Bizalmi Szolgáltatási Rend
a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz
(BR-ESZIG)

Verziószám:	**2.5**
OID:	**0.2.216.1.200.1100.100.42.3.1.11.**
Hatályba lépés dátuma:	**2026.06.14.**
Dokumentum besorolása:	**NYILVÁNOS**

Jóváhagyó	Adorján István
Adorján István	Digitálisan aláírta: Adorján István Dátum: 2026.05.15 16:28:41 +02'00'

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0	2015.11.27.	Hatóságnak benyújtott változat nyilvántartásba vételhez	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.1	2016.01.07.	Hatóság észrevételei alapján módosított változat	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.2	2016.04.27.	eSZIG tároló elemének BALE tanúsítása miatt módosított változat	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.3	2016.08.01.	On-line tanúsítványigénylés kapcsán tett módosítások	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.4[1]	2016.12.29.	eIDAS megfelelőségértékelésre átdolgozott változat.	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.5[2]	2017.04.28.	Megfelelőségértékelő szervezet észrevételei alapján módosított változat. On-line tanúsítványigényléssel kapcsolatos rendelkezések törlése.	Polysys Kft. Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.6	2017.05.31.	NMHH észrevétele alapján módosított változat	Papp Eszter	Kővári Ferenc	Ferencz Attila
1.7	2018.11.30.	Tanúsítvány érvényességi idő módosítása 2 évről 1 évre	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.8	2019.03.14.	EN szabványok változásainak követése, egyéb frissítések	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.9	2021.03.25.	Tanúsítvány érvényességi idő módosítása a QSCD tanúsítás lejáratával egyezőre	Polysys Kft.	Kővári Ferenc	Adorján István
2.0	2021.05.03	Tanúsítvány Aláíró érdekkörében felmerült okból történő visszavonás következményének rögzítése Tanúsítvány érvényességi időszakával kapcsolatos adatok törlése és átvezetése BSZ-be új QSCD miatt ArchiveCutoff pontosítás	Polysys Kft. Kővári Ferenc	Kővári Ferenc Dr. Kovács Ferenc	Adorján István
2.1.	2023.03.20.	A tanúsítványok alkalmazhatósági szabályainak módosítása	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
2.2.	2024.01.02	Székhelyváltozás átvezetése	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
2.3.[3]	2024.09.01.	• jogszabályi környezet változásából adódó módosítások (E-ügyintézési tv., DÁP tv., eIDAS) • általános felülvizsgálat • tanúsítványkiadás kivezetése	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
2.4.	2024.09.01.	• jogszabályi környezet változásából adódó módosítások (E-ügyintézési tv., DÁP tv., eIDAS)	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István

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

		• általános felülvizsgálat • tanúsítványkiadás kivezetése • OID kiosztási rend módosításának alkalmazása a fedlapon			
2,5	2026.06.14	kapcsolati adatok módosítása	Buczynskiné dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán	Adorján István

NISZ

Tartalom

1. BEVEZETÉS

(1.) Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: mint Kormányzati Hitelesítés Szolgáltató vagy Szolgáltató) Bizalmi Szolgáltatási Rendje, amely a tároló elemmel rendelkező személyazonosító igazolvány (a továbbiakban: eSzemélyi) elektronikus aláírás funkciójához szükséges minősített tanúsítvánnyal kapcsolatos bizalmi szolgáltatására vonatkozik (a továbbiakban: BR-ESZIG).

(2.) A Szolgáltató a fenti tárgykörben az alábbi szolgáltatás-elemeket nyújtja:

a) a 2024. szeptember 1. napját megelőzően kiadott, érvényes tanúsítványokhoz kapcsolódóan visszavonási és tanúsítvány állapot információk.

(3.) Jelen bizalmi szolgáltatási rend a fenti szolgáltatás-elemek (együttesen a továbbiakban Szolgáltatások) keretében kibocsátott minősített tanúsítványok kezelésére (előállítás, kibocsátás, közzététel, megújítás, visszavonás) vonatkozó követelményeket, a tanúsítványok tartalmának és érvényességének ellenőrzési eljárásait és a Szolgáltató működtetésének követelményeit tartalmazza.

(4.) A Szolgáltató a Szolgáltatásait a vele szerződéses viszonyban álló állampolgárok (a továbbiakban: Aláírók) részére nyújtja, de egyes szolgáltatási elemeket hozzáférhetővé tesz az elektronikus aláírások hitelességét ellenőrző Érintett Felek részére is.

1.1. Áttekintés

(5.) A bizalmi szolgáltatási rend egy olyan szabálygyűjtemény, amely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára, valamint rögzíti azokat a követelményeket, melyeket a Szolgáltatónak a Szolgáltatások nyújtása során teljesítenie kell.

(6.) Jelen bizalmi szolgáltatási rend az {Sz7} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában szigorúan követi annak előírásait.

(7.) Jelen bizalmi szolgáltatási rend előírja a természetes személyek számára kibocsátott minősített 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 {Sz1}
b) EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements {Sz2}
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 {Sz3}
d) EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz4}
e) EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz5}
f) EN 319 412-5: Certificate Profiles; Part 5: QCStatements {Sz6}

(8.) Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a NISZ Zrt. "Bizalmi Szolgáltatási Szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz" (BSZ-ESZIG) dokumentum tartalmazza.

(9.) Jelen bizalmi szolgáltatási rendnek megfelelően kibocsátott tanúsítványok az {Sz4} EN 319 412-1 szabvány 3.1 fejezetében meghatározott "EU minősített tanúsítványok", és tartalmazzák jelen dokumentum objektum azonosítóját, mely alapján az érintett felek képesek meghatározni az adott tanúsítvány alkalmazhatóságát és megbízhatóságát. A jelen bizalmi szolgáltatási rend v1.2 verziójával kezdődően kibocsátott tanúsítványok

minősített elektronikus aláírást létrehozó eszköz (korábbi elnevezése: biztonságos aláírás-létrehozó eszköz) használatát megkövetelő, minősített tanúsítványok.

1.2. Dokumentum neve és azonosítása

(10.) Jelen bizalmi szolgáltatási rend teljes neve: NISZ Zrt. "Bizalmi Szolgáltatási Rend a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz".

(11.) A bizalmi szolgáltatási rend rövid neve: BR-ESZIG.

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

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

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

1.2.1. Hitelesítési rendek

(15.) A BR-ESZIG bizalmi szolgáltatási rend megfelel az {Sz3} EN 319 411-2 szabvány 5.5.1 fejezetében definiált `QCP-n-qscd` (OID: 0.4.0.194112.1.2) hitelesítési rendnek.

1.3. PKI közösség

(16.) Jelen bizalmi szolgáltatási rendben szereplő PKI közösség az alábbi felekből áll:

a) Szolgáltató: a jelen bizalmi szolgáltatási rendnek megfelelő tanúsítványokat kibocsátó hitelesítés-szolgáltató, amely a tanúsítványok kibocsátásával és menedzsmentjével kapcsolatos műszaki tevékenységeket végzi;

b) Közreműködő Felek: a Szolgáltatóval szerződéses kapcsolatban álló vagy jogszabályban meghatározott, a Szolgáltatások nyújtásában közreműködő felek;

c) Végfelhasználók: a 2024. szeptember 1. napját megelőzően kiadott, érvényes tanúsítvánnyal rendelkező állampolgárok (Aláírók);

d) Érintett Felek: a tanúsítvány felhasználásával létrehozott elektronikus aláírásokat fogadó harmadik felek;

e) és Egyéb Felek, azon felek, akik e fenti szerepkörök egyikébe sem sorolhatók.

(17.) Azon tevékenységek vonatkozásában, melyeket a Szolgáltató nem maga lát el, Szolgáltató teljes körű felelősséget vállal azért, hogy a Közreműködő Fél tevékenysége során jelen szabályzatban foglalt követelmények teljesülnek.

1.3.1. Hitelesítő szervezet

(18.) A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítő központokból, a szolgáltatás-támogató informatikai rendszerek erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladatai közé tartozik a kibocsátott tanúsítványokra vonatkozóan a visszavonási információk szolgáltatása CRL és OCSP formájában.

(19.) Jelen bizalmi szolgáltatási rend hatálya alatt Szolgáltató, a fenti tvékenységét, kizárólag az állampolgárok részére, az elektronikus személyazonosító igazolványokhoz (a továbbiakban: eSzemélyi) kapcsolódóan kibocsátott tanúsítványok kapcsán végzi.

1.3.1.1. Szabályozási Csoport

(20.) A Szabályozási Csoport a Szolgáltató által létrehozott szervezeti egység, amely a hitelesítés szolgáltatással kapcsolatos bizalmi szolgáltatási rendek, szolgáltatási szabályzatok és egyéb szabályzatok elkészítéséért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős.

1.3.1.2. Telefonos Ügyfélszolgálat

(21.) Szolgáltató Telefonos Ügyfélszolgálatot (Kormányzati Ügyfélvonal - 1818) tart fenn, melynek révén heti hét napban, napi 24 órában biztosítja Aláírók számára a tanúsítvány telefonos visszavonásának kezelését, továbbá ellátja a Szolgáltatásokkal kapcsolatos ügyfélszolgálatot.

