Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz (BR-MTT)

Verziószám: **v.2.0**

Hatályba lépés dátuma: **2026.05.28.**

Dokumentum besorolása: **NYILVÁNOS**

Jóváhagyó	Adorján István
Adorján István	Digitálisan aláírta: Adorján István Dátum: 2026.04.28 17:24:18 +02'00'

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0[1]	2016.12.29	Első, eIDAS megfelelőségértékeléshez elkészített változat	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.1[2]	2017.04.28	Megfelelőségértékelő szervezet észrevételei alapján módosított változat	Polysys Kft. Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.2	2017.05.31.	Teszt tanúsítványok OID számának javítása	Papp Eszter	Kővári Ferenc	Ferencz Attila
1.3	2019.03.14	EN szabványok változásainak követése, visszavonás pontosítása, egyéb frissítések	Polysys Kft. Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.4	2023.04.01	• új algoritmuskészletek bevezetésével kapcsolatos módosítások; • kiegészítés tanúsítványmegújítás részleges bevezetéséhez kapcsolódó szabályokkal	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.5	2023.11.09	új ECC alapú CA bevezetéséhez kapcsolódó módosítások	Kővári-Szabó Zoltán	Nagy Benjámin Melo Sándor	Adorján István
1.6.[3]	2024.09.01.	• jogszabályi környezet változásából adódó módosítások (E-ügyintézési tv., DÁP tv., eIDAS) • visszavonást érintő folyamatok frissítése • általános felülvizsgálat	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
1.7.	2024.09.01.	• jogszabályi környezet változásából adódó módosítások (E-ügyintézési tv., DÁP tv., eIDAS) • visszavonást érintő folyamatok frissítése • általános felülvizsgálat • OID kiosztási rend módosításának alkalmazása a fedlapon	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
1.8	2025.03.24.	• Általános felülvizsgálat • Jogszabályi változások követése • EN szabványok változásainak követése	Polysys Kft.	Kővári-Szabó Zoltán Nagy Benjámin	Adorján István
1.9	2025.11.01	• ÁSZF alapú szerződéskötés • egyéb pontosítások	Buczynskiné dr. Szabó Zsuzsanna Kővári-Szabó Zoltán	Kővári-Szabó Zoltán Nagy Benjámin	Adorján István
2.0	2026.04.28.	• kiberbiztonsági felügyelet változás • akadálymentes sablon használata	Buczynskiné dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán Gál Ferenc	Adorján István

[1] Nem lépett hatályba
[2] Nem lépett hatályba
[3] Nem lépett hatályba

NISZ

Tartalom

1. BEVEZETÉS

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

(2.) A BR-MTT az alábbi jelöléseket használja:

a) a tanúsítvány alanyától függően:
- BÉLY: a tanúsítvány alanya jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet
- ALA: a tanúsítvány alanya természetes személy

b) attól függően, hogy a tanúsítvány használható-e digitális szolgáltatások nyújtásához, illetve közigazgatási célra:
- KET: a tanúsítvány a {J9} 322/2024 rendelet szerinti digitális szolgáltatások nyújtására, illetve közigazgatási célra használható
- NKET: a tanúsítvány a {J9} 322/2024 rendelet szerint digitális szolgáltatások nyújtására, illetve közigazgatási célra nem használható

c) a tanúsítványhoz kapcsolódó magánkulcsot tároló eszköztől függően:
- P12: a tanúsítványhoz kapcsolódó magánkulcsot szoftveres (az {Sz14} szabványnak megfelelő) kulcstároló tárolja
- QSCD: a tanúsítványhoz kapcsolódó magánkulcsot Szolgáltató által forgalmazott QSCD (minősített elektronikus aláírást/bélyegzőt létrehozó eszköz) hozza létre és tárolja.

(3.) A BR-MTT a Tanúsítványok alábbi típusait különbözteti meg:

BÉLY+KET+P12	digitális szolgáltatások nyújtás nyújtására használható, minősített, szoftveres, bélyegzés célú tanúsítvány
BÉLY+KET+QSCD	digitális szolgáltatások nyújtására használható, minősített, bélyegzés célú tanúsítvány
BÉLY+NKET+P12	minősített, szoftveres, bélyegzés célú tanúsítvány
BÉLY+NKET+QSCD	minősített, bélyegzés célú tanúsítvány
ALA+KET+P12	digitális szolgáltatások nyújtására használható, minősített, szoftveres, aláírás célú tanúsítvány
ALA+KET+QSCD	digitális szolgáltatások nyújtására használható, minősített, aláírás célú tanúsítvány
ALA+NKET+P12	minősített, szoftveres, aláírás célú tanúsítvány
ALA+NKET+QSCD	minősített, aláírás célú tanúsítvány

(4.) Jelen bizalmi szolgáltatási rend a kibocsátott Tanúsítványok kezelésére (előállítás, kibocsátás, közzététel, megújítás, felfüggesztés, újra-érvényesítés, visszavonás, továbbiakban együttesen: Szolgáltatások) vonatkozó követelményeket, a tanúsítványok tartalmának és érvényességének ellenőrzési eljárásait és a Szolgáltatások működtetésének követelményeit tartalmazza.

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

1.1. Áttekintés

(6.) A BR-MTT egy olyan szabálygyűjtemény, amely a Szolgáltatások használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára, valamint meghatározza a Tanúsítványok felhasználhatóságát.

(7.) Jelen bizalmi szolgáltatási rend az {Sz1} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában szigorúan követi annak előírásait.

(8.) Jelen bizalmi szolgáltatási rend előírja a Tanúsítványokkal kapcsolatos, a Szolgáltatások nyújtása során teljesíteni szükséges összes követelményt, melyeket az alábbi nemzetközi 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; Part 1: General requirements {Sz3}

c) EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates {Sz4}

d) EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz5}

e) EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz6}

f) EN 319 412-3: Certificate Profiles; Part 3: Certificate profiles for certificates issued to legal persons {Sz7}

g) EN 319 412-5: Certificate Profiles; Part 5: QcStatements {Sz8}

(9.) Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a „Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BSZ-MTT) dokumentum tartalmazza.

(10.) A jelen bizalmi szolgáltatási rendnek megfelelően kibocsátott tanúsítványok tartalmazzák jelen dokumentum objektum azonosítóját, mely alapján az érintett felek képesek meghatározni az adott tanúsítvány alkalmazhatóságát és megbízhatóságát.

1.2. Dokumentum neve és azonosítása

(11.) Jelen bizalmi szolgáltatási rend teljes neve NISZ Zrt. „Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz”.

(12.) A bizalmi szolgáltatási rend rövid neve: BR-MTT.

(13.) A bizalmi szolgáltatási rend objektum azonosítója és verziószáma a címlapon található.

(14.) A jelen BR-MTT hatálya alatt kiadott tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat a BSZ-MTT szolgáltatási szabályzat tartalmazza.

(15.) Jelen BR-MTT-nek csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.1. Hitelesítési rendek

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

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

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

1.3. PKI közösség

1.3.1. Hitelesítő szervezet

(17.) 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.

(18.) A Szolgáltató saját szervezetén kívül más szervezetek is közreműködhetnek a Szolgáltatások nyújtásában, azonban a Szolgáltató teljes körű felelősséggel tartozik azért, hogy a jelen szabályzatban foglalt követelmények teljesülnek.

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 a saját szervezetén kívüli regisztrációs szervezetet (ügyfélkapcsolati irodát) is működtethet, a vele szerződéses alapon együttműködő társaságokkal (mint szerződött közreműködőkkel) együtt. Ezen regisztrációs szervezetek elvégzi a saját igénylők adatainak rögzítését, az igénylők személyazonosságának megállapítását, a tanúsítvány kérelmek összeállítását és Szolgáltatóhoz történő továbbítását. Biztosítják a tanúsítványok és az aláírást létrehozó eszközök szétosztását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el. Azon tevékenységek vonatkozásában, melyeket a Szolgáltató nem maga lát el, teljes körű felelősséget vállal azért, hogy a jelen szabályzatban foglalt követelmények teljesülnek.

1.3.3. Előfizetők és Alanyok, Aláírók és Bélyegző Létrehozók

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

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

a) [ALA] természetes személy: az Előfizetővel kapcsolatban álló személy, aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hoz létre;

b) [BÉLY] jogi személy: az Előfizető szervezete, vagy annak valamely szervezeti egysége, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hoz létre;

c) [BÉLY] eszköz: az Előfizető által vagy nevében működtetetett informatikai eszköz vagy rendszer, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hoz létre.

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

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

1.3.3.1. Előfizető Kapcsolattartója

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

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

1.3.4. Érintett felek

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

1.3.5. Egyéb felek

Bizalmi Felügyelet

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

1.4. A tanúsítvány alkalmazhatósága

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

a) [ALA] üzleti tanúsítvány: a tanúsítvány Alanya az Előfizetővel kapcsolatban álló természetes személy (képviseleti joggal rendelkező vagy cégjegyzésre jogosult személy vagy Előfizető szervezete által foglalkoztatott személy, akinek Előfizetővel való kapcsolata igazolásra és a tanúsítványban megjelölésre került), aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hozhat létre;

b) [ALA] személyes tanúsítvány: a tanúsítvány Alanya az Előfizetővel kapcsolatban álló természetes személy (akinek Előfizetővel való kapcsolata a tanúsítványban megjelölésre nem került), aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hozhat létre;

c) [BÉLY] szervezeti tanúsítvány: a tanúsítvány Alanya az Előfizető szervezet, vagy annak valamely szervezeti egysége, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hozhat létre;

d) [BÉLY] eszköz tanúsítvány: a tanúsítvány Alanya az Előfizető által vagy nevében működtetett informatikai eszköz vagy rendszer, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hozhat létre.

(32.) [ALA+QSCD] Az üzleti és személyes tanúsítványok a {J1} eIDAS 25. cikke szerinti minősített elektronikus aláírás létrehozására és ellenőrzésére használhatók.
(33.) [ALA+P12] Az üzleti és személyes tanúsítványok minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás létrehozására és ellenőrzésére használhatók.
(34.) [BÉLY+QSCD] A szervezeti és eszköz tanúsítványok a {J1} eIDAS 35. cikke szerint minősített elektronikus bélyegző létrehozására és ellenőrzésére használhatók.
(35.) [BÉLY+P12] A szervezeti és eszköz tanúsítványok minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzők létrehozására használhatók.
(36.) [QSCD] A minősített elektronikus aláírások és bélyegzők joghatását a {J4} Pp. 325. § f) pontja határozza meg. E szerint a minősített elektronikus aláírással vagy bélyegzővel hitelesített dokumentum teljes bizonyító erejű magánokirat.
(37.) [P12] A minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírások és bélyegzők joghatását a {J4} Pp. 325. § f) pontja határozza meg. E szerint a minősített tanúsítványon alapuló elektronikus aláírással vagy bélyegzővel hitelesített dokumentum teljes bizonyító erejű magánokirat.

