Szolgáltatási Szabályzat titkosító és autentikációs tanúsítványokhoz (HSZSZ-T)

Verziószám:	**v.1.12**
OID:	**0.2.216.1.200.1100.100.42.3.5.23.**
Hatályba lépés dátuma:	**2026.05.04.**
Dokumentum besorolása:	**NYILVÁNOS**

Jóváhagyó	Adorján István
Adorján István	Digitálisan aláírta: Adorján István Dátum: 2026.04.28 17:23:28 +02'00'

NISZ

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0	2013.08.01.	Első változat	Kővári Ferenc Joláthy Dániel	Kővári Ferenc	Ferencz Attila
1.1	2014.03.17.	CAB BR követelmények szerint módosított változat	Kővári Ferenc Joláthy Dániel	Kővári Ferenc	Ferencz Attila
1.2	2014.05.14.	Jogi hivatkozásokkal és pontosításokkal módosított változat	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila
1.3	2015.03.04	HSM és BALE tanúsítások átvezetése, bizalmi munkakörök kiegészítése	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila
1.4	2015.06.01	Új HSM modulok feltüntetése	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila
1.5	2016.08.01	• RFC 3647 szerint átdolgozás • SSL szerver tanúsítványok kivezetése • OID változás: 0.2.216.1.200.1100.100.42.3.5.10 → 0.2.216.1.200.1100.100.42.3.5.22	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.6	2022.09.23	• új algoritmuskészletek bevezetésével kapcsolatos módosítások • egyéb pontosítások	Kővári-Szabó Zoltán	Nagy Benjámin Melo Sándor	Adorján István
1.7	2023.09.21	• A 2048 bit hosszúságú RSA kulcsok kivezetése	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.8	2024.01.02	• Székhelyváltozás átvezetése	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.9.	2024.09.01.	• általános felülvizsgálat • változó jogszabályi környezet (E-ügyintézés tv., DÁP tv.) okán történő módosítás • OID kepzes megváltozott szabályainak átvezetése	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
1.10	2025.11.14.	• ÁSZF alapú szerződéskötés • általános felülvizsgálat	Buczynskiné dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán Nagy Benjámin	Adorján István
1.11	2025.12.05	4 éves tanúsítványra történő áttérés	Buczynskiné dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán	Adorján István
1.12.	2026.04.24.	• felfüggesztés időtartam módosítása • akadálymentes sablon használata	Buczynskiné dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán	Adorján István

NISZ

Tartalom

1. BEVEZETÉS

(1.) Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: Szolgáltató) Szolgáltatási Szabályzata, mely a titkosító, autentikációs és egyéb speciális célú tanúsítványokkal kapcsolatos szolgáltatásaira vonatkozik (a továbbiakban: HSZSZ-T).

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

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

1.1. Áttekintés

(4.) 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.

(5.) Jelen szolgáltatási szabályzat a „Hitelesítési Rend titkosító és autentikációs tanúsítványokhoz” (HR-TET) hatálya alá tartozó Szolgáltatásokra vonatkozik.

(6.) 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.

(7.) 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.

1.2. Dokumentum neve és azonosítása

(8.) Jelen szolgáltatási szabályzat teljes neve NISZ Zrt. „Szolgáltatási Szabályzat titkosító és autentikációs tanúsítványokhoz”.

(9.) A szolgáltatási szabályzat rövid neve: HSZSZ-T.

(10.) A szolgáltatási szabályzat objektum azonosítója és verziószáma a címlapon található.

(11.) Jelen HSZSZ-T tartalmazza a HR-TET hitelesítési 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 HSZSZ-T-nek csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.1. Hitelesítési rendek

(12.) A jelen szolgáltatási szabályzathoz kapcsolódó HR-TET hitelesítési rend megfelel az {Sz3} EN 319 411-1 szabvány 5.3 fejezet c) pontjában meghatározott LCP hitelesítési rendnek:

```
LCP: Lightweight Certificate Policy
```

```
itu-t(0) identified-organization(4) etsi(0) other-certificate-
policies(2042) policy-identifiers(1) lcp (3)
```

1.3. PKI közösség

1.3.1. Hitelesítő szervezet

(13.) 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.

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

1.3.1.1. Gyökér hitelesítő központ

(15.) 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.

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

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

(16.) 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

(17.) 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

1.3.1.2. Produktív hitelesítő központ

(18.) A Szolgáltató ECC alapú produktív hitelesítő központja P-384-es görbét alkalmazó ECC kulcsával és SHA384 algoritmus felhasználásával ECC és RSA alapú végtanúsítványokat bocsát ki az Előfizetők, illetve a velük kapcsolatban álló Alanyok részére. Az ECC produktív hitelesítő központ főbb adatai a következők:

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

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

1.3.2. Regisztrációs szervezet

(19.) A Szolgáltató – saját szervezetén belül – Ügyfélkapcsolati irodát és Regisztrációs irodát működtet.

(20.) 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.

(21.) 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.

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

1.3.3. Előfizetők és Alanyok

(23.) Előfizető az {D1} ÁSZF-GOVCA szerinti feltételeknek megfelelő, 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.

(24.) A tanúsítvány alanya (a továbbiakban: Alany):

a) természetes személy: az Előfizetővel kapcsolatban álló személy;

b) jogi személy: az Előfizető szervezete, vagy annak valamely szervezeti egysége;

c) eszköz: az Előfizető által vagy nevében működtetetett informatikai eszköz vagy rendszer.

1.3.3.1. Előfizető Kapcsolattartója

(25.) 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 képvisletre jogosult személy(ek)en felül – ezen személy aláírását fogadja el a tanúsítványokkal kapcsolatos ügyekben, különösen a tanúsítvány igénylési folyamatban, a tanúsítvány visszavonási folyamatban, átvételében az ezekhez kapcsolódó kérelmeken. Kapcsolattartó kijelölésének hiányában Szolgáltató csak képviseleti joggal rendelkező személy aláírását fogadja el a tanúsítványokkal kapcsolatos ügyekben.

(26.) 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, ha a szöveg adott szakasza ettől eltérő megállapítást nem tesz.

1.3.4. Érintett felek

(27.) Érintett Fél: olyan természetes vagy jogi személy, aki/amely a HR-TET hitelesítési rend hatálya alatt kiadott tanúsítvány érvényességét ellenőrzi, és erre hagyatkozva jár el.

1.3.5. 1.3.5 Egyéb felek

(28.) Nincs kikötés.

1.4. A tanúsítvány alkalmazhatósága

(29.) A HR-TET hatálya alatt kiadott titkosító és autentikációs tanúsítványok típusai az {Sz3} EN 319 411-1 szerint az alábbiak lehetnek:

a) 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);

b) szervezeti tanúsítvány: a tanúsítvány Alanya az Előfizető szervezet, vagy annak valamely szervezeti egysége;

c) eszköz tanúsítvány: a tanúsítvány Alanya az Előfizető által vagy nevében működtetett informatikai eszköz vagy rendszer.

(30.) A titkosító tanúsítvány, illetve a hozzá kapcsolódó kulcspár adatok vagy üzenetek titkosításához és visszafejtéséhez alkalmazható.

(31.) Az autentikációs tanúsítvány, illetve a hozzá kapcsolódó kulcspár személy, eszköz vagy szervezet PKI alapú azonosítására alkalmazható.

1.4.1. Teszt tanúsítványok

(32.) 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.

(33.) 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.

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

(35.) A teszt tanúsítványokhoz semmilyen joghatás nem kapcsolódik.

1.4.2. Engedélyezett tanúsítvány használat

(36.) A titkosító tanúsítványhoz kapcsolódó nyilvános kulcs kizárólag adatok vagy üzenetek titkosítására (kódolására), a kapcsolódó magánkulcs kizárólag a titkosított adatok vagy üzenetek visszafejtésére (dekódolására) használható fel.

(37.) Az autentikációs tanúsítványok, illetve a kapcsolódó magánkulcs személyek, eszközök vagy szervezetek hiteles azonosítására használható fel, a vonatkozó műszaki szabványok és protokollok szerint (pl. {Sz7} RFC 5246}).

(38.) Az üzleti tanúsítványokat az Alanyok csak és kizárólag az Előfizetőhöz kapcsolódó tevékenységükhöz (munkaviszonyukból fakadó feladataik elvégzéséhez) használhatják fel.

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

1.4.3. Tiltott tanúsítvány használat

(40.) Tilos a tanúsítványt, illetve a hozzá kapcsolódó kulcspárt felhasználni az 1.4.1 fejezetben leírt célokon kívüli bármilyen más célra, vagy bármilyen – Szolgáltatóval nem egyeztetett - hitelesítés szolgáltatás nyújtásához.

(41.) A fentieken túl, tilos felhasználni a titkosító tanúsítványt és a kapcsolódó kulcspárt titkosításra vagy visszafejtésre minden olyan esetben, amelyben valamilyen jogszabály korlátozásokat vagy tiltásokat ír elő (pl. államellenes tevékenységek). Tilos felhasználni az autentikációs tanúsítvány és a kapcsolódó kulcspárt bármilyen csalárd indíttatású azonosítási, illetve félrevezetési céllal, vagy szándékos megtévesztés céljából.

(42.) Mind az üzleti, szervezeti és eszköz tanúsítványokat az Alanyok 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

(43.) A Szolgáltató szervezetén belül Szabályozási Csoportot működtet, amely többek között jelen szolgáltatási szabályzat karbantartásáért is felelős.

1.5.2. Kapcsolat

1.5.2.1. 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 https://hiteles.gov.hu/szabalyzatok oldalon, az „Adatkezelési tájékoztató kormányzati hitelesítés-szolgáltatásokhoz” címen érhető el.

1.5.2.2. Ügyfélkapcsolati Iroda

(44.) 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 mindenkori nyitvatartási időket a Szolgáltató a Szolgáltatások internetes honlapján teszi közé.

Cím:	1097 Budapest, Vaskapu utca 30/b.
Telefon:	+36 1 795-7200
E-mail:	info@hiteles.gov.hu
Szolgáltatások internetes honlapja:	https://hiteles.gov.hu/

1.5.2.3. Telefonos HelpDesk

(45.) 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

1.5.2.4. Illetékes fogyasztóvédelmi felügyelőség

Budapest Főváros Kormányhivatala, Fogyasztóvédelmi Főosztály

Cím:	1051 Budapest, Sas u. 19.
Telefon:	+36 1 450-2598
E-mail:	fogyved_kmf_budapest@bfkh.gov.hu

1.5.2.5. 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

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

(47.) A változtatási igényeket a Szabályozás Csoport gyűjti, a módosításokat elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

1.5.4. Szabályzat jóváhagyásának eljárása

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

(49.) A jóváhagyás előtt a Szolgáltató megvizsgálja a szolgáltatási szabályzat hitelesítési rendnek való megfelelését.

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

(51.) A jóváhagyott szolgáltatási szabályzatot a Szolgáltatásokért felelős vezető lépteti hatályba a szabályzat hitelesítése által. A hatályba lépés napját a dokumentum címlapja tartalmazza. A szolgáltatási szabályzat új verziója mindig új verziószámmal kerül nyilvánosságra és közzétételre Szolgáltató internetes honlapján.

