még 4.9.5.

A tanúsítvány visszavonásáról vagy a visszavonási kérelem visszautasításáról Szolgáltató Előfizetőt és/vagy Aláírót emailben értesíti.

Abban az esetben, ha az előfizetői tanúsítványhoz kapcsolódó vagy a Szolgáltató által használt kulcs algoritmus, paramétere nem megfelelően erős a kulcshoz tartozó tanúsítvány teljes érvényességi időtartamára, Szolgáltató intézkedik az érintett tanúsítványok megfelelő időben történő visszavonásáról, melynek időpontjáról az Alanyt, Előfizető Kapcsolattartóját és az Érintett Feleket előzetesen értesíti.

Szolgáltató biztosítja, hogy a tanúsítvány visszamenőleges visszavonása ne történhessen meg.

Szolgáltató az egyszer már visszavont tanúsítvány érvényességét soha nem állítja vissza érvényesre.

4.9.4 Kivárási idő visszavonási kérelem esetén

Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

4.9.5 Visszavonási kérelem feldolgozásának időbelisége

Szolgáltató a visszavonási kérelmet sikeres ellenőrzések esetén a benyújtástól számított huszonnégy (24) óra időtartamon belül feldolgozza és a tanúsítvány státuszát visszavontra állítja.

Postai úton beküldött visszavonási kérelem esetén a huszonnégy órás időtartam akkor kezdődik, amikor a postai küldemény a Regisztrációs Irodához megérkezik. Ez utóbbi időpontot a Szolgáltató {D10} Visszavonási kérelmen rögzíti.

Amennyiben 24 óránál hamarabb szükséges intézkedés, akkor a tanúsítvány felfüggesztését javasolt kérni telefonon a NISZ Telefonos HelpDesk-nél napi 24 órában, a 4.9.15 fejezetben leírtak szerint.

4.9.6 Visszavonás ellenőrzésének ajánlása az Érintett felek számára

Az Érintett Feleknek a tanúsítvány és az ahhoz felépített tanúsítványlánc minden elemének visszavonási állapotát javasolt ellenőriznie a tanúsítványból megállapított vagy a 4.10.1 fejezetben megadott elérhetőségekről letöltött CRL vagy megkért OCSP válasz alapján.

4.9.7 CRL kibocsátási gyakoriság

Az előfizetői tanúsítványokra vonatkozó CRL kibocsátásának gyakorisága: 24 óránként legalább egy CRL. A CRL tartalmazza a következő kibocsátás időpontját (a `nextUpdate` mezőben). A Szolgáltató egy-egy tanúsítvány felfüggesztését, visszavonását, illetve újra-érvényesítését követően haladéktalanul, de legfeljebb egy órán belül új CRL-t állít elő, illetve tesz közzé. Szolgáltató minden kibocsátáskor törli a CRL-ről azokat a tanúsítványokat, melyek érvényessége a CRL kibocsátásnak időpontjában már lejárt.

A szolgáltatói tanúsítványokhoz kapcsolódó CRL kibocsátásának gyakorisága: 30 naponként legalább egy CRL. A CRL tartalmazza a következő kibocsátás időpontját (a `nextUpdate` mezőben). Szolgáltató minden kibocsátáskor törli a CRL-ről azokat a tanúsítványokat, melyek érvényessége a CRL kibocsátásnak időpontjában már lejárt.

4.9.8 CRL előállítása és közzététele között leghosszabb idő

Szolgáltató a CRL-t az előállítását követően haladéktalanul, de legfeljebb egy órán belül közzéteszi.

4.9.9 OCSP szolgáltatás biztosítása

Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokhoz OCSP szolgáltatást is nyújt, a 4.10 fejezetben ismertetett elérhetőségen, működési jellemzőkkel és rendelkezésre állással.

4.9.10 OCSP alapú visszavonás ellenőrzés követelményei

Az Érintett Feleknek az OCSP szolgáltatást javasolt elsődlegesen használnia a tanúsítványok visszavonási állapotának megállapítására, mivel ezen szolgáltatás keretében (ellentétben a CRL-el) Szolgáltató a lejárt tanúsítványokhoz is biztosítja a visszavonási állapot információt.

4.9.11 Visszavonási állapot közlés más formái

Szolgáltató, a honlapján elérhető nyilvános tanúsítványtárban is közzé teszi a visszavonási állapot információt, tájékoztatási jelleggel. Ez az információ elektronikus aláírás vagy bélyegző ellenőrzéséhez nem használható fel.

4.9.12 Különleges követelmények a kulcs kompromittálódása esetére

Szolgáltató a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről honlapján tájékoztatást tesz közzé, Előfizetőket és Aláírókat emailben értesíti.

A produktív hitelesítő központ magánkulcsának kompromittálódása esetén Szolgáltató képes az összes érintett végfelhasználói tanúsítvány visszavonására és az érintett CRL-nek a 24 órán belüli kibocsátására és közzétételére, majd ezt követően, az adott szolgáltatói tanúsítvány visszavonására és az érintett CRL-nek a 12 órán belüli kibocsátására és közzétételére.

4.9.13 Felfüggesztés körülményei

Szolgáltató felfüggeszti a tanúsítványt, ha:

- Előfizető Kapcsolattartója vagy Aláíró ezt kéri;
- a Bizalmi Felügyelet jogerős és végrehajtható határozatában elrendeli a felfüggesztést;
- a felfüggesztést jogszabály kötelezővé teszi.

4.9.14 Ki kérelmezhet felfüggesztést

Felfüggesztést kezdeményezhet, a 4.9.13 fejezetben megjelölt esetekben:

- Előfizető Kapcsolattartója vagy Aláíró;
- Szolgáltató (ide értve azt az esetet, amikor a felfüggesztés a Bizalmi Felügyelet határozata vagy jogszabályi előírás miatt történik).

4.9.15 Felfüggesztésre vonatkozó eljárás

A felfüggesztési kérelem telefonon kezdeményezhető a Telefonos HelpDesk 1.5.2 pontban foglalt elérhetőségén, a felfüggesztési jelszó bemondásával.

A felfüggesztési kérelem teljesítéséhez a következő adatokat kell megadni:

- a tanúsítvány sorozatszám, vagy egyéb olyan adatok, amely alapján a Szolgáltató rendszerében a tanúsítvány egyértelműen azonosítható;
- felfüggesztést kérő azonosító adatai és email címe;
- felfüggesztés oka, az ahhoz vezető körülmények;
- felfüggesztési jelszó (telefonos kérelem esetén).

Szolgáltató azonosítja a felfüggesztést kérő személyét és elbírálja, hogy jogosult-e a tanúsítvány felfüggesztését kérni. Ha a kérelmező azonosítása-hitelesítése megtörtént, az adatok egyeznek és a kérelmező jogosult a felfüggesztést kérni, akkor a Szolgáltató azonnal elvégzi a tanúsítvány felfüggesztését, ellenkező esetben a felfüggesztési kérelmet visszautasítja.

A tanúsítvány felfüggesztéséről vagy a felfüggesztési kérelem visszautasításáról Szolgáltató Előfizetőt és/vagy Aláírót a telefonon történő folyamat során értesíti.

Ha a felfüggesztést Előfizető kezdeményezte, akkor a 4.9.16 fejezetben megjelölt időtartamon belül intézkedhet a felfüggesztett tanúsítvány újra-érvényesítéséről. Az újra-érvényesítés személyesen, az Ügyfélkapcsolati Irodánál kérhető.

4.9.16 A felfüggesztés megengedett időtartama

A tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig – illetve, ha utolsó naptári nap nem munkanap, akkor a következő munkanapig - lehet.

Ha a felfüggesztést Előfizető kezdeményezte, és ezen időtartamon belül nem kérte a tanúsítvány újra-érvényesítését, akkor Szolgáltató a tanúsítványt visszavonja. A tanúsítvány visszavonásáról Szolgáltató Előfizetőt és/vagy Aláírót emailben értesíti.

Ha a felfüggesztést Szolgáltató kezdeményezte, és ezen időtartamon belül nem képes a felfüggesztéshez vezető körülmények kivizsgálására, akkor a tanúsítványt visszavonja, és Előfizető igénye esetén térítésmentesen új tanúsítványt bocsát ki.

4.10 Visszavonási állapot szolgáltatások

4.10.1 Működési jellemzők

Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában szolgáltatja.

Szolgáltató biztosítja, hogy a visszavonási állapot információ változása mind a CRL, mind az OCSP szolgáltatásban azonosan, konzisztens módon megjelenik, figyelembe véve az egyes szolgáltatásokban eltérő frissítési időket is.

CRL

A Szolgáltató által kibocsátott CRL megfelel az {Sz9} RFC 5280 szabványnak.

Szolgáltató a CRL aláírásához ugyanazt a szolgáltatói magánkulcsot használja, melyet a kérdéses tanúsítvány aláírására használt.

A CRL minden esetben tartalmazza a következő kibocsátás időpontját (`nextUpdate`). A záró CRL (az adott hitelesítő központ által kiadott utolsó CRL) esetén a `nextUpdate` mező tartalma a „99991231235959Z” RFC 5280 {Sz9} szerinti speciális időpont. Szolgáltató biztosítja, hogy az új CRL kibocsátása a `nextUpdate` mezőben jelzett időpont előtt minden esetben megtörténik.

A CRL tartalmaz minden olyan visszavont tanúsítványt, amelynek érvényessége a CRL kibocsátásának időpontjában nem járt még le.

A Szolgáltató záró CRL-t bocsát ki, amikor egy adott hitelesítő központ működtetését megszünteti:

- kulcs átállás (5.6 fejezet) miatt; vagy
- a szolgáltatói magánkulcs kompromittálódása (5.7.3 fejezet) miatt; vagy
- a szolgáltatói tevékenység (5.8 fejezet) megszüntetése miatt.

A Szolgáltató csak azt követően bocsátja ki a záró CRL-t, miután minden, az adott hitelesítő központ által kibocsátott tanúsítvány lejárt vagy azok visszavonását elvégezte. Szolgáltató (illetve a szolgáltatási tevékenység megszüntetése esetén a szolgáltatás átvevő bizalmi szolgáltató, lásd 5.8 fejezet) a záró CRL kibocsátását követő 10 évig biztosítja a záró CRL elérhetőségét.

ECC környezet	
Végfelhasználói tanúsítványokra vonatkozó CRL elérhetősége	[NKET] http://qca.hiteles.gov.hu/ecc/crl/govca-ecc-q.crl vagy http://qca.hiteles.gov.hu/ecc/crl/govca-ecc-q2024.crl [KET] http://qca.hiteles.gov.hu/ecc/crl/govca-ecc-qket.crl
Szolgáltatói tanúsítványokra vonatkozó CRL elérhetősége	[NKET] http://qca.hiteles.gov.hu/ecc/crl/govca-ecc-root.crl [KET] http://crl.kgyhsz.gov.hu/KGYHSZ_CA_20091210.crl

RSA környezet	
Végfelhasználói tanúsítványokra vonatkozó CRL elérhetősége	[NKET] http://qca.hiteles.gov.hu/crl/GOVCA-Qv2.crl
Szolgáltatói tanúsítványokra vonatkozó CRL elérhetősége	[NKET] http://qca.hiteles.gov.hu/crl/GOVCA-ROOT.crl

OCSP

A Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz13} RFC 6960 szabványnak.

Az OCSP szolgáltatást Szolgáltató az {Sz13} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően működteti.

Az OCSP szolgáltatás keretében csak olyan tanúsítványra vonatkozóan kerül pozitív („good” státuszt tartalmazó) válasz kiadásra, amely tanúsítványt az adott hitelesítő központ bocsátott ki (azaz szerepel a tanúsítványtárban) és a tanúsítvány nincs felfüggesztett vagy visszavont állapotban.

Az OCSP válaszadó számára minimum 4 és maximum 21 óránként új, 24 órás érvényességű tanúsítvány kerül kiadásra, annak érdekében, hogy az OCSP választ aláíró tanúsítvány visszavonási állapotát ne kelljen ellenőrizni, ennek jelzésére az OCSP válaszadó tanúsítványában szerepel az `id-pkix-ocsp-nocheck` kiterjesztés.

Az OCSP szolgáltatás keretében a Szolgáltató biztosítja a visszavonási információt a tanúsítvány lejáratát követően is, 10 évig, illetve az érintett hitelesítő központ működtetési időtartamában. Egy adott hitelesítő központ működtetésének megszűntetésekor záró CRL kerül kiadásra, és ezzel egyidejűleg Szolgáltató az OCSP válaszadó működését átkonfigurálja olyan módon, hogy minden OCSP kérés visszautasításra kerüljön („unathorized” hibajelzéssel).

RSA környezet	
Végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége	[NKET] http://qocsp.hiteles.gov.hu/ocsp
Szolgáltatói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége	[NKET] http://qocsp.hiteles.gov.hu/ocsp-root

ECC környezet	
Végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége	[NKET] http://qca.hiteles.gov.hu/ecc/ocsp-q vagy http://qca.hiteles.gov.hu/ecc/ocsp-q2024 [KET] http://qca.hiteles.gov.hu/ecc/ocsp-ket
Szolgáltatói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége	[NKET] http://qca.hiteles.gov.hu/ecc/ocsp-root [KET] http://ocsp.kgyhsz.gov.hu/ocsp/

4.10.2 Szolgáltatás rendelkezésre állása

A CRL, illetve az OCSP szolgáltatás az év minden napján, napi 24 órában elérhető, 99,9%-os rendelkezésre állással, úgy, hogy a kiesés nem lépheti túl esetenként a 3 órás időtartamot.