Teszt tanúsítványok

(38.) 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.
(39.) 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.
(40.) A teszt tanúsítványok megjelölése olyan módon történik, hogy a tanúsítványban feltüntetett hitelesítési rend objektumazonosító: 0.2.216.1.200.1100.100.42.3.999.
(41.) A teszt tanúsítványokhoz és azon alapuló elektronikus aláírásokhoz vagy bélyegzőkhöz semmilyen joghatás nem kapcsolódik.

1.4.1. Engedélyezett tanúsítvány használat

(42.) [ALA] A kibocsátott üzleti vagy személyes tanúsítványhoz kapcsolódó magánkulcs kizárólag elektronikus aláírások létrehozására, a tanúsítvánnyal hitelesített nyilvános kulcs kizárólag az elektronikus aláírások érvényesítésére használható.
(43.) [BÉLY] A kibocsátott szervezeti vagy eszköz tanúsítványhoz kapcsolódó magánkulcs kizárólag elektronikus bélyegzők létrehozására, a tanúsítvánnyal hitelesített nyilvános kulcs kizárólag az elektronikus bélyegzők érvényesítésére használhatók.
(44.) [ALA+QSCD] A kibocsátott üzleti vagy személyes tanúsítványok minősített elektronikus aláírást létrehozó eszköz (QSCD) használatát megkövetelő tanúsítványok.
(45.) [BÉLY+QSCD] A kibocsátott szervezeti vagy eszköz tanúsítványok minősített elektronikus bélyegzőt létrehozó eszköz (QSCD) használatát megkövetelő tanúsítványok.
(46.) A személyes tanúsítványokat az Alanyok csak és kizárólag az Előfizetőhöz kapcsolódó tevékenységükhöz (munkaviszonyukból fakadó feladataik elvégzéséhez) használhatják fel.
(47.) A fentieken túl, a kibocsátott tanúsítványok és kapcsolódó kulcspárok csak a {D1} Általános Szerződési Feltételekben, illetve a {D2} Szolgáltatási Szerződésben rögzített feltételekkel használhatók fel.

1.4.2. Tiltott tanúsítvány használat

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

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

1.5. Szabályzat adminisztráció

1.5.1. Szabályzatot karbantartó szervezet

(50.) A Szolgáltatónak szervezetén belül Hitelesítési Rend és Szabályozási Csoportot kell működtetnie, amely többek között jelen bizalmi szolgáltatási rend karbantartásáért is felelős.

1.5.2. Kapcsolat

(51.) Az Ügyfélkapcsolati Iroda elérhetőségét, nyitva tartását, a Szolgáltatóval való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a szolgáltatási szabályzat tartalmazza.

1.5.3. Szabályzat alkalmasságának meghatározása

(52.) A Szolgáltató legalább évente egyszer meg kell vizsgálja a bizalmi szolgáltatási rend, illetve a szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit változtatási igényként figyelembe kell vegye.
(53.) Amennyiben a változtatási igények befolyásolhatják a Szolgáltatásnak az Alanyok, Előfizetők vagy Érintett Felek általi elfogadását, a Szolgáltató erről előzetes értesítést kell közzé tegyen a Szolgáltatások internetes honlapján.
(54.) A változtatási igényeket a Hitelesítési Rend és Szabályozási Csoport gyűjti, a módosításokat legalább évente egyszer elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

1.5.4. Szabályzat jóváhagyásának eljárása

(55.) Szolgáltatónak rendelkeznie kell a szabályzatainak jóváhagyására és kiadására vonatkozó eljárásrenddel, melyet a szolgáltatási szabályzatában ismertetnie kell. Az eljárásrendben meg kell jelölni az eljárásért felelős személyt, valamint az egyéb fontos részleteket (pl. hatályba lépés napja).
(56.) A jóváhagyott szabályzatot Szolgáltató azonnal közzé kell tegye a Szolgáltatások internetes honlapján.

1.6. Fogalmak, rövidítések és hivatkozások

1.6.1. Fogalmak

(57.) A jelen szabályzatban használt fogalmak értelmezése megegyezik a Szolgáltatásokra vonatkozó jogszabályokban (1.6.3.1 fejezet) szereplő meghatározásokkal.
(58.) Az ezen felül alkalmazott fogalmak meghatározása az alábbiakban olvasható:

a) Alany: a tanúsítványban a bizalmi szolgáltató által igazolt azonosságú vagy tulajdonságú természetes személy vagy jogi személy, illetve közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet. Jelen dokumentumban az Alany kifejezés elektronikus aláírás célú tanúsítvány esetén az Aláírót, elektronikus bélyegzés célú tanúsítvány esetén a Bélyegző Létrehozót jelenti.

b) Aláíró: az elektronikus aláírás célú tanúsítvány alanya - a természetes személy - aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hoz létre.

c) Bélyegző Létrehozó: az elektronikus bélyegzés célú tanúsítvány alanya - a jogi személy, illetve közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet - amely a tanúsítvány és a

kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hoz létre.

d) **Bizalmi horgony** (Trust Anchor): olyan felső szintű hitelesítés-szolgáltatói tanúsítvány, amely megbízhatóságát az illetékes hatóság vagy maga a szolgáltató garantálja. A {J1} eIDAS rendelet értelmében az EU tagállamok bizalmi listáin szereplő, minősített bizalmi szolgáltatások tanúsítványai bizalmi horgonynak tekintendők. A bizalmi horgonyokat egy informatikai rendszer előre meghatározott konfigurációban kezeli, és a megbízhatósági döntésekhez használja. Az elektronikus aláírások és bélyegzők, valamint az elektronikus időbélyegzők érvényesítésének egyik lépése a létrehozásukhoz használt tanúsítványhoz a tanúsítási útvonal felépítése, mely akkor fogadható el, ha bizalmi horgonyban végződik.

e) **Digitális szolgáltatás**: a digitális szolgáltatást biztosító szervezet feladat- és hatáskörébe tartozó ügy, valamint a digitális szolgáltatást biztosító szervezet által jogszabály alapján biztosítandó szolgáltatáshoz kapcsolódó ügyintézést a {J2} DÁP tv. szerint biztosító szolgáltatás, valamint ezek együttműködő rendszere.

f) **Előfizető**: a Szolgáltatóval kapcsolatban álló jogi személy, illetve közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet, amely megrendeli a Szolgáltatótól a Szolgáltatásokat, jellemzően tanúsítvány kibocsátását az általa megnevezett tanúsítvány alanyok számára.

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

h) **Kiberbiztonsági Felügyelet**: a {J12} kiberbiztonsági törvény hatálya alá tartozó információs rendszerek felügyeletét ellátó hatóság, amely a NISZ Nemzeti Infokommunikációs Zrt. esetében a Nemzeti Kibervédelmi Intézet (NKI).

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
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
QSCD	Qualified Signature/Seal Creation Device	a {J1} eIDAS II. mellékletének megfelelő, minősített aláírást/bélyegzőt létrehozó eszköz
P12	PKCS#12	az {Sz14} szabványnak megfelelő, szoftveres kulcstároló
RA	Registration Authority	regisztrációs szervezet
SHA	Secure Hash Algorithm	lenyomatképző algoritmus

UTC	Coordinated Universal Time	koordinált univerzális idő

1.6.3. Hivatkozások

1.6.3.1. Jogszabályi hivatkozások

{J1}	910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (röviden: eIDAS)
{J2}	2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (a továbbiakban: DÁP tv.)
{J3}	1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról (a továbbiakban: Nytv.)
{J4}	2016. évi CXXX. törvény a polgári perrendtartásról (röviden: Pp.)
{J5}	2013. évi V. törvény a Polgári Törvénykönyvről (a továbbiakban: Ptk.)
{J6}	321/2024 (XI. 6.) Korm. rendelet a digitális állampolgárság egyes szabályairól
{J7}	320/2024 (XI. 6.) Korm. rendelet a digitális állam megvalósításához kapcsolódó egyes szervezetek kijelöléséről
{J8}	24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
{J9}	322/2024 (XI. 6.) Korm. rendelet a digitális szolgáltatások, a digitális állampolgárság szolgáltatások és támogató szolgáltatások részletes műszaki követelményeiről
{J10}	679/2016/EU Európai Parlament és a Tanács rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: GDPR)
{J11}	2555/2022/EU Európai Parlament és a Tanács irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról (a továbbiakban: NIS2 irányelv)
{J12}	2024. évi LXIX. Törvény Magyarország kiberbiztonságáról (a továbbiakban: kiberbiztonsági tv.)
{J13}	7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

1.6.3.2. Szabványok és műszaki-technikai specifikációk

{Sz1}	RFC 3647	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz2}	EN 319 401	General policy requirements for Trust Service Providers
{Sz3}	EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
{Sz4}	EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

{Sz5}	EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures
{Sz6}	EN 319 412-2	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
{Sz7}	EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issues to legal persons
{Sz8}	EN 319 412-5	Certificate Profiles; Part 5: QCStatements
{Sz9}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz10}	ITU-T X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz11}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz12}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz13}	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
{Sz14}	PKCS#12	Personal Information Exchange Syntax Standard
{Sz15}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz16}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz17}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules
{Sz18}	FIPS 140-3	FIPS PUB 140-3 (2019): Security Requirements for Cryptographic Modules
{Sz19}	TS 119 615	Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists
{Sz20}	TS 119 172-4	Signature policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists

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
{D4}	NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}	NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}	NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}	NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}	Tanúsítvány profilok a NISZ eIDAS rendelet szerinti bizalmi szolgáltatásaihoz

2. KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR

2.1. Tanúsítványtár

(59.) A Szolgáltatónak gondoskodnia kell 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, napi 24 órában, heti hét napban rendelkezésre álljanak. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy az információk elérhetetlensége ne haladhassa meg a szolgáltatási szabályzatban meghatározott időtartamot.

2.2. A szolgáltatói információ közzététele

(60.) A Szolgáltató a szolgáltatói tanúsítványokat, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat internetes honlapján közzé kell tegye.
(61.) A Szolgáltatónak a kiadott (hitelesített) végfelhasználói tanúsítványokat belső tanúsítványtárában meg kell őriznie és az Előfizető számára rendelkezésre kell bocsátania. A Szolgáltatónak a végfelhasználói tanúsítványt a tanúsítvány Alany – szervezeti vagy eszköz tanúsítvány esetén az Előfizető - hozzájárulása esetén közzé kell tennie az internetes honlapján nyilvánosan elérhető, kereshető tanúsítványtárában.
(62.) Szolgáltatónak a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítania kell. A visszavonási állapot információk közzétételével kapcsolatos információkat a 4.10 fejezet tartalmazza.