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

1.6. Fogalmak, rövidítések és hivatkozások

1.6.1. Fogalmak

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

(54.) Az ezen felül alkalmazott fogalmak meghatározását a HR-TET 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 Cryptogaphy	elliptikus görbe alapú kriptográfia
LCP	Lightweight Certificate Policy	könnyűsúlyú hitelesítési rend
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
RA	Registration Authority	regisztrációs szervezet

RSA	Riverst-Shamir-Adleman	aláíró algoritmus
SHA	Secure Hash Algorithm	lenyomatképző algoritmus
SSL	Secure Socket Layer	a TLS protokoll elődje
TSL	Transport Layer Security	Interneten keresztüli kommunikációhoz védelmet biztosító titkosítási protokoll

1.6.3. Hivatkozások

1.6.3.1. Jogszabályi hivatkozások

{J1}	2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (a továbbiakban: DÁP tv.)
{J2}	2013. évi V. törvény a Polgári Törvénykönyvről (a továbbiakban: Ptk.)
{J3}	321/2024. (XI.6.) Korm.rend. a digitális állampolgárság egyes szabályairól
{J4}	320/2024. (XI.6.) Korm.rend.
{J5}	a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (a továbbiakban: Nytv.)

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 319 412-2	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
{Sz6}	EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issues to legal persons
{Sz7}	RFC 5246	The Transport Layer Security (TSL) Protocol, Version 1.2
{Sz8}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz9}	ITU-T X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz10}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz11}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework

{Sz12}	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
{Sz13}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz14}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz15}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules
{Sz16}	TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

1.6.3.3. Hivatkozott dokumentumok

{D1}	Általános Szerződési Feltételek a NISZ Zrt. kormányzati hitelesítés szolgáltatásaihoz (ÁSZF-GOVCA)
{D2}	Szolgáltatási Szerződés (SZSZ)
{D3}	NISZ Zrt. Szervezeti és Működési Szabályzata (SZMSZ)
{D4}	NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}	NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}	NISZ Zrt. PKI szolgáltatások biztonsági szabályzata (GOVCA-BSZ)
{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. 2 KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR

2.1. Tanúsítványtár

(55.) 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 %-os rendelkezésre állással biztosítja, úgy, hogy a kiesés nem lépheti túl esetenként a 24 órás időtartamot.

(56.) 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

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

(58.) A Szolgáltató a végfelhasználói tanúsítványt internetes honlapján nyilvánosan elérhető, kereshető tanúsítványtárában csak akkor teszi közzé, ha a tanúsítvány alanya a tanúsítvány közzétételéhez hozzájárult.

(59.) 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

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

(61.) Szolgáltató a végfelhasználói tanúsítványokat a nyilvánosan kereshető tanúsítványtárban Előfizető hozzájárulása esetén a kibocsátást követő 24 órán belül teszi közzé.

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

(63.) 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 7 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

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

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

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

(67.) 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. 3 AZONOSÍTÁS ÉS HITELESÍTÉS

3.1. Elnevezések

3.1.1. Név típusok

(68.) A tanúsítványban szereplő nevek megadása megfelel az {Sz9} ITU-T X.520 szabványnak. Ezen túl:

(69.) A tanúsítvány alanya (`Subject`) mező tartalma megfelel:

a) üzleti tanúsítvány esetén: az {Sz5} EN 319 412-2 szabvány 4.2.4 fejezetében foglalt előírásoknak;

b) szervezeti vagy eszköz tanúsítvány esetén: az {Sz6} EN 319 412-3 szabvány 4.2.1 fejezetében foglalt előírásoknak.

(70.) A tanúsítvány kibocsátója (`Issuer`) mező tartalma megfelel:

a) az {Sz5} EN 319 412-2 szabvány 4.2.3.1 fejezetében foglalt előírásoknak.

3.1.2. Nevek jelentése

(71.) A tanúsítványban szereplő név-attribútumok jelentése megegyezik az {Sz9} ITU-T X.520 szerintivel.

(72.) Ezen felül, az 1.4 fejezet szerinti tanúsítványtípusok `Subject` mezőjében szereplő névattribútumokra a következő alfejezetekben megadott képzési és igazolási szabályok érvényesek. A Szolgáltató fenntartja a jogot az egyes személyeket vagy csoportokat esetlegesen sértő (pl. jó ízlést, szemérmet, etnikai hovatartozást sértő) álnevek és egyéb adatok visszautasítására.

3.1.2.1. Üzleti tanúsítvány alanyára vonatkozó képzési és igazolási szabályok

(73.) Üzleti tanúsítvány esetén mind a természetes személy Alanyra, mind az Előfizető szervezetére vonatkozó, a tanúsítványban feltüntetésre kerülő név-attribútumokat ellenőrizni és igazolni kell.

név-attribútum	leírás	igazolás / ellenőrzés módja
surname	Az Alany vezetékneve, betű szerint azonos a személy azonosítására használt okmányban feltüntetetett 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 utóneve, betű szerint azonos a személy azonosítására használt okmányban feltüntetett viselt utónévvel, amely egy vagy több keresztnevet 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.	
title	Az Alany szervezetben viselt beosztása. Opcionális.	Hivatalos szervezeti dokumentum (pl. cégkivonat) alapján ellenőrzött, vagy a {D9} űrlapon Előfizető Kapcsolattartójának írásos nyilatkozata alapján igazolt adat.
countryName	A szervezet székhelyének ország kódja. Kötelező.	Hivatalos szervezeti dokumentum (pl. alapító okirat, cégkivonat) alapján ellenőrzött és igazolt adat.
localityName	A szervezet székhelyének helység neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat vagy, cégkivonat) alapján ellenőrzött, igazolt adat.
organizationName	A szervezet hivatalos (teljes vagy rövid) neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat vagy cégkivonat) alapján ellenőrzött, 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.

1. táblázat - Üzleti tanúsítvány név attribútumai

(74.) 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. Szervezeti tanúsítvány alanyára vonatkozó képzési és igazolási szabályok

(75.) Szervezeti tanúsítvány esetén az Előfizető szervezetére vonatkozó, a tanúsítványban feltüntetésre kerülő név-attribútumokat ellenőrizni és igazolni kell.

név-attribútum	**leírás**	**igazolás / ellenőrzés módja**
`commonName`	A szervezet hivatalos (teljes vagy rövid) neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat vagy 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 vagy cégkivonat) alapján ellenőrzött, igazolt adat.
`localityName`	A szervezet székhelyének helységneve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat vagy cégkivonat) alapján ellenőrzött, igazolt adat.
`organizationName`	A szervezet hivatalos (teljes vagy rövid) neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat vagy 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.

2. táblázat - Szervezeti tanúsítvány név-attribútumai

(76.) 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. Eszköz tanúsítvány alanyára vonatkozó képzési és igazolási szabályok

(77.) Eszköz tanúsítvány esetén az Előfizető szervezetére vonatkozó, a tanúsítványban feltüntetésre kerülő név-attribútumokat ellenőrizni és igazolni kell.

név-attribútum	**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 vagy cégkivonat) alapján ellenőrzött, igazolt adat.
localityName	A szervezet székhelyének helységneve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat vagy cégkivonat) alapján ellenőrzött, igazolt adat.
organizationName	A szervezet hivatalos (teljes vagy rövid) neve. Kötelező.	Hivatalos szervezeti dokumentum (pl. létesítő okirat vagy 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.

3. táblázat - Eszköz tanúsítvány név-attribútumai

(78.) 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

(79.) Az Előfizetők névtelensége nem megengedett.

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

(81.) Az álneves tanúsítványok felismerhetőségére vonatkozó szabályok:

a) az álnév a tanúsítvány `Subject` / `pseudonym` mezőjében szerepel; és

b) a `Subject` / `commonName` mező az álnevet „~" (tilde) karakterekkel határolva tartalmazza[1].

3.1.4. Különféle név formák megjelenítési szabályai

(82.) A tanúsítványba foglalt megkülönböztető nevek (`Distinguished Name`) ASN.1 szintaxisa az [Sz8} RFC 5280 szerinti, megjelenítési szabályait az {Sz10} RFC 4514 adja meg.

3.1.5. A nevek egyedisége

(83.) A tanúsítvány alanyának 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

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

(85.) Szolgáltatónak nem kötelessége a márkanevek és védjegyek jogos használatának ellenőrzése, nem vállal közvetítő vagy döntnöki szerepet az ilyen jellegű viták feloldásában.

(86.) Szolgáltató nem garantálja Előfizetők számára a védjegyeik feltüntetését a tanúsítványban.

3.2. Kezdeti azonosítás

(87.) Szolgáltató a vonatkozó szabványoknak 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.

(88.) A szervezeti azonosság igazolásához megfelelő hivatalos dokumentum (pl. hatályos alapító okirat, törzskönyvi kivonat, 30 napnál nem régebbi cégkivonat) szükséges, amennyiben ennek adattartalma nem vagy nem megfelelően szerepel közhiteles nyilvántartásban, továbbá aláírási címpéldány vagy ezzel egyenértékű hivatalos dokumentum (pl. aláírás minta és kinevezési okirat) elektronikus másolatának Szolgáltató részére történő eljuttatása, valamint az eredeti dokumentumok bemutatása szükséges.

(89.) Az Előfizető által kijelölt Kapcsolattartó azonosítását a személyazonosításra alkalmas hatósági igazolvány személyes bemutatásával kell elvégezni Szolgáltató előtt.

(90.) Szolgáltató a vonatkozó nemzetközi szabványoknak megfelelően, közvetlenül vagy harmadik fél révén, ellenőrzi annak a természetes vagy jogi személynek az azonosságát és - adott esetben – egyedi jellemzőit, akinek vagy amelynek a részére a tanúsítványt kibocsátja.

3.2.1. A magánkulcs birtoklása

(91.) Szolgáltató meggyőződik arról, hogy az Alany a tanúsítványhoz kapcsolódó magánkulcsot birtokolja.Mivel az igényelt tanúsítványhoz kapcsolódó kulcspárt Szolgáltató állította elő, a magánkulcs a szoftveres kulcstároló

[1] Pl. ~Ludas Matyi~

eszköz vagy hardveres kulcstároló eszköz (chipkártya, USB token) és az ahhoz tartozó aktivizáló adat (PIN kód) átadásával kerül az Alany birtokába.

3.2.2. A szervezeti azonosság hitelesítése

(92.) 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 valódiságát és hatályosságát közhiteles nyilvántartás alapján, vagy ha ilyen közhiteles nyilvántartás nincsen, az igényléshez bekért hivatalos dokumentum (pl. 30 napnál nem régebbi cégkivonat, alapító okirat) alapján ellenőrzi. A tanúsítvány kibocsátása előtt Szolgáltató ellenőrzi a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személy képviseleti jogának fennállását, a tanúsítványba foglalt jogviszony meglétét, jogszabály, közhiteles nyilvántartás, létesítő okirat vagy ezek hiányában meghatalmazás alapján.

3.2.3. A személyazonosság hitelesítése

(93.) Szolgáltató a természetes személy alany személyazonosságát az alany vagy nem természetes személy alany esetén alany kapcsolattartója személyes megjelenését igénylő regisztrációval ellenőrzi, kivéve azon esetekben, amikor alkalmazható az aláíró vagy bélyegző tanúsítvánnyal történő személyazonosítás elvégzése összhangban a DÁP tv. foglaltakkal. Szolgáltató a természetes személy alany 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.

(94.) Amennyiben a természetes személy alany külföldi állampolgár és nem rendelkezik az Nytv. szerinti személyazonosító igazolvánnyal, akkor a Szolgáltató EGT állampolgár esetén az állandó személyazonosító igazolványának vagy külföldi útlevelének, továbbá harmadik országbeli állampolgár esetén a külföldi útlevelének másolata alapján ellenőrzi az adatokat.

3.2.4. Előfizető nem ellenőrzött adatai

(95.) Szolgáltató ellenőriz és igazol minden, a tanúsítvány alany mezőjébe (`Subject`) kerülő adatot.

(96.) Az ellenőrzés és igazolás módszere:

a) üzleti tanúsítvány esetén a 3.1.2.1 fejezetben;

b) szervezeti tanúsítvány esetén a 3.1.2.2 fejezetben;

c) eszköz tanúsítvány esetén a 3.1.2.3 fejezetben került ismertetésre.