4.10.3 Opcionális funkciók

Nincs kikötés.

4.11 Az előfizetés vége

Előfizető szerződéses viszonya megszűnik a tanúsítvány érvényességének lejáratával vagy ha a tanúsítvány az érvényességének lejáratá előtt Előfizető kérésére vagy bármely más okból kifolyólag visszavonásra kerül.

4.12 Kulcsletét és visszaállítás

A Szolgáltató nem nyújt kulcsletét szolgáltatást.

4.12.1 Kulcsletét és visszaállítás szabályai

Nincs kikötés.

4.12.2 Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nincs kikötés.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

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

Szolgáltató a rendszer kialakításakor kockázat elemzést végzett üzleti kockázatainak felmérésére, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására; a kockázatok felülvizsgálatáról évente rendszeresen, valamint szükség esetén eseti jelleggel gondoskodik. Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatikai biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bármilyen változtatást a Szolgáltató vezetősége hagy jóvá.

A biztonságkezelési szabályokat a Szolgáltató {D5} PKI szolgáltatások biztonságpolitikája tartalmazza. Ez a szabályzat biztonsági okokból nem nyilvános. A Szolgáltató informatikai rendszerei vonatkozásában a {D6} PKI szolgáltatások biztonsági szabályzata 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 összeférhetlenségi kritériumokat.

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 Szolgáltatásokra vonatkozó előírások teljesülését rendszeres időközönként vizsgálja.

A fenti eljárásokat a Szolgáltatóval munkaviszonyban álló, megbízható és szakértő üzemeltető személyzet biztosítja.

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

Szolgáltató a tanúsítványok előállításában, a visszavonási információk menedzsmentjében közreműködő informatikai rendszereit, berendezéseit és eszközeit a legmagasabb védelmi szintet képező központi géptermben helyezi el.

5.1 Fizikai óvintézkedések

5.1.1 Telephely elhelyezése és szerkezeti felépítése

A Szolgáltató a Szolgáltatások nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumában helyezte el és üzemelteti. A telephely elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és Szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2 Fizikai hozzáférés

A Szolgáltató megvédi a Szolgáltatások nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

Ehhez biztosítja az alábbiakat:

- a gépterembe történő minden belépés naplózásra kerül;

- a gépterembe csak a bizalmi szerepkört betöltő, erre feljogosított munkatárs léphet be, azonosítást követően;
- önálló jogosultsággal nem rendelkező személy csak indokolt és engedélyezett esetben, a szükséges időtartamig tartózkodhat a gépteremben megfelelő jogosultságú kísérő személy állandó felügyelete mellett;
- az eszközök aktivizáló adatai (jelszavak, PIN kódok, stb.) a géptermen belül sem tárolhatók nyílt formában;
- jogosulatlan személy jelenlétében:
 - a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
 - a bejelentkezett terminálok nem maradnak felügyelet nélkül;
 - nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet;
- a gépterem elhagyásakor ellenőrzésre kerül:
 - minden eszköz és berendezés megfelelően biztonságos üzemállapotban van;
 - minden terminálon megtörtént a kijelentkezés;
 - a fizikai tároló eszközök megfelelően elzárásra kerültek;
 - a fizikai védelmet biztosító rendszerek és berendezések megfelelően működnek.

5.1.3 Áramellátás és légkondicionálás

A Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert alkalmaz, amely:

- megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

Szolgáltató a gépteremben olyan légkondicionáló berendezést alkalmaz, mely biztosítja az alábbiakat:

- az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított;
- a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;
- hűtés történik a szükséges üzemi hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására

5.1.4 Beázás és elárasztás veszélyeztetettség

Szolgáltató megvédi a géptermet a beázástól, víz betöréstől és elárasztástól nedvességérzékelő és riasztó rendszer alkalmazásával.

5.1.5 Tűz megelőzés és tűzvédelem

Szolgáltató a géptermet füst- és tűzérzékelőkkel szerelte fel, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen van elhelyezve a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készülék. A gépteremben automatikus tűzoltó rendszer került kialakításra, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6 Adathordozók tárolása

Szolgáltató megvédi valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól, jellemzően páncélszekrénybe történő elzárással.

5.1.7 Selejt kezelése és megsemmisítése

Szolgáltató a környezetvédelmi előírások betartásával gondoskodik feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközök és adathordozók az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel kerülnek használhatatlanná tételre vagy visszaállíthatatlan módon törlésre.

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

Szolgáltató azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan külső helyszínen tárolja, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítja helyszínek között a mentett adatok biztonságos továbbítását.

Az adatmentést, vagy abból a helyreállítást rendszerüzemeltető bizalmi munkakört betöltő személy végzi el.

5.2 Eljárásbeli előírások

A Szolgáltató gondoskodik arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. Szolgáltató személyzete a feladatokat olyan eljárásbeli előírások alapján végzi, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

Az eljárásbeli szabályokat a következő szabályzatok tartalmazzák:

- {D3} a Szolgáltató Szervezeti és Működési szabályzata, mely meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes szervezetekhez kapcsolt feladat-, felelősség- és hatásköröket;
- jelen szolgáltatási szabályzat, mely a Szolgáltató és a PKI közösség (Előfizetők, Alanyok, Érintett Felek, stb.) viszonyát szabályozza;
- {D6} PKI szolgáltatások biztonsági szabályzata, mely részletesen előírja az adatokhoz és informatikai rendszerekhez, valamint a személyi és fizikai környezethez kapcsolódó biztonsági szabályokat.

5.2.1 Bizalmi munkakörök

Szolgáltató az alábbi bizalmi munkaköröket azonosította, melyektől a Szolgáltatások biztonsága függ:

- a) a Szolgáltató informatikai rendszeréért általánosan felelős vezető;
- b) biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;
- c) rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy;
- d) rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;
- e) független 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;

- f) regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának jóváhagyásáért, az életciklus menedzsment tevékenységek és adminisztráció szabályszerű végzéséért felelős személy;
- g) visszavonás felelős: a végtanúsítványok visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.*

* A vonatkozó jogszabály ({J7} 84/2012. (IV. 21.) Korm. rendelet) a visszavonás felelős feladatkörét a regisztrációs felelős tevékenységi körébe tartozóan rögzíti.

A bizalmi munkakörökhöz tartozó feladatkörök és felelősségek leírását a Szolgáltató belső, nem nyilvános szabályzata tartalmazza. A bizalmi munkakört betöltő személy munkaviszonyban áll a Szolgáltatóval. Bizalmi munkakörbe Szolgáltató felső vezetősége nevezi ki a munkatársakat. Minden bizalmi munkakört legalább két személy tölt be.

A bizalmi munkakörökön kívül Szolgáltató bizalmi szerepköröket is alkalmaz a Szolgáltatások nyújtásához szükséges feladatok hatékony ellátása céljából. A bizalmi szerepkört betöltő személyek munkaviszonyban állnak a Szolgáltatóval.

A bizalmi munkaköröket és szerepköröket betöltő személyekről Szolgáltató nyilvántartást vezet. A bizalmi munkaköröket tartalmazó nyilvántartásban bekövetkező minden változást a változtatás bevezetése előtt a Bizalmi Felügyeletnek bejelenti.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Szolgáltató {D6} biztonsági szabályzata előírja, hogy csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű jelenléte mellett, illetéktelen személy jelenlétét kizárva végezhető el az alábbi műveletek:

- szolgáltatói kulcspár létrehozása;
- szolgáltatói magánkulcs mentése és visszaállítása;
- szolgáltató magánkulcs aktiválása;
- szolgáltatói magánkulcs megsemmisítése.

5.2.3 Bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkaköröket betöltő személyek azonosítása és hitelesítése erős PKI eljárásokkal, pl. tokenen tárolt tanúsítványok és az azt aktivizáló PIN kód megadásával történik meg, mielőtt a Szolgáltatások nyújtásában érintett kritikus informatikai rendszerekhez hozzáférhetnének.

5.2.4 Egymást kizáró munkakörök

Szolgáltató biztosítja, hogy a bizalmi munkakörök vonatkozásában:

- a) biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a rendszeradminisztrátor, és az informatikai rendszerért általánosan felelős vezető feladatait;
- b) a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető, a regisztrációs felelős, és a rendszeradminisztrátor feladatait;
- c) törekedni kell a bizalmi munkakörök teljes személyi szétválasztására.

5.3 Személyzetre vonatkozó előírások

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

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

Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa mentes minden olyan ütköző érdektől, ami hátrányosan érinthetné a Szolgáltatások megbízhatóságát és biztonságát.

A munkatársak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai alapján meghatározott munkaköri leírásokkal rendelkeznek.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Szolgáltató biztosítja, hogy bizalmi munkakört csak olyan személyek töltsenek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

A Szolgáltató informatikai rendszeréért általánosan felelős vezető kinevezéséhez szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik. Szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség.

A biztonsági tisztviselők és rendszervizsgálók esetén szakirányú közép- vagy felsőfokú végzettség, középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatikai biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.

A regisztrációs felelős esetén középfokú szakirányú végzettség és legalább egy év informatikai biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.

A rendszerüzemeltető és rendszeradminisztrátor esetén középfokú szakirányú végzettség és legalább egy év, hasonló munkakörben szerzett szakmai gyakorlat szükséges.

Az egyes bizalmi munkakörök betöltéséhez elvárt szakirányú végzettségek meghatározását a Szolgáltató belső, nem nyilvános szabályzata tartalmazza.

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben vagy szerepkörben csak olyan alkalmazottakat foglalkoztat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

Szolgáltató ellenőrzi a felvételi eljárásban benyújtott önéletrajzban megadott, releváns információkat.

Az 5.2.1 fejezetben meghatározott bizalmi munkakör betöltését a legmagasabb szintű biztonsági ellenőrzés (a nemzetbiztonsági szolgálatokról szóló 1885. évi CXXV. törvényben meghatározott nemzetbiztonsági ellenőrzés) előzi meg. A többi, a Szolgáltatások nyújtásával kapcsolatos munkakörben, a munkakör betöltését fokozott szintű, a Szolgáltató által végzett biztonsági

ellenőrzés előzi meg. Mind a legmagasabb, mind a fokozott biztonsági ellenőrzés lefolytatásához szükséges az érintett személy hozzájárulása. Nem tölthet be bizalmi munkakört az a személy, akinél a biztonsági ellenőrzés kockázatot tár fel.

A bizalmi munkakörhöz történő hozzárendeléskor az érintett személy:

- pontos és írásos munkakör leírást vesz át a fölérendelt vezetőtől vagy a Szolgáltató humán szervezetétől;
- titoktartási nyilatkozatot kell aláírnia, melyben három év titoktartási kötelezettség szerepel a kilépés időpontjától számítva;
- szükséges mértékű oktatásban részesül, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

- A kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságai azonnal megszüntetésre kerülnek. Ezt követően, a kilépő személy csak biztonsági tisztviselő kíséretében léphet be a Szolgáltatásokkal kapcsolatos körletekbe.
- Azonnal vissza kell venni az azonosításhoz és hitelesítéshez használt eszközt, és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítványokat vissza kell vonni.

5.3.3 Képzési követelmények

A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztat, akik az adott munkakör vagy szerepkör ellátásához szükséges mértékben elsajátították:

- a PKI elméletet;
- Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkör ellátáshoz szükséges speciális ismereteket;
- Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó biztonsági szabályokat.

A Szolgáltató éles informatikai rendszereihez csak a képzést sikeresen záró alkalmazottak kaphatnak hozzáférési jogosultságot.

5.3.4 Továbbképzési gyakoriságok és követelmények

Szolgáltató gondoskodik arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlődő jellegű képzést tart.

Szolgáltató minden lényeges változás esetén megismétli az érintett személyek részére a képzést vagy annak elemeit.

Jelentős változás, azaz a szervezeti biztonságpolitika módosulása, a szoftver vagy hardver változása (upgrade), valamint a kulcs kezelés és biztonság kezelési óvintézkedések változása esetén, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat.

Kisebb változások esetén a munkatársak a változás bekövetkezte előtt írásos tájékoztatást kapnak.

Szolgáltató legalább évente egyszer továbbképzést biztosít az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

Szolgáltató a dolgozóval kötött munkaszerződésben szabályozza a dolgozó felelősségre vonásának lehetőségét a dolgozó által elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7 Szerződéses munkavállalókra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződés keretében a beszállítóval Szolgáltató írásos megállapodást köt. A szerződő fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a szerződés teljesítésében közreműködő személyek a munkavégzés során birtokukba kerülő üzleti titkokat és bizalmas információkat illetéktelen személynek fel nem fedik, más módon sem hasznosítják, és amely tartalmazza a megszegése esetén alkalmazott szankciókat.

5.3.8 A személyzet számára biztosított dokumentációk

Szolgáltató folyamatosan biztosítja a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

Minden bizalmi munkakört betöltő munkatárs megkapja írásban:

- egyéni munkaköri leírást;
- a Szolgáltató szervezeti és biztonsági szabályzatait;
- rendszeres és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

Szolgáltató naplóz minden, az informatikai rendszerével és Szolgáltatások nyújtásával kapcsolatos eseményt. A naplózott adatállomány átfogja a szolgáltatás nyújtásának teljes folyamatát, és lehetővé teszi, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatásokkal kapcsolatos eseményt rekonstruálni lehessen.