1.3.2. Regisztrációs Szervezet és Kártyakibocsátó Szervezet

1.3.2.1. Regisztrációs Szervezet

(22.) Regisztrációs Szervezet: a {J4} SzigR. 11. § (1) bekezdésben megjelölt *eljáró hatóság*, amely az általa működtetett helyszínekből, valamint az ott dolgozó személyzetből áll. A Regisztrációs Szervezet a Kártyakibocsátó Szervezet által erre a célra kifejlesztett és üzemeltetett informatikai rendszereket és eszközöket használja.

(23.) A Regisztrációs Szervezet a Szolgáltatások nyújtásában Közreműködő Fél, feladata a visszavonására irányuló igénylésekkel kapcsolatos adminisztratív és operatív tevékenységek ellátása.

1.3.2.1.1. Regisztrációs Irodák

(24.) A Regisztrációs Szervezet Regisztrációs Irodákat tart fenn minden olyan helyen, ahol az állampolgár állandó személyazonosító igazolványt igényelhet, azaz az okmányirodákban és kormányablakokban.

(25.) A Regisztrációs Szervezet felelősségét és kötelezettségeit a 9.6.2.1 fejezet írja le.

1.3.2.2. Kártyakibocsátó Szervezet

(26.) Kártyakibocsátó Szervezet: a Szolgáltatóval szerződéses kapcsolatban álló, {J4} SzigR. 2. § szerinti *nyilvántartást kezelő szerv*, az állandó személyazonosító igazolvány (eSzemélyi) kibocsátója, és az általa működtetett helyszínek és informatikai rendszerek hardver és szoftver összetevőiből, az ezeket körül vevő biztonságos fizikai környezetből, valamint az üzemeltetést ellátó személyzetből áll.

(27.) A Kártyakibocsátó Szervezet felelősségét és kötelezettségeit a 9.6.2.2 fejezet írja le.

1.3.3. Előfizetők

(28.) Előfizető: az Aláíró, aki a tároló elemmel rendelkező személyazonosító igazolványa elektronikus aláírás funkcióját használni kívánja és 2024. szeptember 1. napját megelőzően Szolgáltatási Szerződést kötött a Szolgáltatóval a Szolgáltatások igénybevételére. Aláíró csak a saját nevére szóló tanúsítványt igényelhetett, így jelen dokumentum fogalomrendszerében az Előfizető és az Aláíró személye azonos.

(29.) Aláíró kizárólagosan birtokolja az eSzemélyi-t és így az annak tároló elemén levő aláírói kulcspárokat.

(30.) Az Aláíró felelősségét és kötelezettségeit a 9.6.3 fejezet írja le.

1.3.4. Érintett Felek

(31.) Érintett Fél: a tanúsítványon alapuló elektronikus aláírással ellátott elektronikus dokumentumot fogadó természetes vagy jogi személy, aki/amely az elektronikus aláírásra hagyatkozva jár el a dokumentum hitelességének ellenőrzésekor. Az Érintett Fél nem áll szerződéses viszonyban a Szolgáltatóval.

(32.) Az Érintett Félnek az elektronikus aláírás ellenőrzéséhez, a tanúsítvány érvényességének megállapításához minden esetben javasolt igénybe vennie a Szolgáltató visszavonási információt szolgáltató Szolgáltatásait (CRL vagy OCSP).

(33.) Az Érintett Felek felelősségét a 9.6.4 fejezet írja le.

1.3.5. Felügyeleti Szerv

(34.) A jogszabályokban megjelölt Felügyeleti Szerv biztosítja a Szolgáltató felügyeletét, ellenőrzi a Szolgáltatások jogszabályi megfelelőségét, ellátja az ezzel kapcsolatos felügyeleti feladatokat. Többek között, figyelemmel kíséri az elektronikus aláírásokkal kapcsolatos technológiai és kriptográfiai algoritmusok fejlődését és határozatba foglalja Szolgáltató szolgáltatásainak nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket; határozatában elrendelheti Szolgáltató számára az aláírói tanúsítvány(ok) visszavonását.

1.4. A tanúsítvány alkalmazhatósága

(35.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványokra vonatkozó alkalmazhatósági megkötéseket lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, melyek Szolgáltató weboldalán közzétett archív szabályzatok között találhatók meg.

1.4.1. Teszt tanúsítványok

(36.) A Szolgáltató jelen BR-ESZIG hatálya alatt nem bocsájt ki teszt tanúsítványokat.

1.4.2. Engedélyezett tanúsítvány használat

(37.) Jelen BR-ESZIG keretében nem értelmezett.

1.4.3. Tiltott tanúsítvány használat

(38.) Jelen BR-ESZIG keretében nem értelmezett.

1.5. Szabályzat adminisztráció

1.5.1. Szabályzatot karbantartó szerv

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

1.5.2. Kapcsolat

(40.) A Regisztrációs Irodák elérhetőségét, nyitvatartását, a Szolgáltatóval való kapcsolattartás módját a szolgáltatási szabályzat tartalmazza.

(41.) A Szolgáltató hatályos adatai (cégjegyzékszám, székhely, levelezési cím stb.), az illetékes fogyasztóvédelmi felügyelőség, valamint az illetékes békéltető testület elérhetősége a hiteles.gov.hu/kapcsolat menüpont alatt elérhető.

1.5.3. BR/BSZ alkalmasságának meghatározása

(42.) 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.

(43.) A változtatási igényeket a Szabályozási Csoport gyűjti, a módosításokat legalább évente egyszer elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

1.5.4. BR/BSZ jóváhagyásának eljárása

(44.) 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).

1.6. Fogalmak, rövidítések és hivatkozások

1.6.1. Fogalmak

a) **Alany**: A Szolgáltató által kiadott tanúsítványban azonosított entitás, aki/amely a tanúsítványban szereplő nyilvános kulcsnak (elektronikus aláírást érvényesítő adat) megfelelő magánkulcsot (elektronikus aláírás létrehozásához használt adat) birtokolja.

b) **Aláíró**: elektronikus aláírást létrehozó természetes személy

c) **Aláírást érvényesítő adat** vagy **Elektronikus aláírást érvényesítő adat**: olyan egyedi adat, amelyet az elektronikus aláírt dokumentumot megismerő személy (vagy eszköz) az elektronikus aláírás ellenőrzésére használ. Jellemzően kriptográfiai nyilvános kulcs, korábbi elnevezése: aláírás-ellenőrző adat.

d) **Aláírás létrehozásához használt adat** vagy **Elektronikus aláírás létrehozásához használt adat**: olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ. Jellemzően kriptográfiai magánkulcs, korábbi elnevezése: aláírás-létrehozó adat.

e) **Aláírást létrehozó eszköz** vagy **Elektronikus aláírást létrehozó eszköz**: elektronikus aláírás létrehozásához használt, konfigurált hardver- vagy szoftvereszköz. Korábbi elnevezése: aláírás-létrehozó eszköz.

f) **Bizalmi felügyelet**: lásd „Felügyeleti Szerv”

g) **Bizalmi Lista**: a tagállam által összeállított, fenntartott és közzétett elektronikus lista, amelyben kötelezően szerepelnek a tagállam felelőssége alá tartozó minősített bizalmi szolgáltatókra (opcionálisan a nem minősített bizalmi szolgáltatók is) valamint e szolgáltatók által nyújtott bizalmi szolgáltatásokra vonatkozó információk. A Bizalmi Lista automatizált feldolgozásra alkalmas, hitelességét elektronikus aláírás vagy elektronikus bélyegző biztosítja.

h) **Bizalmi szolgáltatás**: rendszerint díjazás ellenében nyújtott, az alábbiakból álló szolgáltatások:

- elektronikus aláírások, elektronikus bélyegzők, vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése vagy érvényesítése; vagy
- weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy

- elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése

i) **Bizalmi szolgáltató**: egy vagy több bizalmi szolgáltatást nyújtó természetes vagy jogi személy; a bizalmi szolgáltató lehet minősített vagy nem minősített bizalmi szolgáltató

j) **Bizalmi szolgáltatási rend**: olyan szabálygyűjtemény, amelyben egy bizalmi szolgáltató igénybe vevő vagy más személy valamely bizalmi szolgáltatás használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára

k) **Biztonsági tisztviselő**: a bizalmi szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért felelős személy

l) **Biztonságos környezet**: olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól

m) **Elektronikus aláírás**: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ

n) **Elektronikus aláírást érvényesítő adat**: lásd „Aláírást érvényesítő adat”

o) **Elektronikus aláírás létrehozásához használt adat**: lásd „Aláírás létrehozásához használt adat”

p) **Elektronikus aláírás célú tanúsítvány**: olyan elektronikus igazolás, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja és igazolja legalább az érintett személy nevét vagy álnevét

q) **Elektronikus aláírás célú minősített tanúsítvány**: olyan elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a {J1} eIDAS I. mellékletében megállapított követelményeknek

r) **Elektronikus aláírás ellenőrzése**: az elektronikusan aláírt elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a bizalmi szolgáltató által közzétett elektronikus aláírást érvényesítő adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával

s) **Elektronikus aláírás felhasználása**: elektronikus adat elektronikus aláírással történő ellátása, illetve az elektronikus aláírás ellenőrzése

t) **Elektronikus aláírási termék**: olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevő, amely elektronikus aláírással kapcsolatos bizalmi szolgáltatások nyújtásához, így különösen elektronikus aláírások, elektronikus bélyegzők, illetőleg elektronikus időbélyegző létrehozásához vagy érvényesítéséhez használható

u) **Elektronikus azonosítás**: a természetes vagy jogi személyt, illetve jogi személyt képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata

v) **Elektronikus azonosító eszköz**: olyan hardver- és/vagy szoftvereszköz, amely a személyazonosító adatokat tartalmazza, és amelyet online szolgáltatások céljából történő azonosításra használnak

w) **Elektronikus bélyegző**: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét. Korábbi elnevezése: szervezeti elektronikus aláírás.