2.3. A közzététel gyakorisága

(63.) Szolgáltató a szolgáltatói tanúsítványokat legkésőbb azok éles üzembe helyezését megelőző 24 órán belül teszi közzé.
(64.) Szolgáltató a végfelhasználói tanúsítványokat a nyilvánosan kereshető tanúsítványtárban a tanúsítvány alany – szervezeti vagy eszköz tanúsítvány esetén az Előfizető - hozzájárulása esetén a kibocsátást követő 24 órán belül teszi közzé.
(65.) Szolgáltató a tanúsítványokkal kapcsolatos szabályzatokat azok változása esetén közzé teszi legalább 30 nappal a változás hatályba lépését megelőzően.
(66.) 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 a szolgáltatási szabályzatban meghatározott időtartamon belül új CRL-t állít elő és tesz közzé.
(67.) Szolgáltató az OCSP szolgáltatása keretében minden OCSP kérésre friss választ állít elő és ad vissza.

2.4. Hozzáférés-ellenőrzések

(68.) Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a szolgáltatói tanúsítványokhoz, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokhoz, a tanúsítványokkal kapcsolatos visszavonási információkhoz.
(69.) A végfelhasználói tanúsítványokkal kapcsolatban biztosítja a nyilvános tanúsítványtár kereshetőségét a tanúsítványban tárolt adatok alapján.
(70.) Szolgáltató biztonsági intézkedésekkel és eljárási szabályokkal gondoskodik az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.
(71.) A kibocsátott tanúsítványokkal kapcsolatos szabályzatoknak csak az elektronikus, aláírással vagy bélyegzővel ellátott formája tekinthető hitelesnek, a dokumentumok nyomtatott változatai semmilyen formában nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

3. AZONOSÍTÁS ÉS HITELESÍTÉS

3.1. Elnevezések

3.1.1. Név típusok

(72.) A tanúsítványban szereplő nevek megadása meg kell, hogy feleljen az {Sz10} ITU-T X.520 szabványnak. Ezen túl:

(73.) A tanúsítvány alanya (Subject) mező tartalma meg kell, hogy feleljen:

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

(74.) A tanúsítvány kibocsátója (Issuer) mező tartalma meg kell, hogy feleljen:

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

3.1.2. Nevek jelentése

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

(76.) Ezen felül, a szolgáltatási szabályzatban ismertetni kell az 1.4 fejezet szerinti tanúsítványtípusokra vonatkozóan a tanúsítvány Subject mezőjében szereplő névattribútumok képzési és igazolási szabályait.

3.1.3. Előfizetők névtelensége és álnév használata

(77.) Az Előfizetők névtelensége nem megengedett.

(78.) Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell az álneves tanúsítvány felismerhetőségére vonatkozó szabályokat.

3.1.4. Különféle név formák megjelenítési szabályai

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

3.1.5. A nevek egyedisége

(80.) A Szolgáltatónak biztosítania kell a tanúsítvány Subject mezőjébe foglalt megkülönböztető név (Distinguished Name) egyediségét, azaz gondoskodnia kell arról, hogy egy adott megkülönböztető nevet soha nem fog egy másik Aláíróhoz vagy Bélyegző Létrehozóhoz rendelni.

3.1.6. Márkanevek elismerése, hitelesítése és szerepe

(81.) A szolgáltatási szabályzatban ismertetni kell a márkanevek, védjegyek stb. elismerésével, hitelesítésével kapcsolatos információkat.

3.2. Kezdeti azonosítás

(82.) Szolgáltatónak a vonatkozó jogszabályoknak megfelelően kell elvégeznie 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.

(83.) [KET] digitális szolgáltatások nyújtására használható tanúsítványok esetén Szolgáltatónak a tanúsítvány kibocsátásához kapcsolódó személyazonosítás (regisztráció) során a {J9} 322/2024 előírásainak megfelelően kell eljárnia.

3.2.1. A magánkulcs birtoklása

(84.) Szolgáltatónak meg kell győződnie arról, hogy az Alany (Aláíró vagy a Bélyegző Létrehozó) a tanúsítványhoz kapcsolódó magánkulcsot birtokolja. A szolgáltatási szabályzatban ismertetni kell a magánkulcs birtoklás ellenőrzésének módszerét és eljárását.

3.2.2. A szervezeti azonosság hitelesítése

(85.) Ha a tanúsítvány alanya nem természetes személy, akkor Szolgáltatónak ellenőriznie kell Előfizető szervezetének hivatalos nevét és egyedi azonosító adatát (adószámát vagy cégjegyzékszámát). Az adatok valódiságát és hatályosságát közhiteles nyilvántartás alapján, vagy ha ilyen közhiteles nyilvántartás nincsen, az igényléshez csatolt hivatalos dokumentum alapján kell ellenőrizni.
(86.) Szolgáltató köteles a tanúsítvány kibocsátása előtt, a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személy képviseleti jogának fennállásáról jogszabály, közhiteles nyilvántartás, létesítő okirat, vagy ezek hiányában meghatalmazás alapján meggyőződni, az ellenőrzés eredményét rögzíteni.

3.2.3. A személyazonosság hitelesítése

(87.) Ha a tanúsítvány alanya természetes személy, akkor a {D9} tanúsítvány megrendelő és regisztrációs űrlapon megadott, a regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét az adott személy az űrlapon saját kezű aláírásával igazolja.
(88.) Ha a tanúsítvány alanya természetes személy, akkor Szolgáltató köteles a tanúsítvány kibocsátása előtt az alany személyazonosságát, a személyazonosság megállapításához használt adatok valódiságát és – ha van ilyen – közhiteles vagy más központi nyilvántartásban foglalt adatokkal való megegyezőségét ellenőrizni.

3.2.4. Előfizető nem ellenőrzött adatai

(89.) Szolgáltatónak ellenőriznie kell minden, a tanúsítvány alany mezőjébe (Subject) kerülő adatot.
(90.) A tanúsítvány egyéb mezőibe és kiterjesztéseibe kerülő adatok tekintetében Szolgáltatónak a szolgáltatási szabályzatában meg kell jelölnie azokat, melyek nem kerülnek ellenőrzésre.

3.2.5. Jogosultság ellenőrzése

(91.) Szolgáltatónak ellenőriznie kell, hogy a tanúsítvány megrendelő és regisztrációs űrlapot az arra jogosult személy – Előfizető Kapcsolattartója – írta alá.
(92.) Az egyes tanúsítvány alanyok tanúsítványra való jogosultságának elbírálása és ellenőrzése Előfizető döntésköre és felelőssége.

3.2.6. Együttműködési kritériumok

(93.) Nincs kikötés.

3.3. Azonosítás és hitelesítés kulcscsere esetén

(94.) A kulcscsere az a folyamat, melynek során az eredeti tanúsítványba foglalt változatlan adatokhoz, megegyező érvényességi időtartammal új nyilvános kulcs kerül hitelesítésre.
(95.) A Szolgáltató nem nyújt kulcscsere szolgáltatást.
(96.) A tanúsítvány kulcsának cseréjéhez Előfizető új tanúsítványt kell igényeljen.

3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

(97.) Nincs kikötés.

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

(98.) Nincs kikötés.

3.4. Azonosítás és hitelesítés visszavonási vagy felfüggesztési kérelem esetén

(99.) Szolgáltatónak azonosítania és hitelesítenie kell a visszavonási és felfüggesztési kérelmeket azok feldolgozása előtt. Ennek eljárását a szolgáltatási szabályzatban kell ismertetni.

4. A TANÚSÍTVÁNYOK ÉLETCIKLUSA

4.1. Tanúsítványigénylés

4.1.1. Ki nyújthat be tanúsítványigénylést

(100.) Tanúsítvány igénylést Előfizető Kapcsolattartója nyújthat be Szolgáltató részére.

4.1.2. Igénylési folyamat és felelősségek

(101.) A tanúsítványigénylés folyamata röviden a következő:

a) tanúsítványigénylést, szerződéskötést megelőző tájékoztatás
b) szerződéskötés előkészítése, adatok előzetes megküldése
c) Szolgáltatási Szerződés megkötése (ÁSZF-GOVCA elfogadásával vagy egyedi szolgáltatási szerződés megkötésével)
d) tanúsítvány alanyok regisztrációja és a tanúsítványba kerülő adatok ellenőrzése és igazolása
e) tanúsítványkérelmek összeállítása

(102.) Szolgáltatónak a szolgáltatási szabályzatban részletesen ismertetnie kell a fenti folyamat eljárását és az egyes lépéseket.

(103.) Az igénylési folyamattal kapcsolatos felelősségeket a 9.6 fejezet és annak alfejezetei tartalmazzák.

4.2. Tanúsítványigénylés feldolgozása

4.2.1. Azonosítási és hitelesítési műveletek

(104.) A tanúsítványigénylés elfogadása előtt Szolgáltatónak el kell végeznie Előfizető Kapcsolattartójának, valamint a tanúsítvány alanyának azonosítását és adatainak ellenőrzését.

(105.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia annak az (a kezdeti azonosítás időpontjával induló) időtartamnak a hosszát, amelyen belül a tanúsítvány kibocsátása a kezdeti azonosítás megismétlése nélkül elvégezhető.

4.2.2. Tanúsítványigénylés elfogadása vagy visszautasítása

(106.) Szolgáltatónak el kell fogadnia a tanúsítványigénylést, ha:

a) Előfizető szervezeti azonosságát sikeresen igazolta; és
b) Előfizető Kapcsolattartóját, valamint üzleti- és személyes tanúsítvány esetén a természetes személy alanyt is sikeresen azonosította; és
c) a regisztrációs és a tanúsítványba kerülő adatokat sikeresen ellenőrizte és igazolta.

(107.) Szolgáltatónak vissza kell utasítania a tanúsítványigénylés elfogadását, ha valamely adat, bemutatott okmány vagy dokumentum eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel vagy az igényelt tanúsítvány valamely jogszabály (különösen a {J6} 321/2024 és {J7} 320/2024) vonatkozó rendelkezése miatt nem adható ki.

4.2.3. Tanúsítványigénylés feldolgozás időtartama

(108.) Szolgáltatónak a tanúsítványigényléseket azok benyújtását követően a Szolgáltatási Szerződésben rögzített időtartamon belül, ennek hiányában a {D1} Általános Szerződési Feltételekben jelzett 15 naptári napon belül fel kell dolgoznia.

4.3. Tanúsítvány kibocsátás

4.3.1. Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

(109.) Az Ügyfélkapcsolati Iroda továbbítja az elfogadott tanúsítványigénylést a Regisztrációs Irodának.

(110.) A Regisztrációs Iroda elindítja a Szolgáltatásokat támogató informatikai rendszerben a tanúsítvány létrehozását, majd értesíti az Ügyfélkapcsolati Irodát a tanúsítvány elkészültéről.