Az informatikai rendszerrel kapcsolatos események különösen a rendszer indítás és leállítás, biztonsági profil változása, rendszer összeomlás és hardver hibák, tűzfal aktivitás, hozzáférési kísérletek, szolgáltatói kulcs kezelés eseményei, óraszinkronizációs események, naplózási funkció elindítása és leállítása, naplózási paraméterek megváltoztatása, naplóadatok tárolásával kapcsolatos hibák, napló adatok integritásának sérülése eseményei.

A Szolgáltatások nyújtásával kapcsolatos események különösen az alábbiak:

- szolgáltatói tanúsítványok életciklusával kapcsolatos minden esemény;
- végfelhasználói tanúsítványok életciklusával kapcsolatos minden esemény, beleértve a tanúsítvány kérelmek benyújtása és teljesítése, a visszavonási kérelmek benyújtása és az annak eredményeképpen végzett tevékenység eseményei.

A naplózott adatállomány tartalmazza a naplózott esemény bekövetkeztének dátumát és pontos időpontját, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

5.4.2 Naplóállomány feldolgozásának gyakorisága

Szolgáltató biztosítja a naplóállományok rendszeres ellenőrzését és kiértékelését.

A Szolgáltatások nyújtásával kapcsolatos események naplóállományait naponta feldolgozzák a rendszervizsgálók.

Az informatikai rendszer eseményeinek naplóállományait a rendszervizsgálók rendszeres időközönként, a biztonsági szabályzatban meghatározott sűrűséggel végzik el.

5.4.3 Naplóállomány megőrzési időtartama

Szolgáltató a naplóállományokat archiválja és gondoskodik azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig. Ezen időtartamig Szolgáltató biztosítja az archivált állományok olvashatóságát, megőrzi az ehhez szükséges hardver és szoftver eszközöket.

5.4.4 Naplóállomány védelme

Szolgáltató a naplóállományokat és azok mentéseit biztonságos, fizikailag is védett környezetben tárolja. A naplóállományokat időbélyegzővel, a naplóállományok archív mentéseit időbélyegzőt is tartalmazó elektronikus aláírással vagy bélyegzővel látja el.

Szolgáltató gondoskodik arról, hogy a naplóállományokhoz és azok menteseihez csak az arra feljogosított személyek férhessenek hozzá.

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról Szolgáltató rendszeres mentést készít. A mentéssel kapcsolatos eljárásokat és szabályokat a Szolgáltató belső szabályzata tartalmazza.

5.4.6 Naplózás gyűjtési rendszere

A naplóbejegyzések gyűjtését belső komponens oldja meg. A naplóbejegyzések gyűjtése megkezdődik rendszer indításkor és rendszer leállításig folyamatosan működik, és közben biztosítja a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltató felfüggeszti az érintett területek működését az üzemzavar elhárításáig.

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

A rendellenes eseményeket kiváltó alanyokat (személyeket, szervezeteket) Szolgáltató nem feltétlenül értesíti minden esetben. Szolgáltató szükség esetén bevonhatja az eseményt kiváltó alanyt az esemény kivizsgálásába. Ilyen esetben az érintett Előfizető, Aláíró vagy Bélyegző Létrehozó kötelessége a Szolgáltatóval való együttműködés az esemény feltárása érdekében.

5.4.8 Sebezhetőség értékelések

Szolgáltató a vonatkozó szabványok által meghatározott rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet végez, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek jogosulatlan hozzáférést eredményezhetnek vagy hatással lehetnek a tanúsítvány kibocsátási folyamatra, a tanúsítványban tárolandó adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik.

A sebezhetőség vizsgálathoz kapcsolódóan Szolgáltató kockázatelemzésben értékeli az egyes fenyegetések bekövetkeztének valószínűségét és a bekövetkezés esetén várható kárt. Értékeli az alkalmazott folyamatokat, informatikai rendszereket, védelmi intézkedéseket, hogy azok megfelelően képesek-e ellenállni a fenyegetésnek.

A kiértékelést követően Szolgáltató megteszi a megfelelő intézkedéseket annak érdekében, hogy a feltárt sebezhetőség kihasználhatósága ne következzen be.

Szolgáltató folyamatosan figyelemmel kíséri az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül megteszi. Bármely olyan sebezhetőség esetén, melynek kihatása lehet a Szolgáltatások nyújtására, Szolgáltató vagy cselekvési tervet készít és hajt végre annak érdekében, hogy a sebezhetőség ne legyen kihasználható illetve annak hatása elhanyagolható legyen, vagy dokumentálja annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

Szolgáltató gondoskodik arról, hogy megőrzésre kerüljön minden olyan információ, amely szükséges ahhoz, hogy egy elektronikus aláírás vagy bélyegző érvényessége bizonyítható legyen, továbbá amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja.

Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

- tanúsítványok igénylésével, regisztrációval kapcsolatos minden adat vagy irat, különösen a Szolgáltatási Szerződés, Előfizető által aláírt nyilatkozatok és átvételi elismervények;
- tanúsítványokkal kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- a bizalmi szolgáltatási rend és szolgáltatási szabályzat valamennyi kibocsátott verziója;
- az Általános Szerződési Feltételek valamennyi kibocsátott verziója;
- a Szolgáltató működésével kapcsolatos szerződések;
- valamennyi naplóállomány.

5.5.2 Archívum megőrzési időtartama

Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat, a tanúsítványokkal kapcsolatos adatok esetében a tanúsítvány érvényességnek lejáratáról számított 10 évig, illetve a tanúsítvánnyal előállított elektronikus aláírással vagy bélyegzővel kapcsolatos jogvita jogerős lezárásáig, szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 10 évig őrzi meg.

5.5.3 Archívum védelme

Szolgáltató olyan fizikai védelmet biztosít és biztonsági óvintézkedéseket alkalmaz, melyek fenntartják az archivált adatok sértetlenségét, hitelességét, rendelkezésre állását és a

bizalmasságát. Az elektronikus formában archivált adatokat Szolgáltató legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, valamint minősített időbélyegzővel látja el.

5.5.4 Archívum mentési eljárásai

Szolgáltató a papír alapú iratokat, dokumentumokat a dokumentumtárban, az elektronikus állományokat pedig több példányban, fizikailag elkülönített helyszíneken őrzi meg, illetve tárolja.

Szolgáltató biztosítja az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi naplóbejegyzésben olyan időjel szerepel, amely a 6.8 fejezetben ismertetett időforrásokkal szinkronizált rendszeridőt tartalmazza, melynek pontossága egy másodpercen belüli.

Az elektronikus formában archivált adatokon elhelyezett elektronikus aláírás vagy bélyegző minősített időbélyeget tartalmaz.

Szolgáltató az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodik az elektronikus aláírások vagy bélyegzők, valamint az időbélyegzők hitelességnek fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

A naplóállományok és az egyéb elektronikus keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül gyűjti. A védett informatikai rendszerből történő kimozzgatás során az adatok minősített időbélyeget tartalmazó elektronikus aláírással vagy bélyegzővel kerülnek hitelesítésre.

A papíralapú iratokat Szolgáltató elhelyezi a saját dokumentumtárában tárolás és megőrzés céljából.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

Szolgáltató az archivált adatokat megvédi a jogosulatlan hozzáféréstől. Szolgáltató a jogosultságot ellenőrzi, és a hozzáféréseket naplózza.

Szolgáltató az Ügyfélkapcsolati Iroda közreműködésével biztosítja az Aláírók számára a róluk tárolt személyes adatokra vonatkozó tájékoztatást.

Szolgáltató a 9.4.6 fejezetben ismertetett hatósági vagy jogi eljárásokban a szükséges mértékben a biztosítja a hozzáférést az archívumban tárolt adatokhoz.

5.6 Kulcs átállítás

Szolgáltató biztosítja, hogy a hitelesítő központok folyamatosan rendelkezzenek a működésükhöz szükséges érvényes kulccsal és tanúsítvánnyal.

Szolgáltató a végfelhasználói tanúsítványok aláírására használt kulcspárhoz tartozó szolgáltatói tanúsítvány lejáratát előtt új szolgáltatói tanúsítványt bocsát ki - és azt a 2.2 és 2.3 fejezetekben leírt módon közzé teszi -, kellő időben ahhoz, hogy a bizalmi szolgáltatás megszakítás nélkül üzemeljen, a kiadott végtanúsítványok érvényességének lejáratát figyelembe véve.

Amennyiben új szolgáltatói kulcspár és tanúsítvány előállítása szükséges, Szolgáltató ezt olyan módon teszi meg, hogy az átállítás az Előfizetők és Érintett Felek számára a lehető legkisebb kényelmetlenséget jelentse:

- a kulcs átállást követően kibocsátott tanúsítványokat kizárólag csak az új szolgáltatói kulcs felhasználásával írja alá;
- a régi szolgáltató kulcspárból a nyilvános kulcsot és a szolgáltatói tanúsítványt megőrzi a legutoljára kibocsátott tanúsítvány érvényességének lejártát követő két évig vagy a kulcs átállástól számított tíz évig, amely időtartam a hosszabb.

Szolgáltató a tervezett kulcs átállást megelőzően legalább 30 nappal értesíti a Bizalmi Felügyeletet és vele egyeztet a szükséges feladatokról.

5.7 Helyreállítás rendkívüli üzemi helyzetek esetén

Szolgáltató minden szükséges intézkedést meghoz annak érdekében, hogy rendkívüli üzemeltetési helyzet, katasztrófa esetén a szolgáltatás kiesésből származó károkat minimalizálja és a Szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa. A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását megelőzi.

A visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás 3 órát meghaladó kiesése esetén Szolgáltató haladéktalanul értesíti a Bizalmi Felügyeletet.

Egyéb incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra -, Szolgáltató az esetről való értesüléstől számított 24 órán belül értesíti az Érintett Feleket, valamint jelenti az incidenst a Bizalmi Felügyeletnek.

A bekövetkezett incidens kiértékelése alapján Szolgáltató meghozza a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

Szolgáltató rendelkezik {D7} üzletmenet folytonossági tervvel. Ez a dokumentum biztonsági okokból kifelé nem nyilvános.

A rendkívüli üzemeltetési helyzetben a Szolgáltató dokumentálja az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

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

A helyreállítás időtartamát az esemény súlyossága, azaz az üzletmenet folytonossági terv szerint értelmezett osztályba sorolása határozza meg.

Szolgáltató kialakította és fenntartja azt a tartalék CA rendszert, mely a rendkívüli üzemeltetési helyzetben képes a tanúsítványtár és a nyilvános szabályzatok elérhetőségét, a visszavonás kezelési szolgáltatások teljes értékű működését, a CRL-ek közzétételét biztosítani.

A rendkívüli üzemeltetési helyzet határidőn túli fennállása esetén Szolgáltató haladéktalanul értesíti a Bizalmi Felügyeletet, az esemény bekövetkeztéről, annak hatásáról, várható időtartamáról, az elhárítás érdekében tett és tervezett intézkedésekről, továbbá a rendkívüli üzemeltetési helyzet megszűnéséről.

A rendkívüli üzemeltetési helyzetben Szolgáltató a lehető legrövidebb időn belül tájékoztatást tesz közzé internetes honlapján, valamint, lehetőség szerint, elektronikus levélben értesíti azokat a személyeket, akiket az esemény érint.

A biztonságot érintő vagy a sértetlenség megszűnését eredményező incidens esetén – amennyiben annak hátrányos kihatása van a Szolgáltatást igénybe vevő Előfizetőkre – Szolgáltató indokolatlan késedelem nélkül értesíti az érintett Előfizetőket.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltató olyan megbízható rendszert működtet, mely redundáns műszaki megoldásokkal, biztonsági mentésekkel és eljárásokkal a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatások működtetését és elérhetőségét. A pontos és részletes előírásokat és intézkedéseket az üzletmenet folytonossági terv, illetve a Szolgáltató belső szabályzatai tartalmazzák.

5.7.3 Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás

A Szolgáltató magánkulcsának kompromittálódása esetére akciótervvel rendelkezik, melyet az üzletmenet folytonossági tervében tervezett meg. E szerint megteszi az alábbi főbb lépéseket:

- visszavonja az összes érintett tanúsítványt;
- záró CRL-t (4.10.1) bocsát ki;
- megszünteti az érintett magánkulcs használatát;
- új szolgáltatói kulcspárokat és tanúsítványokat hoz létre;
- értesíti a Bizalmi Felügyeletet;
- intézkedik valamennyi érintett fél értesítéséről.

5.7.4 Üzletmenet folytonosság helyreállítás katasztrófát követően

Szolgáltató rendelkezik tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

A súlyos üzemzavar és a katasztrófa eseteit - 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 egy válságstáb az üzletmenet folytonossági tervben meghatározott módon intézkedik a tartalék helyszínre való áttelepülésről és ott az informatikai rendszer szükséges mértékű visszaállításáról a tartalék helyszínen korábban elhelyezett mentések segítségével.