x) **Elektronikus bélyegzés célú tanúsítvány**: olyan elektronikus tanúsítvány, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét. Korábbi elnevezése: szervezeti tanúsítvány.

y) **Elektronikus bélyegzés célú minősített tanúsítvány**: olyan elektronikus bélyegzés célú tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a {J1} eIDAS III. mellékletében megállapított követelményeknek

z) **Elektronikus bélyegző létrehozásához használt adatok**: olyan egyedi adatok, melyeket az elektronikus bélyegző létrehozója elektronikus bélyegző létrehozásához használ (jellemzően kriptográfiai magánkulcs).

aa) **Elektronikus bélyegzőt létrehozó eszköz**: elektronikus bélyegző létrehozására használt, konfigurált hardver- vagy szoftvereszköz

bb) **Elektronikus dokumentum**: elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom

cc) **Elektronikus időbélyegző** vagy **időbélyegző**: olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban

dd) **Előfizető (Aláíró)**: a természetes személy, aki a Szolgáltatóval érvényes, 2024. szeptember 01. napját megelőzően megkötött Szolgáltatási Szerződéssel rendelkezik a Szolgáltatások igénybevételére.

ee) **Email cím**: az Aláíró a Szolgáltatási Szerződés megkötésekor kötelezően meg kellett, hogy adjon egy email címet. Ez elsődlegesen a Szolgáltató általi kapcsolattartásra szolgál („értesítési email cím"); emellett ez a cím befoglalásra került a tanúsítványba is, ha ezt Aláíró kérte. Ha a későbbiekben Aláíró email címe megváltozik (azaz lesz egy új email címe is), és az új címre szeretné megkapni a Szolgáltató értesítéseit, de ezzel együtt a tanúsítványba foglalt email címe nem változott meg (azaz nem szűnt meg, azt továbbra is használja), akkor a két email cím eltérhet egymástól.

ff) **Entitás:** a nyilvános kulcsú infrastruktúra (PKI) eleme, pl. egy tanúsítványkiadó, regisztrációs szervezet, végfelhasználó vagy eszköz

gg) **eSzemélyi**: A {J3} Nytv. 29. § (1) bekezdésében meghatározott, tároló elemmel ellátott, állandó személyazonosító igazolvány (elektronikuskártya), amely alkalmas az ügyfél elektronikus úton történő közhiteles azonosítására, a polgár kérelmére elektronikus aláírás létrehozására, valamint a polgár a törvényben megjelölt esetekben gyakorolhatja vele a külföldre utazás jogát. A polgár kérelmére tároló eleme tartalmazza az elektronikus aláírás létrehozásához használt adatot és az ahhoz tartozó elektronikus aláírást érvényesítő adatot hitelesítő, elektronikus aláírás célú tanúsítványt.

hh) **EU minősített tanúsítvány**: a {J1} eIDAS rendelet közül azzal összhangban kibocsátott minősített tanúsítvány, amely hatályos a tanúsítvány kibocsátásának időpontjában

ii) **Érintett fél**: az a természetes személy vagy jogi személy, aki/amely az elektronikusan aláírt, és/vagy elektronikusan időbélyegzett dokumentum fogadója, és az adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az elektronikus aláírás és/vagy az elektronikus időbélyegző hitelességének ellenőrzésekor

jj) **Érvényesítés**: olyan folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus aláírás vagy elektronikus bélyegző érvényes

kk) **Érvényesítési adatok:** elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt adatok (jellemzően kriptográfiai nyilvános kulcs)

ll) **Érvényességi lánc**: az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk sorozata (így különösen azon tanúsítványok, tanúsítványokkal kapcsolatos információk, érvényesítési adatok, a tanúsítvány állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényesítési adatára és annak visszavonási állapotára vonatkozó információk), melyek alapján megállapítható, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás, elektronikus bélyegző vagy elektronikus időbélyegző, valamint az azokhoz kapcsolódó tanúsítványok az elektronikus aláírás, elektronikus bélyegző vagy elektronikus időbélyegző elhelyezésének időpontjában érvényes volt

mm) **Felhasználó (végfelhasználó)**: olyan entitás, aki/amely a Szolgáltatások keretében előállított kulcsokat és tanúsítványokat és/vagy időbélyegeket rendeltetésüknek megfelelően használja

nn) **Felügyeleti Szerv vagy Hatóság**: az adott tagállamban kijelölt felügyeleti szerv (Magyarországon a Nemzeti Média- és Hírközlési Hatóság), amely a bizalmi szolgáltatók felügyeletét végzi, melynek keretében előzetes és utólagos felügyeleti tevékenységek révén ellenőrzi, hogy a szolgáltatók és az általuk nyújtott szolgáltatások eleget tesznek a jogszabályban megállapított követelményeknek

oo) **Fokozott biztonságú elektronikus aláírás**: olyan elektronikus aláírás, amely megfelel a {J1} eIDAS 26. cikkben meghatározott követelményeknek, azaz:

- kizárólag az aláíróhoz köthető;
- alkalmas az aláíró azonosítására;
- olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozták létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
- olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok későbbi változása kimutatható.

pp) **Fokozott biztonságú elektronikus bélyegző**: olyan elektronikus bélyegző, amely megfelel a {J1} eIDAS 36. cikkben meghatározott követelményeknek, azaz:

- kizárólag a bélyegző létrehozójához kötött;
- alkalmas a bélyegző létrehozójának azonosítására;
- olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozták létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;
- olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása kimutatható.

qq) **Gyökér hitelesítő központ (ROOT CA, vagy Főtanúsítvány kiadó)**: az elsőnek létrehozott, fizikailag is működő hitelesítő központ, amely az alá rendelt másodlagos (produktív) hitelesítő központokat hitelesíti

rr) **Hitelesítés**: olyan elektronikus folyamat, amely lehetővé teszi a természetes vagy jogi személy elektronikus azonosításának vagy az elektronikus adatok eredetének és sértetlenségének az igazolását

ss) **Hitelesítési rend (Certificate Policy - CP)**: olyan bizalmi szolgáltatási rend, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik

tt) **Hitelesítő központ (CA)**: a Szolgáltató azon egysége, amely a hitelesítés-szolgáltatás magánkulccsal folytatott tevékenységét végzi. Egy hitelesítő központhoz mindig egy magánkulcs tartozik. A hitelesítő központ fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.

uu) **Időbélyegzés**: az a folyamat, melynek során az elektronikus dokumentumhoz elektronikus időbélyegző hozzárendelése történik

vv) **Igénybe vevő fél**: olyan természetes vagy jogi személy, aki vagy amely elektronikus azonosítási vagy bizalmi szolgáltatást vesz igénybe

ww) **Informatikai rendszer**: a Szolgáltató által a bizalmi szolgáltatásokhoz, illetve annak elemeihez, így különösen a szolgáltatói kulcspár kezeléséhez, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezeléséhez, az időbélyegzés szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt, a {J1} eIDAS 24. cikk (2) bekezdés e) és f) pontja szerinti megbízható rendszerek és termékek.

xx) **Kompromittálódás**: az az eset, amikor a magánkulcs (elektronikus aláírás létrehozásához használt adat vagy elektronikus bélyegző létrehozásához használt adat) használatára arra nem jogosított személy képessé válik vagy azokat megismeri

yy) **Kriptográfiai kulcs**: olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a kriptográfiai transzformáció elvégzéséhez, különösen az elektronikus aláírás vagy bélyegző előállításához vagy ellenőrzéséhez szükséges

zz) **Kriptográfiai modul (Hardware Security Module - HSM)**: olyan hardver alapú biztonságos eszköz, amely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására

aaa) **Lenyomat**: olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:

- a képzett lenyomat egyértelműen származtatható az elektronikus dokumentumból;
- a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés;
- a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, melyre alkalmazva a lenyomatképző eljárást, annak eredményeképp az adott lenyomat keletkezik.

bbb) **Magánkulcs aktiválása**: az a folyamat, melynek során a jogosult - különféle azonosító elemek (pl. jelszó, PIN kód megadásával - engedélyezi, hogy az elektronikus aláírást létrehozó eszközön tárolt magánkulcs megkezdje üzemszerű működését. Az aktiválás általában a tanúsítványt igénylő környezetben (dokumentum kezelő, levelező rendszer) történik, és érvényes lehet a visszavonásig (deaktiválásig), illetve egyszeri használatra.