4.3.2. Előfizető értesítése a tanúsítvány kibocsátásról

(111.) Szolgáltatási Szerződés megléte esetén, illetve megkötését követően a Regisztrációs Iroda emailben értesíti Előfizető Kapcsolattartóját – és aláírás célú tanúsítvány esetén az Aláírót - a tanúsítvány elkészültéről és átvételének módjáról.

(112.) A tanúsítvány átadása csak az arra jogosult (Előfizető Kapcsolattartója, vagy aláírás célú tanúsítvány esetén az Aláíró) részére történhet.

4.4. Tanúsítvány-elfogadás

4.4.1. Tanúsítvány Előfizető általi elfogadása

(113.) Az üzleti- és személyes tanúsítványok esetén az Aláíró, a szervezeti- és eszköz tanúsítványok esetén az Előfizető Kapcsolattartójának kötelezettsége, hogy az átvett tanúsítványban feltüntetett adatok helyességét mihamarabb ellenőrizze. Amennyiben bármilyen eltérést talált, haladéktalanul intézkednie kell a tanúsítvány visszavonásáról.

4.4.2. Tanúsítvány közzététele

(114.) Az Előfizető - valamint az üzleti- és személyes tanúsítványok esetén az Aláíró – írásos hozzájárulása esetén Szolgáltatónak a kibocsátott tanúsítványt közzé kell tennie a Szolgáltatások internetes honlapján elérhető nyilvános tanúsítványtárban.

4.4.3. További felek értesítése a tanúsítvány kibocsátásáról

(115.) Nincs kikötés.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. Az Előfizető magánkulcs- és tanúsítvány használata

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

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

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

4.5.2. Az Érintett felek nyilvános kulcs- és tanúsítvány használata

(119.) A jelen bizalmi szolgáltatási rend hatálya alatt kibocsátott tanúsítványon alapuló elektronikus aláírások vagy bélyegzők elfogadása során szükséges, hogy az Érintett Fél megfelelő körültekintéssel járjon el, melyhez javasolt betartania a szolgáltatási szabályzatban leírt követelményeket, különös tekintettel az alábbiakra:

a) a tanúsítványokat csak olyan alkalmazásokban fogadja el, melyek összhangban vannak a tanúsítvány „kulcshasználat" (KeyUsage) és „kiterjesztett kulcshasználat" (ExtendedKeyUsage) kiterjesztésének tartalmával;
b) ellenőrizze a tanúsítvány érvényességét és visszavonási állapotát;
c) vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítvány által hivatkozott szabályzatokban szerepel.

4.6. Tanúsítványok megújítása

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

(121.) A Szolgáltató nem nyújt tanúsítványmegújítás szolgáltatást, kivéve a BSZ-MTT-ben foglalt eseteket.

(122.) Ha a tanúsítvány lejár, de a szolgáltatásra a továbbiakban is szükség van, Előfizető új tanúsítványt kell igényeljen, az erre vonatkozó folyamatok szerint. Szolgáltató a lejárat előtt 30 nappal értesítést küld Előfizetőnek.

4.6.1. Tanúsítvány megújítás körülményei

(123.) Tanúsítványmegújítás a BSZ-MTT-ben foglalt esetekben kezdeményezhető.

4.6.2. Ki kérelmezhet tanúsítvány megújítást

(124.) Lásd 4.1.1 fejezet, egyéb kikötés nincs.

4.6.3. Tanúsítvány megújítási kérelmek feldolgozása

(125.) Lásd 4.2 fejezet, egyéb kikötés nincs.

4.6.4. Előfizető értesítése a megújított tanúsítvány kibocsátásáról

(126.) Lásd 4.3.2 fejezet, egyéb kikötés nincs.

4.6.5. Tanúsítvány Előfizető általi elfogadása

(127.) Lásd 4.4 fejezet, egyéb kikötés nincs.

4.6.6. Megújított tanúsítvány közzététele

(128.) Lásd 4.4.2 fejezet, egyéb kikötés nincs.

4.6.7. További felek értesítése tanúsítvány megújításról

(129.) Lásd 4.4.3 fejezet, egyéb kikötés nincs.

4.7. Kulcscsere

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

(131.) A Szolgáltató nem nyújt kulcscsere szolgáltatást.

(132.) A tanúsítvány kulcsának cseréjéhez Előfizető új tanúsítványt kell igényeljen.

4.7.1. Ki kérelmezhet kulcscserét

(133.) Nincs kikötés.

4.7.2. Kulcscsere kérelmek feldolgozása

(134.) Nincs kikötés.

4.7.3. Előfizető értesítése az új tanúsítvány kibocsátásáról

(135.) Nincs kikötés.

4.7.4. Új tanúsítvány Előfizető általi elfogadása

(136.) Nincs kikötés.

4.7.5. Új tanúsítvány közzététele

(137.) Nincs kikötés.

4.7.6. További felek értesítése az új tanúsítvány kibocsátásáról

(138.) Nincs kikötés.

4.8. Tanúsítvány-módosítás

(139.) 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.

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

(141.) A tanúsítványba foglalt adatok változása esetén Előfizetőnek új tanúsítványt kell igényelnie és intézkednie kell a meglevő tanúsítvány visszavonásáról.

4.8.1. Tanúsítvány-módosítás körülményei

(142.) Nincs kikötés.

4.8.2. Ki kérelmezhet tanúsítvány-módosítást

(143.) Nincs kikötés.

4.8.3. Tanúsítvány-módosítási kérelmek feldolgozása

(144.) Nincs kikötés.

4.8.4. Előfizető értesítése az új tanúsítvány kibocsátásáról

(145.) Nincs kikötés.

4.8.5. Módosított tanúsítvány Előfizető általi elfogadása

(146.) Nincs kikötés.

4.8.6. Módosított tanúsítvány közzététele

(147.) Nincs kikötés.

4.8.7. További felek értesítése a módosított tanúsítvány kibocsátásáról

(148.) Nincs kikötés.

4.9. Tanúsítvány visszavonása és felfüggesztése

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

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

(151.) A visszavont / felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

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

4.9.1. Visszavonás körülményei

(153.) Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a visszavonáshoz vezető körülményeket.

4.9.2. Ki kezdeményezheti a visszavonást

(154.) Visszavonást kezdeményezhet:

a) Előfizető Kapcsolattartója, továbbá aláírás célú tanúsítvány esetén maga az Aláíró;
b) Szolgáltató.

4.9.3. Visszavonási kérelemre vonatkozó eljárás

(155.) Szolgáltatónak ellenőriznie kell a visszavonást kérelmező azonosságát és jogosultságát, valamint ellenőriznie kell a visszavonási kérelemben foglalt adatokat. Ha az ellenőrzések sikeresek, Szolgáltató el kell végezze a tanúsítvány visszavonását és a megváltozott visszavonási állapot információt közzé kell tennie, valamint értesítenie kell az Alanyt, illetve Előfizetőt a tanúsítvány visszavonásáról.

(156.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az arra az esetre vonatkozó eljárásrendet, ha a visszavonási kérelem huszonnégy (24) órán belül nem igazolható.

(157.) A tanúsítvány visszamenőleges visszavonása nem megengedett.

(158.) Szolgáltató az egyszer már visszavont tanúsítvány érvényességét nem állíthatja vissza érvényesre.

4.9.4. Kivárási idő visszavonási kérelem esetén

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

4.9.5. Visszavonási kérelem feldolgozásának időbelisége

(160.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azt a maximális időtartamot, melyen belül a visszavonási kérelmet feldolgozza.

4.9.6. Visszavonás ellenőrzésének ajánlása az Érintett felek számára

(161.) 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

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

(163.) A szolgáltatói tanúsítványokhoz kapcsolódó CRL kibocsátásának gyakorisága: 30 naponként legalább egy CRL. A CRL-nek tartalmaznia kell 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

(164.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azt a maximális időtartamot, melyen belül a CRL-t az előállítását követően közzéteszi.

4.9.9. OCSP szolgáltatás biztosítása

(165.) Szolgáltatónak az előfizetői és szolgáltatói tanúsítványok visszavonási állapotának megállapításához OCSP szolgáltatást is kell nyújtania.

4.9.10. OCSP alapú visszavonás ellenőrzés követelményei

(166.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az OCSP alapú visszavonás ellenőrzésével kapcsolatban az Érintett Felek számára fontos figyelmeztetéseket.

4.9.11. Visszavonási állapot közlés más formái

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

4.9.12. Különleges követelmények a kulcs kompromittálódása esetére

(168.) Szolgáltatónak mindent meg kell tennie annak érdekében, hogy a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről az Érintett Feleket értesítse.

(169.) A produktív hitelesítő központ magánkulcsának kompromittálódása esetén a Szolgáltatónak képesnek kell lennie az összes érintett végfelhasználói tanúsítvány visszavonására, valamint az adott szolgáltatói tanúsítvány visszavonására. Ebben az esetben a CRL-ben és OCSP válaszokban a tanúsítványok visszavonási ok információt "kulcs kompromittálódás" (keyCompromise) értékre kell állítani.

4.9.13. Felfüggesztés körülményei

(170.) Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a felfüggesztéshez vezető körülményeket.

4.9.14. Ki kérelmezhet felfüggesztést

(171.) Felfüggesztést kezdeményezhet:

a) Előfizető Kapcsolattartója, továbbá aláírás célú tanúsítvány esetén maga az Aláíró;
b) Szolgáltató.

4.9.15. Felfüggesztésre vonatkozó eljárás

(172.) Szolgáltatónak ellenőriznie kell a felfüggesztést kérelmező azonosságát és jogosultságát, valamint ellenőriznie kell a felfüggesztési kérelemben foglalt adatokat. Ha az ellenőrzések sikeresek, Szolgáltató el kell végezze a tanúsítvány felfüggesztését és a megváltozott visszavonási állapot információt közzé kell tennie.

4.9.16. A felfüggesztés megengedett időtartama

(173.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a felfüggesztés megengedett időtartamát. Ha a tanúsítvány újra-érvényesítése a felfüggesztésre megengedett időtartamon belül nem történik meg, Szolgáltatónak vissza kell vonnia a tanúsítványt.

4.10. Visszavonási állapot szolgáltatások

4.10.1. Működési jellemzők

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

(175.) Szolgáltatónak biztosítania kell, hogy a visszavonási állapot információ változása mind a CRL, mind az OCSP szolgáltatásban azonosan, konzisztens módon megjelenjen, figyelembe véve az egyes szolgáltatásokban eltérő frissítési időket is.

CRL

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

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

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

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

(180.) A Szolgáltatónak záró CRL-t kell kibocsátania, amikor egy adott hitelesítő központ működtetését megszünteti:

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

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

OCSP

(182.) A Szolgáltató által biztosított OCSP szolgáltatás meg kell feleljen az {Sz13} RFC 6960 szabványnak.