(97.) A tanúsítvány egyéb mezőibe és kiterjesztésébe kerülő adatok tekintetében azok valódiságáról Előfizető Kapcsolattartója – üzleti tanúsítvány esetén a természetes személy alany is - írásban nyilatkozott a {D9} Űrlap kitöltésével és aláírásával.

3.2.5. Jogosultság ellenőrzése

(98.) Szolgáltató ellenőrzi, hogy a {D9} Űrlapot az arra jogosult személy írta alá.

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

3.2.6. Együttműködési kritériumok

(100.) Szolgáltató a Szolgáltatások nyújtása során nem működik együtt más hitelesítés-szolgáltatókkal.

3.3. Azonosítás és hitelesítés kulcscsere esetén

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

(102.) A Szolgáltató nem nyújt kulcscsere szolgáltatást.

(103.) 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

(104.) Nincs kikötés.

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

(105.) Nincs kikötés.

3.4. Azonosítás és hitelesítés visszavonási vagy felfüggesztési kérelem esetén

3.4.1. Visszavonási kérelem esetén

(106.) Visszavonási igényt az Előfizető Kapcsolattartója – vagy üzleti célú tanúsítvány esetén – maga az Alany (ezen fejezet esetében a továbbiakban együttesen: jogosult ügyfél) az Ügyfélkapcsolati Iroda számára az alábbiak szerint nyújthat be:

a) Személyesen, saját kézzel aláírt papír alapú dokumentumon

A jogosult ügyfél személyesen, a Szolgáltató Ügyfélkapcsolati irodájában a Szolgáltató weboldalán elérhető {D10} Visszavonási kérelem űrlap kitöltésével, saját kezű aláírásával az Ügyfélkapcsolati munkatárs számára történő átadásával vagy a Szolgáltató számára postai úton beküldött {D10} Visszavonási kérelem űrlap beküldésével igényelhet tanúsítványvisszavonást.

b) Elektronikus aláírással ellátott dokumentumon

A jogosult ügyfél tanúsítványvisszavonást elektronikusan a Szolgáltató weboldalán elérhető {D10} Visszavonási kérelem űrlap kitöltésével, legalább fokozott biztonságú elektronikus aláírásával a Szolgáltató e-mail címére megküldve.

3.4.2. Felfüggesztési kérelem esetén

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

(108.) Az üzleti tanúsítvány felfüggesztését az Alany vagy Előfizető Kapcsolattartója kérheti.

(109.) A szervezeti vagy eszköz tanúsítvány felfüggesztését Előfizető Kapcsolattartója kérheti.

(110.) A fentiek szerint, az Alanynak vagy Előfizető Kapcsolattartójának azonosításához a hívónak 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. 4 A TANÚSÍTVÁNYOK ÉLETCIKLUSA

4.1. Tanúsítványigénylés

4.1.1. Ki nyújthat be tanúsítvány igénylést

(111.) A tanúsítványigénylési kérelmeket Előfizető Kapcsolattartójaként megjelölt személy nyújthatja be Szolgáltató részére.

4.1.2. Igénylési folyamat és felelősségek

(112.) A tanúsítványigénylés folyamata az alábbi:

1) A {D9} Űrlap lentebb olvasható módon történő beküldésével és az Ügyfélkapcsolati Iroda általi feldolgozásával megvalósuló sikeres tanúsítványigénylés esetén a Szolgáltató munkatársa az Előfizető számára Szolgáltatási Szerződést készít elő. A Szolgáltató az Előfizetőt a Szolgáltatási Szerződésben részletesen tájékoztatja az alábbiakról:

   a) a tanúsítvány használati lehetőségeiről;

   b) a kulcstároló eszköz (chipkártya, USB token) használatáról;

   c) a magánkulcs használatával kapcsolatos intézkedésekről, a magánkulcs védelméhez szükséges biztonsági intézkedésekről;

   d) az Alanyok és a tanúsítványt elfogadni 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 tárgybeli, időbeni, földrajzi vagy egyéb korlátozásokról; i) a szolgáltatói nyilvános kulcsról;

   j) a szolgáltatási szabályzat elérhetőségéről és tartalmáról.

2) A Szolgáltató kétféle szerződéskötési folyamatot követ:

   a) bizonyos feltételek együttes fennállása esetén a szolgáltatási szerződés létrejön az Általános Szerződési Feltételek (ÁSZF-GOVCA) elfogadásával,

   b) minden más esetben a Szolgáltató és az Előfizető egyedileg létrejött szolgáltatási szerződést (a továbbiakban: Egyedi Szolgáltatási Szerződés) köt.

3) A Szolgáltató és az Előfizető az alábbi feltételek együttes fennállása esetén szolgáltatási szerződést köt Általános Szerződési Feltételek (ÁSZF-GOVCA) elfogadásával:

   a) az Előfizető számára az igényelt tanúsítvány-szolgáltatás jogszabály alapján díjmentesen biztosítható(ak)[2],

   b) az Előfizető az adott tanúsítvány-szolgáltatáshoz nem igényelt úgynevezett Minősített Elektronikus Aláírást Létrehozó Eszközt (röviden: MALE, angolul: QSCD; az elérhető termékeket a Szolgáltató hivatalos honlapján teszi közzé),

   c) az Előfizető személyazonosítása és az elkészült tanúsítvány-szolgáltatás átadás-átvétele díjmentes formában valósul meg (különösképpen a Szolgáltató telephelyén),

[2] A DÁP tv. 39. § (6) bekezdés szerint a tanúsítvány-szolgáltatás díjmentesen biztosítható a DÁP tv. 9. § (2) bekezdés szerinti szerveknek, szervezeteknek és intézményeknek. Az adott jogszabály alapján a díjmentességet az Ügyfélkapcsolati Iroda állapítja meg (úgynevezett igénybevételi jogalap validáció).

d) az Előfizető a megrendelő űrlapon egyértelmű nyilatkozatával megértette és elfogadta az ÁSZF-GOVCA aktuális verzióját és a benne foglaltakat,

e) a megrendelő űrlap Szolgáltató számára történő elektronikus levélformában történő beküldésekor az Előfizető nem élt az egyedi Szolgáltatási szerződéskötés lehetőségével.

4) A Szolgáltató nyilvános ajánlata és a szolgáltatás ÁSZF-GOVCA-ban foglaltakkal összhangban történő igénylése eredményeképp a Szolgáltatási Szerződés megkötöttnek minősül, ha:

a) az Előfizető igénye megfelel az előzőekben megjelölt feltételeknek,

b) a megrendelő űrlap hiánypótlás nélkül feldolgozható;

c) a tanúsítvány-szolgáltatás kibocsátása (gyártás) megvalósult.

5) A Szolgáltatási szerződés 3) pontban megjelölt módon történő megkötése írásbelinek minősül.

6) Egyedi Szolgáltatási Szerződés megkötése

Szolgáltató és Előfizető a 2) b. pontjában rögzített esetben írásbeli egyedi szerződést köt egymással.

(113.) Az 1) pontban foglalt tanúsítványigénylésekhez kitöltésre és Előfizető Kapcsolattartója által aláírásra kerül egy {D9} Űrlap.

(114.) A {D9} Űrlap benyújtható [...]

a) papíralapon, személyesen az Ügyfélkapcsolati Irodában,

b) papíralapon postai úton az Szolgáltatónak címezve,

c) elektronikus aláírással/aláírásokkal ellátva a Szolgáltató hivatalos honlapján feltüntetett e-mail címre megküldve.

(115.) A {D9} Űrlapot az Előfizető Kapcsolattartója és üzleti tanúsítvány esetén annak leendő alanyának saját kezű vagy elektronikus aláírásával kell ellátni.

(116.) Az űrlapok aláírt és beszkennelt 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.

(117.) Az űrlap kitöltésével és aláírásával Előfizető Kapcsolattartója, továbbá üzleti tanúsítvány esetén a természetes személy alany is:

a) nyilatkozik az űrlapon megadott adatok valódiságáról;

b) nyilatkozik a {D1} Általános Szerződési Feltételek, valamint a szolgáltatási szabályzat elfogadásáról;

c) hozzájárul ahhoz, hogy személyes adatait Szolgáltató kezelje;

d) hozzájárul ahhoz, hogy Szolgáltató a kibocsátott tanúsítványt a nyilvános tanúsítványtárban közzé tegye.

(118.) A kitöltött {D9} regisztrációs űrlapot, valamint csatolmányait (pl. alapító okirat, aláírási címpéldány) a Szolgáltató Ügyfélkapcsolati Irodája ellenőrzi és szükség esetén hiánypótlást kér.

(119.) Hiánytalan igénylés esetén az Ügyfélkapcsolati Iroda a 3.2 fejezetben leírt módon és eljárásokkal elvégzi a szervezeti azonosság, illetve a személyazonosság ellenőrzését és igazolását, és intézkedik a tanúsítványkérelem előállításáról és annak feldolgozásáról.

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

4.2. Tanúsítványigénylés feldolgozása

4.2.1. Azonosítási és hitelesítési műveletek

(121.) A tanúsítványigénylés elfogadása előtt Szolgáltató a 3.2 fejezetben leírt módon elvégzi Előfizető Kapcsolattartójának, valamint a tanúsítvány alanyának azonosítását és adatainak ellenőrzését, a kitöltött {D9} Űrlap és csatolmányainak (pl. cégkivonat, alapító okirat, törzskönyvi kivonat, aláírási címpéldány) a felhasználásával.

4.2.2. Tanúsítványigénylés elfogadása vagy visszautasítása

(122.) 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:

a) üzleti tanúsítvány esetén a 3.1.2.1 fejezetben;

b) szervezeti tanúsítvány esetén a 3.1.2.2 fejezetben;

c) eszköz tanúsítvány esetén a 3.1.2.3 fejezetben került ismertetésre.

(123.) Szolgáltató visszautasítja a tanúsítványigénylés elfogadását:

a) hiányos vagy nem megfelelően kitöltött űrlap esetén;

b) ha úgy ítéli meg, hogy az igényelt tanúsítvány valamely jogszabály (különösen a {J1} DÁP tv., {J3} 321/2024 Korm. rendelet) vonatkozó rendelkezése miatt nem adható ki;

c) ha a személyazonosító adatokkal, az okmányok személyhez tartozásával, eredetiségével, valódiságával kapcsolatban kétség merül fel;

d) ha a szervezeti azonosság, a képviseleti jog, a szervezethez való tartozás igazolására bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével

e) kapcsolatban kétség merül fel;

f) az esetlegesen kért álnév egyes személyeket vagy csoportokat esetlegesen sért (pl. jó ízlést, szemérmet, etnikai hovatartozást).

4.2.3. Tanúsítványigénylés feldolgozás időtartama

(124.) Szolgáltató a tanúsítványigényléseket a benyújtást követően a Szolgáltatási Szerződésben rögzített időtartamon belül, ennek hiányában a {D1} Általános Szerződési Feltételekben jelzett 15 naptári napon belül feldolgozza.

4.3. Tanúsítvány kibocsátás

4.3.1. Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

(125.) Az Ügyfélkapcsolati Iroda továbbítja az elfogadott tanúsítványigénylésén alapuló kérelmet a Regisztrációs Irodának.

(126.) A Regisztrációs Iroda:

a) a Szolgáltatásokat támogató informatikai rendszerben elindítja a tanúsítvány létrehozását, melynek során a kulcspár generálása a 6.1.6 fejezetben leírt módon történik meg.