ccc) **Magánkulcs deaktiválása**: az a folyamat, melynek során az elektronikus aláírást létrehozó eszközön tárolt magánkulcs üzemszerű működésre megszüntetésre kerül

ddd) **Megfelelőségértékelő szervezet**: a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére

eee) **Minősített bizalmi szolgáltatás**: olyan bizalmi szolgáltatás, amely megfelel a {J1} eIDAS rendeletben foglalt alkalmazandó követelményeknek, azaz a Bizalmi Listán szerepel.

fff) **Minősített bizalmi szolgáltató**: olyan bizalmi szolgáltató, amely egy vagy több bizalmi szolgáltatást nyújt és amelynek minősített státuszát a Felügyeleti Szerv jóváhagyta, azaz a Bizalmi Listán szerepel.

ggg) **Minősített elektronikus aláírás**: olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás célú minősített tanúsítványon alapul

hhh) **Minősített elektronikus aláírást létrehozó eszköz**: olyan elektronikus aláírást létrehozó eszköz, amely megfelel a {J1} eIDAS II. mellékletben megállapított követelményeknek, rövidítése: QSCD (Qualified Signature Creation Device). Korábbi elnevezése: biztonságos aláírás-létrehozó eszköz (BALE).

iii) **Minősített elektronikus bélyegző**: olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegzés célú minősített tanúsítványon alapul

jjj) **Minősített elektronikus bélyegzőt létrehozó eszköz**: olyan elektronikus bélyegzőt létrehozó eszköz, amely értelemszerűen megfelel a {J1} eIDAS II. mellékletben megállapított követelményeknek

kkk) **Nyilvános (publikus) kulcsú infrastruktúra (PKI):** az elektronikus aláírás vagy elektronikus bélyegző, valamint titkosítás létrehozására, érvényesítésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző bizalmi szolgáltatókat és eszközöket is

lll) **Produktív hitelesítő központ**: a gyökér hitelesítő központ által létrehozott logikailag vagy fizikailag létező hitelesítő központ, amely egy adott alkalmazási, szervezeti, földrajzi, stb. területre ad ki tanúsítványokat

mmm) **PIN kód:** az eSzemélyi tároló eleméhez rendelt, az elektronikus aláírás funkció használatához szükséges, az aláíró hozzáférési jogosultságát ellenőrző adat. Jelen szabályzat a PIN kód alatt minden esetben az elektronikus aláíráshoz tartozó PIN kódot (nem az állandó személyazonosító igazolványhoz tartozó PIN kódot) érti. Ha az állampolgár az eSzemélyi igénylésekor tanúsítványt is igényel, akkor személyesen vette át a PIN kódot (és a visszavonási jelszót) tartalmazó borítékot. A borítékban átvett PIN kód úgynevezett aktiváló (transzport) PIN kód, amely szükséges az elektronikus aláíráshoz tartozó PIN kód létrehozásához.

nnn) **PUK kód:** az eSzemélyi tároló eleméhez rendelt, a személyazonosító igazolványhoz tartozó PIN kód és az elektronikus aláíráshoz tartozó PIN sikertelen megadása után használható feloldó adat. A PUK kódot is tartalmazó borítékot az állampolgár személyesen vette át az eSzemélyi igénylésekor.

ooo) **Regisztrációs szervezet**: a Szolgáltató és a vele szerződéses alapon vagy jogszabályban meghatározott együttműködő társaságok azon szervezeti egységei, amelyek az állampolgárok adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a hitelesítő szervezethez történő továbbítását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el

ppp) **Regisztrációs adatok**: azon információk, adatok összessége, amelyeket a Szolgáltató a tanúsítványkiadás érdekében az Aláíróról begyűjt

qqq) **Rendkívüli üzemeltetési helyzet**: olyan, a Szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amikor a Szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincs lehetőség, beleértve a szolgáltatói magánkulcsok kompromittálódását is, vagy annak közvetlen veszélyét.

rrr) **Rendszeradminisztrátor**: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy

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

ttt) **Rendszervizsgáló**: a bizalmi szolgáltató naplózott, illetve archivált adatállományait vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglevő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy

uuu) **Személyazonosító adat**: egy természetes vagy jogi személy vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő adat

vvv) **Szolgáltatói kulcspár**: a szolgáltatói magánkulcsból és a szolgáltatói nyilvános kulcsból álló, kriptográfiai kulcspár

www) **Szolgáltatói magánkulcs**: olyan kriptográfiai magánkulcs, melyet a szolgáltató a saját bizalmi szolgáltatásának igazolására, így különösen a tanúsítványok kibocsátására, visszavonási nyilvántartásokra, az időbélyegzésre, az archiváláshoz használ

xxx) **Szolgáltatói nyilvános kulcs**: olyan kriptográfiai nyilvános kulcs, melyet a szolgáltató magánkulcsának használatával létrehozott elektronikus aláírás, elektronikus bélyegző vagy elektronikus időbélyegző érvényesítésére használnak

yyy) **Szolgáltatási szabályzat (Certificate Practice Statement - CPS)**: a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről

zzz) **Tanúsítvány**: elektronikus aláírás célú tanúsítvány rövidített megnevezése

aaaa) **Tanúsítvány visszavonási lista (Certificate Revocation List - CRL)**: valamely okból visszavont vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a bizalmi szolgáltató bocsát ki és hitelesít

bbbb) **Tanúsítványokkal kapcsolatos szabályzatok**: a bizalmi szolgáltatási rend, a szolgáltatási szabályzat, a szolgáltatási kivonat, valamint az általános szerződéses feltételek

cccc) **Visszavonási jelszó**: az elektronikus aláíró tanúsítvány ügyfél kérelmére történő visszavonásához szükséges kód. Az állampolgár a visszavonási jelszót az eSzemélyi igénylésekor személyesen, lezárt borítékban vette át.

1.6.2. Rövidítések

Rövidítés	Angol megfelelő	Megnevezés
CA	Certification Authority	hitelesítő szervezet
CRL	Certification Revocation List	tanúsítvány visszavonási lista
CP	Certificate Policy	hitelesítési rend
CPS	Certificate Practice Statement	hitelesítési szolgáltatási szabályzat
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
NEK	-	Nemzeti Egységes Kártyarendszer
NTP	Network Time Protocol	időforrás protokoll
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
QSCD	Qualified Signature Creation Device	minősített elektronikus aláírást létrehozó eszköz
RA	Registration Authority	regisztrációs szervezet
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 (a továbbiakban: 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 (Nytv.)

{J4} 414/2015. (XII.23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól (SzigR.)

{J5} 2014. évi LXXXIII. törvény az elektronikuskártya-kibocsátási keretrendszerről (Nektv.)

{J6} 53/2015. (IX.24.) BM rendelet az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény végrehajtásához szükséges kapcsolódási, műszaki, technológiai, biztonsági előírásokról, követelményekről és a hitelesítési rendről (NekR.)

{J7} 2016. évi CXXX. törvény a polgári perrendtartásról

{J8} 2013. évi V. törvény a Polgári Törvénykönyvről

{J9}	24/2016. (VI.30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
{J10}	679/2016/EU Európai Parlament és Tanács rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: GDPR)

1.6.3.2. Szabványok és műszaki-technikai hivatkozások

{Sz1}	EN 319 401	General policy requirements for Trust Service Providers
{Sz2}	EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates
{Sz3}	EN 319 411-2	Policy and security requirements for Trust Service Providers issuing EU qualified certificates
{Sz4}	EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures
{Sz5}	EN 319 412-2	Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons
{Sz6}	EN 319 412-5	Certificate Profiles; Part 5: QCStatements
{Sz7}	RFC 3647	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz8}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz9}	ITU-T X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz10}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz11}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz12}	RFC 6960	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP
{Sz13}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz14}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz15}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules

1.6.3.3. Hivatkozott dokumentumok

{D1}	ÁSZF-GOVCA	Általános Szerződési Feltételek a NISZ Zrt. kormányzati hitelesítés szolgáltatásaihoz
{D2}	-	Szolgáltatási Szerződés
{D3}	-	NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}	-	NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai

{D5}	-	NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}	-	NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}	-	NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}	-	Tanúsítvány profilok a NISZ eIDAS Rendelet szerinti bizalmi szolgáltatásaihoz

2. KÖZZÉTÉTEL ÉS ADATTÁRAK

2.1. Tanúsítványtár

(45.) 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 Aláírók 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. Szolgáltatói információ közzététele

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

(47.) A Szolgáltató a végfelhasználói tanúsítványokat belső tanúsítványtárában tárolja, a kiadott tanúsítványt az Aláíró számára rendelkezésre bocsátja. A szolgáltató a végfelhasználói tanúsítványt internetes honlapján nyilvánosan elérhető, kereshető tanúsítványtárában csak akkor tette közzé, ha Aláíró a tanúsítvány közzétételéhez hozzájárult.