5.8 A szolgáltatási tevékenység megszüntetése

Szolgáltató rendelkezik olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket. Ha Szolgáltató ellen felszámolási, végelszámolási vagy egyéb kényszertörlési eljárás indult, erről és a felszámolóról vagy végelszámolóról Szolgáltató haladéktalanul tájékoztatja a Felügyeleti Szervet.

Szolgáltató az alábbi, a szolgáltatási tevékenység megszüntetésére vonatkozó tervvel rendelkezik:

- A tervezett megszűnés előtt kellő időben tárgyalásokat kezdeményez más minősített bizalmi szolgáltatókkal a Szolgáltatásokkal járó kötelezettségek - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig - átadás-átvételéről.
- Szolgáltató gondoskodik a Szolgáltatások megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról. Különösképpen gondoskodik a tanúsítvány visszavonási kezelés és közzététel szolgáltatások folyamatos fenntartásáról.
- A megszüntetés előtt legalább 60 nappal korábban:

- értesíti a Bizalmi Felügyeletet, és internetes honlapján tájékoztatja az felhasználói közösség tagjait;
 - megszünteti a nevében eljáró szerződött alvállalkozói összes felhatalmazását, felbontja a velük kötött szerződéseket, és jogosultságait megvonja;
 - beszünteti a tanúsítványok előállítását és kibocsátását;
 - egy másik minősített bizalmi szolgáltatóval megállapodást köt a Szolgáltatásokkal járó kötelezettségeknek átadás-átvételéről, és ennek másolatát megküldi a Bizalmi Felügyeletnek;
- A megszüntetés előtt legalább 20 nappal korábban:
 - visszavonja az összes végfelhasználói tanúsítványt és kibocsátja a záró CRL-t;
 - leállítja a visszavonás kezelés szolgáltatást;
 - visszavonja az érintett szolgáltatói tanúsítványokat és kibocsátja a záró CRL-t;
 - a szolgáltatói magánkulcsokat és azok mentéseit olyan módon semmisíti meg, hogy azok használata a továbbiakban már nem lehetséges;
 - beszünteti a tanúsítványok és visszavonási állapot információk közzétételét (mind a CRL publikációt, mind az OCSP szolgáltatást) és gondoskodik arról, hogy ezzel egyidejűleg a visszavonási információk az átvevő szolgáltatónál elérhetővé váljanak;
- A megszüntetés napjával:
 - Szolgáltató az informatikai rendszerében foglalt adatokról teljes körű, időbélyegzővel és elektronikus aláírással vagy bélyegzővel ellátott mentést készít. Szolgáltató a mentett adatállományokat védi a jogosulatlan módosítástól, és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. Szolgáltató a megkötött szerződés révén biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

6.1.1.1 Szolgáltatói kulcspárok előállítása

Szolgáltató a tanúsítványok és visszavonási listák aláírására használt, valamint az időbélyegző egységek által a kiadott elektronikus időbélyegzők hitelesítésére használt kulcspárokat fizikailag védett környezetben, az erre szolgáló HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, más személy jelenlétének kizárásával generálja. Szolgáltató a tanúsítványok hitelesítésére használt kulcspárok előállítását dokumentált „kulcs-ceremónia” eljárás szerint végzi, melyről a vonatkozó szabványi követelményeknek megfelelő jegyzőkönyv készül. A kriptográfiai modul megfelel a 6.2.1 fejezet szerinti követelményeknek, a magánkulcsok teljes életciklusuk alatt a kriptográfiai modulban maradnak.

6.1.1.2 Előfizetői kulcspárok előállítása

Amennyiben Előfizető az általa biztosított kulcspárhoz kéri a tanúsítvány kibocsátását, akkor:

- az Alany a kulcspárt a 6.1.5 és 6.1.6 fejezetek szerinti algoritmusra és kulcshosszra vonatkozó követelményeknek megfelelően kell előállítania, a felügyelete alatt álló, megfelelően biztonságos környezetben;
- az Alany gondoskodnia kell a magánkulcs és aktivizáló adatának megfelelő védelméről.

Ha a kulcspárt Szolgáltató állítja elő, akkor:

- [QSCD] Szolgáltató a 6.1.5 és 6.1.6 fejezetek szerinti algoritmusú és kulcshosszú kulcspárt szigorúan védett környezetben, a QSCD-n, kizárólag bizalmi munkakört betöltő személyek jelenlétében állítja elő;
- [P12] Szolgáltató a 6.1.5 és 6.1.6 fejezetek szerinti algoritmusú és kulcshosszú kulcspárt szigorúan védett környezetben, a hitelesítő-központi rendszerében, kizárólag bizalmi munkakört betöltő személyek jelenlétében állítja elő;
- [P12] a magánkulcsot annak átadásáig Szolgáltató megfelelően biztonságos környezetben tárolja a felfedés megakadályozása érdekében;
- [P12] a magánkulcs dokumentált átadását követően Szolgáltató haladéktalanul megsemmisíti a magánkulcs minden tárolt példányát olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

Amennyiben Előfizető az általa biztosított kulcspárhoz kéri a tanúsítvány kibocsátását, akkor a magánkulcs eljuttatása az Alany számára nem szükséges, mert azzal maga rendelkezik.

[QSCD] Amennyiben az Alany kulcspárját Szolgáltató állította elő, akkor Szolgáltató a 4.3.2 fejezetben leírt módon biztosítja, hogy a QSCD-t és az ahhoz tartozó aktivizáló adatokat csak a jogosult Alany vehesse át.

[P12] Amennyiben az Alany kulcspárját Szolgáltató állította elő, akkor Szolgáltató a 4.3.2 fejezetben leírt módon biztosítja, hogy a magánkulcsot (szoftveres kulcstároló eszközt) és az ahhoz tartozó aktivizáló adatot csak a jogosult Alany vehesse át.

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Amennyiben Előfizető az általa biztosított kulcspárhoz kéri a tanúsítvány kibocsátását, akkor a nyilvános kulcsot PKCS#10 formátumnak megfelelő, a nyilvános kulcshoz tartozó magánkulccsal létrehozott digitális aláírással hitelesített tanúsítványkérelemben juttatja el Szolgáltatónak. Szolgáltató a tanúsítványkérelemben elhelyezett digitális aláírás ellenőrzésével meggyőződik arról, hogy az Alany a magánkulcsot birtokolja.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

Szolgáltató a nyilvános kulcsait a szolgáltatói tanúsítványban teszi közzé a 2.2 fejezetben leírtak szerint. A szolgáltatói tanúsítvány elérhetősége minden esetben szerepel a kérdéses tanúsítvány `AuthorityInformationAccess` kiterjesztésében.

Az Alanyok számára Szolgáltató a nyilvános kulcsait az aláírói tanúsítványhoz kapcsolódó tanúsítványlánc formájában - mely az opcionálisan megrendelt aláírás- vagy bélyegző létrehozó eszközön, vagy a PKCS#12 formátumnak megfelelő kulcstárolóban tárolásra kerül - teszi közzé.

Érintett Feleknek a szolgáltatói tanúsítványokra az {Sz9} RFC 5280 6. fejezetében leírt tanúsítási útvonallal felépítést és érvényesítést javasolt elvégezniük az érintett nyilvános kulcs használata előtt.

6.1.5 Kulcs méretek

Szolgáltató a Szolgáltatások nyújtása során – mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében - a Bizalmi Felügyelet vonatkozó határozatának megfelelő szabványos algoritmusokat, paramétereket és kulcshosszokat használ.

Az RSA környezetben a szolgáltatói tanúsítványokban használt kulcspárok algoritmusa és kulcshossza:

„Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató”	SHA256withRSA	RSA 4096 bit
[NKET] „Minősített Tanúsítványkiadó v2 – GOV CA”	SHA256withRSA	RSA 2048 bit
OCSP válaszadó	SHA256withRSA	RSA 2048 bit

Az Alanyok RSA környezetből származó tanúsítványaiban használt aláíró algoritmus és kapcsolódó kulcspár mérete: SHA256withRSA, 2048 bit.

Az ECC környezetben a szolgáltatói tanúsítványokban használt aláíró algoritmus és kulcs típusa:

[KET] „GovCA Minősített Közigazgatási Tanúsítványkiadó”	SHA384withECDSA	NIST P-384
[NKET] „GovCA Minősített Tanúsítványkiadó” vagy „GovCA Minősített Tanúsítványkiadó 2024”	SHA384withECDSA	NIST P-384
OCSP válaszadó	SHA384withECDSA	NIST P-256

Az Alanyok ECC környezetből származó tanúsítványaiban használt aláíró algoritmus és kapcsolódó kulcspár típusa, mérete:

- SHA384withECDSA, NIST P-256
vagy
- ilyen irányú egyedi igény esetén SHA384withECDSA, RSA 3072 bit

A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén gondoskodik az algoritmus váltásról vagy a kulcshosszak növeléséről. Amennyiben az Előfizetők vagy a Szolgáltató által használt kulcspárok algoritmusai vagy valamely paramétere nem kellően erős a kapcsolódó tanúsítvány teljes érvényességi időtartamára vonatkozóan, Szolgáltató értesíti Előfizetőket és az érintett feleket, valamint előjegyzzi az érintett tanúsítványok visszavonását.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

A Szolgáltatói kulcspárok előállítása a 6.1.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva történik. A szolgáltatói kulcspárok generálása során Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat is.

Az előfizetői kulcspárok tekintetében:

- ha a hitelesítendő nyilvános kulcs PKCS#10 formátumnak megfelelő tanúsítványkérelemben került Szolgáltató számára eljuttatásra, akkor Szolgáltató ellenőrzi, hogy a nyilvános kulcs algoritmusai, paraméterei és kulcshossza megfelelnek a Bizalmi Felügyelet vonatkozó határozatába foglalt követelményeknek;
- [P12] ha az Alany kulcspárját Szolgáltató állítja elő és nem igényelték hozzá QSCD-t, akkor a kulcspárt védett környezetben a hitelesítő-központi rendszerében, kizárólag bizalmi munkakört betöltő személyek jelenlétében állítja elő. Az előfizetői kulcspárok generálása során Szolgáltató betartja a Bizalmi Felügyelet vonatkozó határozatába foglalt előírásokat is.
- [QSCD] Szolgáltató az Alany kulcspárjának generálását védett, biztonságos környezetben és eljárásokkal végzi, a QSCD erre szolgáló biztonsági funkciójának meghívásával, melynek során betartja a QSCD tanúsítási jelentésében foglalt előírásokat is. Az előfizetői kulcspárok generálása során Szolgáltató betartja a Bizalmi Felügyelet vonatkozó határozatába foglalt előírásokat is.

6.1.7 A kulcs használat célja (X.509 v3 kulcs használati mezőnek megfelelően)

A szolgáltatói magánkulcsok használati célja kizárólag tanúsítványok és visszavonási listák aláírása. Az OCSP válaszadó magánkulcsának használati célja kizárólag OCSP válaszok aláírása.

Az Alanyok számára kibocsátott végfelhasználó tanúsítványokhoz kapcsolódó magánkulcs kizárólag elektronikus aláírás vagy bélyegző létrehozására használható.

Szolgáltató a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz12} ITU-T X.509 v3 szabványnak megfelelően jelzi a kulcs használat célját.

	kiterjesztés		kiterjesztés	
	kritikus?	KeyUsage	kritikus?	Extended KeyUsage
[KET] CA: GovCA Minősített Közigazgatási Tanúsítványkiadó	igen	keyCertSign cRLSign	-	-
[NKET] CA: GovCA Minősített Tanúsítványkiadó	igen	keyCertSign cRLSign	nem	documentSigning
[NKET] CA: GovCA Minősített Tanúsítványkiadó 2024	igen	keyCertSign cRLSign	nem	documentSigning emailProtection

OCSP válaszadó tanúsítványa	igen	contentCommitment ³	nem	OCSPSigning
Időbélyegző egység tanúsítványa	igen	contentCommitment	nem	timeStamping
Alany tanúsítványa GovCA Minősített Tanúsítványkiadó CA által kiadva	igen	contentCommitment	nem	documentSigning
Alany tanúsítványa GovCA Minősített Tanúsítványkiadó 2024 CA és GovCA Minősített Közigazgatási Tanúsítványkiadó által kiadva	igen	contentCommitment	nem	documentSigning emailProtection

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és műszaki szabályozások

Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára olyan kriptográfiai modult alkalmaz, amely:

- olyan megbízható rendszer, amelynek értékelése az MSZ/ISO/IEC 15408 {Sz15} szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg; vagy
- megfelel az ISO/IEC 19790 {Sz16} követelményeinek; vagy
- megfelel a FIPS 140-2 {Sz17} 3-as, illetve annál magasabb szintű követelményeknek.

[ALA+QSCD] Szolgáltató az aláírói tanúsítvánnyal hitelesített kulcspár előállítására olyan minősített elektronikus aláírást létrehozó eszközt használ, amely – összhangban a {J1} eIDAS 30. cikkével - a tanúsításra jogosult szervezet által kiadott tanúsítvánnyal igazoltan megfelel a {J1} eIDAS II. mellékletében foglalt követelményeknek, vagy olyan biztonságos elektronikus aláírást létrehozó eszköz, melynek megfelelőségét az 1999/93/EK irányelv 3. cikke (4) bekezdésével összhangban állapították meg.

