NetLock Hitelesítési Rend nem minősített tanúsítványokra

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

A dokumentum angol neve	**NETLOCK CERTIFICATE POLICY**
Verziószám:	**1.1**
Azonosító szám (OID):	**1.3.6.1.4.1.3555.1.60.20160630**
Jóváhagyás időpontja:	**2016.06.30.**
Hatály kezdőnapja:	**2016.07.01.**
Oldalak száma:	**788 oldal** fedlappal együtt 78
Készítette	**Almási János,** Termékfejlesztési vezető **dr. Barabás Anett,** Hatósági ügyintéző, belső ellenőr **Varga Viktor,** Senior PKI szakértő **Szabó Zoltán,** PKI termékmenedzser
Jóváhagyta	**dr. Szűcs Katalin,** Szabályzatvezető

NYILVÁNOS

Revíziók

OID	Változás leírása	Készítő	Ellenőrző
1.3.6.1.4.1.3555.1.60.20160531	eIDAS rendeletnek megfelelő első nyilvános verzió	Almási János Dr. Barabás Anett Varga Viktor Szabó Zoltán	dr. Szűcs Katalin
1.3.6.1.4.1.3555.1.60.20160630	Jogszabályi rendelkezéseknek megfelelő pontosítások, kiegészítések	Almási János Dr. Barabás Anett Varga Viktor Szabó Zoltán	dr. Szűcs Katalin

Tartalom

1 Bevezetés

Jelen hitelesítési rend célja, hogy összefoglalja, rendszerezze azokat a minimum követelményeket, amelyek a nem minősített tanúsítványok igénylésére, kibocsátására, használatára és életciklusára vonatkoznak.

1.1 Áttekintés

Jelen dokumentum a NETLOCK Kft. (továbbiakban Szolgáltató vagy Bizalmi szolgáltató) nem minősített tanúsítványkiadási szolgáltatására vonatkozó elvárásokat tartalmazó leírás.

A hitelesítési rend az RFC 3647 szabvány formai és tartalmi elvárásai szerint készült. A dokumentum az eIDAS, az Eüt. (lásd 1.6.2 Rövidítések) és egyéb releváns hazai jogszabályok, valamint az ETSI EN 319401, ETSI EN 319411, ETSI EN 319412 szabványok elvárásait foglalja össze.

Az elvárásoknak való megfelelést a *NetLock szolgáltatási szabályzat nem minősített tanúsítványokra* dokumentum ismerteti.

1.2 A dokumentum neve és azonosítás

Lásd a dokumentum fedőlapját.

1.2.1 Hitelesítési Rendek

A Bizalmi szolgáltatónak a végfelhasználói tanúsítványokban szabványos azonosítót vagy maga által képzett és nyilvántartott azonosítót kell elhelyeznie a Hitelesítési Rend (Certificate Policy - CP) jelzésére szolgáló mezőben, hogy azonosítsa az adott tanúsítványra vonatkozó szabványos vagy egyedi hitelesítési szabályokat és kinyilvánítsa az azoknak való megfelelését. (Ilyen szabványos azonosítók lehetnek pl. az ITU és a CAB Forum által definiált szabályzatazonosítók.) Az RFC 5280 ajánlásai szerint ilyen azonosítóból egy javasolt, így ahol lehetséges, szabványos azonosító egyedül kerüljön feltüntetésre.

Jelen dokumentum az alábbi Hitelesítési Rendeknek megfelelő tanúsítványokra vonatkozó rendelkezéseket tartalmazza. Amennyiben adott rendelkezések csak egyes Hitelesítési Rendre vonatkoznak, az adott rendelkzéseket a Hitelesítési Rendek azonosítója vezeti be, s kapcsos zárójelek határolják a rá vonatkozó szabályozást. Ennek hiányában a dokumentum rendelkezése minden Hitelesítési Rendre vonatkozik.