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

2.3. A közzététel gyakorisága

(49.) Szolgáltató a szolgáltatói tanúsítványokat azok kibocsátását követő 24 órán belül teszi közzé.

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

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

(52.) 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 egy órán belül új CRL-t állít elő és tesz közzé.

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

2.4. Hozzáférés-ellenőrzések

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

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

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

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

3. AZONOSÍTÁS ÉS HITELESÍTÉS

3.1. Elnevezések

(58.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványokban szereplő *elnevezések* értelmezését lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

3.1.1. Nevek típusa

(59.) Jelen BR-SZIG keretében nem értelmezett.

3.1.2. Nevek jelentése

(60.) Jelen BR-SZIG keretében nem értelmezett.

3.1.3. Előfizetők névtelensége és álnév használata

(61.) Jelen BR-SZIG keretében nem értelmezett.

3.1.4. Különféle név formák megjelenítési szabályai

(62.) Jelen BR-SZIG keretében nem értelmezett.

3.1.5. A nevek egyedisége

(63.) Jelen BR-SZIG keretében nem értelmezett.

3.1.6. Márkanevek elismerése, hitelesítése és szerepe

(64.) Jelen BR-SZIG keretében nem értelmezett.

3.2. Kezdeti azonosítás

(65.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást, így a hozá kapcsolódó kezdeti azonosítást sem. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok esetén alkalmazott kezdeti azonostási eljárást lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, melyek Szolgáltató weboldalán közzétett archív szabályzatok között találhatók meg.

3.2.1. A magánkulcs birtoklása

(66.) Jelen BR-SZIG keretében nem értelmezett.

3.2.2. A szervezeti azonosság hitelesítése

(67.) Jelen BR-SZIG keretében nem értelmezett.

3.2.3. A személyazonosság hitelesítése

(68.) Jelen BR-SZIG keretében nem értelmezett.

3.2.4. Előfizető nem ellenőrzött adatai

(69.) Jelen BR-SZIG keretében nem értelmezett.

3.2.5. Jogosultság ellenőrzése

(70.) Jelen BR-SZIG keretében nem értelmezett.

3.2.6. Együttműködési kritériumok

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

3.3. Azonosítás és hitelesítés kulcscsere esetén

(72.) A Szolgáltató nem nyújt kulcscsere szolgáltatást.

3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

(73.) Nincs kikötés.

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

(74.) Nincs kikötés.

3.4. Azonosítás és hitelesítés visszavonási kérelem esetén

(75.) A tanúsítvány visszavonási kérelmet fogadó fél a kérelmező azonosítását és hitelesítését az alábbiak szerint végzi:

a) Aláíró kérelmező esetében: a Regisztrációs Szervezet személyes jelenléte útján az okmányigénylési eljárásrendnek megfelelően vagy a Kormányzati Ügyfélvonal (1818) a visszavonási jelszónak a telefon nyomógombjaival történő megadásával azonosítja és hitelesíti Aláírót;

b) okmányérvénytelenítést, illetve át nem vett okmányt jelző hatóság esetében: a Szolgáltató PKI, tanúsítvány alapú X.509 azonosítással, valamint a visszavonási kérelmen elhelyezett elektronikus bélyegző ellenőrzésével hitelesíti a kezdeményezőt.

4. A TANÚSÍTVÁNYOK ÉLETCIKLUSA

(76.) A tanúsítványok életciklusának folyamataiban Szolgáltatón kívül a Regisztrációs Szervezet és a Kártyakibocsátó Szervezet működik közre. Szolgáltató teljeskörűen felelős a közreműködők tevékenységéért, valamint azért, hogy jelen szabályzatban leírt követelmények teljesülnek.

(77.) A Szolgáltató felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okozott, azon kötelezettségei megszegéséből eredően, mely kötelezettségek az esemény időpontjában hatályos, vonatkozó jogszabályban meghatározottak.

(78.) A Szolgáltató nem felelős olyan kárért, melyre bizonyítja, hogy az szándékos vagy gondatlan közrehatása nélkül következett be.

(79.) Szolgáltató nem felelős a tanúsítvány felhasználására vonatkozó korlátozások be nem tartásából származó károkért.

4.1. Tanúsítványigénylés

(80.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást, így a hozá kapcsolódó tanúsítványigénylés sem értelmezett. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok esetén alkalmazott tanúsítványigénylési eljárást lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

4.1.1. Ki nyújthat be tanúsítványigénylést

(81.) Jelen BR-ESZIG keretében nem értelmezett.

4.1.2. Igénylési folyamat és felelősségek

(82.) Jelen BR-ESZIG keretében nem értelmezett.

4.2. Tanúsítványigénylés feldolgozása

(83.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást, így a hozá kapcsolódó tanúsítványigénylés feldolgozása sem értelmezett. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok esetén alkalmazott tanúsítványigénylés-feldolgozási eljárást lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

4.2.1. Azonosítási és hitelesítési műveletek

(84.) Jelen BR-ESZIG keretében nem értelmezett.

4.2.2. Tanúsítványigénylés elfogadása vagy visszautasítása

(85.) Jelen BR-ESZIG keretében nem értelmezett.

4.2.3. Tanúsítványigénylés feldolgozás időtartama

(86.) Jelen BR-ESZIG keretében nem értelmezett.

4.3. Tanúsítvány kibocsátás

(87.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok esetén alkalmazott eljárást lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

4.3.1. Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

(88.) Jelen BR-ESZIG keretében nem értelmezett.

4.3.2. Előfizető értesítése a tanúsítvány kibocsátásról

(89.) Jelen BR-ESZIG keretében nem értelmezett.

4.4. Tanúsítványelfogadás

(90.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást, így a hozá kapcsolódó tanúsítványelfogadás sem értelmezett. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok esetén alkalmazott eljárást lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

4.4.1. Tanúsítvány Előfizető általi elfogadása

(91.) Jelen BR-ESZIG keretében nem értelmezett.

4.4.2. Tanúsítvány közzététele

(92.) Jelen BR-ESZIG keretében nem értelmezett.

4.4.3. További felek értesítése a tanúsítvány kibocsátásáról

(93.) Jelen BR-ESZIG keretében nem értelmezett.

4.5. A kulcspár és a tanúsítvány használata

(94.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványokra és kapcsolódó kulcspárokra vonatkozó alkalmazhatósági megkötéseket lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

4.5.1. Az Előfizető magánkulcs- és tanúsítvány használata

(95.) Jelen BR-ESZIG keretében nem értelmezett.

4.5.2. Az Érintett Felek nyilvános kulcs- és tanúsítvány használata

(96.) Jelen BR-ESZIG keretében nem értelmezett.

4.6. Tanúsítványok megújítása

(97.) A Szolgáltató nem nyújt tanúsítványmegújítás szolgáltatást.

4.6.1. Tanúsítvány megújítás körülményei

(98.) Nincs kikötés.

4.6.2. Ki kérelmezhet tanúsítvány megújítást

(99.) Nincs kikötés.

4.6.3. Tanúsítvány megújítási kérelmek feldolgozása

(100.) Nincs kikötés.

4.6.4. Az Előfizető értesítése a megújított tanúsítvány kibocsátásáról

(101.) Nincs kikötés.

4.6.5. Tanúsítvány Előfizető általi elfogadása

(102.) Nincs kikötés.

4.6.6. Megújított tanúsítvány közzététele

(103.) Nincs kikötés.

4.6.7. További felek értesítése tanúsítvány megújításról

(104.) Nincs kikötés.

4.7. Kulcscsere

(105.) A Szolgáltató nem nyújt kulcscsere szolgáltatást.

4.7.1. Kulcscsere körülményei

(106.) Nincs kikötés.

4.7.2. Ki kérelmezhet kulcscserét

(107.) Nincs kikötés.

4.7.3. Kulcscsere kérelmek feldolgozása

(108.) Nincs kikötés.

4.7.4. Előfizető értesítése az új tanúsítvány kibocsátásáról

(109.) Nincs kikötés.

4.7.5. Új tanúsítvány Előfizető általi elfogadása

(110.) Nincs kikötés.

4.7.6. Új tanúsítvány közzététele

(111.) Nincs kikötés.

4.7.7. További felek értesítése az új tanúsítvány kibocsátásáról

(112.) Nincs kikötés.

4.8. Tanúsítványmódosítás

(113.) A Szolgáltató nem nyújt tanúsítványmódosítás szolgáltatást. Aláírónak a meglevő tanúsítványában foglalt adatok módosulása esetén a tanúsítvány visszavonásáról kell gondoskodnia.

4.8.1. Tanúsítványmódosítás körülményei

(114.) Nincs kikötés.

4.8.2. Ki kérelmezhet tanúsítványmódosítást

(115.) Nincs kikötés.

4.8.3. Tanúsítványmódosítási kérelmek feldolgozása

(116.) Nincs kikötés.

4.8.4. Előfizető értesítése az új tanúsítvány kibocsátásáról

(117.) Nincs kikötés.

4.8.5. Módosított tanúsítvány Előfizető általi elfogadása

(118.) Nincs kikötés.

4.8.6. Módosított tanúsítvány közzététele

(119.) Nincs kikötés.