[BÉLY+QSCD] Szolgáltató a bélyegző tanúsítvánnyal hitelesített kulcspár előállítására olyan minősített elektronikus bélyegzőt létrehozó eszközt használ, amely – összhangban a {J1} eIDAS 39.

³ X.509 előző verzióban és RFC 5280 szabványban: nonRepudiation

cikkével - a tanúsításra jogosult szervezet által kiadott tanúsítvánnyal igazoltan megfelel a {J1} eIDAS II. mellékletében foglalt, értelemszerűen alkalmazandó követelményeknek.

A Szolgáltató kétféle QSCD eszközt használ a minősített tanúsítványok kiadásához illetve az Előfizetők aláírás-létrehozó adatának előállításához; mindkettő rendelkezik az Európai Unió tagállamában nyilvántartásba vett, eszköztanúsításra jogosult szervezet által erre a célra kiadott tanúsítással⁴. A Szolgáltató által használt QSCD eszközök az alábbiak:

- SafeNet IDPrime 940 illetve SafeNet IDPrime 3940 típusú intelligens kártya, melynek neve és verziója (a megfelelőségi tanúsítási jelentés szerint) IAS Classic v4.4.2, MOC v1.1 szerverrel, Java Card MultiApp V4.0.1 platformon, Infineon M7892 G12 chipkártyán. Ezen eszköz használatához megfelelő kártyakezelő alkalmazás szükséges (SafeNet Authentication Client, SAC), melyet Előfizető díjmentesen letölthet a Szolgáltatások internetes honlapjáról.

[QSCD] Szolgáltató heti rendszerességgel ellenőrzi minden általa forgalmazott QSCD tanúsított állapotának meglétét, tovább a QSCD tanúsítás lejárátát összeveti azon kiadott tanúsítványok lejárátával, melyek az adott QSCD-n kerültek kibocsátásra. Szolgáltató – amennyiben az lehetséges – időben intézkedik a QSCD tanúsítás meghosszabbításáról vagy megújításáról. A QSCD tanúsítási állapotának megszűnte esetén Szolgáltató intézkedik az összes érintett tanúsítvány visszavonásáról. Amennyiben a QSCD tanúsítás meghosszabbítása vagy megújítása nem lehetséges, akkor Szolgáltató időben intézkedik új, tanúsított QSCD eszközök beszerzéséről.

6.2.2 Több szereplős ("n-ből m") ellenőrzés

Szolgáltató a hitelesítő központokban alkalmazza a több szereplős "n-ből m" ellenőrzést a gyökér hitelesítő központ kulcsgondozási funkcióinak aktivizálásánál.

6.2.3 Magánkulcs letét

Szolgáltató a hitelesítő központok magánkulcsait nem teszi letétbe.

Szolgáltató nem nyújt az Aláírók vagy Bélyegző Létrehozók számára magánkulcs letét szolgáltatást.

6.2.4 Magánkulcs visszaállítása

A hitelesítő központok szolgáltatói magánkulcsai biztonsági okokból mentésre kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik. Szolgáltató a hitelesítő központok magánkulcsait rendkívüli üzemi helyzetek esetén a titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a magánkulcs előállítása eredetileg történt.

Szolgáltató az Aláírók vagy Bélyegző Létrehozók magánkulcsát semmilyen formában nem menti, nem tárolja.

6.2.5 Magánkulcs mentése

A hitelesítő központok szolgáltatói magánkulcsai biztonsági okokból mentésre kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik, megfelelő biztonsági óvintézkedések és eljárási szabályok betartásával, melyek garantálják a magánkulcs sértetlenségét

⁴ Mindkét tanúsítvány, valamint a kapcsolódó tanúsítási jelentések eredeti, francia nyelvű változata elérhető a <https://hiteles.gov.hu> honlap „Termékek” menüpontjában, ahol ezek magyar nyelvű fordítása is megtalálható

és bizalmasságát. A mentett példányok titkosított formában, fizikailag biztonságos környezetben kerülnek megőrzésre.

Szolgáltató az Aláírók vagy Bélyegző Létrehozók magánkulcsát semmilyen formában nem menti, nem tárolja.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

A hitelesítő központok magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra.

Amennyiben az Alany kulcspárját Szolgáltató állította elő:

- [QSCD] Az Aláíró, illetve Bélyegző Létrehozó kulcspárjának előállítása magán a QSCD eszközön (kriptográfiai modulban) történt, így a magánkulcs bejuttatására nincs szükség.
- [P12] Szolgáltató a magánkulcsot szabványos, titkosított kulcstároló formátumban (PKCS#12) készíti elő az átadásra, és ha ezt Előfizető kriptográfiai modulban kívánja tárolni, akkor a bejuttatásról neki kell gondoskodnia. Előfizető feladata a kriptográfiai modulba bejuttatást követően a magánkulcs minden példányának haladéktalan és visszaállíthatatlan módon történő megsemmisítése.

Amennyiben a kulcspárt az Alany maga állította elő és ezt kriptográfiai modulban kívánja tárolni, akkor a bejuttatásról neki kell gondoskodnia.

6.2.7 Magánkulcs kriptográfiai modulban történő tárolásának módja

A hitelesítő központok magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra. A kulcsok tárolása során Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat.

6.2.8 Magánkulcs aktiválásának módja

A hitelesítő központok magánkulcsainak aktiválását Szolgáltató a HSM modul gyártói dokumentációjában előírtak szerint végzi el.

Ha az Alany kulcspárját Szolgáltató állította elő, akkor az Aláíró vagy Bélyegző Létrehozó a magánkulcs aktiválását a lezárt borítékban átadott PIN kód megadásával végzi.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

Szolgáltató biztosítja, hogy az aktivált HSM modul jogosulatlan hozzáférés ellen védett legyen. A HSM modul működése során csak a kiadott tanúsítványok, visszavonási listák és opcionálisan OSCP válaszok hitelesítésére használható. A magánkulcs eltávolításra kerül a HSM modulból, amikor a hitelesítő központ működése megszűnik.

Az Alany vagy Bélyegző Létrehozó magánkulcsának deaktiválását az általa elektronikus aláírások vagy bélyegzők létrehozására használt alkalmazás végzi el, kijelentkezéskor, az alkalmazásból való kilépéskor, vagy a QSCD eszköznek az olvasóból való eltávolításakor.

6.2.10 Magánkulcs megsemmisítésének módja

Szolgáltató a hitelesítő központok magánkulcsát visszaállíthatatlan módon megsemmisíti, amikor használatuk már nem szükséges vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcs és az aktiválásához szükséges minden adat megsemmisítését olyan módon végzi,

hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkeztethető vagy levezethető.

6.2.11 Kriptográfiai modul értékelése

A 6.2.1 fejezet tartalmazza.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

Az elektronikus aláírás vagy bélyegző érvényesítéséhez használt adatot (a nyilvános kulcsot) a tanúsítvány tartalmazza. Szolgáltató minden általa kibocsátott tanúsítványt archivál és az érvényesség lejártától számított tíz évig, illetve a tanúsítványhoz kapcsolódó aláírás-létrehozó adat (magánkulcs) felhasználásával létrehozott elektronikus aláírással vagy bélyegzővel kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrzi. Az archiválás biztonsági okokból két példányban (redundáns rendszer alkalmazásával) történik. A megőrzési kötelezettségnek Szolgáltató minősített archiválás szolgáltató igénybe vételével is eleget tehet.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

A kulcspár felhasználás időtartama azonos a nyilvános kulcs hitelességét igazoló tanúsítvány érvényességi idejével:

RSA környezet

"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"	20 év
[NKET] "Minősített Tanúsítványkiadó v2 – GOV CA"	15 év
OCSP válaszadó	legfeljebb 30 nap
Előfizetői tanúsítvány	legfeljebb 2 év *

**: Előfizető és Szolgáltató egyedi megállapodása alapján a tanúsítvány érvényessége egy év is lehet.*

ECC környezet

"GovCA Főtanúsítványkiadó"	2047. augusztus 2-ig.
[KET] "GovCA Minősített Közigazgatási Tanúsítványkiadó"	2029. december 10-ig.
[NKET] "GovCA Minősített Tanúsítványkiadó"	2043. szeptember 14-ig.
[NKET] "GovCA Minősített Tanúsítványkiadó 2024"	2044. március 12-ig.
OCSP válaszadó	legfeljebb 30 nap
Előfizetői tanúsítvány	legfeljebb 3 év *

**: Előfizető és Szolgáltató egyedi megállapodása alapján a tanúsítvány érvényessége kevesebb is lehet.*

Szolgáltató úgy biztosítja, hogy az előfizetői tanúsítvány érvényességi időszakának lejáratát ne legyen későbbi, mint a hitelesítéséhez használt szolgáltatói tanúsítvány lejáratának időpontja, hogy kellő időben végrehajtsa az 5.6 fejezetben leírt kulcs átállást.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

Amennyiben az Alany kulcspárját Szolgáltató állította elő, a magánkulcs aktiválásához szükséges PIN kódot (QSCD szolgáltatása esetén a PUK kódot is) előállítja megfelelő minőségű véletlenszámgenerátor segítségével, fizikailag védett környezetben és biztonságos körülmények között, és hozzárendeli a szolgáltatott QSCD eszközhöz, illetve a PKCS#12 formátumnak megfelelő kulcstárolóhoz.

6.4.2 Aktivizáló adatok védelme

A PIN (és QSCD eszköz szolgáltatása esetén a PUK) kódot tartalmazó borítékot annak átadásáig Szolgáltató biztonságosan, az eszköztől, illetve kulcstárolótól elkülönítve tárolja.

Az átvételt követően az Alany (Aláíró vagy Bélyegző Létrehozónak) kell biztosítania az aktivizáló adatok kizárólagos birtoklását és védelmét.

6.4.3 Aktivizáló adatok egyéb szempontjai

Nincs kikötés.

6.5 Informatikai biztonsági óvintézkedések

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz2} EN 319 401, {Sz3} EN 319 411-1 és {Sz4} EN 319 411-2 szabványoknak a nyilvános kulcsú tanúsítványokat kibocsátó, minősített bizalmi szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg, melyek különösen az alábbiak:

#	hivatkozás	leírás
1.	EN 319 401 REQ-7.4-01 REQ-7.4-02 REQ-7.4-03	A Szolgáltató rendszerei csak feljogosított személyek számára férhetők hozzá. A szolgáltató belső hálózatát tűzfalakkal kell megvédeni a jogosulatlan hozzáférés ellen, beleértve az előfizetők és harmadik felek hozzáférését is. A tűzfalakon le kell tiltani minden protokollt és hozzáférést, amely nem szükséges a működtetéséhez.
2.	EN 319 401 REQ-7.4-10	Az érzékeny adatokat meg kell védeni az ellen, hogy újrafelhasznált tároló objektumokon (pl. törölt fájlok) át jogosulatlan személyek számára hozzáférhetővé váljanak.
3.	EN 319 411-1 GEN-6.5.5-02 GEN-6.5.5-03	Tanúsítvány előállítása során a lokális hálózati komponenseket (pl. router) fizikailag és logikailag biztonságos környezetben kell fenntartani,

		és ezek konfigurációját a követelményeknek való megfelelés vonatkozásában rendszeres időközönként ellenőrizni kell.
4.	EN 319 411-1 GEN-6.5.5-04	Multi-faktoros azonosítást kell alkalmazni minden olyan személy és folyamat azonosítására, mely tanúsítvány előállítását közvetlenül kiválthatja.
5.	EN 319 411-1 GEN-6.5.5-05	A tanúsítványtárakat kezelő alkalmazásoknak hozzáférés ellenőrzést kell végrehajtaniuk minden esetben, amely tanúsítvány hozzáadását, törlését vagy a kapcsolódó információk megváltoztatását eredményezheti.
6.	EN 319 411-1 GEN-6.5.5-06	A visszavonási státuszt kezelő alkalmazásnak hozzáférés ellenőrzést kell végrehajtaniuk minden esetben, amely a visszavonási státusz információ megváltozását eredményezheti.
7.	EN 319 411-1 GEN-6.5.5-07	A Szolgáltató erőforrásainak folyamatos monitorozását és riasztást kell megvalósítani arra, hogy Szolgáltató képes legyen észlelni a jogosulatlan és/vagy a normálistól eltérő hozzáférési kísérleteket és az ellenintézkedéseket kellő időn belül megtegye.

6.5.2 Informatikai biztonsági értékelés

Szolgáltató az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezései szerint végzi.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

Szolgáltató gondoskodik arról, hogy az általa vagy a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény meghatározási fázisban figyelembe vegyék annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató belső információbiztonsági szabályzata tartalmazza, amely pontosan meghatározza a tervezés és előkészítés, a projekt és kivitelezés, a működtetés és a menedzselés, valamint a visszacsatolás, illetve visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat. A belső információbiztonsági szabályzat figyelembe veszi az {Sz4} EN 319 411-2 szabvány 6.5.6 fejezetében előírt követelményeket.

6.6.2 Biztonságkezelési óvintézkedések

Szolgáltató olyan eszközöket és eljárásokat alkalmaz, melyek garantálják a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

A biztonságkezelési szabályokat a Szolgáltató PKI informatikai biztonságpolitikája {D5}, illetve biztonsági szabályzata {D6} tartalmazza.