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

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

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

(186.) Az OCSP szolgáltatás keretében a Szolgáltató biztosítja a visszavonási információt a tanúsítvány lejáratát követően is, 10 évig, illetve az érintett hitelesítő központ működtetési időtartamában. Egy hitelesítő központ működtetésének megszüntetésekor a Szolgáltató záró CRL-t kell kiadjon, és ezzel egyidejűleg az OCSP válaszadó működését át kell konfigurálja olyan módon, hogy minden OCSP kérés visszautasításra kerüljön.

4.10.2. Szolgáltatás rendelkezésre állása

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

4.10.3. Opcionális funkciók

(188.) Nincs kikötés.

4.11. Az előfizetés vége

(189.) 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

(190.) A Szolgáltató nem nyújt kulcsletét szolgáltatást.

4.12.1. Kulcsletét és visszaállítás szabályai

(191.) Nincs kikötés.

4.12.2. Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

(192.) Nincs kikötés.

5. FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

(193.) Szolgáltatónak gondoskodnia kell arról, hogy kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

5.1. Fizikai óvintézkedések

5.1.1. Telephely elhelyezése és szerkezeti felépítése

(194.) A Szolgáltató a Szolgáltatások nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumában kell elhelyezni és üzemeltetni. A telephely elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat kell alkalmazni, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és Szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2. Fizikai hozzáférés

(195.) Szolgáltatónak védenie kell a Szolgáltatások nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

(196.) Ehhez biztosítania kell 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;
f) 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

(197.) Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert kell biztosítson, 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.

(198.) Szolgáltatónak a gépteremben olyan légkondicionáló berendezést kell alkalmazni, 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

(199.) Szolgáltatónak a géptermet meg kell védenie a beázástól, víz betöréstől és elárasztástól.

5.1.5. Tűzmegelőzés és tűzvédelem

(200.) Szolgáltatónak a géptermet füst- és tűzérzékelőkkel kell felszerelni, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen kell elhelyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket. A gépteremben automatikus tűzoltó rendszert kell kialakítani, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6. Adathordozók tárolása

(201.) Szolgáltatónak meg kell védenie valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól.

5.1.7. Selejt kezelése és megsemmisítése

(202.) Szolgáltatónak a környezetvédelmi előírások betartásával kell gondoskodnia feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközöket és adathordozókat az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel használhatatlanná kell tenni vagy visszaállíthatatlan módon törölni kell.

5.1.8. Fizikailag elkülönítetten őrzött mentési példányok

(203.) Szolgáltatónak azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan külső helyszínen kell tárolnia, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítani kell a helyszínek között a mentett adatok biztonságos továbbítását.

(204.) Szolgáltatónak biztosítania kell, hogy az adatmentést vagy abból a helyreállítást csak rendszerüzemeltető bizalmi munkakört betöltő személy végezze el.

5.2. Eljárásbeli előírások

(205.) Szolgáltatónak gondoskodnia kell arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. Szolgáltató személyzete a feladatokat olyan eljárásbeli előírások alapján kell végezze, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

5.2.1. Bizalmi munkakörök

(206.) Szolgáltatónak egyértelműen azonosítania kell azokat a munkaköröket, amelyektől a Szolgáltatások biztonsága függ. Ezeket a bizalmi munkaköröket és felelősségeket dokumentálni kell. A jogosultságokat és funkciókat olyan módon kell megosztani az egyes bizalmi munkakörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére. Szolgáltatónak biztosítania kell, hogy minden bizalmi munkakör betöltésre kerüljön.

(207.) A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia Szolgáltatóval. Bizalmi munkakörbe a Szolgáltató felső vezetősége kell kinevezze a munkatársakat.

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

(208.) Szolgáltató biztonsági szabályzataiban elő kell írni, hogy csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

a) szolgáltatói kulcspár létrehozása;
b) szolgáltatói magánkulcs mentése és visszaállítása;
c) szolgáltató magánkulcs aktiválása;
d) szolgáltatói magánkulcs megsemmisítése.

5.2.3. Bizalmi munkakörökben elvárt azonosítás és hitelesítés

(209.) A bizalmi munkaköröket betöltő személyeket azonosítani és hitelesíteni kell, mielőtt a Szolgáltatások nyújtásában érintett, kritikus informatikai rendszerekhez hozzáférnének.

(210.) Minden olyan személyt, aki tanúsítvány kibocsátásában közreműködik, multi-faktoros autentikációs mechanizmusokkal kell azonosítani.

5.2.4. Egymást kizáró munkakörök

(211.) A Szolgáltatónak biztosítania kell, 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

(212.) Szolgáltatónak gondoskodnia kell arról, hogy személyzeti előírásai, a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

(213.) Biztosítani kell, hogy bizalmi munkakört csak olyan személyek tölthetnek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét a Szolgáltató erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

5.3.2. Biztonsági háttér ellenőrzés eljárásai

(214.) A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben csak olyan alkalmazottakat foglalkoztathat, 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 bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

5.3.3. Képzési követelmények

(215.) A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztathat, akik az adott munkakör ellátásához szükséges mértékben elsajátították:

a) a PKI elméletet;
b) a kiberbiztonsággal és a személyes adatokkal kapcsolatos szabályokat;
c) Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
d) a szerepkör ellátáshoz szükséges speciális ismereteket;
e) Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;
f) az egyes tevékenységek jogi következményeit;
g) az alkalmazandó biztonsági szabályokat.

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

5.3.4. Továbbképzési gyakoriságok és követelmények

(217.) Szolgáltatónak gondoskodnia kell arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést kell tartania.

(218.) Legalább évente egyszer továbbképzést kell biztosítani az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5. Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

(219.) Szolgáltatónak a dolgozókkal kötendő munkaszerződésben szabályoznia kell a dolgozó felelősségre vonásának lehetőségét a dolgozó által elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7. Szerződéses munkavállalókra vonatkozó követelmények

(220.) Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztathat.

(221.) Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződésben foglalkoztatott személyeket Szolgáltató csak előzetes biztonsági ellenőrzést követően foglalkoztathatja. Az ellenőrzött személyekkel írásos megállapodást kell kötni, melyben rögzíteni kell az esetleges biztonsági szabályokat és a titoktartásra vonatkozó kikötéseket.

5.3.8. A személyzet számára biztosított dokumentációk

(222.) Szolgáltatónak folyamatosan biztosítania kell a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

5.4. A biztonsági naplózás folyamatai

5.4.1. Naplózott esemény típusok

(223.) Szolgáltatónak minden, az informatikai rendszerével és a Szolgáltatások nyújtásával kapcsolatos eseményt naplóznia kell. A naplózott adatállománynak a szolgáltatás nyújtásának teljes folyamatát át kell fognia, és lehetővé tennie, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatásokkal kapcsolatos eseményt rekonstruálni lehessen.

5.4.2. Naplóállomány feldolgozásának gyakorisága

(224.) Szolgáltatónak biztosítania kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

5.4.3. Naplóállomány megőrzési időtartama

(225.) A naplóállományokat archiválni kell és gondoskodni azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig.

5.4.4. Naplóállomány védelme

(226.) A naplóállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személyek férhessenek hozzá.

(227.) A naplóállományok kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisülése, a napló bejegyzések törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása.

5.4.5. Naplóállomány mentési folyamatai

(228.) A naplóállományokról rendszeres mentést kell készíteni.

5.4.6. Naplózás gyűjtési rendszere

(229.) A naplóbejegyzések gyűjtését belső komponenssel kell megoldani. A naplóbejegyzések gyűjtésének meg kell kezdődnie rendszer indításkor és rendszer leállításig folyamatosan működnie kell, és közben biztosítania kell a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

(230.) A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltatónak fel kell függesztenie az érintett területek működését az üzemzavar elhárításáig.

5.4.7. Rendellenes eseményeket kiváltó alanyok értesítése

Nincs kikötés.

5.4.8. Sebezhetőség értékelések

(231.) Szolgáltatónak rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet kell végeznie, 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.

(232.) Szolgáltatónak folyamatosan figyelemmel kell kísérnie az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül meg kell tennie. Bármely olyan sebezhetőség esetén, melynek kihatása lehet a Szolgáltatások nyújtására, Szolgáltatónak vagy cselekvési tervet kell készítenie és végrehajtania annak érdekében, hogy a sebezhetőség ne legyen kihasználható, illetve annak hatása elhanyagolható legyen, vagy dokumentálnia kell annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

5.5. Adatok archiválása

5.5.1. A tárolt adatok típusai

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

(234.) Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

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

5.5.2. Archívum megőrzési időtartama

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

5.5.3. Archívum védelme

(236.) Szolgáltatónak biztosítania kell valamennyi archivált adatra azok sértetlenségét és hitelességét, a rendelkezésre állását és a bizalmasságát.

5.5.4. Archívum mentési eljárásai

(237.) Szolgáltatónak biztosítania kell az iratok, dokumentumok, elektronikus állományok biztonságos, hosszú távú megőrzését, illetve tárolását, továbbá az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

(238.) Valamennyi naplóbejegyzést el kell látni olyan időjellel, melyben legalább egy másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

(239.) Az elektronikus formában archivált adatokon legalább fokozott biztonságú elektronikus aláírást vagy bélyegzőt, valamint minősített időbélyeget kell elhelyezni.

(240.) Az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodni kell az elektronikus aláírások, bélyegzők és időbélyegzők hitelességének fenntartásáról.

5.5.6. Archívum gyűjtési rendszere

(241.) A naplóállományokat és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül kell gyűjteni. A védett informatikai rendszerből történő kimozgatás során az adatokat minősített időbélyeget tartalmazó elektronikus aláírással vagy bélyegzővel kell ellátni.

(242.) A papíralapú iratokat Szolgáltató dokumentumtárában kell tárolni.

5.5.7. Archívum hozzáférés és ellenőrzés eljárásai

(243.) Szolgáltatónak az archivált adatokat meg kell védenie a jogosulatlan hozzáféréstől. A jogosult hozzáféréseket naplózni kell.

5.6. Kulcs átállás

(244.) Szolgáltatónak biztosítania kell, hogy a hitelesítő központok folyamatosan rendelkezzenek a működésükhöz szükséges érvényes kulccsal és tanúsítvánnyal.

(245.) Amennyiben új szolgáltatói kulcspár és tanúsítvány előállítása szükséges, Szolgáltatónak ezt olyan módon kell kiviteleznie, hogy az átállás az Előfizetők és Érintett Felek számára a lehető legkisebb kényelmetlenséget jelentse és megfeleljen a vonatkozó jogszabályi és szabványi követelményeknek.