4.8.7. További felek értesítése a módosított tanúsítvány kibocsátásáról

(120.) Nincs kikötés.

4.9. Tanúsítvány visszavonás és felfüggesztés

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

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

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

4.9.1. Visszavonás körülményei

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

4.9.2. Ki kezdeményezheti a visszavonást

(125.) Visszavonást kezdeményezhet:

a) Aláíró;
b) az át nem vett okmányokat jelző eljáró hatóság;
c) az eSzemélyi érvénytelenítéséről jogszabály alapján döntő hatóság;
d) Szolgáltató.

4.9.3. Visszavonási kérelemre vonatkozó eljárás

(126.) 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 Aláírót a tanúsítvány visszavonásáról.

(127.) A tanúsítvány visszamenőleges visszavonása nem megengedett, és az sem, hogy a kérelmező egy jövőbeni visszavonási időpontot jelöljön meg a kérelemben.

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

4.9.4. Kivárási idő visszavonási kérelem esetén

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

4.9.5. Visszavonási kérelem feldolgozásának időbelisége

(130.) 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

(131.) 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

(132.) A végfelhasználói tanúsítványokra vonatkozó CRL kibocsátásának gyakorisága: 24 óránként 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.

(133.) 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

(134.) 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

(135.) Szolgáltatónak a végfelhasználói és szolgáltatói tanúsítványok visszavonási állapotának megállapításához OCSP szolgáltatást is kell nyújtania.

4.9.10. OCSP alapú visszavonás ellenőrzés követelményei

(136.) 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

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

4.9.12. Különleges követelmények a kulcs kompromittálódása esetére

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

(139.) 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

(140.) Mivel Aláíró a tanúsítvány felfüggesztését a {J4} SzigR. rendelkezései értelmében nem kezdeményezheti, Szolgáltató nem nyújt felfüggesztési szolgáltatást.

4.9.14. Ki kérelmezhet felfüggesztést

(141.) Nincs kikötés.

4.9.15. Felfüggesztésre vonatkozó eljárás

(142.) Nincs kikötés.

4.9.16. A felfüggesztés megengedett időtartama

(143.) Nincs kikötés.

4.10. Visszavonási állapot szolgáltatások

4.10.1. Működési jellemzők

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

(145.) 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.

4.10.1.1. CRL

(146.) A Szolgáltató által kibocsátott CRL megfelel a {Sz8} RFC 5280 szabványnak.

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

(148.) 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.

(149.) 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.

(150.) 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.

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

(152.) Végfelhasználói tanúsítványokra vonatkozó CRL elérhetősége:
http://cca.hiteles.gov.hu/crl/GOVCA-CCA.crl

(153.) Szolgáltatói tanúsítványokra vonatkozó CRL elérhetősége:

http://qca.hiteles.gov.hu/crl/GOVCA-ROOT.crl

4.10.1.2. OCSP

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

(155.) Az OCSP szolgáltatást Szolgáltató az {Sz12} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően működteti.

(156.) 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.

(157.) 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.

(158.) 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.

(159.) Végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége:
http://cca.ocsp.hiteles.gov.hu/ocsp-cca

(160.) Szolgáltatói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége:
http://qocsp.hiteles.gov.hu/ocsp-root

4.10.2. Szolgáltatás rendelkezésre állása

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

4.10.3. Opcionális lehetőségek

(162.) Nincs kikötés.

4.11. Az előfizetés vége

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

4.12. Kulcsletét és visszaállítás

(164.) Szolgáltató nem nyújt kulcsletét és visszaállítás szolgáltatást.

4.12.1. Kulcsletét és visszaállítás szabályai

(165.) Nincs kikötés.

4.12.2. Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

(166.) Nincs kikötés.

5. FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

(167.) 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

(168.) 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

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

(170.) 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

(171.) 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.

(172.) 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

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

5.1.5. Tűzmegelőzés és tűzvédelem

(174.) 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

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

5.1.7. Selejt kezelése és megsemmisítése

(176.) 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

(177.) 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.

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

5.2. Eljárásbeli előírások

(179.) 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

(180.) 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.

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

(182.) A bizalmi munkakörökön kívül Szolgáltató bizalmi szerepköröket is alkalmazhat. A bizalmi szerepkört betöltő személynek munkaviszonyban kell állnia Szolgáltatóval vagy a Regisztrációs és Kártyakibocsátó Szervezettel.

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

(183.) 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

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

5.2.4. Egymást kizáró munkakörök

(185.) 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

(186.) 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

(187.) 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

(188.) 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

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

a) a PKI elméletet;

b) Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;

c) a szerepkör ellátáshoz szükséges speciális ismereteket;

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

e) az egyes tevékenységek jogi következményeit;

f) az alkalmazandó biztonsági szabályokat.

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

5.3.4. Továbbképzési gyakoriságok és követelmények

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

(192.) 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

(193.) Nincs kikötés.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

(194.) 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

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

(196.) 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

(197.) 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

(198.) 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

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

5.4.3. Naplóállomány megőrzési időtartama

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

5.4.4. Naplóállomány védelme

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

(202.) 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

(203.) A naplóállományokról rendszeres mentést kell készíteni.

5.4.6. Naplózás gyűjtési rendszere

(204.) 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.

(205.) 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

(206.) Nincs kikötés.

5.4.8. Sebezhetőség értékelések

(207.) 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.

(208.) Szolgáltatónak folyamatosan figyelemmel kell kísérnie az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül meg kell tennie, illetve – ha az ellenintézkedés költsége nem áll arányban a sebezhetőség lehetséges kihatásaival – cselekvési tervet kell készítenie és végrehajtania annak érdekében, hogy a sebezhetőség ne legyen kihasználható vagy annak hatása elhanyagolható legyen.

5.5. Adatok archiválása

5.5.1. A tárolt adatok típusai

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

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

a) tanúsítványok igénylésével, regisztrációval kapcsolatos minden adat vagy irat, különösen a Szolgáltatási Szerződés, Aláíró 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, különösen a Közreműködő Felekkel kötött megállapodások;

f) valamennyi naplóállomány.

5.5.2. Archívum megőrzési időtartama

(211.) 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 kapcsolatos jogvita jogerős lezárásáig, szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 10 évig.

5.5.3. Archívum védelme

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

5.5.4. Archívum mentési eljárásai

(213.) 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

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

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

(216.) 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

(217.) 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.

(218.) A papíralapú iratokat a Regisztrációs Irodákból be kell gyűjteni, azokat Szolgáltató dokumentumtárában kell tárolni.

5.5.7. Archívum hozzáférés és ellenőrzés eljárásai

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

5.6. Kulcs átállás

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

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

5.7. Helyreállítás rendkívüli üzemi helyzetek esetén

(222.) 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.

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

(224.) 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 Felügyeleti Szervnek.

(225.) 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

(226.) Szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel.

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

(228.) 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.

(229.) 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

(230.) 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

(231.) 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 Felügyeleti Szervet;
f) intézkedni valamennyi érintett fél értesítéséről.

5.7.4. Üzletmenet folytonosság helyreállás katasztrófát követően

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

5.8. A szolgáltatási tevékenység megszüntetése

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

(234.) 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.

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

a) Aláírók és Érintett Felek értesítésének módja;

b) a Szolgáltatásokban Közreműködő Felek jogosultságainak megvonása;

c) 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;

d) szolgáltatói magánkulcsok és azok mentései megsemmisítésének módja;

e) Szolgáltató informatikai rendszerében foglalt adatokról teljes körű mentés készítése.

6. MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1. Kulcspár előállítás és telepítés

6.1.1. Kulcspár előállítás

(236.) Szolgáltató maga kell előállítsa a tanúsítványok és visszavonási listák aláírására használandó kulcspárokat fizikailag védett környezetben, kriptográfiai modulban (HSM). A kriptográfiai modulnak meg kell felelnie a (245.) fejezet szerinti követelményeknek. A tanúsítványok hitelesítésére használt kulcspárok előállítását Szolgáltató dokumentált „kulcsceremónia” 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.

(237.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást, így a hozzá kapcsolódó aláírói kulcspár előállítás sem értelmezett. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok esetén alkalmazott aláírói kulcspár előállítási eljárást lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között találhatók meg.

6.1.2. Magánkulcs eljuttatása a tulajdonoshoz

(238.) Jelen BR-ESZIG keretében nem értelmezett.

6.1.3. Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

(239.) Jelen BR-ESZIG keretében nem értelmezett.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

(240.) 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

(241.) A Szolgáltatónak a Szolgáltatások nyújtása során - mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében -, valamint a Szolgáltatások nyújtásában közreműködő feleknek biztosítaniuk kell avonatkozó szabványok szerint biztonságosnak tekinthető algoritmusok, paraméterek és kulcshosszak alkalmazását.

6.1.6. A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

(242.) A szolgáltatói kulcspárok előállítása a 6.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva kell történjen.

(243.) Az aláírói kulcspárok előállítása jelen BR-ESZIG keretében nem értelmezett.

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

(244.) Szolgáltatónak a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz11} ITU-T X.509 v3 szabványnak megfelelően kell jeleznie a kulcs használat célját.