6.6.3 Életciklus biztonsági óvintézkedések

Szolgáltató az alábbi táblázatban megadott rendszerességgel elvégzi a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

biztonsági ellenőrzés típusa		végzi	rendszeresség
operatív	IT infrastruktúra	rendszerüzemeltető operátorok	naponta
	szolgáltatás nyújtásához használt alkalmazások és naplók	rendszervizsgálók	naponta
belső ellenőrzés	IT infrastruktúra	biztonsági tisztviselő	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások és naplók	biztonsági tisztviselő	évente egyszer
külső ellenőrzés	IT infrastruktúra	külső auditor	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások és naplók	külső auditor	évente egyszer

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató {D6} biztonsági szabályzatában meghatározott követelményeknek megfelelően valósítja meg, melyek figyelembe veszik az {Sz4} EN 319 411-2 szabvány 6.5.7 fejezetében leírt követelményeket is.

6.8 Időforrások

A Szolgáltatások nyújtásához használt megbízható rendszereket Szolgáltató 24 óránként legalább egyszer, megbízható időforrásokkal (NTP) szinkronizálja az UTC időhöz.

A megbízható időforrások Szolgáltató saját rendszerén belüli, redundáns kialakítású, speciális célberendezések (referencia időforrások), melyek pontossága századmásodpercen belüli, és amelyek GPS alapúak, így visszavezethetők az UTC időforrásra.

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK / CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Tanúsítvány profil

Szolgáltató által kiadott tanúsítványok megfelelnek az {Sz9} RFC 5280, {Sz5} EN 319 412-1, {Sz6} EN 319-412-2, {Sz7} EN 319 412-3, {Sz8} EN 319-412-5 szabványoknak, valamint a vonatkozó jogszabályi előírásoknak.

Szolgáltató a kiadott tanúsítvány típusát, az {Sz8} EN 319-412-5 szabvány 4.2.3 fejezetének megfelelően, a `QcStatements` / `QcType` mezőben az alábbiak szerint jelöli meg:

tanúsítvány típusa	tanúsítvány alanya	QcStatements / QcType mező tartalma
[ALA] üzleti tanúsítvány	az Előfizetővel kapcsolatban álló természetes személy, akinek Előfizetővel való kapcsolata igazolásra került	id-etsi-qct-esign (0.4.0.1862.1.6.1)
[ALA] személyes tanúsítvány	az Előfizetővel kapcsolatban álló természetes személy, akinek Előfizetővel való kapcsolata igazolásra nem került	
[BÉLY] szervezeti tanúsítvány	az Előfizető szervezete vagy annak valamely szervezeti egysége	id-etsi-qct-es seal (0.4.0.1862.1.6.2)
[BÉLY] eszköz tanúsítvány	az Előfizető által vagy nevében működtetett informatikai eszköz vagy rendszer	

[KET] Szolgáltató a {J9} 137/2016 rendelet szerinti, kiadmányozási célra kiadott tanúsítványt úgy jelöli meg, hogy a tanúsítvány `CertificatePolicies` kiterjesztése a következő, technikai OID-t tartalmazza: 0.2.216.1.200.1100.100.42.3.7.

A tanúsítványprofil részletes leírását a {D8} dokumentum tartalmazza, melyet Szolgáltató igény esetén az Érintett Felek rendelkezésére bocsát.

7.1.1 Verziószám

A tanúsítványok verziószáma: V3.

7.1.2 Tanúsítvány kiterjesztések

A tanúsítványokban alkalmazott kiterjesztések mindenben követik az {Sz9} RFC 5280, {Sz5} EN 319 412-1, {Sz6} EN 319-412-2, {Sz7} EN 319 412-3, {Sz8} EN 319-412-5 szabványok, valamint a vonatkozó jogszabályok előírásait.

7.1.3 Algoritmus azonosítók

A tanúsítványok aláírásához alkalmazott algoritmus azonosítók RSA környezetben az alábbiak:

```
SHA256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
```

A tanúsítványok aláírásához alkalmazott algoritmus azonosítók ECC környezetben az alábbiak:

```
ecdsa-with-sha384 {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}
```

7.1.4 Név formák

A név formák leírását és azok értelmezési szabályait a 3.1 fejezet tartalmazza.

7.1.5 Név megszorítások

Szolgáltató a tanúsítványokban név megszorításokat (`NameConstraints`) nem tüntet fel.

7.1.6 Hitelesítési rend objektumazonosító

Szolgáltató a tanúsítványokban feltünteti a hitelesítési rend objektumazonosítóját.

7.1.7 Szabályzati megszorítások kiterjesztés használata

Szolgáltató a tanúsítványokban szabályzati megszorításokat (`PolicyConstraints`) nem tüntet fel.

7.1.8 Szabályzat minősítők szintaktikája és szemantikája

A tanúsítványban feltüntetett szabályzat minősítők (`PolicyQualifiers`) és megfelelő szöveg (`UserNotice`) jelzi a tanúsítvány alkalmazhatóságát.

7.1.9 A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása

A tanúsítvány hitelesítési rendek (`CertificatePolicies`) kiterjesztése nincs kritikusként megjelölve.

7.2 CRL profil

Szolgáltató által kiadott visszavonási listák megfelelnek az {Sz9} RFC 5280 műszaki szabványnak.

7.2.1 Verziószám

A visszavonási listák verziószáma: V2.

7.2.2 CRL és CRL bejegyzés kiterjesztések

A visszavonási lista az alábbi kiterjesztéseket tartalmazza „nem kritikus” megjelöléssel:

<code>CRLNumber</code>	a visszavonási lista szigorúan növekvő sorszáma
<code>AuthorityKeyIdentifier</code>	a kibocsátó CA kulcs azonosítója

A visszavonási lista a fentiekén túl más szabványos kiterjesztést is tartalmazhat, azonban ezek a kiterjesztések nem lehetnek „kritikus” jelzésűek.

Mivel a Szolgáltató a lejárt tanúsítványokhoz CRL formájában nem biztosít visszavonási információt, a CRL soha nem tartalmazza az `ExpiredCertsOnCRL` kiterjesztést.

7.3 OCSP profil

Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz13} RFC 6960 műszaki szabványnak.

7.3.1 Verziószám

Az OCSP válaszok verziószáma: V1.

7.3.2 OCSP kiterjesztések

Az OCSP válasz az alábbi kiterjesztéseket tartalmazza „nem kritikus” megjelöléssel:

<code>Nonce</code>	az OCSP kérdésben megadott, visszajátszásos támadások megelőzésére szolgáló véletlenszám (csak akkor, ha a kérdés tartalmazta azt)
<code>ArchiveCutoff</code>	az időpont, ameddig a Szolgáltató a tanúsítvány lejáratát után is biztosítja a visszavonási státuszt

Az OCSP válasz fentiekén túl más szabványos kiterjesztést is tartalmazhat, azonban ezek a kiterjesztések nem lehetnek „kritikus” jelzésűek.

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen bizalmi szolgáltatási szabályzat tartalmazza az összes, a nyilvános körben kibocsátott, minősített, elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokkal kapcsolatos szolgáltatás nyújtása során teljesíteni szükséges követelményt, melyet különösen az alábbi szabványok határoznak meg:

- EN 319 401: General policy requirements for Trust Service Providers {Sz2}
- EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements {Sz3}
- EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates {Sz4}
- EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz5}
- EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz6}
- EN 319 412-3: Certificate Profiles; Part 3: Certificate profiles for certificates issued to legal persons {Sz7}
- EN 319 412-5: Certificate Profiles; Part 5: QcStatements {Sz8}

8.1 Vizsgálatok gyakorisága és körülményei

Szolgáltató külső és belső vizsgálatokat végez, illetve végeztet annak érdekében, hogy a Szolgáltatásaival kapcsolatos folyamatai, eszközei, személyzete és környezete mindenkor megfeleljenek a vonatkozó jogszabályi és szabványi követelményeknek. A Szolgáltató érintett szervezetei és munkatársai kötelesek együttműködni a Szolgáltató által kijelölt auditorral, és biztosítani az ellenőrzéshez szükséges feltételeket.

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 Bizalmi Felügyelet is megvizsgálja a nyilvántartásba vételi eljárása során, valamint a szabályzatok módosításakor, és megfelelőség esetén közzé teszi a kötelezően benyújtandó szabályzatokat. A Bizalmi Felügyelet rendszeres időközönként átfogó helyszíni ellenőrzés keretében ellenőrizheti Szolgáltató tevékenységét.

Szolgáltató rendelkezik minőségbiztosítási rendszerrel és információbiztonsági irányítási rendszerrel, melyek megfelelő működését független rendszervizsgáló ellenőrzési tevékenysége biztosítja. Szolgáltató a külső, illetve a saját ellenőrző szervezet által végzett belső vizsgálatokat a {D6} PKI szolgáltatások biztonsági szabályzatában megjelölt rendszerességgel - évente legalább egyszer biztosítja.

Szolgáltató legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot végeztet a {J1} eIDAS, illetve a {J2} E-ügyintézési tv. követelményeinek való megfelelés tárgykörben. Szolgáltató az elkészült megfelelőségértékelés jelentést annak kézhezvételétől számított három munkanapon belül benyújtja a Bizalmi Felügyeletnek.

8.2 Auditor azonosítása és képesítése

A megfelelőségértékelés előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére Szolgáltató külső rendszervizsgálót alkalmaz.

A külső rendszervizsgáló által végzett auditokat Szolgáltató olyan szakértővel vagy szakértői szolgáltatásokat nyújtó szervezettel végezteti el, aki független Szolgáltatótól, illetve az ellenőrzött

rendszerből, területről, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

A megfelelőségértékelési vizsgálatot Szolgáltató olyan, a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezettel végezteti el, melyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére.

A Szolgáltató tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket a Szolgáltató belső szervezete végzi, az ott dolgozó biztonsági tisztviselők bevonásával.

8.3 Auditor függetlensége

A megfelelőségértékelő szervezet, a külső vizsgálatokat végző szervezet, annak munkatársai, valamint a külső rendszervizsgáló teljes mértékben függetlenek Szolgáltatótól.

8.4 Audit során vizsgált területek

Az audit az alábbi területeket fedi le:

- szabályzatok és dokumentációk;
- irányítási és ellenőrzési követelmények;
- személyzeti biztonsági követelmények;
- a szolgáltatói kulcspár kezeléséhez kapcsolódó követelmények;
- üzemeltetési és hozzáférési biztonság;
- fizikai és környezeti biztonság;
- folyamatos szolgáltatás biztosítása;
- adatbiztonság és archiválás.

Az audit során megvizsgálásra kerül, hogy Szolgáltató és az általa nyújtott Szolgáltatások megfelelnek-e:

- a hatályos jogszabályoknak és szabványoknak;
- a szolgáltatási szabályzatnak, illetve a bizalmi szolgáltatási rendnek.

8.5 Hiányosságok esetén végrehajtandó tevékenységek

Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére Szolgáltató intézkedési tervet készít. A hiányosságokat késlekedés nélkül orvosolja, az intézkedéseket dokumentálja és ellenőrzi.

A Bizalmi Felügyelet által végzett helyszíni ellenőrzések során feltárt esetleges hiányosságokat Szolgáltató a hatósággal megállapodott határidőn belül megszünteti a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembe vételével.

8.6 Eredmény kommunikációja

A belső és külső auditot, szakértői elemzést 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, azonban a hiányosságok felszámolásáról a Bizalmi Felügyeletet a következő helyszíni ellenőrzés során tájékoztatni kell. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 *Díjak*

A szolgáltatási díjakat Szolgáltató a Szolgáltatások internetes honlapján teheti közzé, vagy ártájékoztatót küldhet az érdeklődők számára. Szolgáltató jogosult a díjakat egyoldalúan meghatározni, módosítani.

Az Előfizetőre vonatkozó szolgáltatási díjak a Szolgáltatási Szerződésben kerülnek rögzítésre.

9.1.1 **Tanúsítvány kibocsátás díja**

Szolgáltató a kibocsátott, illetve megújított tanúsítványokért egyszeri vagy éves díjat számít fel Előfizető felé, ami tartalmazza:

- a tanúsítványok kibocsátásának díját;
- a tanúsítványtárban történő közzététel díját (ha a tanúsítvány közzétételéhez Előfizető hozzájárult)
- a tanúsítvány felfüggesztésének, újra-érvényesítésének, illetve visszavonásának díját (amennyiben ilyen tevékenységre sor kerül)
- a tanúsítványok lejárat után archiválásának díját.

9.1.2 **Tanúsítványhozzáférés díja**

Szolgáltató nem számít fel díjat a szolgáltatói, valamint a nyilvános tanúsítványtárban közzétett előfizetői tanúsítványok eléréséért.

9.1.3 **Visszavonási és állapot információ hozzáférés díja**

Szolgáltató nem számít fel díjat a tanúsítványok visszavonási állapotára vonatkozó státusz információk (CRL és OCSP) szolgáltatásáért.

9.1.4 **Egyéb szolgáltatások díja**

Amennyiben Előfizető azt megrendelte, Szolgáltató az elektronikus aláírást vagy bélyegzőt létrehozó eszközért (chipkártya + kártyaolvasó vagy USB token) egyszeri díjat számít fel, ami tartalmazza az eszköz megszemélyesítésének díját is.