Azonosító	Hitelesítési Rend neve	OID
LCP	Lightweight Certificate Policy Könnyített Hitelesítési Rend	0.4.0.2042.1.3[1]
NCP	Normalized Certificate Policy Normalizált Hitelesítési Rend	0.4.0.2042.1.1
NCP+	Extended Normalized Certificate Policy	0.4.0.2042.1.2

[1] itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1)

	Kiterjesztett (Ügyféleszköz használatát megkövetelő) normalizált Hitelesítési Rend	
OVCP	Organizational Validation Certificate Policy Jogi személyek SSL tanúsítványára vonatkozó Hitelesítési Rend	0.4.0.2042.1.7
IVCP	Individual Validation Certificate Policy Természetes személyek SSL tanúsítványára vonatkozó Hitelesítési Rend	2.23.140.1.2.3[2]
DVCP	Domain Validation Certificate Policy Domain ellenőrzött SSL tanúsítványokra vonatkozó Hitelesítési Rend	0.4.0.2042.1.6
EHR_Ü	Közigazgatási ügyfél tanúsítványokra vonatkozó Hitelesítési Rend	0.2.216.1.100.42.101.5.2.1[3]
EHR_K	Közigazgatási köztisztviselőhöz tanúsítványokra vonatkozó Hitelesítési Rend	0.2.216.1.100.42.101.7.2.1
EHR+_Ü	Közigazgatási ügyfél tanúsítványokra vonatkozó, Ügyféleszköz használatát megkövetelő Hitelesítési Rend	0.2.216.1.100.42.101.3.2.1[4]
EHR+_K	Közigazgatási köztisztviselőhöz tanúsítványokra vonatkozó, Ügyféleszköz használatát Megkövetelő Hitelesítési Rend	0.2.216.1.100.42.101.4.2.1
EHR_ÜA	Közigazgatási ügyfél tanúsítványokra vonatkozó, automatizmushoz kötött Hitelesítési Rend	0.2.216.1.100.42.101.6.2.1[5]
EHR_KA	Közigazgatási köztisztviselőhöz tanúsítványokra vonatkozó, automatizmushoz kötött Hitelesítési Rend	0.2.216.1.100.42.101.8.2.1
CSCP	Code Signing Certificate Policy (non EV) Kódaláíró tanúsítványokra vonatkozó Hitelesítési Rend (nem EV)	2.23.140.1.4.1

A szolgáltató a tanúsítványában az előzőekben ismertetett hitelesítési rendek mellett egy másodlagos hitelesítési rendet is feltűntethet. Ezt a hitelesítési rendet a NetLock (1.3.6.1.4.1.3555.6) vagy a MELASZ azonosítója (1.3.6.1.4.1.48016.3) vezeti be.

A hitelesítési rend felépítése: Szint.Kulcstárolás.Alany.Kulcsfelhasználás.Azonosítás, ahol az egyes jellemzők az alábbi értékeket vehetik fel:

[2] joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)
[3] IHM ajánlás szerint
[4] IHM ajánlás szerint
[5] IHM ajánlás szerint

Szint:	0 - teszt 1 - fokozott
Kulcstárolás:	1 - szoftver 2 - hardveres (nonQSCD) 4 - központi menedzselt (nonQSCD hardver alapú)
Alany:	1 - természetes személy 2 - jogi személy 3 - álnév 4 - domain név 5 - IP Cím 6 - terméknév és védjegy 9 - szabályozott szakmai és egyéb speciális 12 - természetes és jogi személy együtt 41 - domain és természetes személy 42 - domain és jogi személy[6] 91 - Ügyvéd
Azonosítás:	0 - Ellenőrzés nélküli 1 - Személyes megjelenés nélküli 2 - Személyes megjelenésen alapuló
Kulcsfelhasználás: (opcionális)	1 - aláírás 2 - bélyegzés 3 - authentikáció 4 - titkosítás 5 - SSL 6 - Kódaláírás

1.2.2 Dokumentum revíziók

Verzió	Hatály kezdete	Változás leírása	Készítő
0.1	-	-	Almási János, Barabás Anett, Szabó Zoltán, Varga Viktor
1.0	2016.07.01	Draft verzió pontosításai	

1.3 A PKI szereplők

A fogalommeghatározásokat lásd az 1.6.1 fejezetben.