4.3.2. Előfizető értesítése a tanúsítvány kibocsátásról

(127.) A Regisztrációs Iroda emailben értesíti Előfizető Kapcsolattartóját – és üzleti tanúsítvány esetén az Alanyt - a tanúsítvány elkészültéről és egyeztetnek az elkészült tanúsítvány átvételének módjáról és időpontjáról.

(128.) Az átvétel történhet az Ügyfélkapcsolati Iroda helyszínén, vagy az Előfizető helyszínén.

(129.) A 3.2. fejezetben foglalt Kapcsolattartó az átvétel során átveszi:

a) a felfüggesztési jelszót tartalmazó lezárt borítékot;

b) a tanúsítványt és a magánkulcsot:

- a megrendelt kulcstároló eszközt (chipkártya, USB token) és az ahhoz tartozó PIN és PUK kódot tartalmazó lezárt borítékot; vagy
- a PKCS#12 formátumnak megfelelő (szoftveres) kulcstárolót (CD adathordozón) és az ahhoz tartozó PIN kódot tartalmazó lezárt borítékot.

(130.) 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 szakrendszerében naplózza, hogy a tanúsítványt és a kapcsolódó magánkulcsot mikor adta át az arra jogosultnak.

4.4. Tanúsítvány-elfogadás

4.4.1. Tanúsítvány Előfizető általi elfogadása

(131.) A 4.3.2 fejezetben említett „Átvételi elismervény és tanúsítvány elfogadás” bizonylat kinyomtatva tartalmazza a kiadott tanúsítvány adatait és a tanúsítványba foglalt adatokat.

(132.) A tanúsítványt átvevő Kapcsolattartó ez alapján ellenőrzi és aláírásával igazolja, hogy a tanúsítványba foglalt adatok megegyeznek a {D9} Űrlapon szereplő adatokkal, a kiadott tanúsítványt elfogadja. Ezen felül, az Alanynak 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 a {D9} Űrlapon szereplő adatokkal vagy nem felelnek meg a valóságnak, akkor a tanúsítvány nem kerül átadásra, és a Szolgáltató a tanúsítványt visszavonja.

(133.) Ha a tanúsítvány átvételére nem került sor az Ügyfélkapcsolati Iroda általi értesítéstől számított 60 napon belül, akkor Szolgáltató a tanúsítványt visszavonja.

4.4.2. Tanúsítvány közzététele

(134.) Az Előfizető - valamint az üzleti tanúsítványok esetén az Alany - 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

(135.) Nincs kikötés.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. Az Előfizető magánkulcs- és tanúsítvány használata

(136.) Az Alany csak azt követően használhatja a tanúsítványt és a kapcsolódó magánkulcsot, hogy a tanúsítványban foglalt adatok helyességéről meggyőződött.

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

(138.) Az Alanynak a magánkulcs és tanúsítvány használata során be kell tartania a 9.6.3 fejezetben ismertetett kötelezettségeit, különösen gondoskodnia kell kulcstároló eszköz (chipkártya, USB token vagy a PKCS#12 formátumnak megfelelő szoftveres kulcstároló) és az aktivizáló adat (PIN kód) illetéktelen hozzáférés elleni védelméről.

4.5.2. Az Érintett felek nyilvános kulcs- és tanúsítvány használata

(139.) A jelen szabályzat hatálya alatt kibocsátott tanúsítvány elfogadása során szükséges, hogy az Érintett Fél megfelelő körültekintéssel és gondossággal járjon el, melyhez javasolt betartania az alábbi ajánlásokat:

a) a tanúsítványok ellenőrzését olyan megbízható alkalmazással végezze, amely képes az 1.6.3.2 fejezetben megadott műszaki szabványok támogatására és azokat helyesen valósítja meg;

b) az előző pontban említett alkalmazást megbízható, vírusmentes környezetben használja, továbbá az alkalmazás beállítási lehetőségei helyesen legyenek konfigurálva;

c) a tanúsítványokat csak olyan alkalmazásokban fogadja el, melyek összhangban vannak a tanúsítvány „kulcshasználat” (`KeyUsage`) és „kiterjesztett kulcshasználat” (`ExtendedKeyUsage`) kiterjesztésének tartalmával;

d) végezze el a tanúsítványra az {Sz8} RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítési, valamint visszavonás ellenőrzést, a tanúsítványt csak ezen ellenőrzések pozitív eredménye esetén fogadja el;

e) vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítvány által hivatkozott szabályzatokban szerepel. 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

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

(141.) A Szolgáltató nem nyújt tanúsítványmegújítás szolgáltatást.

(142.) 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} Űrlapon megadott email címre.

4.6.1. Tanúsítvány megújítás körülményei

(143.) Nincs kikötés.

4.6.1.1. Ki kérelmezhet tanúsítvány megújítást

(144.) Nincs kikötés.

4.6.1.2. Tanúsítvány megújítási kérelmek feldolgozása

(145.) Nincs kikötés.

4.6.1.3. Az Előfizető értesítése a megújított tanúsítvány kibocsátásáról

(146.) Nincs kikötés.

4.6.1.4. Tanúsítvány Előfizető általi elfogadása

(147.) Nincs kikötés.

4.6.1.5. Megújított tanúsítvány közzététele

(148.) Nincs kikötés.

4.6.1.6. További felek értesítése tanúsítvány megújításról

(149.) Nincs kikötés.

4.7. Kulcscsere

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

(151.) A Szolgáltató nem nyújt kulcscsere szolgáltatást.

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

4.7.1.1. Kulcscsere körülményei

(153.) Nincs kikötés.

4.7.1.2. Ki kérelmezhet kulcscserét

(154.) Nincs kikötés.

4.7.1.3. Kulcscsere kérelmek feldolgozása

(155.) Nincs kikötés.

4.7.1.4. Előfizető értesítése az új tanúsítvány kibocsátásáról

(156.) Nincs kikötés.

4.7.1.5. Új tanúsítvány Előfizető általi elfogadása

(157.) Nincs kikötés.

4.7.1.6. Új tanúsítvány közzététele

(158.) Nincs kikötés.

4.7.1.7. További felek értesítése az új tanúsítvány kibocsátásáról

(159.) Nincs kikötés.

4.8. Tanúsítvány-módosítás

(160.) 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.

(161.) A Szolgáltató nem nyújt tanúsítvány-módosítás szolgáltatást.

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

4.8.1.1. Tanúsítvány-módosítás körülményei

(163.) Nincs kikötés.

4.8.1.2. Ki kérelmezhet tanúsítvány-módosítást

(164.) Nincs kikötés.

4.8.1.3. Tanúsítvány-módosítási kérelmek feldolgozása

(165.) Nincs kikötés.

4.8.1.4. Előfizető értesítése az új tanúsítvány kibocsátásáról

(166.) Nincs kikötés.

4.8.1.5. Módosított tanúsítvány Előfizető általi elfogadása

(167.) Nincs kikötés.

4.8.1.6. Módosított tanúsítvány közzététele

(168.) Nincs kikötés.

4.8.1.7. További felek értesítése a módosított tanúsítvány kibocsátásáról

(169.) Nincs kikötés.

4.9. Tanúsítvány visszavonás és felfüggesztése

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

(171.) 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.

(172.) A visszavont / felfüggesztett tanúsítványt nem lehet felhasználni.

(173.) A visszavont tanúsítványhoz tartozó magánkulcs használatát azonnal be kell szüntetni. A visszavonási kérelemnek a Szolgáltatóhoz történő megérkezéséig az Előfizető, illetve az Alany 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.

(174.) Az Érintett Feleknek javasolt ellenőrizniük a tanúsítvány visszavonási állapotát a tanúsítvány elfogadása előtt.

4.9.1. Visszavonás körülményei

(175.) Szolgáltató visszavonja a tanúsítványt, ha:

(176.) Előfizető Kapcsolattartója vagy az Alany ezt kéri;

- fennáll az a lehetőség vagy gyanú, hogy a tanúsítványhoz tartozó magánkulcs kompromittálódott;
- adatváltozás vagy egyéb ok miatt.

(177.) a felfüggesztett tanúsítvány újra-érvényesítése nem történik meg 4.9.16 fejezet szerinti, felfüggesztésre megengedett időtartamon belül;

(178.) a tanúsítvány átvételére nem került sor az Ügyfélkapcsolati Iroda általi értesítéstől számított 60 napon belül;

(179.) Szolgáltató a Szolgáltatásokkal kapcsolatos rendellenességről szerez tudomást;

(180.) Szolgáltató tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy a tanúsítványt jogellenesen használták, vagy a Szolgáltató által biztosított kulcstároló eszközt jogosulatlan személy használhatta;

(181.) a visszavonást jogszabály kötelezővé teszi;

(182.) Szolgáltató a tevékenységét befejezi;

(183.) a tanúsítvány formátuma vagy műszaki tartalma (pl. kriptográfiai algoritmus vagy kulcsméret már nem biztonságos) elfogadhatatlan kockázatot jelent az Érintett Felek részére.

4.9.2. Ki kezdeményezheti a visszavonást

(184.) Visszavonást kezdeményezheti a 4.9.1 fejezetben megjelölt esetekben:

a) Előfizető Kapcsolattartója vagy az Alany;

b) Szolgáltató (ide értve azt az esetet is, amikor a visszavonás jogszabályi előírás miatt történik).

4.9.3. Visszavonási kérelemre vonatkozó eljárás

(185.) A visszavonási kérelem érvényes, legalább 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.

(186.) A visszavonási kérelem kitöltéséhez, illetve teljesítéséhez a következő adatok szükségesek:

a) a tanúsítvány alanyának neve (CN érték),
b) a tanúsítvány sorozatszáma,
c) tanúsítvány érvényességének kezdete,
d) visszavonást kérő személy azonosító adatai,
e) visszavonás oka, az ahhoz vezető körülmények.

(187.) 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.

(188.) 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.

(189.) 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.

(190.) A tanúsítvány visszavonásáról vagy a visszavonási kérelem visszautasításáról a Szolgáltató emailben tájékoztatást küld.

(191.) A tanúsítvány visszavonásáról vagy a visszavonási kérelem visszautasításáról a Szolgáltató emailben elsősorban a {D10} Visszavonási kérelmet beküldő felet értesíti. Amennyiben nem állapítható meg a kérelmet beküldő fél, abban az esetben az adott eset körülményeit figyelembe véve az értesítés az Előfizető Kapcsolattartója vagy az Aláíró számára kerül megküldésre.

(192.) A határidők megállapítása okán a postai vagy személyes úton beérkező kérelmet az Ügyfélkapcsolati- vagy Regisztrációs Iroda munkatársa saját kezűleg aláírja és dátummal látja el. Az elektronikusan keletkezett {D10} Visszavonási kérelem nem kerül a Szolgáltató által aláírásra.

4.9.4. Kivárási idő visszavonási kérelem esetén

(193.) Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

4.9.5. Visszavonási kérelem feldolgozásának időbelisége

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

4.9.6. Visszavonás ellenőrzésének ajánlása az Érintett felek számára

(195.) 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

(196.) Az előfizetői tanúsítványokra vonatkozó CRL kibocsátásának gyakorisága: 24 óránként legalább egy CRL. A CRL tartalmazza a következő kibocsátás időpontját (a `nextUpdate` mezőben).

(197.) 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.

(198.) Szolgáltató minden kibocsátáskor törli a CRL-ről azokat a tanúsítványokat, melyek érvényessége a CRL kibocsátásnak időpontjában már lejárt.

(199.) 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

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

4.9.9. OCSP szolgáltatás biztosítása

(201.) 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

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

4.9.11. Visszavonási állapot közlés más formái

(203.) Szolgáltató a honlapján elérhető nyilvános tanúsítványtárban is közzé teszi a visszavonási állapot információt, tájékoztatási jelleggel.