5.7. Helyreállítás rendkívüli üzemi helyzetek esetén

(246.) Szolgáltató köteles meghozni minden szükséges intézkedést 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 meg kell, hogy előzze.

(247.) A visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás 3 órát meghaladó kiesése esetén Szolgáltatónak haladéktalanul értesítenie kell a Bizalmi Felügyeletet.

(248.) Egyéb incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra -, az esetről való értesüléstől számított 24 órán belül értesíteni kell az Érintett Feleket, valamint jelenteni kell az incidenst a Bizalmi Felügyeletnek.

(249.) A bekövetkezett incidens kiértékelése alapján Szolgáltatónak meg kell hoznia a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1. Rendkívüli események és kompromittálódás kezelésének eljárásai

(250.) Szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel.

(251.) Rendkívüli üzemeltetési helyzetben Szolgáltatónak dokumentálnia kell az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

(252.) Szolgáltatónak ki kell alakítani és fenntartani egy 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.

(253.) A rendkívüli üzemeltetési helyzetben Szolgáltatónak a lehető legrövidebb időn belül tájékoztatást kell közzé tennie internetes honlapján, valamint - lehetőség szerint - elektronikus levélben kell értesítenie azokat a személyeket, akiket az esemény érint.

5.7.2. Sérült számítási erőforrások, szoftverek és/vagy adatok

(254.) Szolgáltatónak olyan megbízható rendszert kell működtetni, mely a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatások működtetését és elérhetőségét.

5.7.3. Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás

(255.) A Szolgáltató magánkulcsának kompromittálódása esetén haladéktalanul meg kell tenni a szükséges lépéseket:

a) visszavonni az összes érintett tanúsítványt;
b) záró CRL-t (4.10.1 fejezet) kibocsátani;
c) megszüntetni az érintett magánkulcs használatát;
d) új szolgáltatói kulcspárokat és tanúsítványokat hozni létre;
e) értesíteni a Bizalmi Felügyeletet;
f) intézkedni valamennyi érintett fél értesítéséről.

5.7.4. Üzletmenet folytonosság helyreállás katasztrófát követően

(256.) Szolgáltatónak rendelkeznie kell tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

5.8. A szolgáltatási tevékenység megszüntetése

(257.) Szolgáltatónak rendelkeznie kell a szolgáltatási tevékenység megszüntetésére vonatkozó, aktualizált tervvel.

(258.) Szolgáltatónak rendelkeznie kell olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket.

(259.) A szolgáltatási tevékenység megszüntetésére vonatkozó tervnek tartalmaznia kell legalább az alábbiakat:

a) Előfizetők és Érintett Felek értesítésének módja;
b) a Szolgáltatásokkal kapcsolatos azon kötelezettségeknek átadása egy másik minősített bizalmi szolgáltatónak, melyek arra vonatkoznak, hogy bizonyítékot szolgáltassanak a Szolgáltató működésével kapcsolatban - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig;
c) szolgáltatói magánkulcsok és azok mentései megsemmisítésének módja;
d) Szolgáltató informatikai rendszerében foglalt adatokról teljes körű mentés készítése.

6. MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK / TECHNICAL SECURITY CONTROLS

6.1. Kulcspár előállítás és telepítés

6.1.1. Kulcspár előállítás

6.1.1.1. Szolgáltatói kulcspárok előállítása

(260.) Szolgáltató maga kell előállítsa a tanúsítványok és visszavonási listák aláírására használandó, valamint az időbélyegző egységek által a kiadott elektronikus időbélyegzők hitelesítésére használandó kulcspárokat fizikailag védett környezetben, kriptográfiai modulban (HSM), legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétének kizárásával. A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek. A tanúsítványok hitelesítésére használt kulcspárok előállítását Szolgáltató dokumentált „kulcs-ceremónia” eljárás szerint kell végezze, melyről a vonatkozó szabvány követelményeinek megfelelő tartalmú jegyzőkönyvet kell felvennie. A szolgáltató magánkulcsai teljes életciklusuk alatt a kriptográfiai modulban kell maradjanak.

6.1.1.2. Előfizetői kulcspárok előállítása

(261.) Amennyiben Előfizető az általa biztosított kulcspárhoz kéri a tanúsítvány kibocsátását, akkor:

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

(262.) Ha a kulcspárt Szolgáltató állítja elő, akkor:

a) [QSCD] Szolgáltatónak a 6.1.5 és 6.1.6 fejezetek szerinti algoritmusú és kulcshosszú kulcspárt szigorúan védett környezetben, a QSCD-n, kizárólag bizalmi munkakört betöltő személyek jelenlétében kell előállítania;
b) [P12] Szolgáltatónak 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 kell előállítania;
c) [P12] a magánkulcsot annak átadásáig Szolgáltatónak megfelelően biztonságos környezetben kell tárolnia a felfedés megakadályozása érdekében;
d) [P12] a magánkulcs dokumentált átadását követően Szolgáltatónak haladéktalanul meg kell semmisíteni a magánkulcs minden tárolt példányát olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

6.1.2. Magánkulcs eljuttatása a tulajdonoshoz

(263.) Amennyiben Előfizető az általa biztosított kulcspárhoz kérte a tanúsítvány kibocsátását, akkor a magánkulcs eljuttatása az Alanynak nem szükséges, mert azzal maga rendelkezik.
(264.) [QSCD] Amennyiben az Alany kulcspárját Szolgáltató állította elő, akkor Szolgáltatónak biztosítania kell, hogy a QSCD-t és az ahhoz tartozó aktivizáló adatokat csak a jogosult Alany vehesse át.
(265.) [P12] Amennyiben az Alany kulcspárját Szolgáltató állította elő, akkor Szolgáltatónak biztosítania kell, hogy a magánkulcsot és az ahhoz tartozó aktivizáló adatokat csak a jogosult Alany vehesse át.

6.1.3. Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

(266.) Amennyiben Előfizető az általa biztosított kulcspárhoz kéri a tanúsítvány kibocsátását, akkor a nyilvános kulcsot PKCS#10 formátumnak megfelelő, a nyilvános kulcshoz tartozó magánkulccsal létrehozott digitális aláírással hitelesített tanúsítványkérelemben kell eljuttatnia Szolgáltatónak. Szolgáltató a tanúsítványkérelmen elhelyezett digitális aláírás ellenőrzésével kell meggyőződnie arról, hogy az Alany a magánkulcsot birtokolja.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

(267.) Szolgáltatónak biztosítania kell, hogy a szolgáltató nyilvános kulcsa a kicserélésen alapuló támadás (substitution attack) ellen védett módon legyen eljuttatva az Érintett Felekhez.

6.1.5. Kulcs méretek

(268.) A Szolgáltatónak a Szolgáltatások nyújtása során - mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében - a Bizalmi Felügyelet vonatkozó határozatának megfelelő szabványos algoritmusokat, paramétereket és kulcshosszokat kell használnia.
(269.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a Szolgáltatások nyújtása során használt aláírási algoritmusokat és paramétereket.

6.1.6. A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

(270.) 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 kell történjen. A szolgáltatói kulcspárok generálása során Szolgáltatónak be kell tartania a HSM modul tanúsítási jelentésében foglalt előírásokat is.
(271.) Az előfizetői kulcspárok tekintetében:

a) ha a hitelesítendő nyilvános kulcs PKCS#10 formátumnak megfelelő tanúsítványkérelemben került Szolgáltató számára eljuttatásra, akkor Szolgáltatónak ellenőrizni kell, hogy a nyilvános kulcs algoritmusa, paraméterei és kulcshossza megfelelnek a Bizalmi Felügyelet vonatkozó határozatába foglalt követelményeknek;
b) [P12] ha az Alany kulcspárját Szolgáltató állítja elő és nem igényeltek hozzá QSCD-t, akkor a kulcspárt védett környezetben, a hitelesítő-központi rendszerében, kizárólag bizalmi munkakört betöltő személyek jelenlétében kell előállítania. Az előfizetői kulcspárok generálása során Szolgáltatónak be kell tartania a Bizalmi Felügyelet vonatkozó határozatában foglalt előírásokat is.
c) [QSCD] Szolgáltató az Alany kulcspárjának generálását védett, biztonságos környezetben és eljárásokkal kell végezze, a QSCD erre szolgáló biztonsági funkciójának meghívásával, melynek során be kell tartani a QSCD tanúsítási jelentésében foglalt előírásokat. Az előfizetői kulcspárok generálása során Szolgáltatónak be kell tartania a Bizalmi Felügyelet vonatkozó határozatában foglalt előírásokat is.

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

(272.) Szolgáltatónak a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz12} ITU-T X.509 v3 szabványnak megfelelően kell jeleznie a kulcs használat célját.

6.2. Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1. Kriptográfiai modul szabványok és műszaki szabályozások

(273.) Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára csak olyan kriptográfiai modult alkalmazhat, amely:

a) olyan megbízható rendszer, amelynek értékelése az MSZ/ISO/IEC 15408 {Sz15} szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg; vagy
b) megfelel az ISO/IEC 19790 {Sz16} követelményeinek; vagy
c) megfelel a FIPS 140-2 {Sz17} 3-as, illetve annál magasabb szintű követelményeknek; vagy
d) megfelel a FIPS 140-3 {Sz18} 3-as, illetve annál magasabb szintű követelményeknek.

(274.) [QSCD] Szolgáltató az előfizetői tanúsítványokhoz kapcsolódó kulcspárok előállítására csak olyan eszközt alkalmazhat, amely rendelkezik a Bizalmi Felügyelet által nyilvántartott tanúsító szervezet, vagy az Európai Unió valamely tagállamában nyilvántartásba vett, tanúsításra jogosult szervezet által kiadott igazolással.

(275.) [ALA+QSCD] A minősített elektronikus aláírást létrehozó eszköznek – összhangban a {J1} eIDAS 30. cikkével - a tanúsításra jogosult szervezet által kiadott tanúsítvánnyal igazoltan meg kell felelnie a {J1} eIDAS II. mellékletben foglalt követelményeknek, vagy olyan biztonságos elektronikus aláírást létrehozó eszköznek kell lennie, melynek megfelelőségét az 1999/93/EK irányelv 3. cikke (4) bekezdésével összhangban állapították meg.

(276.) [BÉLY+QSCD] A minősített elektronikus bélyegzőt létrehozó eszköznek – összhangban a {J1} eIDAS 39. cikkével - a tanúsításra jogosult szervezet által kiadott tanúsítvánnyal igazoltan meg kell felelnie a {J1} eIDAS II. mellékletében foglalt, értelemszerűen alkalmazandó követelményeknek.