6.2. Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

(245.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok esetén alkalmazott magánkulcsvédelmi szabályozást lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

6.2.1. Kriptográfiai modul szabványok és szabályozások

(246.) 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 {Sz13} szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg; vagy

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

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

(247.) Aláírói magánkulcsok esetén jelen BR-ESZIG keretében nem értelmezett.

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

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

6.2.3. Magánkulcs letét

(249.) Szolgáltató a hitelesítő központok magánkulcsait nem teszi letétbe semmilyen célból.

(250.) Aláírói magánkulcsok esetén jelen BR-ESZIG keretében nem értelmezett.

6.2.4. Magánkulcs visszaállítása

(251.) 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.

(252.) Aláírói magánkulcsok esetén jelen BR-ESZIG keretében nem értelmezett.

6.2.5. Magánkulcs mentése

(253.) Aláírói magánkulcsok esetén jelen BR-ESZIG keretében nem értelmezett.

6.2.6. Magánkulcs bejuttatása a kriptográfiai modulba

(254.) Szolgáltató a hitelesítő központok magánkulcsait a 6.1.1 fejezetben leírtak szerint HSM modulban állítja elő, és azok teljes életciklusuk alatt a HSM modulban maradnak. Amennyiben a magánkulcs visszaállítása rendkívüli üzemi helyzet során szükséges, akkor Szolgáltató a 6.2.4 fejezet szerint végzi a magánkulcsot bejuttatását a kriptográfiai modulba.

(255.) Aláírói magánkulcsok esetén jelen BR-ESZIG keretében nem értelmezett.

6.2.7. Magánkulcs kriptográfiai modulban történő tárolásának módja

(256.) A hitelesítő központok magánkulcsai teljes életciklusuk alatt a (245.) fejezetben leírt HSM modulban kerülnek tárolásra.

(257.) Aláírói magánkulcsok esetén jelen BR-ESZIG keretében nem értelmezett.

6.2.8. Magánkulcs aktiválásának módja

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

(259.) Aláírói magánkulcsok esetén jelen BR-ESZIG keretében nem értelmezett.

6.2.9. Magánkulcs aktív állapotának megszüntetési módja

(260.) Szolgáltatónak biztosítani kell, hogy az aktivált HSM modul jogosulatlan hozzáférés ellen védett legyen. A HSM modul működése során csak az azonosított és feljogosított Kártyakibocsátó Szervezettől érkezett, hiteles tanúsítványkérelmekre kiadott tanúsítványok, visszavonási listák és opcionálisan OCSP válaszok aláírására használható. A magánkulcs eltávolításra kerül a HSM modulból, amikor a hitelesítő központ működése megszűnik.

6.2.10. Magánkulcs megsemmisítésének módja

(261.) 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

(262.) Lásd a (245.) fejezetben.

6.3. Kulcspár gondozás egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

(263.) 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

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

"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"	20 év
"Minősített Állampolgári Tanúsítványkiadó"	legfeljebb 15 év
OCSP válaszadó	legfeljebb 30 nap

(265.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok és kulcsok esetén a felhasználási idő szabályozását lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

6.4. Aktivizáló adatok

(266.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott tanúsítványok esetén az magánkulcs aktiválsának szabályozását lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

6.4.1. Aktivizáló adatok előállítása és telepítése

(267.) Jelen BR-ESZIG keretében nem értelmezett.

6.4.2. Aktivizáló adatok védelme

(268.) Jelen BR-ESZIG keretében nem értelmezett.

6.4.3. Aktivizáló adatok egyéb szempontjai

(269.) Jelen BR-ESZIG keretében nem értelmezett.

6.5. Informatikai biztonsági óvintézkedések

6.5.1. Informatikai biztonsági műszaki követelmények meghatározása

(270.) Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz1} EN 319 401, {Sz2} EN 319 411-1 és {Sz3} EN 319 411-2 szabványoknak a nyilvános kulcsú tanúsítványokat kibocsátó, minősített bizalmi szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg.

(271.) 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 a Szolgáltató részben a szolgáltatási szabályzatában (BSZ-ESZIG), részben a belső biztonsági szabályzataiban írja le.

6.5.2. Informatikai biztonsági értékelés

(272.) Szolgáltatónak az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezései szerint kell elvégeznie.

6.6. Életciklusra vonatkozó műszaki óvintézkedések

6.6.1. Rendszerfejlesztési óvintézkedések

(273.) 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

(274.) 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.

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

6.6.3. Életciklus biztonsági óvintézkedések

(276.) 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

(277.) A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzatában meghatározott követelményeknek megfelelően kell megvalósítani, figyelembe véve az {Sz3} EN 319 411-2 szabvány 6.5.7 fejezetében leírt követelményeket is.

6.8. Időforrások

(278.) 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

(279.) Szolgáltató – figyelembe véve a {J2} DÁP tv. 119. § (8) bekezdését – a jelen BR-ESZIG hatálya alatt nem végez tanúsítványkibocsátási szolgáltatást. A jelen BR-ESZIG korábbi verzióinak hatálya alatt kibcsátott

tanúsítványok esetén tanúsítványprofil-követelményeket lásd a kibocsátás időpontjának megfelelő korábbi verzió azonos fejezetében, mely Szolgáltató weboldalán közzétett archív szabályzatok között található meg.

7.1.1. Verziószám

(280.) Jelen BR-ESZIG keretében nem értelmezett.

7.1.2. Tanúsítvány kiterjesztések

(281.) Jelen BR-ESZIG keretében nem értelmezett.

7.1.3. Algoritmus azonosítók

(282.) Jelen BR-ESZIG keretében nem értelmezett.

7.1.4. Név formák

(283.) Jelen BR-ESZIG keretében nem értelmezett.

7.1.5. Név megszorítások

(284.) Jelen BR-ESZIG keretében nem értelmezett.

7.1.6. Hitelesítési rend objektumazonosító

(285.) Jelen BR-ESZIG keretében nem értelmezett.

7.1.7. Szabályzati megszorítások kiterjesztés használata

(286.) Jelen BR-ESZIG keretében nem értelmezett.

7.1.8. Szabályzat minősítők szintaktikája és szemantikája

(287.) Jelen BR-ESZIG keretében nem értelmezett.

7.1.9. A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása

(288.) Jelen BR-ESZIG keretében nem értelmezett.

7.2. CRL profil

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

7.2.1. Verziószám

(290.) A visszavonási listák verziószáma: V2.

7.2.2. CRL és CRL bejegyzés kiterjesztések

(291.) A visszavonási lista az alábbi kiterjesztéseket tartalmazza "nem kritikus" megjelöléssel:

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

(292.) A visszavonási lista a fentieken túl más szabványos kiterjesztést is tartalmazhat, azonban ezen kiterjesztések nem lehetnek "kritikus" jelzésűek.

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

7.3. OCSP profil

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

7.3.1. Verziószám

(295.) Az OCSP válaszok verziószáma: V1.

7.3.2. OCSP kiterjesztések

(296.) Az OCSP válasz az alábbi kiterjesztéseket tartalmazza "nem kritikus" megjelöléssel:

Nonce	az OCSP kérésben megadott, visszajátszásos támadások megelőzésére szolgáló véletlenszám (csak akkor, ha a kérés tartalmazta azt)
ArchiveCutoff	jelzi, hogy a Szolgáltató a tanúsítvány lejárata után is biztosítja a visszavonási státuszt, a 4.10.1 fejezetben megadott időtartamig

(297.) Az OCSP válasz a fentieken túl más szabványos kiterjesztést is tartalmazhat, azonban ezen kiterjesztések nem lehetnek "kritikus" jelzésűek.

8. MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

(298.) Jelen bizalmi szolgáltatási rend előírja az összes, a természetes személyek számára kibocsátott minősített tanúsítványokkal kapcsolatos szolgáltatások során teljesíteni szükséges követelményt, melyeket a különösen az alábbi nemzetközi szabványok határoznak meg:

a) EN 319 401: General policy requirements for Trust Service Providers {Sz1}
b) EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates {Sz2}
c) EN 319 411-2: Policy and security requirements for Trust Service Providers issuing EU qualified certificates {Sz3}
d) EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz4}
e) EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz5}
f) EN 319 412-5: Certificate Profiles; Part 5: QCStatements {Sz6}

8.1. Vizsgálatok gyakorisága és körülményei

(299.) A Szolgáltató vizsgálatának gyakorisága és körülményei meg kell feleljen a hatályos jogszabályi előírásoknak.

(300.) Szolgáltatónak legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot kell végeztetnie a {J1} eIDAS, illetve a {J2} DÁP tv. követelményeinek való megfelelés tárgykörben. Szolgáltató köteles az elkészült megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül benyújtani a Felügyeleti Szervnek.

8.2. Auditor azonosítása és képesítése

(301.) A megfelelőségértékelés előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére Szolgáltató külső rendszervizsgálót alkalmazhat.

(302.) 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.

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

(304.) 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

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

8.4. Audit során vizsgált területek

(306.) 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.

(307.) 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

(308.) 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.