4.9.12. Különleges követelmények a kulcs kompromittálódása esetére

(204.) Szolgáltató a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről honlapján tájékoztatást tesz közzé, Előfizetőket és az Alanyokat emailben értesíti.

(205.) 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

(206.) Szolgáltató felfüggeszti a tanúsítványt, ha:

a) Előfizető Kapcsolattartója vagy az Alany ezt kéri;

b) a felfüggesztést jogszabály kötelezővé teszi.

4.9.14. Ki kérelmezhet felfüggesztést

(207.) Felfüggesztést kezdeményezhet, a 4.9.13 fejezetben megjelölt esetekben:

a) Előfizető Kapcsolattartója vagy az Alany;

b) Szolgáltató (ide értve azt az esetet, amikor a felfüggesztés jogszabályi előírás miatt történik).

4.9.15. Felfüggesztésre vonatkozó eljárás

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

(209.) A felfüggesztési kérelem teljesítéséhez a következő adatokat kell megadni:

a) a tanúsítvány sorszáma, vagy egyéb olyan adatok, amely alapján a Szolgáltató rendszerében a tanúsítvány egyértelműen azonosítható;

b) felfüggesztést kérő azonosító adatai és email címe;

c) felfüggesztés oka, az ahhoz vezető körülmények;

d) felfüggesztési jelszó.

(210.) 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.

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

(212.) 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

(213.) A tanúsítvány felfüggesztett állapotban legfeljebb 30 naptári napig - illetve, ha utolsó naptári nap nem munkanap, akkor a következő munkanapig - lehet.

(214.) 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 emailben értesíti.

(215.) 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

(216.) Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában biztosítja.

4.10.1.1. CRL

(217.) A Szolgáltató által kibocsátott CRL megfelel az {Sz8} RFC 5280 szabványnak.

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

(219.) Végfelhasználói tanúsítványokra vonatkozó CRL elérhetősége:

http://nqca.hiteles.gov.hu/ecc/crl/govca-ecc-sec.crl

(220.) Szolgáltatói tanúsítványokra vonatkozó CRL elérhetősége:

http://qca.hiteles.gov.hu/ecc/crl/govca-ecc-root.crl

4.10.1.2. OCSP

(221.) A Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz12} RFC 6960 szabványnak. Az OCSP szolgáltatást Szolgáltató az {Sz12} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően működteti.

(222.) 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 érvényességét ne kelljen ellenőrizni.

(223.) Az OCSP szolgáltatás keretében a Szolgáltató biztosítja a visszavonási információt a tanúsítvány lejárját követően is, 10 évig.

(224.) Végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége:

http://nqocsp.hiteles.gov.hu/ocsp-sec

(225.) Szolgáltatói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége:

http://qocsp.hiteles.gov.hu/ocsp-root

4.10.2. Szolgáltatás rendelkezésre állása

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

4.10.3. Opcionális funkciók

(227.) Nincs kikötés.

4.11. Az előfizetés vége

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

4.12. Kulcsletét és visszaállítás

(229.) A Szolgáltató nem nyújt kulcsletét szolgáltatást.

4.12.1. Kulcsletét és visszaállítás szabályai

(230.) Nem értelmezett.

4.12.2. Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

(231.) Nem értelmezett.

5. FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

(232.) 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.

(233.) 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 bárminemű változtatást a Szolgáltató vezetősége hagy jóvá.

(234.) A biztonságkezelési szabályokat a Szolgáltató {D5} GovCA szolgáltatások biztonságpolitikája tartalmazza. Ez a szabályzat biztonsági okokból nem nyilvános. A Szolgáltató informatikai rendszerei vonatkozásában a {D6} GovCA 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 összeférhetetlenségi kritériumokat.

(235.) Szolgáltató megvalósította és folyamatosan fenntartja a Szolgáltatásokat nyújtó eszközök, rendszerek biztonsági ellenőrzéseit és üzemeltetési eljárásait. A Szolgáltató belső ellenőrzései és külső auditjai ezen eljárásokat, a vonatkozó dokumentumokat és a Szolgáltatásokra vonatkozó előírások teljesülését rendszeres időközönként vizsgálja.

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

(237.) 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.

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

5.1. Fizikai óvintézkedések

5.1.1. Telephely elhelyezése és szerkezeti felépítése

(239.) 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

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

(241.) Ehhez biztosítja az alábbiakat:

a) a gépterembe történő minden belépés naplózásra kerül;

b) a gépterembe csak a bizalmi szerepkört betöltő, erre feljogosított munkatárs léphet be, azonosítást követően;

c) önálló jogosultsággal nem rendelkező személy csak indokolt és engedélyezett esetben, a szükséges időtartamig tartózkodhat a gépteremben megfelelő jogosultságú kísérő személy állandó felügyelete mellett;

d) az eszközök aktivizáló adatai (jelszavak, PIN kódok, stb.) a géptermen belül sem tárolhatók nyílt formában;

e) 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

(242.) A Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert alkalmaz, amely:

a) megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;

b) megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;

c) tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

(243.) Szolgáltató a gépteremben olyan légkondicionáló berendezést alkalmaz, mely biztosítja az alábbiakat:

a) az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított;

b) a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;

c) hűtés történik a szükséges üzemi hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

5.1.4. Beázás és elárasztás veszélyeztetettség

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

5.1.5. Tűzmegelőzés és tűzvédelem

(245.) 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

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

5.1.7. Selejt kezelése és megsemmisítése

(247.) 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

(248.) Szolgáltató azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan – az üzemeltetés helyétől eltérő - helyszínen tárolja, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítja a helyszínek között a mentett adatok biztonságos továbbítását. Az adatmentést, vagy abból a helyreállítást rendszerüzemeltető bizalmi munkakört betöltő személy végzi el.

5.2. Eljárásbeli előírások

(249.) 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.

(250.) Az eljárásbeli szabályokat a következő szabályzatok tartalmazzák:

a) {D3} a Szolgáltató Szervezeti és Működési szabályzata, mely meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes szervezetekhez kapcsolt feladat-, felelősség- és hatásköröket;

b) jelen szolgáltatási szabályzat, mely a Szolgáltató és a PKI közösség (Előfizetők, Alanyok, Érintett Felek, stb.) viszonyát szabályozza;

c) {D6} GovCA 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

(251.) 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, felfüggesztésének és visszavonásának jóváhagyásáért, az életciklus menedzsment tevékenységek és adminisztráció szabályszerű végzéséért felelős személy;

(252.) 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.

(253.) 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.

(254.) A bizalmi munkaköröket és szerepköröket betöltő személyekről Szolgáltató nyilvántartást vezet.

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

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

a) szolgáltatói kulcspár létrehozása;

b) szolgáltatói magánkulcs mentése és visszaállítása; szolgáltató magánkulcs aktiválása;

c) szolgáltatói magánkulcs megsemmisítése.

5.2.3. Bizalmi munkakörökben elvárt azonosítás és hitelesítés

(256.) 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

(257.) 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

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

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

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

(261.) A munkatársak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai alapján meghatározott munkaköri leírássokkal rendelkeznek.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

(262.) 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.

(263.) 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.

(264.) 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.

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

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

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

5.3.2. Biztonsági háttér ellenőrzés eljárásai

(268.) A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben vagy szerepkörben csak olyan alkalmazottakat foglalkoztat, akik:

a) büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);

b) nem állnak a hitelesítés-szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

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

(270.) 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:

a) pontos és írásos munkakör leírást vesz át a fölérendelt vezetőtől vagy a Szolgáltató humán szervezetétől;

b) titoktartási nyilatkozatot kell aláírnia, melyben három év titoktartási kötelezettség szerepel a kilépés időpontjától számítva;

c) szükséges mértékű oktatásban részesül, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

(271.) Kilépéskor:

a) 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.

b) Azonnal vissza kell venni az azonosításhoz és hitelesítéshez használt eszközét, és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítványokat vissza kell vonni.

5.3.3. Képzési követelmények

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

a) a PKI elméletet;

b) Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;

c) a szerepkör ellátáshoz szükséges speciális ismereteket;

d) Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;

- az egyes tevékenységek jogi következményeit;
- az alkalmazandó biztonsági szabályokat.

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

5.3.4. Továbbképzési gyakoriságok és követelmények

(274.) Szolgáltató gondoskodik arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést tart.

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

(276.) 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.

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

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

5.3.5. Munkabeosztás körforgásának gyakorisága és sorrendje

(279.) Nincs kikötés.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

(280.) 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

(281.) Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztat.

(282.) Az egyéb feladatok ellátására, vállalkozási vagy megbízásos 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

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

(284.) Minden bizalmi munkakört betöltő munkatárs megkapja írásban:

a) egyéni munkaköri leírást;

b) a Szolgáltató szervezeti és biztonsági szabályzatait;

c) rendszeres és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

5.4. A biztonsági naplózás folyamatai

5.4.1. Naplózott esemény típusok

(285.) 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.

(286.) 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.

(287.) A Szolgáltatások nyújtásával kapcsolatos események különösen az alábbiak:

a) szolgáltatói tanúsítványok életciklusával kapcsolatos minden esemény;

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

(288.) 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

(289.) Szolgáltató biztosítja a naplóállományok rendszeres ellenőrzését és kiértékelését.

(290.) A Szolgáltatások nyújtásával kapcsolatos események naplóállományait naponta feldolgozzák a rendszervizsgálók.

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

5.4.3. Naplóállomány megőrzési időtartama

(292.) 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

(293.) 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.

(294.) Szolgáltató gondoskodik arról, hogy a naplóállományokhoz és azok mentéseihez csak az arra feljogosított személyek férhessenek hozzá.

5.4.5. Naplóállomány mentési folyamatai

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

5.4.6. Naplózás gyűjtési rendszere

(296.) 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.

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

5.4.7. Rendellenes eseményeket kiváltó alanyok értesítése

(298.) 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, vagy az Alany kötelessége a Szolgáltatóval való együttműködés az esemény feltárása érdekében.

5.4.8. Sebezhetőség értékelések

(299.) 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.

(300.) 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.

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

(302.) Szolgáltató folyamatosan figyelemmel kíséri az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül megteszi, illetve – ha az ellenintézkedés

költsége nem áll arányban a sebezhetőség lehetséges kihatásaival – cselekvési tervet készít és hajt végre annak érdekében, hogy a sebezhetőség ne legyen kihasználható vagy annak hatása elhanyagolható legyen.

5.5. Adatok archiválása

5.5.1. A tárolt adatok típusai

(303.) Szolgáltató gondoskodik arról, hogy megőrzésre kerüljön minden olyan információ, amely szükséges ahhoz, hogy egy tanúsítvány érvényessége bizonyítható legyen, továbbá amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja. Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

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

5.5.2. Archívum megőrzési időtartama

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

5.5.3. Archívum védelme

(305.) 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

(306.) 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

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

(308.) Az elektronikus formában archivált adatokon elhelyezett elektronikus aláírás vagy bélyegző minősített időbélyegzőt tartalmaz.

(309.) 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

(310.) A naplóállományok és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül gyűjti. A védett informatikai rendszerből történő kimozgatás során az adatok minősített időbélyegzőt tartalmazó elektronikus aláírással vagy bélyegzővel kerülnek hitelesítésre.

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

5.5.7. Archívum hozzáférés és ellenőrzés eljárásai

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

(313.) Szolgáltató az Ügyfélkapcsolati Iroda közreműködésével biztosítja az Alanyok számára a róluk tárolt személyes adatokra vonatkozó tájékoztatást.

(314.) 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 átállás

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

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

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

a) a kulcs átállást követően kibocsátott tanúsítványokat kizárólag csak az új szolgáltatói kulcs felhasználásával írja alá;

b) 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.