[6] A kettős Alanyok más variációi is előfordulhatnak egyes esetekben, amik hasonló módon kerülhetnek jelölésre az egyedi Alanyok azonosítóiból két számjegyet képezve

1.3.1 A bizalmi szolgáltató és a hitelesítő egység

A bizalmi szolgáltatónak általános felelőssége van az általa nyújtott szolgáltatások tekintetében. Ezek nyújtásához igénybe vehet külső feleket, de biztosítania kell a kikötéseinek és feltételeinek való megfelelőséget az általuk nyújtott szolgáltatások tekintetében, s tevékenységükért feleősséggel tartozik az Ügyfelek felé.

A hitelesítő egység és a bizalmi szolgáltató az általa kibocsátott tanúsítványokban (mint kibocsátó) megnevezésre kerül, s a tanúsítvány az ő magánkulcsával kerül bélyegzésre.

1.3.2 Regisztrációs Egység

Regisztrációs Egység működhet a bizalmi szolgáltató részeként, de lehet önálló, független szervezet is (Kihelyezett Regisztrációs Egység).

A Regisztrációs Egység működésének meg kell felelnie a vonatkozó Hitelesítési rend(ek)ben, Szolgáltatási szabályzat(ok)ban és egyéb dokumentumokban megfogalmazott követelményeknek. A bizalmi szolgáltató minden esetben teljes felelősséggel tartozik a Regisztrációs Egységre vonatkozó előírások betartatásáért.

Kihelyezett Regisztrációs Egység működése esetén a bizalmi szolgáltatónak szerződésben köteleznie kell azt a vonatkozó követelmények betartására.

1.3.3 Előfizető, Végfelhasználó és Igénylő

Előfizető és Igénylő a Bizalmi Szolgáltató Ügyfelei, akikkel Szolgáltató szerződéses kapcsolatba kerül. Végfelhasználó személye megegyezhet bármelyikkel, de el is térhet tőlük (ez esetben Szolgáltató nem is ismeri a személyét csak Előfizető, aki Végfelhasználó kötelezettségeinek betartásáért felel). A tanúsítványban Előfizető és Végfelhasználó együttesen is megnevezésre kerülhet Alanyként, de egyes hitelesítési rendek csak egyiküket vagy egyiküket sem tüntetik fel a tanúsítványban.

1.3.4 Érintett felek

Érintett Félnek kell tenkinteni azokat a természetes és jogi személyeket, akik a Szolgáltató által kiadott tanúsítvány érvényességének ellenőrzésének céljából a Szolgáltató által karbantartott nyilvántartásokat és szabályzatokat igénybe veszik.

1.3.5 Egyéb szereplők

Nincs megkötés.

1.4 Tanúsítványok alkalmazhatósága

Az NCP, NCP+ és LCP hitelesítési rendek nem határoznak meg korlátozásokat a tanúsítványok alkalmazhatóságát és a felhasználók körét illetően.

A DVCP, IVCP és OVCP hitelesítési rendek szerint kibocsátott tanúsítványok SSL és TLS protokollon keresztül elért webszerverek azonosítására használhatók.

1.5 Hitelesítési rend adminisztrációja

A bizalmi szolgáltató hitelesítési rendjének kibocsátását, karbantartását a bizalmi szolgáltató szabályzatért felelős egysége végzi. A bizalmi szolgáltató a szabályzatért felelős egységet saját egységén belül működteti s ennek pontos felépítését, feladatát, hatáskörét és felelősségét a külön szabályzat tartalmazza. A Hitelesítési rend szervezeten belüli jóváhagyást követően a bizalmi szolgáltató Felügyeleti Szerve is (Nemzeti Média és Hírközlési Hatóság) nyilvántartásba veszi.