9.1.5 **Visszatérítési szabályzat**

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

- a kibocsátott tanúsítvány valamely adata Szolgáltató hibájából nem megfelelő;
- a kibocsátott tanúsítvány, a magánkulcs és aktivizáló adat nem összetartozó;
- az elektronikus aláírást vagy bélyegzőt létrehozó eszközön szereplő adatok Szolgáltató hibájából fakadóan nem megfelelők (pl. a kártyára nyomtatott név hibás);
- a kibocsátott elektronikus aláírást vagy bélyegzőt létrehozó eszköz és aktivizáló kód nem összetartozó;

- e. Előfizető tanúsítványának kezelésekor Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét.

A visszatérítésre vonatkozó igényt Előfizetőnek a tanúsítvány kibocsátását követő 30 naptári napon belül írásban kell az Ügyfélkapcsolati Irodának bejelentenie Szolgáltató részére. Az igényt Szolgáltató köteles 15 naptári napon belül elbírálni.

A visszatérítési igény pozitív elbírálása esetén a Szolgáltató a tanúsítványt visszavonja, és:

- vagy új tanúsítványt bocsát ki Előfizető számára,
- vagy a fenntartási díjat 20 naptári napon belül Előfizető által megadott bankszámla számra vissza utalja.

A tanúsítvány kibocsátását követő 30 naptári napon túl az Előfizető kizárólag csak a Szolgáltató bizonyított szerződés- vagy kötelezettségszegése esetén jogosult a díj visszatérítésére.

Szolgáltató az egyéb tevékenységeiért számlázott díjak esetén díjvisszafizetésre nem köteles.

9.2 Anyagi felelősség

A Szolgáltató anyagi felelősségének mértékéről, illetve annak korlátairól a {D1} Általános Szerződési Feltételek rendelkezik.

A Szolgáltató kártérítésre a {D1} Általános Szerződési Feltételeknek megfelelően, az előfizetői szerződésben megjelölt összeghatárig kötelezhető, bizonyított helytállási kötelezettség esetén.

9.2.1 Biztosítási fedezet

A Szolgáltató rendelkezik olyan felelősségbiztosítással, mely egyaránt kiterjed az elektronikus aláírással vagy bélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, és amely fedezetet biztosít az összes károsultnak okozott kárra, a tanúsítványban jelzett, vagy a {D1} Általános Szerződési Feltételekben rögzített tranzakciós limit értékének legalább ötszöröséig. A tranzakciós limit összegét a Szolgáltatási Szerződés rögzíti, valamint a tanúsítvány minősített tanúsítvány nyilatkozatok (QCStatements) kiterjesztése tartalmazza (a `QcLimitValue` mezőben). A biztosítási szerződésben szereplő felelősségvállalási érték 3.000.000 Ft, vagy ennél esetenként magasabb összeg.

A felelősségbiztosítás ezen felül kiterjed az alábbiakra is:

- az E-ügyintézési tv. 88 §-ban foglalt kötelezettsége nem teljesítése miatt a Bizalmi Felügyeletnél felmerült, az E-ügyintézési tv. 89. §-a szerinti költségekre;
- a {J1} eIDAS 17. cikk (4) bekezdés e) pontja alapján a Bizalmi Felügyelet által felkért megfelelőségértékelő szervezet eljárásainak költségeire, ha ezt a Bizalmi Felügyelet eljárási költségként érvényesíti.

9.2.2 További követelmények

Szolgáltató rendelkezik a {J12} 24/2016 rendelet 20. §-a szerinti, huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával.

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltató minden olyan adatot és információt bizalmasnak tekint, melyek nem kerültek felsorolásra a 9.3.2 fejezetben.

9.3.2 Nem bizalmasnak tekintett információk köre

Nem bizalmasnak tekintett információk az alábbiak:

- szolgáltatói tanúsítványok és az azokban foglalt adatok;
- Előfizető tanúsítványba foglalt adatai;
- a tanúsítványokhoz kapcsolódó visszavonási információk;
- a Szolgáltató internetes honlapján közzétett nyilvános információk, szabályzatok és egyéb dokumentumok;
- az olyan adatok, melyek nyilvános adatforrásból elérhetők.

9.3.3 Bizalmas információk védelmének felelőssége

Szolgáltató a bizalmas információkhoz való hozzáférést csak az arra feljogosított személyek és szervezetek számára teszi lehetővé. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel juttatja érvényre.

9.4 Személyes adatok védelme

9.4.1 Adatvédelmi terv

Szolgáltató rendelkezik mind társasági szintű adatvédelmi tervvel ({D4}), mind pedig a Szolgáltatásokra vonatkozó adatvédelmi tájékoztatóval, melyek nyilvános dokumentumok, és elérhetők Szolgáltató internetes honlapján. Ezen dokumentumok összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

9.4.2 Bizalmasként kezelendő személyes adatok

Szolgáltató csak Előfizetőtől és Aláírótól közvetlenül, azok kifejezett írásos hozzájárulásával gyűjt személyes adatot és csak olyan mértékben, ami a tanúsítvány kiállításához, valamint Aláíró tájékoztatásához, személyazonosságának megállapításához szükséges.

Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

- Előfizető részéről a Szolgáltatói Szerződésben érintett személyek (pl. cégjegyzésre jogosult vezető, vagy Előfizető Kapcsolattartója) minden adatát;
- Aláírónak azon adatait, melyek a tanúsítványba nem kerülnek befoglalásra.

9.4.3 Bizalmasként nem kezelendő személyes adatok

Szolgáltató nem bizalmasként kezelendő személyes adatnak tekinti Aláírónak a tanúsítványba foglalt adatait, amennyiben Aláíró tanúsítványa közzétételéhez írásban hozzájárult.

Továbbá, nem bizalmas adat a tanúsítványhoz kapcsolódó státusz információ, minden tanúsítvány vonatkozásában. A státusz információba beleértendő a tanúsítvány - esetleges - visszavonásának oka és időpontja.

9.4.4 Személyes adatok védelmének felelőssége

Szolgáltató gondoskodik a személyes adatok védelméről, működése és szabályzatai megfelelnek a {J10} GDPR rendelkezéseinek.

9.4.5 Hozzájárulás a személyes adatok felhasználásához

Aláírónak a regisztrációs űrlap kitöltésével és aláírásával hozzá kell járulnia a tanúsítvány kiállításához szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához, valamint a kibocsátott tanúsítvány nyilvános közzétételéhez.

Bélyegzés célú tanúsítvány esetén Előfizető Kapcsolattartójának a regisztrációs űrlap kitöltésével és aláírásával hozzá kell járulnia a tanúsítvány kiállításához szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

Előfizetőnek a Szolgáltatási Szerződés aláírásával hozzá kell járulnia a tanúsítvány kiállításához és a szerződés megkötéséhez szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

9.4.6 Felfedés bírósági vagy polgári peres eljárás keretében

A Szolgáltató bűncselekmények felderítése vagy megelőzése céljából, illetve nemzetbiztonsági érdekből - az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén - a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztatja érintett Előfizetőt és/vagy Aláírót.

Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, és arról tájékoztatja érintett Előfizetőt és/vagy Aláírót.

Álneves tanúsítvány esetén Szolgáltató a tanúsítvány alany valódi személyazonosságára vonatkozó adatot is – mint jogszabályban meghatározott bizalmas információt – feltárja a fentiek szerint.

Álneves tanúsítvány esetén Szolgáltató a tanúsítvány alany valódi személyazonosságára vonatkozó adatot harmadik félnek – ide nem értve az első két bekezdésben leírt esetet – csak az Előfizető és Aláíró beleegyezésével adhatja át.

9.4.7 Egyéb, felfedést eredményező körülmények

Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatások nyújtásának megszüntetése esetén Előfizetők és Aláírók adatait a jogszabályi kötelezettségeire tekintettel átadja harmadik félnek.

9.5 Szellemi tulajdonjogok

A Szolgáltató által ügyfelei részére kibocsátott tanúsítványok és az ahhoz tartozó kulcspár tulajdonosa az Előfizető, teljes jogú használója pedig az Alany, aki/amely számára a tanúsítvány kibocsátásra került, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

Szolgáltató a szabályzataiban és feltételeiben ismertetett esetekben és módon a tanúsítványt közzé teheti, sokszorosíthatja, felfüggesztheti, visszavonhatja és egyéb módon is kezelheti. A végfelhasználói tanúsítványokban szereplő megkülönböztető név és egyéb azonosítók használatára Előfizető és/vagy az Alany jogosult.

A Szolgáltató tulajdonát képezik a szolgálati tanúsítványok, visszavonási információk, a végfelhasználói tanúsítványokban szereplő, Szolgáltató által létrehozott azonosítók.

Szolgáltató kizárólagos tulajdonát képezik a szabályzatai, szerződéses feltételei és egyéb, a Szolgáltatások internetes honlapján közzétett dokumentumai. Ezen dokumentumok felhasználása csak és kizárólag a Szolgáltatások használatával összefüggésben engedélyezett, minden egyéb kereskedelmi vagy egyéb célú felhasználása szigorúan tilos.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

Szolgáltató felel a bizalmi szolgáltatási rendben és jelen szolgáltatási szabályzatban, valamint az Előfizetővel megkötött Szolgáltatási Szerződésben megfogalmazott valamennyi kötelezettsége maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat egyéb alvállalkozók végeznék.

Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a {J5} Polgári Törvénykönyv 6:519. §-a szerint, a vele szerződéses jogviszonyban álló Előfizetővel szemben a szerződésszegésért való felelősség ({J5} Polgári Törvénykönyv 6:142. §) szabályai szerint felelős az elektronikus aláírással vagy bélyegzővel hitelesített elektronikus dokumentummal okozott kárért, ha megszegte a bizalmi szolgáltatási rendben és a jelen szolgáltatási szabályzatban, valamint az Előfizetővel megkötött Szolgáltatási Szerződésben előírtakat, vagy az esemény időpontjában hatályos jogszabály szerinti, rá vonatkozó kötelezettségeket. E kötelezettségek megtartását kétség esetén Szolgáltatónak kell bizonyítania. Szolgáltató sajátjaként felel az egyéb alvállalkozók által a Szolgáltatások nyújtása során okozott kárért.

Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért az Előfizetővel megkötött Szolgáltatási Szerződésben és a 9.8 fejezetben foglalt korlátozásokkal kártérítést fizet.

Szolgáltató nem felel:

- az Alanyok (Aláírók és Bélyegző Létrehozók) magánkulccsal, illetve az aláírás- vagy bélyegző létrehozó eszközzel kapcsolatos tevékenységéért;
- az Érintett felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért;
- az Érintett Felek vagy mások által kibocsátott szabályzatokért.

Szolgáltató kötelezettsége

Szolgáltató azzal, hogy kibocsát egy előfizetői tanúsítványt – mely jelen szolgáltatás szabályzat hatálya alatt került kiadásra – arra vállal kötelezettséget, hogy a Szolgáltatások nyújtása során ő maga és a Szolgáltatások nyújtásában közreműködő egyéb alvállalkozói a jelen szabályzatban foglaltakat maradéktalanul betartják. Szolgáltató megteszi a szükséges és tőle telhető intézkedéseket ahhoz, hogy az Előfizetők és Alanyok is jelen szabályzat előírásainak megfelelően járjanak el.

9.6.2 A regisztrációs szervezet felelőssége és helytállása

A regisztrációs tevékenységeket Szolgáltató saját szervezetén belül üzemeltetett Ügyfélkapcsolati Irodája és Regisztrációs Irodája végzi. Az Ügyfélkapcsolati Iroda és a Regisztrációs Iroda betartja a rá vonatkozó, jogszabályokban, illetve a Szolgáltató szabályzataiban foglalt előírásokat.

Szolgáltató felelőssége a tanúsítvány kiadása során:

- Előfizető teljes körű és közérthető tájékoztatása a 4.1.2 fejezet 1) pontjában meghatározottakról;
- a tanúsítvány alanyának azonosítása:
 - üzleti- és személyes tanúsítvány esetén a természetes személy alany azonosítása a 3.2.3 fejezetben leírt eljárással, továbbá üzleti tanúsítvány esetén a szervezeti azonosságot is hitelesítenie kell a 3.2.2 fejezetben leírt eljárással;
 - szervezeti- és eszköz tanúsítvány esetén a szervezeti azonosság hitelesítése a 3.2.2 fejezetben leírt eljárással;
- Előfizető Kapcsolattartója személyének azonosítása és eljárási jogosultságának megállapítása;
- a tanúsítvány alanyának megkülönböztető nevébe (Subject) kerülő minden adat ellenőrzése közhiteles nyilvántartások alapján, ahol ez lehetséges (kivéve a {J9} 137/2016 13.§ szerinti esetben, ha az Előfizetővel ezirányú szerződést kötöttek, és az ellenőrzés elvégzését Előfizető igazolni tudja);
- a tanúsítvány egyéb mezőibe és kiterjesztéseibe kerülő adatok ellenőrzése;
- a regisztrációhoz és a tanúsítvány kiállításához szükséges adatok rögzítése az erre szolgáló informatikai rendszerben;
- a rögzített kérelemben foglalt adatokkal a megfelelő tanúsítvány előállítása az Előfizető által biztosított kulcspárhoz vagy a Szolgáltató által előállított kulcspárhoz;
- az opcionálisan megrendelt aláírás- vagy bélyegző létrehozó eszköz megfelelő megsemmisítése;
- ha a kulcspárt Szolgáltató állította elő, akkor a magánkulcshoz tartozó aktivizáló adatok biztonságos előállítása, tárolása, és átadása az arra jogosult személynek.