5.7. Helyreállítás rendkívüli üzemi helyzetek esetén

(318.) 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.

(319.) 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.

(320.) 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

(321.) Szolgáltató rendelkezik {D7} üzletmenet folytonossági tervvel. Ez a dokumentum biztonsági okokból kifolyólag nem nyilvános.

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

(323.) 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.

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

(325.) 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.

(326.) 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.

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

5.7.2. Sérült számítási erőforrások, szoftverek és/vagy adatok

(328.) 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

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

a) visszavonja az összes érintett tanúsítványt;
b) megszünteti az érintett magánkulcs használatát;
c) új szolgáltatói kulcspárokat és tanúsítványokat hoz létre;
d) intézkedik valamennyi érintett fél értesítéséről.

5.7.4. Üzletmenet folytonosság helyreállás katasztrófát követően

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

(331.) 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

(332.) Szolgáltató az alábbi, a szolgáltatási tevékenység megszüntetésére vonatkozó tervvel rendelkezik:

a) A tervezett megszűnés előtt kellő időben tárgyalásokat kezdeményez más szolgáltatókkal a Szolgáltatásokkal járó kötelezettségek - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig - átadás-átvételéről.

b) Szolgáltató gondoskodik a Szolgáltatások megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról. Különösképpen gondoskodik a tanúsítvány visszavonási kezelés és közzététel szolgáltatások folyamatos fenntartásáról.

c) A megszüntetés előtt legalább 60 nappal korábban:

- internetes honlapján tájékoztatja a felhasználói közösség tagjait;
- megszünteti a nevében eljáró szerződött alvállalkozói összes felhatalmazását és jogosultságaikat megvonja;
- beszünteti a tanúsítványok előállítását és kibocsátását;

d) A megszüntetés előtt legalább 20 nappal korábban:

- visszavonja az összes végfelhasználói tanúsítványt;
- leállítja a visszavonás kezelés szolgáltatást. ○ visszavonja az érintett szolgáltatói tanúsítványokat;
- 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;

e) 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

(333.) Szolgáltató a tanúsítványok és visszavonási listák aláírására 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 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, az aláírás-létrehozó adatok (magánkulcsok) teljes életciklusuk alatt a kriptográfiai modulban maradnak.

(334.) Szolgáltató az OCSP válaszokat aláíró kulcspárokat fizikailag védett környezetben állítja elő, a magánkulcsok teljes életciklusuk alatt ezen fizikailag védett környezetben maradnak.

6.1.1.2. Előfizetői kulcspárok előállítása

(335.) 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;

a) a magánkulcsot annak átadásáig Szolgáltató megfelelően biztonságos környezetben tárolja a felfedés megakadályozása érdekében;

b) 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

(336.) Szolgáltató a 4.3.2 fejezetben leírt módon biztosítja, hogy a magánkulcsot és az ahhoz tartozó aktivizáló adatokat csak a jogosult Alany vehesse át.

6.1.3. Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

(337.) A titkosító és autentikációs tanúsítványokhoz kapcsolódó kulcspárt Szolgáltató állítja elő, így annak eljuttatása nem szükséges.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

(338.) 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.

(339.) Az Alanyok számára Szolgáltató a nyilvános kulcsait a tanúsítványhoz kapcsolódó tanúsítványlánc formájában - mely az opcionálisan megrendelt kulcstároló eszközön (chipkártya, USB token), vagy a PKCS#12 formátumnak megfelelő kulcstárolóban tárolásra kerül - teszi közzé.

(340.) Érintett Feleknek a szolgáltatói tanúsítványokra az {Sz8} RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítést javasolt elvégezniük az érintett nyilvános kulcs használata előtt.

6.1.5. Kulcs méretek

(341.) Szolgáltató a Szolgáltatások nyújtása során – mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében -, a vonatkozó nemzetközi szabványoknak és ajánlásoknak megfelelő szabványos algoritmusokat, paramétereket és kulcshosszakat használ.

(342.) A szolgáltatói tanúsítványokban használt aláíró algoritmus és kulcs típusa:

„GovCA Főtanúsítványkiadó”	SHA384withECDSA	NIST P-384
„GovCA Titkosító Tanúsítványkiadó”	SHA384withECDSA	NIST P-384
OCSP válaszadó	SHA384withECDSA	NIST P-256

4. táblázat - Kulcspár méretek

(343.) Az Alanyok tanúsítványaiban használt aláíró algoritmus és kulcs típusa, mérete:

a) SHA384withECDSA, RSA 3072 bit
vagy
b) SHA384withECDSA, NIST P-256

(344.) A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén gondoskodik az algoritmus váltásról vagy a kulcshosszak növeléséről.

6.1.6. A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

(345.) 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.

(346.) Az előfizetői kulcspárok tekintetében Szolgáltató a kulcspárt védett környezetben, a hitelesítőközponti rendszerében vagy – Előfizető kérelmére – a kulcstároló eszközön (chipkártya, USB token), kizárólag bizalmi munkakört betöltő személyek jelenlétében állítja elő. Az előfizetői kulcspárok generálása során Szolgáltató betartja a vonatkozó nemzetközi szabványokban és ajánlásokban foglalt előírásokat is.

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

(347.) 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 kulcspár kizárólag autentikációra, illetve titkosításra és visszafejtésre használható.

(348.) Szolgáltató a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz11} ITU-T X.509 v3 szabványnak megfelelően jelzi a kulcs használat célját.

	kiterjesztés		kiterjesztés	
	kritikus?	KeyUsage	kritikus?	ExtendedKeyUsage

CA tanúsítványa	igen	keyCertSign cRLSign	-	-
OCSP válaszadó tanúsítványa	igen	contentCommitment[3]	nem	OCSPSigning
előfizetői autentikációs tanúsítvány	igen	digitalSignature keyAgreement	nem	clientAuth[4] SCLogon[5]
előfizetői titkosító tanúsítvány	igen	keyEncipherment dataEncipherment digitalSignature	nem	emailProtection[6] ipsecEndSystem[7] ipsecProtection[8]

5. táblázat - Kulcshasználat célja

6.2. Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1. Kriptográfiai modul szabványok és műszaki szabályozások

(349.) Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára olyan kriptográfiai modult alkalmaz, amely:

a) olyan megbízható rendszer, amelynek értékelése az MSZ/ISO/IEC 15408 {Sz13} szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg; vagy

b) megfelel az ISO/IEC 19790 {Sz14} követelményeinek; vagy

c) megfelel a FIPS 140-2 {Sz15} 3-as, illetve annál magasabb szintű követelményeknek.

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

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

6.2.3. Magánkulcs letét

(351.) Szolgáltató a hitelesítő központok magánkulcsait nem teszi letétbe.

(352.) A Szolgáltató nem nyújt kulcsletét szolgáltatást.

6.2.4. Magánkulcs visszaállítása

(353.) 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.

(354.) A Szolgáltató nem nyújt kulcsletét szolgáltatást.

---

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

[4] OID: 1.3.6.1.5.5.7.3.2

[5] OID: 1.3.6.1.4.1.311.20.2.2

[6] 1.3.6.1.5.5.7.3.4

[7] 1.3.6.1.5.5.7.3.5

[8] 1.3.6.1.5.5.8.2.2

6.2.5. Magánkulcs mentése

(355.) Szolgáltatói hitelesítő központok 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 és bizalmasságát. A mentett példányok titkosított formában, fizikailag biztonságos környezetben kerülnek megőrzésre.

6.2.6. Magánkulcs bejuttatása a kriptográfiai modulba

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

(357.) Amennyiben az Előfizető a tanúsítvánnyal együtt kulcstároló eszköz (chipkártya, USB token) szolgáltatását is kérte, akkor a kulcspár ezen az eszközön (kriptográfiai modulban) került létrehozásra, így a bejuttatására nincs szükség.

(358.) Amennyiben Előfizető nem kért kulcstároló eszköz (chipkártya, USB token) szolgáltatást, Szolgáltató a magánkulcsot szabványos, titkosított kulcstároló formátumban (PKCS#12) készíti elő az átadásra, és ha ezt Előfizető kriptográfiai modulban kívánja tárolni, akkor a kulcstárolót az Előfizető Kapcsolattartója veszi át, és gondoskodik annak bejuttatásáról a kriptográfiai modulba. Előfizető feladata a kriptográfiai modulba bejuttatást követően a magánkulcs minden példányának haladéktalan és visszaállíthatatlan módon történő megsemmisítése.

6.2.7. Magánkulcs kriptográfiai modulban történő tárolásának módja

(359.) 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.

(360.) A kulcsok tárolása során Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat.

6.2.8. Magánkulcs aktiválásának módja

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

(362.) Az előfizető tanúsítványok esetében az Alany a magánkulcs aktiválását a lezárt borítékban átadott PIN kód megadásával végzi.

6.2.9. Magánkulcs aktív állapotának megszüntetési módja

(363.) Szolgáltató biztosítja, hogy az aktivált HSM modul jogosulatlan hozzáférés ellen védett legyen. A

(364.) HSM modul működése során csak a kiadott tanúsítványok, visszavonási listák és opcionálisan OCSP válaszok hitelesítésére használható. A magánkulcs eltávolításra kerül a HSM modulból, amikor a hitelesítő központ működése megszűnik.

(365.) Az előfizetői tanúsítványok esetében a magánkulcsnak deaktiválását az autentikációra és/vagy titkosításra és visszafejtésre használt alkalmazás végzi el, kijelentkezéskor, az alkalmazásból való kilépéskor, vagy az eszköznek az olvasóból való eltávolításakor.

6.2.10. Magánkulcs megsemmisítésének módja

(366.) 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. 6.2.11 Kriptográfiai modul értékelése

(367.) A 6.2.1 fejezet tartalmazza.

6.3. Kulcspár gondozás egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

(368.) Az nyilvános kulcsot a tanúsítvány tartalmazza. Szolgáltató minden általa kibocsátott tanúsítványt archivál és az érvényesség lejártától számított tíz évig, illetve a tanúsítvánnyal kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőriz. 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

(369.) A kulcspár felhasználás időtartama azonos a nyilvános kulcs hitelességét igazoló tanúsítvány alábbi érvényességi idejével.

6.3.2.1. ECC környezet

"GovCA Főtanúsítványkiadó"	25 év
"GovCA Titkosító Tanúsítványkiadó"	20 év
OCSP válaszadó ("GovCA Titkosító Tanúsítványkiadó")	legfeljebb 30 nap
Előfizetői tanúsítvány	legfeljebb 4 év *

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

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

(370.) Szolgáltató a magánkulcs aktiválásához szükséges PIN kódot (kulcstároló eszköz (chipkártya, USB token) szolgáltatása esetén a PUK kódot is) megfelelő minőségű véletlenszám-generátor segítségével, fizikailag védett környezetben és biztonságos körülmények között állítja elő, és hozzárendeli az opcionális szolgáltatott kulcstároló eszközhöz, illetve a PKCS#12 formátumnak megfelelő kulcstárolóhoz.

6.4.2. Aktivizáló adatok védelme

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

(372.) Az átvételt követően az Alanynak kell biztosítania az aktivizáló adatok kizárólagos birtoklását és védelmét.

6.4.3. 6.4.3 Aktivizáló adatok egyéb szempontjai

(373.) Nincs kikötés.