(309.) A Felügyeleti Szerv (hatóság) által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat Szolgáltató a hatósággal megállapodott határidőn belül megszünteti a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembe vételével.

8.6. Eredmény kommunikációja

(310.) 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 felügyelet szervet a következő helyszíni ellenőrzés során tájékoztatni kell. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9. EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1. Díjak

(311.) A díjazással kapcsolatos információkat a BSZ-ESZIG szolgáltatási szabályzat tartalmazza.

9.2. Anyagi felelősség

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

9.2.1. Biztosítási fedezet

(313.) Szolgáltatónak felelősségbiztosítással kell rendelkeznie, mely egyaránt kiterjed az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, valamint a Bizalmi Felügyeletnél felmerült jogszabály szerinti költségekre, és amely fedezetet biztosít az összes károsultnak okozott kárra, a tanúsítványban jelzett tranzakciós limit értékének legalább ötszöröséig.

(314.) A felelősségbiztosítási szerződésnek meg kell felelnie a {J9} 24/2016 rendelet előírásainak is.

9.2.2. További követelmények

(315.) Szolgáltatónak teljesítenie kell a {J9} 24/2016 rendelet 19. §-a szerinti pénzügyi követelményeket is.

9.2.3. Felelősségbiztosítás vagy garancia végfelhasználók számára

(316.) Nincs kikötés.

9.3. Üzleti információk bizalmassága

9.3.1. Bizalmasan kezelendő információk köre

(317.) Szolgáltatónak a szolgáltatási szabályzatában meg kell adnia a bizalmasan kezelendő információk körét.

9.3.2. Bizalmasnak nem tekintett információk köre

(318.) Nincs kikötés.

9.3.3. Bizalmas információk védelmének felelőssége

(319.) 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

(320.) 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.

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

9.4.2. Bizalmasként kezelendő személyes adatok

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

(323.) Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

a) Aláíró minden adatát, ha Aláíró nem járult hozzá tanúsítványának közzétételéhez;

b) Aláírónak azon adatait, melyek a tanúsítványba nem kerülnek befoglalásra, ha Aláíró írásban hozzájárult tanúsítványának közzétételéhez.

9.4.3. Bizalmasként nem kezelendő személyes adatok

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

(325.) 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

(326.) 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

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

(328.) Aláíró választása szerint hozzájárulhat vagy megtilthatja tanúsítványának nyilvános közzétételét.

9.4.6. Felfedés hatósági vagy polgári peres eljárás keretében

(329.) 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 Aláírót.

(330.) 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 Aláírót.

9.4.7. Egyéb, felfedést eredményező körülmények

(331.) Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatások nyújtásának megszüntetése esetén Aláíró adatait a jogszabályi kötelezettségeire tekintettel átadja harmadik félnek.

9.5. Szellemi tulajdonjogok

(332.) A Szolgáltató által Aláíró részére kibocsátott tanúsítvány és az ahhoz tartozó kulcspár tulajdonosa az Aláíró. Szolgáltató a tanúsítványt a kikötéseiben és feltételeiben ismertetett esetekben és módon közzé teheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti. A végfelhasználói tanúsítványban szereplő megkülönböztető név használatára Aláíró jogosult.

(333.) A szolgáltatói tanúsítványok a Szolgáltató tulajdonát képezik. A visszavonási információk a Szolgáltató tulajdonát képezik. A Szolgáltató szabályzatai, szerződéses feltételei a Szolgáltató tulajdonát képezik.

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. Szolgáltató felelőssége és helytállása

(334.) Szolgáltató felel a jelen bizalmi szolgáltatási rendben és a vonatkozó szolgáltatási szabályzatban, valamint az Aláíróval megkötött Szolgáltatási Szerződésben megfogalmazott valamennyi kötelezettség maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat a Közreműködő Felek vagy egyéb alvállalkozók végzik.

(335.) A Szolgáltató Telefonos Ügyfélszolgálatának (Kormányzati Ügyfélvonal – 1818) felelőssége:

a) Aláíró telefonos visszavonási igényének fogadása, majd ezt követően – ha az Aláíró sikeresen azonosította magát - a visszavonás kezdeményezése;

b) a Szolgáltatásokkal kapcsolatos teljes körű és közérthető tájékoztatás, különösen a 4.1.2 és 4.9 fejezetben meghatározottakról.

9.6.2. A regisztrációs szervezet felelőssége

9.6.2.1. Regisztrációs Szervezet felelőssége

(336.) Regisztrációs Szervezet betartja a rá vonatkozó jogszabályokban, illetve a Szolgáltató szabályzataiban foglalt előírásokat.

(337.) Regisztrációs Szervezet felelőssége a tanúsítványok visszavonásával kapcsolatban:

a) intézkedni arról, hogy Aláíró kérésére a visszavonási igény rögzítésre kerüljön és a visszavonást kezdeményezze a Szolgáltató felé;

b) intézkedni arról, hogy a bármilyen okból (eltulajdonítás, megsemmisülés, elvesztés, adatváltozás, elhalálozás miatt) érvénytelenített eSzemélyi-hez tartozó tanúsítvány visszavonását kezdeményezze a Szolgáltató felé.

9.6.2.2. Kártyakibocsátó Szervezet felelőssége

(338.) Szolgáltató a Kártyakibocsátó Szervezettel megkötött együttműködési megállapodásban meg kell követelje a bizalmi szolgáltatási rend és a vonatkozó szolgáltatás szabályzat előírásainak maradéktalan betartását.

(339.) Kártyakibocsátó Szervezet felelőssége:

a) a tanúsítvány visszavonási kérelmek hitelesítése elektronikus bélyegzővel és a kérelmek eljuttatása Szolgáltató részére.

9.6.3. Aláíró felelőssége és helytállása

(340.) Aláíró felelős a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért;

(341.) Aláíró felelős a tanúsítványban szereplő adatok ellenőrzéséért;

(342.) Aláíró felelős azért, hogy a tanúsítványt érintő összes adatának megváltozását haladéktalanul bejelentse, beleértve mindazon adataiban bekövetkezett változásokat is, melyeket a regisztrációs eljárás és a Szolgáltatási Szerződés megkötése során megadott;

(343.) Aláíró felelős az eSzemélyi-nek mint minősített elektronikus aláírást létrehozó eszköznek, valamint a kapcsolódó magánkulcsnak a rendeltetésszerű felhasználásáért, a szabályzatoknak és a QSCD tanúsítási jelentésében előírtaknak megfelelően;

(344.) Aláíró felelős a magánkulcsnak, az aktivizáló kódjainak és a visszavonási jelszónak a biztonságos kezeléséért;

(345.) Aláíró felelős azért, hogy a magánkulcsot és a kapcsolódó tanúsítványt csak a tanúsítvány érvényességi időtartamán belül használja, a tanúsítvány visszavonása esetén azok használatát haladéktalanul és végérvényesen beszüntesse;

(346.) Aláíró felelős azért, hogy a magánkulcs és a kapcsolódó tanúsítvány használatát haladéktalanul és végérvényesen beszüntesse, amennyiben tudomására jut, hogy a Szolgáltató valamely, a tanúsítvány kibocsátásában érintett hitelesítő központja kompromittálódott;

(347.) Aláíró felelős Szolgáltatót haladéktalanul értesíteni és teljes körűen tájékoztatni vitás ügyekben;

(348.) Aláíró felelős a Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben meghatározott kötelezettségei betartásáért.

9.6.4. Érintett Felek felelőssége és helytállása

(349.) 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

(350.) Nincs kikötés.

9.7. Helytállás érvénytelenségi köre

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

9.8. Felelősség korlátozása

(352.) 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

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

9.10. Hatályosság és megszűnés

9.10.1. Hatályosság

9.10.1.1. Időbeli hatály

(354.) 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.

9.10.1.2. Tárgyi hatály

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

9.10.1.3. Személyi hatály

(356.) A bizalmi szolgáltatási rend személyi hatálya kiterjed Szolgáltatónak, illetve a Közreműködő Feleknek a Szolgáltatások nyújtásában közreműködő munkatársaira és az Aláírókra.

9.10.2. Megszűnés

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

9.10.3. Megszűnés után is hatályban maradó rendelkezések

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

9.11. Egyéni hirdetmények és kommunikáció a részvevőkkel

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

9.12. Módosítások

9.12.1. Módosítás eljárása

(360.) 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

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

9.12.3. OID megváltozását előidéző körülmények

(362.) A szolgáltatási rend OID-ja nem változik.

9.13. Vitás kérdések rendezése

(363.) A szolgáltatási szabályzat tartalmazza.

9.14. Irányadó jog

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

9.15. Hatályos jognak megfelelés

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

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

(366.) Nincs kikötés.

9.16.2. Átruházás

(367.) Nincs kikötés.

9.16.3. Részleges érvénytelenség

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

9.16.4. Igényérvényesítés

(369.) 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)

(370.) A szolgáltatási szabályzat tartalmazza.

9.17. Egyéb rendelkezések

9.17.1. Hozzáférhetőség a fogyatékossággal élő személyek számára

(371.) A Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználó termékeket hozzáférhetővé kell tenni a fogyatékossággal élő személyek számára.