9.6.3 Előfizető felelőssége és helytállása

Előfizető jogai

Előfizető jogosult:

- a Szolgáltatások igénybe vételére a jelen szolgáltatási szabályzatban, a Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben leírtak szerint;
- kapcsolattartó személyt kijelölni;
- az általa meghatározott Alanyok számára tanúsítványt igényelni;
- a tanúsítványok felfüggesztését és visszavonását kérni;
- a felfüggesztett tanúsítvány újra-érvényesítését kérni.

Előfizető felelőssége

Az Előfizető felelősségét a Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek határozzák meg.

Előfizető kötelezettségei

Előfizető kötelessége a Szolgáltató szabályzatainak és szerződéses feltételeinek megfelelően eljárni a Szolgáltatások használata során, beleértve a tanúsítványok igénylését és alkalmazását. Az Előfizető kötelezettségeit a jelen szolgáltatási szabályzat, a Szolgáltatási Szerződés és annak {D1} Általános Szerződési Feltételek melléklete tartalmazzák.

Az Alany jogai

Az Alany (Aláíró vagy Bélyegző Létrehozó) jogosult:

- a számára kiadott tanúsítványt és a kapcsolódó magánkulcsot az 1.4.1 fejezetben leírt célokra és jelen szabályzatban leírt módon használni;
- a tanúsítvány felfüggesztését vagy visszavonását kérni;
- a felfüggesztett tanúsítvány újra-érvényesítését kérni;
- a tanúsítványhoz kapcsolódó egyéb szolgáltatásokat használni a jelen szabályzatban leírt módon.

Az Alany felelőssége

Az Alany (Aláíró vagy Bélyegző Létrehozó) felelős:

- a regisztráció során megadott adatainak valóságáért, pontosságáért és érvényességéért;
- a tanúsítványba foglalt adatok ellenőrzéséért;
- az adataiban bekövetkezett változás haladéktalan bejelentéséért;
- az aláírás- vagy bélyegző létrehozó eszköze biztonságos kezeléséért;
- a magánkulcs és az aktivizáló adat biztonságos kezeléséért;
- a tanúsítvány és a magánkulcs szabályzatoknak megfelelő felhasználásáért;
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyek esetén;
- általában, a jelen szabályzatban előírt kötelezettségei betartásáért.

Az Alany kötelezettségei:

Az Alany (Aláíró vagy Bélyegző Létrehozó) köteles:

- a Szolgáltatások használata előtt megismerni jelen szolgáltatási szabályzatot;
- a Szolgáltató által kért, a Szolgáltatások igénybe vételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően megadni;
- a Szolgáltatásokat kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a jelen szabályzatban és a hivatkozott dokumentumokban foglaltaknak megfelelően használni;
- adat változás (különösen a tanúsítványba foglalt valamely adat) esetén haladéktalanul írásban értesíteni erről Szolgáltatót, a tanúsítvány felfüggesztését vagy visszavonását kezdeményezni és beszüntetni a tanúsítvány használatát;
- biztosítani, hogy a Szolgáltatások igénybe vételéhez szükséges adatokhoz és eszközökhöz (különösen az aláírás- vagy bélyegző létrehozó eszközhöz, aktivizáló adatokhoz) illetéktelen személy ne férhessen hozzá;
- haladéktalanul kezdeményezni a tanúsítvány felfüggesztését vagy visszavonását, amennyiben a tanúsítványhoz kapcsolódó magánkulcs, az aláírás- vagy bélyegző létrehozó eszköz vagy az aktivizáló adat illetéktelen kezekbe kerültek vagy megsemmisültek, megrongálódtak, elvesztek, valamint haladéktalanul megszüntetni a tanúsítvány és magánkulcs használatát;
- kulcs kompromittálódás vagy jogellenes használat gyanúja esetén a Szolgáltató megkereséseire a Szolgáltató által megadott időtartamon belül reagálni;
- tudomásul venni, hogy Előfizető jogosult a tanúsítvány visszavonását vagy felfüggesztését kérni;
- tudomásul venni, hogy Szolgáltató a tanúsítványt a jelen szabályzatban leírt módon és ellenőrzési lépések elvégzése után bocsátja ki;
- tudomásul venni, hogy Szolgáltató a 4.9.1 fejezetben ismertetett körülmények esetén jogosult a tanúsítványt visszavonni;
- a magánkulcs és a kapcsolódó tanúsítvány használatát haladéktalanul és végérvényesen beszüntetni, amennyiben tudomására jut, hogy a Szolgáltató valamely, a tanúsítvány kibocsátásában érintett hitelesítő központja kompromittálódott;

- haladéktalanul, írásban értesíteni Szolgáltatót, ha a tanúsítvánnyal vagy az annak felhasználásával létrehozott elektronikus aláírással vagy bélyegzővel kapcsolatban jogvita indul.

9.6.4 Érintett felek felelőssége és helytállása

Az Érintett Felek a saját belátásuk és/vagy szabályzataik szerint dönthetnek az egyes tanúsítványok elfogadásáról és a felhasználás módjáról. A tanúsítvány érvényességének elbírálása során az Érintett Félnek megfelelő körültekintéssel kell eljárnia, ezért különös tekintettel javasolt:

- a szolgáltatási szabályzatban foglalt követelmények és előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a tanúsítvány felhasználására vonatkozó valamennyi korlátozás figyelembe vétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel
- a tőle elvárható magatartás tanúsítása a tanúsítvány ellenőrzésekor.

Szolgáltató kizárja a felelősségét (9.8 fejezet), amennyiben az Érintett Fél a tanúsítvány vagy az azon alapuló elektronikus aláírás vagy bélyegző elfogadásakor nem körültekintően, vagy nem a tőle elvárható gondossággal jár el.

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

Szolgáltató kizárja felelősségét, amennyiben:

- az Érintett Fél nem körültekintően jár el a tanúsítványok ellenőrzése és felhasználásra során, azaz nem jelen szolgáltatási szabályzatnak vagy a hatályos jogszabályoknak megfelelően jár el;
- az Érintett Felek vagy mások által kibocsátott szabályzatok nem felelnek meg jelen szabályzatnak;
- az Internet, vagy annak egy részének működési hibájából fakadóan tájékoztatási vagy egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- Aláíró vagy Előfizető Kapcsolattartója által megadott értesítési email cím időközben megváltozott vagy megszűnt, és ebből fakadóan Szolgáltató nem tudja őket értesíteni;
- az Előfizető nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek;
- az Alany (Aláíró vagy Bélyegző Létrehozó) nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek;
- a károkozás a Bizalmi Felügyelet Szolgáltatónak kiadott, hatályos határozatában közölt kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

Szolgáltató korlátozza a kártérítési felelősségét:

- a tanúsítvánnyal egy alkalommal vállalható kötelezettség mértékében (tranzakciós limit), mely a tanúsítványban és a Szolgáltatási Szerződésben feltüntetésre kerül;
- összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban fizetendő kártérítési összeg tekintetében.

Az aláíró tanúsítványokhoz különböző tranzakciós limitek társíthatók, például annak függvényében, hogy az aláíró személy az adott szervezeten belül – a belső folyamatok szerint - milyen értékhatárig

rendelkezik aláírási jogosultsággal. Szolgáltató nem felelős az olyan károkért, melyek a tanúsítványban feltüntetett, egy alkalommal vállalható kötelezettségvállalás összeghatárát (tranzakciós limit) meghaladó ügyletekben aláírt vagy bélyegzett elektronikus dokumentumokból származnak.

Szolgáltató nem felelős az olyan károkért, melyek abból adódnak, hogy az Érintett Fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és a mérvadó műszaki szabványok szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot, illetve magatartást.

A Szolgáltató pénzügyi felelősségének korlátját a Szolgáltatási Szerződés, illetve a {D1} Általános Szerződési Feltételek határozza meg. Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja ezt az összeget, akkor az egyes kártérítési igények megtérítése az összes kártérítési igénynek a megadott összeghez viszonyított arányában történik.

9.9 Kártérítések

A kártérítésekről a jelen szabályzat 9.8 fejezetében leírtakon túl a Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek rendelkeznek.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

A szolgáltatási szabályzat egy adott verziójának időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és határozatlan időre szól. Az időbeli hatály megszűnik a szolgáltatási szabályzat újabb verziójának hatályba lépésével vagy a Szolgáltatások befejezésekor.

Tárgyi hatály

A szolgáltatási szabályzat tárgyi hatálya kiterjed a Szolgáltatások nyújtására és igénybe vételére.

Személyi hatály

A szolgáltatási szabályzat személyi hatálya kiterjed Szolgáltatónak a Szolgáltatások nyújtásában közreműködő munkatársaira, továbbá az Előfizető kapcsolattartójaként kijelölt személyekre, az Aláírókra, és Előfizető szervezetén belül az egyes elektronikus bélyegzők felhasználásáért felelős személyekre.

9.10.2 Megszűnés

A bizalmi szolgáltatási szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket – amennyiben ilyenek vannak – a {D1} Általános Szerződési Feltételek és a Szolgáltatási Szerződés tartalmazza.

9.11 Egyéni hirdetmények és kommunikáció a résztvevőkkel

Azokban az esetekben, melyekre jelen szolgáltatási szabályzat nem rendelkezik a felek közötti értesítésről, illetve annak joghatást kiváltó módjáról, a Szolgáltató értesítése írásban vagy emailben, Előfizető Kapcsolattartója vagy az Aláíró saját kezű vagy elektronikus aláírásával hitelesítve az Ügyfélkapcsolati Iroda elérhetőségeire való beküldéssel történik. Az elektronikus értesítés csak a Szolgáltató általi visszaigazolást követően tekinthető kézbesítettnek. Szolgáltató a megkeresésekre 30 napon belül válaszol elektronikus aláírással vagy bélyegzővel ellátott válasz üzenetben.

9.12 Módosítások

9.12.1 Módosítás eljárása

A szolgáltatási szabályzat módosítása az 1.5.3 és 1.5.4 fejezetekben leírt szabályok szerint történik. A szolgáltatási szabályzat módosulását a verziószám megfelelő változása jelzi.

9.12.2 Értesítés módszere és időtartama

A Szolgáltatások jelentős vagy lényeges változása esetén Szolgáltató internetes honlapján közleményt tesz közzé és emailben tájékoztatást küld Előfizetőknek, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett a felek a változásokra felkészülhessenek.

9.12.3 OID megváltozását előidéző körülmények

A szolgáltatási szabályzat új verziójával az OID verziószámot jelentő része megfelelően változik.

9.13 Vitás kérdések rendezése

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

Panaszt írásban vagy személyesen, az Ügyfélkapcsolati Iroda elérhetőségein lehet előterjeszteni. A panaszt a Szolgáltató az előterjesztéstől számított 30 napon belül kivizsgálja és ennek eredményéről a panaszost írásban tájékoztatja.

A jogviták esetén követendő eljárást a {D1} Általános Szerződési Feltételek tartalmazza.

Bármely vitás kérdés felmerülése esetén Előfizető jogosult az esetleges bírósági eljárást megelőzően békéltető testülethez fordulni, amennyiben jogszabályok szerinti fogyasztónak minősül. Az illetékes békéltető testület megnevezését és elérhetőségeit jelen szabályzat 1.5.2 fejezete tartalmazza.

9.14 Irányadó jog

Szolgáltató szerződéseire, szabályzataira és azok teljesítésére a magyar jog az irányadó és azokat a magyar jog szerint kell értelmezni.

9.15 Hatályos jognak megfelelés

Szolgáltató tevékenységét a mindenkor hatályos Európai Unió, illetve magyar jogszabályoknak megfelelően köteles végezni.

9.16 Vegyes rendelkezések

Nincs kikötés.

9.16.1 Teljességi záradék

Nincs kikötés.

9.16.2 Átruházás

Nincs kikötés.

9.16.3 Részleges érvénytelenség

A jelen szolgáltatási szabályzat egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 Igényérvényesítés

Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben a szolgáltatási szabályzat más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 Force Majeure (Vis maior)

Vis maior: Az olyan – a Szolgáltató akaratától, cselekedeteitől és személyétől függetlenül bekövetkező és érdekkörén kívül eső elháríthatatlan – esemény (pl. sztrájk, háború, polgári felkelés, természeti katasztrófa, a Felek bármelyikének partnerénél felmerülő elháríthatatlan fizikai vagy jogi akadály vagy más elháríthatatlan sürgősségi helyzet) minősül vis maiornak, amely megakadályozza vagy lehetetlenné teszi a jelen szolgáltatási szabályzatban foglalt követelmény teljesítését, feltéve, hogy ezen körülmények a jelen szolgáltatási szabályzat hatálybalépését követően keletkeznek, illetőleg azt megelőzően következtek be, ám a jelen szolgáltatási szabályzat teljesítésére kiható következményeik az említett időpontban még nem voltak előre láthatóak.

Szolgáltató nem felelős a vis maior esetekből fakadó károkért.

9.17 Egyéb rendelkezések

Szolgáltató a Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználói termékeket hozzáférhetővé teszi a fogyatékossgal élő személyek számára, amennyiben az lehetséges.