(277.) [QSCD] Szolgáltatónak rendszeres időközönként ellenőriznie kell minden általa forgalmazott QSCD tanúsított állapotának meglétét, továbbá a QSCD tanúsítás lejáratát össze kell vetnie azon kiadott tanúsítványok lejáratával, melyek az adott QSCD-n kerültek kibocsátásra. A QSCD tanúsított állapotának megváltozása esetén meg kell tennie a szolgáltatási szabályzatában dokumentált, megfelelő intézkedéseket.

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

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

6.2.3. Magánkulcs letét

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

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

6.2.4. Magánkulcs visszaállítása

(281.) A hitelesítő központok szolgáltatói magánkulcsai biztonsági okokból mentésre kell kerüljenek. A mentést titkosított formában, speciális eszközök alkalmazásával kell megvalósítani. 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.

(282.) Szolgáltató az Aláírók vagy Bélyegző Létrehozók magánkulcsát semmilyen formában nem mentheti, nem tárolhatja.

6.2.5. Magánkulcs mentése

(283.) A hitelesítő központok szolgáltatói magánkulcsai biztonsági okokból mentésre kell kerüljenek. A mentést titkosított formában, speciális eszközök alkalmazásával kell megvalósítani, megfelelő biztonsági óvintézkedések és eljárási szabályok betartásával.

(284.) Szolgáltató az Aláírók vagy Bélyegző Létrehozók magánkulcsát semmilyen formában nem mentheti, nem tárolhatja.

6.2.6. Magánkulcs bejuttatása a kriptográfiai modulba

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

(286.) Amennyiben az Alany kulcspárját Szolgáltató állította elő:

a) [QSCD] Az Aláíró, illetve Bélyegző Létrehozó kulcspárjának előállítása magán a QSCD eszközön (kriptográfiai modulban) történt, így a magánkulcs bejuttatására nincs szükség.

b) [P12] Szolgáltató a magánkulcsot szabványos, titkosított kulcstároló formátumban (PKCS#12) készíti elő az átadásra, és ha ezt Előfizető kriptográfiai modulban kívánja tárolni, akkor a bejuttatásról neki kell gondoskodnia. Előfizető feladata a kriptográfiai modulba bejuttatást követően a magánkulcs minden példányának haladéktalan és visszaállíthatatlan módon történő megsemmisítése.

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

6.2.7. Magánkulcs kriptográfiai modulban tárolásának módja

(288.) A hitelesítő központok magánkulcsainak a tárolása a kulcsok teljes életciklusa alatt a 6.2.1 fejezetben leírt HSM modulban kell történjen.

6.2.8. Magánkulcs aktiválásának módja

(289.) A hitelesítő központok magánkulcsainak aktiválását Szolgáltató a HSM modul gyártói dokumentációjában előírtak szerint kell végezze.

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

6.2.9. Magánkulcs aktív állapotának megszüntetési módja

(291.) Szolgáltatónak biztosítani kell, hogy az aktivált HSM modul jogosulatlan hozzáférés ellen védett legyen. A 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.

6.2.10. Magánkulcs megsemmisítésének módja

(292.) A hitelesítő központok magánkulcsát visszaállíthatatlan módon meg kell semmisíteni, amikor használatuk már nem szükséges vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcsot és az aktiválásához szükséges minden adatot olyan módon kell megsemmisíteni, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

6.2.11. Kriptográfiai modul értékelése

(293.) A 6.2.1 fejezet tartalmazza.

6.3. Kulcspár gondozás egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

(294.) Szolgáltató köteles minden általa kibocsátott tanúsítvánnyal hitelesített nyilvános kulcsot a tanúsítványba foglalva archiválni és az érvényesség lejártától számított tíz évig megőrizni.

6.3.2. Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

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

Gyökértanúsítvány (rootCA)	legfeljebb 25 év
Köztes tanúsítvány (produktív CA)	legfeljebb 20 év
OCSP válaszadó	legfeljebb 30 nap
Előfizetői tanúsítvány	legfeljebb 3 év

(296.) Szolgáltatónak biztosítania kell, hogy az előfizetői tanúsítvány érvényességi időszakának lejárata minden esetben korábbi legyen, mint a hitelesítéséhez használt szolgáltatói tanúsítvány lejáratának időpontja vagy azzal megegyező.

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

(297.) Amennyiben az Alany kulcspárját Szolgáltató állítja elő, a magánkulcs aktiválásához az aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag védett környezetben és biztonságos körülmények között kell előállítania, és hozzárendelnie a szolgáltatott QSCD eszközhöz, illetve a PKCS#12 formátumnak megfelelő kulcstárolóhoz.

6.4.2. Aktivizáló adatok védelme

(298.) Az aktivizáló adatokat azok átadásáig biztonságosan, a QSCD eszköztől, illetve kulcstárolótól elkülönítve kell tárolni. Az aktivizáló adatokat Szolgáltató csak az arra jogosult személynek adhatja át.

(299.) Az átvételt követően az Alanynak (Aláírónak vagy Bélyegző Létrehozónak) kell biztosítania az aktivizáló adatok kizárólagos birtoklását és védelmét.

6.4.3. Aktivizáló adatok egyéb szempontjai

(300.) Nincs kikötés.

6.5. Informatikai biztonsági óvintézkedések

6.5.1. Informatikai biztonsági műszaki követelmények meghatározása

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

(302.) Ennek alapján Szolgáltatónak olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technikákat kell kialakítania és üzemeltetnie, melyek biztosítják a Szolgáltató megbízható működését a Szolgáltatások nyújtásához. Ennek ismertetését Szolgáltató részben a szolgáltatási szabályzatában (BSZ-MTT), részben a belső biztonsági szabályzataiban írja le.

6.5.2. Informatikai biztonsági értékelés

(303.) Szolgáltatónak a Szolgáltatások nyújtásához kialakított és üzemeltetett informatikai rendszerét a {J13} 7/2024 MK rendelet 1. mellékletében felsorolt szempontok szerint biztonsági osztályba kell sorolnia.

(304.) Szolgáltatónak az informatikai rendszerek biztonsági értékelését a {J12} kiberbiztonsági törvény rendelkezései szerint kell elvégeznie.

(305.) Szolgáltatónak a Szolgáltatások nyújtásához kialakított és üzemeltetett informatikai rendszerével kapcsolatban teljesítenie kell a {J11} NIS2 irányelv vonatkozó követelményeit.

6.6. Életciklusra vonatkozó műszaki óvintézkedések

6.6.1. Rendszerfejlesztési óvintézkedések

(306.) Szolgáltatónak gondoskodnia kell 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.

6.6.2. Biztonságkezelési óvintézkedések

(307.) Szolgáltató olyan eszközöket és eljárásokat kell alkalmazzon, 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.

(308.) A biztonságkezelési szabályokat a Szolgáltató belső társasági szintű és rendszer szintű információbiztonsági szabályzata tartalmazza.

6.6.3. Életciklus biztonsági óvintézkedések

(309.) Szolgáltatónak a szolgáltatási szabályzatban meghatározott, rendszeres időközönként el kell végeznie 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.

6.7. Hálózatbiztonsági óvintézkedések

(310.) A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzatában meghatározott követelményeknek megfelelően kell megvalósítani, figyelembe véve az {Sz4} EN 319 411-2 szabvány 6.5.7 fejezetében leírt követelményeket is.

6.8. Időforrások

(311.) A Szolgáltatások nyújtásához használt megbízható rendszereket 24 óránként legalább egyszer, megbízható időforrásokkal (NTP) szinkronizálni kell az UTC időhöz.

7. TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1. Tanúsítvány profil

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

(313.) A kiadott tanúsítványoknak az {Sz8} EN 319-412-5 szabvány 4.2.3 fejezetének megfelelően kell tartalmazniuk a tanúsítvány típusának ([ALA] elektronikus aláírás célú tanúsítvány vagy [BÉLY] elektronikus bélyegzés célú tanúsítvány) megjelölését (a QcStatements / QcType mezőben az id-etsi-qct-esign vagy id-etsi-qct-eseal jelzés alkalmazásával).

(314.) [KET] Szolgáltató a {J9} 322/2024 rendelet szerinti, kiadmányozási célra kiadott tanúsítványt úgy jelöli meg, hogy a tanúsítvány CertificatePolicies kiterjesztése a következő, technikai OID-t tartalmazza: 0.2.216.1.200.1100.100.42.3.7.

7.1.1. Verziószám

(315.) A tanúsítványok verziószáma: V3.

7.1.2. Tanúsítvány kiterjesztések

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

7.1.3. Algoritmus azonosítók

(317.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a tanúsítvány aláírásához használt algoritmusok azonosítóit.

7.1.4. Név formák

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

7.1.5. Név megszorítások

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

7.1.6. Hitelesítési rend objektumazonosító

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

7.1.7. Szabályzati megszorítások kiterjesztés használata

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

7.1.8. Szabályzat minősítők szintaktikája és szemantikája

(322.) 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

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

7.2. CRL profil

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

7.2.1. Verziószám

(325.) A visszavonási listák verziószáma: V2.

7.2.2. CRL és CRL bejegyzés kiterjesztések

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

CRLNumber	a visszavonási lista szigorúan növekvő sorszáma
AuthorityKeyIdentifier	a kibocsátó CA kulcs azonosítója

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

(328.) Mivel a Szolgáltató a lejárt tanúsítványokhoz CRL formájában nem biztosít visszavonási információt, a CRL nem tartalmazhatja az ExpiredCertsOnCRL kiterjesztést.

7.3. OCSP profil

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

7.3.1. Verziószám

(330.) Az OCSP válaszok verziószáma: V1.

7.3.2. OCSP kiterjesztések

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

Nonce	az OCSP kérésben megadott, visszajátszásos támadások megelőzésére szolgáló véletlenszám
ArchiveCutoff	az időpont, ameddig a Szolgáltató a tanúsítvány lejárata után is biztosítja a visszavonási státuszt

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

8. MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

(333.) Jelen bizalmi szolgáltatás rend előírja az összes, a nyilvános körben kibocsátott, minősített, elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokkal kapcsolatos szolgáltatás nyújtása során teljesíteni szükséges követelményt, melyet különösen az alábbi szabványok határoznak meg:

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; Part 1: General requirements {Sz3}
c) EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates {Sz4}
d) EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz5}
e) EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz6}

f) EN 319 412-3: Certificate Profiles; Part 3: Certificate profiles for certificates issued to legal persons {Sz7}
g) EN 319 412-5: Certificate Profiles; Part 5: QcStatements {Sz8}

8.1. Vizsgálatok gyakorisága és körülményei

(334.) Szolgáltatónak megfelelőségi vizsgálatokat és értékeléseket kell elvégeznie, illetve elvégeztetnie annak érdekében, hogy a Szolgáltatásaival kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljen a vonatkozó jogszabályi és szakmai követelményeknek.