6.5. Informatikai biztonsági óvintézkedések

6.5.1. Informatikai biztonsági műszaki követelmények meghatározása

(374.) Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz1} EN 319 401és {Sz2} EN 319 411-1 szabványoknak a nyilvános kulcsú tanúsítványokat kibocsátó hitelesítés-szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg, melyek különösen az alábbiak:

#	hivatkozás	leírás
1.	EN 319 401 7.4 a)	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 7.4 f)	Az érzékeny adatokat meg kell védeni az ellen, hogy újrafelhasznált tároló objektumokon (pl. törölt fájlok) át jogosulatlan személyek számára hozzáférhető váljanak.
3.	EN 319 411-1 6.5.5 a)	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 6.5.5 b)	Multi-faktoros azonosítást kell alkalmazni minden olyan személy és folyamat azonosítására, mely tanúsítvány előállítását közvetlenül kiválthatja.
5.	EN 319 411-1 6.5.5 c)	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 6.5.5 d)	A visszavonási státuszt kezelő alkalmazásnak hozzáférés ellenőrzést kell végrehajtaniuk minden esetben, amely a visszavonási státusz információ megváltozását eredményezheti.
7.	EN 319 411-1 6.5.5 e)	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. táblázat - Informatikai biztonsági műszaki követelmények

6.5.2. Informatikai biztonsági értékelés

(375.) 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

(376.) 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.

(377.) 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 {Sz2} EN 319 411-1 szabvány 6.5.6 fejezetében előírt követelményeket.

6.6.2. Biztonságkezelési óvintézkedések

(378.) 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.

(379.) A biztonságkezelési szabályokat a Szolgáltató {D5} GovCA informatikai biztonságpolitikája, illetve {D6} biztonsági szabályzata tartalmazza.

6.6.3. Életciklus biztonsági óvintézkedések

(380.) 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 naplóik	rendszervizsgálók	naponta
belső ellenőrzés	IT infrastruktúra	biztonsági tisztviselő	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások és naplóik	biztonsági tisztviselő	évente egyszer
külső ellenőrzés	IT infrastruktúra	külső auditor	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások és naplóik	külső auditor	évente egyszer

7. táblázat - Életciklus biztonsági óvintézkedések

6.7. Hálózatbiztonsági óvintézkedések

(381.) A hálózati védelmi intézkedéseket a Szolgáltató {D6} biztonsági szabályzatában meghatározott követelményeknek megfelelően valósítja meg, melyek figyelembe veszik az {Sz2} EN 319 411-1 szabvány 6.5.7 fejezetében leírt követelményeket is.

6.8. Időforrások

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

(383.) Szolgáltató a Nemzeti Távközlési Gerinchálózat időforrását használja a megbízható időpont megállapításához.

(384.) A Szolgáltató az *ntp.gov.hu* és *ntp2.gov.hu* referencia időforrásokat használja, melyek pontossága századmásodpercen belüli.

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

7.1. Tanúsítvány profil

(385.) Szolgáltató által kiadott tanúsítványok megfelelnek az {Sz8} RFC 5280, {Sz4} EN 319 412-1, {Sz5} EN 319-412-2, {Sz6} EN 319 412-3 szabványoknak.

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

7.1.1. Verziószám

(387.) A tanúsítványok verziószáma: V3.

7.1.2. Tanúsítvány kiterjesztések

(388.) A tanúsítványokban alkalmazott kiterjesztések mindenben követik az {Sz8} RFC 5280, {Sz4} EN 319 412-1, {Sz5} EN 319-412-2, {Sz6} EN 319 412-3 szabványok előírásait.

7.1.3. Algoritmus azonosítók

(389.) A tanúsítványok aláírásához alkalmazott algoritmus azonosítók 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

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

7.1.5. Név megszorítások

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

7.1.6. Hitelesítési rend objektumazonosító

(392.) Szolgáltató a tanúsítványokban feltünteti a hitelesítési rend objektumazonosítóját.

7.1.7. Szabályzati megszorítások kiterjesztés használata

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

7.1.8. Szabályzat minősítők szintaktikája és szemantikája

(394.) 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

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

7.2. CRL profil

(396.) Szolgáltató által kiadott visszavonási listák megfelelnek az {Sz8} RFC 5280 műszaki szabványnak.

7.2.1. Verziószám

(397.) A visszavonási listák verziószáma: V2.

7.2.2. CRL és CRL bejegyzés kiterjesztések

(398.) A visszavonási lista az alábbi kiterjesztéseket tartalmazza „nem kritikus” megjelöléssel:

a) CRLNumber: a visszavonási lista szigorúan növekvő sorszáma

b) AuthorityKeyIdentifier: a kibocsátó CA kulcs azonosítója

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

7.3. OCSP profil

(400.) Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz12} RFC 6960 műszaki szabványnak.

7.3.1. Verziószám

(401.) Az OCSP válaszok verziószáma: V1.

7.3.2. OCSP kiterjesztések

(402.) Az OCSP válasz az alábbi kiterjesztéseket tartalmazza „nem kritikus” megjelöléssel:

a) `Nonce` : az OCSP kérésben megadott, visszajátszásos támadások megelőzésére szolgáló véletlenszám (csak akkor, ha a kérés tartalmazta azt)

b) `AuthorityKeyIdentifier` : az időpont, ameddig a Szolgáltató a tanúsítvány lejárata után is biztosítja a visszavonási státuszt Az OCSP válasz fentieken túl más szabványos kiterjesztést is tartalmazhat, azonban ezek a kiterjesztések nem lehetnek „kritikus” jelzésűek.

8. MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

(403.) Jelen szolgáltatási szabályzat tartalmazza az összes, a nyilvános körben kibocsátott, autentikációs és titkosító tanúsítványokkal kapcsolatos szolgáltatás nyújtása során teljesíteni szükséges követelményt, melyet különösen az alábbi szabványok határoznak meg:

a) EN 319 401: General policy requirements for Trust Service Providers {Sz2}

b) EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates {Sz3}

8.1. Vizsgálatok gyakorisága és körülményei

(404.) Szolgáltató külső és belső vizsgálatokat végez, illetve végeztet annak érdelében, 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.

(405.) Szabályzatainak megfelelőségét Szolgáltató saját szervezete részéről a Szabályozási Csoport vizsgálja meg. A Szolgáltatások megfelelőségének vizsgálatára Szolgáltató saját belső ellenőrzéseket hajt végre.

(406.) Szolgáltató rendelkezik minőségbiztosítási rendszerrel és információbiztonsági irányítási rendszerrel, melyek megfelelő működését külső független rendszervizsgáló ellenőrzési tevékenysége biztosítja.

(407.) Szolgáltató a külső, illetve a saját ellenőrző szervezet által végzett belső vizsgálatokat a {D6} GovCA szolgáltatások biztonsági szabályzatában megjelölt rendszerességgel - évente legalább egyszer biztosítja.

8.2. Auditor azonosítása és képesítése

(408.) A külső rendszervizsgálói auditokat Szolgáltató olyan szakértővel vagy szakértői szolgáltatásokat nyújtó szervezettel végezteti el, aki független Szolgáltatótól, illetve az ellenőrzött rendszertől, területtől, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

(409.) 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

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

8.4. Audit során vizsgált területek

(411.) Az audit az alábbi területeket fedi le:

a) szabályzatok és dokumentációk;
b) irányítási és ellenőrzési követelmények;
c) személyzeti biztonsági követelmények;
d) a szolgáltatói kulcspár kezeléséhez kapcsolódó követelmények;
e) üzemeltetési és hozzáférési biztonság;
f) fizikai és környezeti biztonság;
g) folyamatos szolgáltatás biztosítása;
h) adatbiztonság és archiválás.

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

a) a hatályos jogszabályoknak és szabványoknak;

b) a szolgáltatási szabályzatnak, illetve a hitelesítési rendnek.

8.5. Hiányosságok esetén végrehajtandó tevékenységek

(413.) 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.

8.6. Eredmény kommunikációja

(414.) 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. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9. EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1. Díjak

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

(416.) Az Előfizetőre vonatkozó szolgáltatási díjak a Szolgáltatási Szerződésben kerülnek rögzítésre.

9.1.1. Tanúsítvány kibocsátás díja

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

a) a tanúsítványok kibocsátásnak díját;

b) a tanúsítványtárban történő közzététel díját (ha a tanúsítvány közzétételéhez Előfizető hozzájárult)

c) a tanúsítvány felfüggesztésének, újra-érvényesítésének, illetve visszavonásának díját

d) (amennyiben ilyen tevékenységre sor kerül)

e) a tanúsítványok lejárat után archiválásának díját.

9.1.2. Tanúsítványhozzáférés díja

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

9.1.3. Visszavonási és állapot információ hozzáférés díja

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

9.1.4. Egyéb szolgáltatások díja

(420.) Amennyiben Előfizető azt megrendelte, Szolgáltató a kulcstároló eszközért (chipkártya + kártyaolvasó vagy USB token) egyszeri díjat számít fel, ami tartalmazza az eszköz megszemélyesítésének díját is.

9.1.5. Visszatérítési szabályzat

(421.) Előfizető a számára kibocsátott tanúsítvány díjának visszakérésére a következő esetekben jogosult:

a) a kibocsátott tanúsítvány valamely adata Szolgáltató hibájából nem megfelelő;

b) a kibocsátott tanúsítvány, a magánkulcs és aktivizáló adat nem összetartozó;

c) a kulcstároló eszközön (chipkártya, USB token) szereplő adatok Szolgáltató hibájából fakadóan nem megfelelők (pl. a kártyára nyomtatott név hibás);

d) az átadott kulcstároló eszköz (chipkártya, USB token) és aktivizáló kód nem összetartozó;

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

(422.) 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.

(423.) A visszatérítési igény pozitív elbírálása esetén a Szolgáltató a tanúsítványt visszavonja, és:

a) vagy új tanúsítványt bocsát ki Előfizető számára,

b) vagy a díjat 20 naptári napon belül Előfizető által megadott bankszámla számra visszautalja.

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

(425.) Szolgáltató az egyéb tevékenységeiért számlázott díjak esetén díjvisszafizetésre nem köteles.

9.2. Anyagi felelősség

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

9.2.1. Biztosítási fedezet

(427.) A Szolgáltató rendelkezik olyan felelősségbiztosítással, mely egyaránt kiterjed a tanúsítványokkal kapcsolatos, 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 háromszorosáig. A biztosítási szerződésben szereplő felelősségvállalási érték 3.000.000 Ft, vagy ennél esetenként magasabb összeg.

9.2.2. További követelmények

(428.) Nincs kikötés.

9.2.3. Felelősségbiztosítás vagy garancia végfelhasználók számára

(429.) Nincs kikötés.

9.3. Üzleti információk bizalmassága

9.3.1. Bizalmasan kezelendő információk köre

(430.) 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

(431.) Nem bizalmasnak tekintett információk az alábbiak:

a) szolgáltatói tanúsítványok és az azokban foglalt adatok;

b) Előfizető hozzájárulása esetén a tanúsítvány és a tanúsítványba foglalt adatok;

c) a tanúsítványokhoz kapcsolódó visszavonási információk;

d) a Szolgáltató internetes honlapján közzétett nyilvános információk, szabályzatok és egyéb dokumentumok;

e) az olyan adatok, melyek nyilvános adatforrásból elérhetők.

9.3.3. Bizalmas információk védelmének felelőssége

(432.) 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

(433.) 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.

(434.) Szolgáltató, mint adatkezelő, szerepel a Nemzeti Adatvédelmi és Információszabadság Hivatal Adatvédelmi Nyilvántartásában.

9.4.2. Bizalmasként kezelendő személyes adatok

(435.) Szolgáltató csak Előfizetőtől és az Alanytól közvetlenül, azok kifejezett írásos hozzájárulásával gyűjt személyes adatot és csak olyan mértékben, ami a tanúsítvány kiállításához, valamint az Alany tájékoztatásához, személyazonosságának megállapításához szükséges. Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

a) Előfizető részéről a Szolgáltatási Szerződésben érintett személyek (pl. cégjegyzésre jogosult vezető, vagy Előfizető Kapcsolattartója) minden adatát;

b) az Alany azon adatait, melyek a tanúsítványba nem kerülnek befoglalásra.