(335.) Szolgáltató legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot kell végeztessen a {J1} eIDAS, illetve a {J2} DÁP tv. követelményeinek való megfelelés tárgykörben. Szolgáltató köteles az elkészült megfelelőségértékelés jelentést annak kézhezvételétől számított három munkanapon belül benyújtani a Bizalmi Felügyeletnek.

(336.) A Szolgáltató a Szolgáltatások nyújtásához kialakított és üzemeltetett informatikai rendszerére vonatkozó kiberbiztonsági követelmények teljesítését a Nemzeti Kibervédelmi Intézet (NKI) hatósági ellenőrzése és felügyelete alatt állva biztosítja."

8.2. Auditor azonosítása és képesítése

(337.) A megfelelőségértékelés, az NKI általi ellenőrzés és a kiberbiztonsági audit előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére Szolgáltató külső rendszervizsgálót alkalmazhat.

(338.) A külső rendszervizsgáló által végzett auditokra Szolgáltató olyan szakértőt vagy szakértői szolgáltatásokat nyújtó szervezetet kell megbízzon, 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.

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

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

8.3. Auditor függetlensége

(341.) A megfelelőségértékelő szervezet, annak munkatársai, valamint a külső rendszervizsgáló teljes mértékben független Szolgáltatótól.

8.4. Audit során vizsgált területek

(342.) 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.

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

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

8.5. Hiányosságok esetén végrehajtandó tevékenységek

(344.) 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.

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

8.6. Eredmény kommunikációja

(346.) A belső és külső auditot, szakértői elemzést végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a Szolgáltató bizalmas üzleti információi, ezért azokat a társaság titokvédelmi előírásai szerint kell kezelni, azonban a hiányosságok felszámolásáról a Bizalmi Felügyeletet a következő helyszíni ellenőrzés során tájékoztatni kell. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9. EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1. Díjak

(347.) A Szolgáltatások díjaival kapcsolatos információkat a szolgáltatási szabályzat kell tartalmazza.

(348.) Szolgáltató nem számíthat fel díjat a tanúsítványok visszavonási állapotára vonatkozó státusz információk szolgáltatásáért, valamint a szolgáltatói és a nyilvános tanúsítványtárban közzétett előfizetői tanúsítványoknak az eléréséért.

9.2. Anyagi felelősség

(349.) Szolgáltatónak az anyagi felelősség mértékéről, illetve annak korlátairól a szolgáltatási szabályzatban rendelkeznie kell.

9.2.1. Biztosítási fedezet

(350.) Szolgáltatónak felelősségbiztosítással kell rendelkeznie, mely egyaránt kiterjed az elektronikus aláírással vagy bélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, valamint a Bizalmi Felügyeletnél felmerült jogszabály szerint költségekre, és amely fedezetet biztosít az összes károsultnak okozott kárra, a tanúsítványban jelzett, vagy a {D1} Általános Szerződési Feltételekben rögzített tranzakciós limit értékének legalább ötszöröséig.

(351.) A felelősségbiztosítási szerződésnek meg kell felelnie a {J8} 24/2016 rendelet előírásainak is.

9.2.2. További követelmények

(352.) Szolgáltatónak teljesítenie kell a {J8} 24/2016 rendelet 19. §-a szerinti pénzügyi követelményeket is.

9.2.3. Felelősségbiztosítás vagy garancia végfelhasználók számára

(353.) Nincs kikötés.

9.3. Üzleti információk bizalmassága

9.3.1. Bizalmasan kezelendő információk köre

(354.) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a bizalmasan kezelendő információk körét.

9.3.2. Nem bizalmasnak tekintett információk köre

(355.) Szolgáltatónak a nem bizalmasnak tekintett információk köréről a szolgáltatási szabályzatban rendelkeznie kell

9.3.3. Bizalmas információk védelmének felelőssége

(356.) Szolgáltatónak meg kell védenie a bizalmas információkat. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel kell érvényre juttatni.

9.4. Személyes adatok védelme

9.4.1. Adatvédelmi terv

(357.) 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.

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

9.4.2. Bizalmasként kezelendő személyes adatok

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

(360.) Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

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

9.4.3. Bizalmasként nem kezelendő személyes adatok

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

(362.) 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

(363.) Szolgáltatónak gondoskodnia kell a személyes adatok védelméről, működése és szabályzatai meg kell feleljenek a {J10} GDPR rendelkezéseinek.

9.4.5. Hozzájárulás a személyes adatok felhasználásához

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

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

(366.) 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

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

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

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

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

9.4.7. Egyéb, felfedést eredményező körülmények

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

9.5. Szellemi tulajdonjogok

(372.) 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.

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

(374.) 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

(375.) Szolgáltató felel a jelen bizalmi szolgáltatási rendben és a vonatkozó 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 végzik.

9.6.2. A regisztrációs szervezet felelőssége és helytállása

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

(377.) Szolgáltató felelőssége a tanúsítvány kiadása során:

a) szerződéskötést megelőző tájékoztatás;
b) a tanúsítvány alanyának azonosítása (a természetes személy alany személyazonosságának és/vagy a szervezeti azonosságának hitelesítése);
c) Előfizető Kapcsolattartója személyének azonosítása és eljárási jogosultságának megállapítása;
d) a tanúsítvány alanyának megkülönböztető nevébe kerülő minden adat ellenőrzése közhiteles nyilvántartások alapján, ahol ez lehetséges;
e) a tanúsítvány egyéb mezőibe és kiterjesztéseibe kerülő adatok ellenőrzése;
f) a regisztrációhoz és a tanúsítvány kiállításához szükséges adatok rögzítése az erre szolgáló informatikai rendszerben;
g) a rögzített kérelemben foglalt adatokkal a megfelelő tanúsítvány előállítása;
h) az opcionálisan megrendelt aláírás- vagy bélyegző létrehozó eszköz megfelelő megszemélyesítése;
i) ha a kulcspárt Szolgáltató állította elő, akkor a magánkulcshoz tartozó aktivizáló adatok biztonságos előállítása, tárolása, és átadása az arra jogosult személynek.

9.6.3. Előfizető felelőssége és helytállása

Előfizető jogai

(378.) Előfizető jogosult:

a) a Szolgáltatások igénybevételére a 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.

Előfizető felelőssége

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

Előfizető kötelezettségei

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

Az Alany jogai

(381.) Az Alany (Aláíró vagy Bélyegző Létrehozó) 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 szolgáltatási szabályzatban leírt módon.

Az Alany felelőssége

(382.) Az Alany (Aláíró vagy Bélyegző Létrehozó) 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) az aláírás- vagy bélyegző létrehozó eszköze 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;
h) általában, a jelen szabályzatban előírt kötelezettségei betartásáért.

Az Alany kötelezettségei:

(383.) Az Alany (Aláíró vagy Bélyegző Létrehozó) köteles:

a) a Szolgáltatások használata előtt megismerni a 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 Szolgáltatás igénybe vételéhez szükséges adatokhoz és eszközökhöz (különösen az aláírás- vagy bélyegző létrehozó eszközhöz, aktivizáló adatokhoz) illetéktelen személy ne férhessen hozzá;
f) haladéktalanul kezdeményezni a tanúsítvány felfüggesztését vagy visszavonását, amennyiben a tanúsítványhoz kapcsolódó magánkulcs, az aláírás- vagy bélyegző létrehozó eszköz vagy az aktivizáló adat illetéktelen kezekbe kerültek vagy megsemmisültek, megrongálódtak, elvesztek, valamint haladéktalanul megszüntetni a tanúsítvány és magánkulcs használatát;
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 vagy az annak felhasználásával létrehozott elektronikus aláírással vagy bélyegzővel kapcsolatban jogvita indul.

9.6.4. Érintett felek felelőssége és helytállása

(384.) 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 tanúsítvány ellenőrzésekor.

9.6.5. Egyéb felek felelőssége és helytállása

(385.) Nincs kikötés.

9.7. Helytállás érvénytelenségi köre

(386.) A helytállás érvénytelenségi körét a szolgáltatási szabályzatban meg kell határozni.

9.8. Felelősség korlátozása

(387.) Szolgáltató korlátozhatja a kártérítési felelősségét:

a) a tanúsítvánnyal egy alkalommal vállalható kötelezettség mértékében (tranzakciós limit);
b) összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban fizetendő kártérítési összeg tekintetében.

9.9. Kártérítések

(388.) A kártérítésekről a szolgáltatási szabályzatban kell rendelkezni.

9.10. Hatályosság és megszűnés

9.10.1. Hatályosság

Időbeli hatály

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

Tárgyi hatály

(390.) A bizalmi szolgáltatási rend tárgyi hatálya kiterjed a Szolgáltatások nyújtására és igénybe vételére.

Személyi hatály

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

9.10.2. Megszűnés

(392.) A bizalmi szolgáltatási rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3. Megszűnés után is hatályban maradó rendelkezések

(393.) A megszűnés után is hatályban maradó rendelkezéseket a szolgáltatási szabályzatban meg kell határozni.

9.11. Egyéni hirdetmények és kommunikáció a részvevőkkel

(394.) A szolgáltatási szabályzatban rendelkezni kell a felek és részvevők közötti kommunikáció joghatást kiváltó módjairól.

9.12. Módosítások

9.12.1. Módosítás eljárása

(395.) A bizalmi szolgáltatási rend módosítása az 1.5.3 és 1.5.4 fejezetekben leírt szabályok szerint történik. A bizalmi szolgáltatási rend módosulását a verziószám megfelelő változása jelzi.

9.12.2. Értesítés módszere és időtartama

(396.) A Szolgáltatások jelentős vagy lényeges változása esetén Szolgáltatónak internetes honlapján közleményt kell közzé tennie, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett felek a változásokra felkészülhessenek.

9.12.3. OID megváltozását előidéző körülmények

(397.) A bizalmi szolgáltatási rend OID-ja nem változik.

9.13. Vitás kérdések rendezése

(398.) A vitás kérdések rendezéséről a szolgáltatási szabályzatban kell rendelkezni.

9.14. Irányadó jog

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

9.15. Hatályos jognak megfelelés

(400.) Szolgáltató tevékenységét a mindenkor hatályos Európai Uniós, illetve magyar jogszabályoknak megfelelően köteles végezni.

9.16. Vegyes rendelkezések

Nincs kikötés.

9.16.1. Teljességi záradék

(401.) Nincs kikötés.

9.16.2. Átruházás

(402.) Nincs kikötés.

9.16.3. Részleges érvénytelenség

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

9.16.4. Igényérvényesítés

(404.) 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 bizalmi szolgáltatási rend más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5. Force Majeure (Vis maior)

(405.) A szolgáltatási szabályzat tartalmazza.

9.17. Egyéb rendelkezések

(406.) A Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználói termékeket hozzáférhetővé kell tenni a fogyatékossággal élő személyek számára, amennyiben az lehetséges.