9.4.3. Bizalmasként nem kezelendő személyes adatok

(436.) Szolgáltató nem bizalmasként kezelendő személyes adatnak tekinti az Alanynak a tanúsítványba foglalt adatait, amennyiben az Alany tanúsítványa közzétételéhez írásban hozzájárult.

(437.) 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

(438.) Szolgáltató felelős a személyes adatok védelméért.

9.4.5. Hozzájárulás a személyes adatok felhasználásához

(439.) Előfizetőnek – és üzleti tanúsítvány esetén az Alanynak is - 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.

(440.) 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

(441.) 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 az Alanyt.

(442.) 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 az Alanyt.

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

(444.) 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 az Alany beleegyezésével adhatja át.

9.4.7. Egyéb, felfedést eredményező körülmények

(445.) Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatások nyújtásának megszüntetése esetén Előfizetők és az Alanyok átadja harmadik félnek.

9.5. Szellemi tulajdonjogok

(446.) 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.

(447.) A Szolgáltató tulajdonát képezik a szolgáltatói tanúsítványok, visszavonási információk, a végfelhasználói tanúsítványokban szereplő, Szolgáltató által létrehozott azonosítók.

(448.) 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

(449.) Szolgáltató felel a hitelesítési 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 végeznek.

(450.) Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a {J2} Polgári Törvénykönyv 6:519. §-a szerint, a vele szerződéses jogviszonyban álló Előfizetővel szemben a szerződésszegésért való felelősség ({J2} Polgári Törvénykönyv 6:142. §) szabályai szerint felelős a tanúsítvány használatával kapcsolatban okozott kárért, ha megszegte a hitelesítési 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.

(451.) 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:

a) az Alanyok magánkulccsal, illetve az kulcstároló eszközzel (chipkártya, USB token) kapcsolatos tevékenységéért;
b) az Érintett felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért;
c) az Érintett Felek vagy mások által kibocsátott szabályzatokért;
d) Szolgáltató nem felelős azokért a károkért, melyek a személyes megjelenés és az adatoknak a közhiteles nyilvántartásban való egyezősége ellenőrzésének hiányából adódnak.

9.6.1.1. Szolgáltató kötelezettsége

(452.) 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

(453.) 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.

(454.) Szolgáltató felelőssége a tanúsítvány kiadása során:

a) Előfizető teljes körű és közérthető tájékoztatása a 4.1.2 fejezet 1) pontjában meghatározottakról;

b) a tanúsítvány alanyának azonosítása:

- üzleti tanúsítvány esetén a természetes személy alany azonosítása a 3.2.3 alfejezetben leírt eljárással, továbbá üzleti tanúsítvány esetén a szervezeti azonosságot is ellenőrizni kell a 3.2.2 fejezetben leírt eljárással;
- szervezeti- és eszköz tanúsítvány esetén a szervezeti azonosság ellenőrzése a 3.2.2 fejezetben leírt eljárással;

c) Előfizető Kapcsolattartója személyének azonosítása és eljárási jogosultságának megállapítása;

d) a tanúsítvány egyéb mezőibe és kiterjesztéseibe kerülő adatok ellenőrzése;

e) a regisztrációhoz és a tanúsítvány kiállításához szükséges adatok rögzítése az erre szolgáló informatikai rendszerben;

f) a rögzített kérelemben foglalt adatokkal a megfelelő tanúsítvány előállítása az Előfizető által biztosított kulcspárhoz vagy a Szolgáltató által előállított kulcspárhoz;

g) az opcionálisan megrendelt kulcstároló eszköz (chipkártya, USB token) megfelelő megszemélyesítése;

h) a titkosító tanúsítványhoz kapcsolódó, opcionálisan megrendelt kulcsletét szolgáltatás esetén a megőrzött magánkulcsok biztonságos tárolásáért, továbbá azért, hogy a tárolt magánkulcs csak az arra jogosult, megfelelő személynek kerüljön kiadásra;

i) a magánkulcshoz tartozó aktivizáló adatok biztonságos előállítása, tárolása, és átadása az arra jogosult személynek.

9.6.3. Előfizető felelőssége és helytállása

9.6.3.1. Előfizető jogai

(455.) Előfizető jogosult:

a) a Szolgáltatásokat igénybe venni a jelen szolgáltatási szabályzatban, a Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben leírtak szerint;

b) Kapcsolattartó személyt kijelölni;

c) az általa meghatározott Alanyok számára tanúsítványt igényelni;

d) a tanúsítványok felfüggesztését és visszavonását kérni;

e) a felfüggesztett tanúsítvány újra-érvényesítését kérni.

9.6.3.2. Előfizető felelőssége

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

9.6.3.3. Előfizető kötelezettségei

(457.) 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 a {D1} Általános Szerződési Feltételek tartalmazzák.

9.6.3.4. Az Alany jogai

(458.) Alany jogosult:

a) a számára kiadott tanúsítványt és a kapcsolódó magánkulcsot az 1.4.1 fejezetben leírt célokra és jelen szabályzatban leírt módon használni;

b) a tanúsítvány felfüggesztését vagy visszavonását kérni;

c) a felfüggesztett tanúsítvány újra-érvényesítését kérni;

d) a tanúsítványhoz kapcsolódó egyéb szolgáltatásokat használni a jelen szabályzatban leírt módon.

9.6.3.5. Az Alany felelőssége

(459.) Az Alany felelős:

a) a regisztráció során megadott adatainak valódiságáért, pontosságáért és érvényességéért;

b) a tanúsítványba foglalt adatok ellenőrzéséért;

c) az adataiban bekövetkezett változás haladéktalan bejelentéséért;

d) a kulcstároló eszköze (chipkártya, USB token) biztonságos kezeléséért;

e) a magánkulcs és az aktivizáló adat biztonságos kezeléséért;

f) a tanúsítvány és a magánkulcs szabályzatoknak megfelelő felhasználásáért;

g) a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyek esetén; általában, a jelen szabályzatban előírt kötelezettségei betartásáért.

9.6.3.6. Az Alany kötelezettségei:

(460.) Alany köteles:

a) a Szolgáltatások használata előtt megismerni jelen szolgáltatási szabályzatot;

b) a Szolgáltató által kért, a Szolgáltatások igénybe vételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően megadni;

c) a Szolgáltatásokat kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a jelen szabályzatban és a hivatkozott dokumentumokban foglaltaknak megfelelően használni;

d) 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;

e) biztosítani, hogy a Szolgáltatások igénybe vételéhez szükséges adatokhoz és eszközökhöz (különösen a kulcstároló eszközhöz (chipkártya, USB token) és az aktivizáló adatokhoz) illetéktelen személy ne férhessen hozzá;

f) haladéktalanul kezdeményezni a tanúsítvány felfüggesztését vagy visszavonását, amennyiben a tanúsítványhoz kapcsolódó magánkulcs, a kulcstároló eszköz vagy az aktivizáló adat illetéktelen kezekbe került vagy megsemmisült, megrongálódott, elveszett, valamint haladéktalanul megszüntetni a tanúsítvány és magánkulcs használatát;

g) kulcs kompromittálódás vagy jogellenes használat gyanúja esetén a Szolgáltató megkereséseire a Szolgáltató által megadott időtartamon belül reagálni;

h) tudomásul venni, hogy Előfizető jogosult a tanúsítvány visszavonását vagy felfüggesztését kérni;

i) tudomásul venni, hogy Szolgáltató a tanúsítványt a jelen szabályzatban leírt módon és ellenőrzési lépések elvégzése után bocsátja ki;

j) tudomásul venni, hogy Szolgáltató a 4.9.1 fejezetben ismertetett körülmények esetén jogosult a tanúsítványt visszavonni;

k) 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;

l) haladéktalanul, írásban értesíteni Szolgáltatót, ha a tanúsítvánnyal kapcsolatban jogvita indul.

9.6.4. Érintett felek felelőssége és helytállása

(461.) 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) a szolgáltatási szabályzatban foglalt követelmények és előírások betartása;

b) megbízható informatikai környezet és alkalmazások használata;

c) a tanúsítvány felhasználására vonatkozó valamennyi korlátozás figyelembe vétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel;

d) a tőle elvárható magatartás tanúsítása a tanúsítványok elfogadásakor.

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

9.6.5. Egyéb felek felelőssége és helytállása

(463.) Nincs kikötés.

9.7. Helytállás érvénytelenségi köre

(464.) Szolgáltató kizárja felelősségét, amennyiben:

a) az Érintett Fél nem körültekintően jár el a tanúsítványok ellenőrzése és felhasználásra során, azaz nem a jelen szolgáltatási szabályzatnak vagy a hatályos jogszabályoknak megfelelően jár el;

b) az Érintett Felek vagy mások által kibocsátott szabályzatok nem felelnek meg jelen szabályzatnak;

c) az Internet, vagy annak egy részének működési hibájából fakadóan tájékoztatási vagy egyéb kommunikációs kötelezettségeit nem tudja ellátni;

d) az Alany vagy Előfizető Kapcsolattartója által megadott értesítési email cím időközben megváltozott vagy megszűnt, és ebből fakadóan Szolgáltató nem tudja őket értesíteni;

e) az Előfizető nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek;

f) az Alany nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek;

g) a károkozás a vonatkozó nemzetközi szabványokban és ajánlásoknak közölt kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8. Felelősség korlátozása

(465.) Szolgáltató korlátozza a kártérítési felelősségét:

a) a tanúsítvánnyal egy alkalommal vállalható kötelezettség mértékében (tranzakciós limit), mely a tanúsítványban és a Szolgáltatási Szerződésben feltüntetésre kerül;

b) összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban fizetendő kártérítési összeg tekintetében.

(466.) 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.

(467.) 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.

(468.) 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

(469.) 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

9.10.1.1. Időbeli hatály

(470.) 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.

9.10.1.2. Tárgyi hatály

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

9.10.1.3. Személyi hatály

(472.) A szolgáltatási szabályzat személyi hatálya kiterjed Szolgáltatónak a Szolgáltatások nyújtásában közreműködő munkatársaira, továbbá az Előfizető kapcsolattartójaként kijelölt személyekre, az Alanyokra, és Előfizető szervezetén belül az egyes tanúsítványok felhasználásáért felelős személyekre.

9.10.2. Megszűnés

(473.) A szolgáltatási szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3. Megszűnés után is hatályban maradó rendelkezések

(474.) 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 részvevőkkel

(475.) 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 Alany 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

(476.) 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

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

9.12.3. OID megváltozását előidéző körülmények

(478.) A szolgáltatási szabályzat új verziójával az OID nem változik.

9.13. Vitás kérdések rendezése

(479.) 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.

(480.) 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.

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

(482.) 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

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

9.15. Hatályos jognak megfelelés

(484.) Szolgáltató tevékenységét a mindenkor hatályos Európai Uniós, illetve magyar jogszabályoknak megfelelően végzi.

9.16. Vegyes rendelkezések

(485.) Nincs kikötés.

9.16.1. Teljességi záradék

(486.) Nincs kikötés.

9.16.2. Átruházás

(487.) Nincs kikötés.

9.16.3. Részleges érvénytelenség

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

9.16.4. Igényérvényesítés

(489.) 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)

(490.) 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 szükséghelyzet) 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.

(491.) Szolgáltató nem felelős a vis maior esetekből fakadó károkért.

9.17. Egyéb rendelkezések

(492.) Szolgáltató a Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználói termékeket hozzáférhetővé teszi a fogyatékossággal élő személyek számára, amennyiben az lehetséges.

10. Ábrajegyzék