1.6 Fogalmak és rövidítések

1.6.1 Fogalmak

Alany	A tanúsítvány “Subject” mezőjében feltüntetésre kerülő természetes és/vagy jogi személy és/vagy eszköz/rendszer azonosítója/más elnevezés. Lásd az Előfizető, Ügyfél és Végfelhasználó entitásokat.
Állapotváltoztatás	Az az eljárás, aminek eredményeként a tanúsítvány állapota (érvényes, felfüggesztett) megváltozik és új értéket vesz fel (érvényes, felfüggesztett, visszavont).
Átvevő	A végfelhasználó valamely kulcsát vagy eszközét (pl. Ügyféleszköz) Szolgáltatótól (személyesen, hagyományos vagy elektronikus kézbesítés útján) átvevő személy, aki az lehet, aki az adott tanúsítvány esetében Igénylő lehet.
Bizalmi munkatárs	A Bizalmi szolgáltatónál vagy Szolgáltatói partnerénél bizalmi munkakört betöltő személy.
Bizalmi munkakör	Az 5.2.1-ben meghatározott munkakörök.
Bizalmi Felügyelet	Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény által a bizalmi szolgáltatások felügyeletére kijelölt szerv.
Bizalmi szolgáltató, Szolgáltató	Jelen Hitelesítési rend szerinti bizalmi szolgáltatásokat nyújtó szolgáltató. A NetLock Kft. vagy más vele szerződött szolgáltató.
Bizalmi szolgáltatás	Jelen szabályzat keretén belül a Bizalmi szolgáltató elektronikus aláírásokhoz, elektronikus bélyegzőkhöz, autentikációhoz és titkosításhoz kapcsolódó tanúsítványok kibocsátását és életciklusmenedzsmentjét biztosító szolgáltatásai.
Biztonságos zóna:	Olyan (logikailag vagy fizikailag) védett terület, amely védi a titkosságát, integritását és elérhetőségét a Bizalmi szolgáltató által használt rendszereknek.
Certificate Revocation List (CRL) – tanúsítvány visszavonási lista	A Bizalmi szolgáltató által készített hiteles lista, azon tanúsítványokról, amelyet már nem tekint érvényesnek a szolgáltató.

Domain Validation Certificate (DVC)	Olyan SSL tanúsítvány, amely nem tartalmaz ellenőrzött szervezeti adatot az Alanyként feltüntetett domain név mellett.
EV tanúsítvány Extended Validation Certificate (EVC)	Olyan SSL tanúsítvány ami megfelel az EVCG követelményeinek.
Elektronikus aláírás	Olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ
Elektronikus bélyegző	Olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét
Fokozott biztonságú elektronikus bélyegző	Olyan elektronikus bélyegző, amely megfelel az eIDAS 36. cikkben meghatá-rozott követelményeknek.
Előfizető	A bizalmi szolgáltatás azon szerződéses partnere, aki a szolgáltatási díjak fizetését vállalja. Jogai és kötelezettségei az ÁSZF-ben és a Szolgáltatási szerződésben elkülönülten megjelennek. Amennyiben a tanúsítvány Alanyként jogi személy is megnevezésre került vagy csak egy természetes személy van benne megnevezve, akkor jellemzően azzal megegyezik. Lásd az Ügyfél és Végfelhasználó entitásokat.
Igénylő	A tanúsítványkezelési eljárásban eljáró, a szolgáltatói szerződést aláíró természetes személy, aki lehet: ● a tanúsítvány Alanyaként megjelölt természetes személy; ● ennek hiányában a tanúsítvány Alanyaként megjelölt jogi személy képviselője vagy meghatalmazottja; ● ezek hiányában a tanúsítvány Alanyaként megjelölt domain név vagy trademark tulajdonosa, ill. jogi személy tulajdonos esetén annak képviselője vagy meghatalmazottja, illetve a domain név fölött kontrollal rendelkező személy.
Érintett felek	Természetes vagy jogi személy, aki valamely bizalmi szolgáltatást igénybe veszi (pl. elektronikus aláírást vagy bélyegzőt ellenőriz Ügyfél és Szolgáltató tanúsítványával).
Hitelesítő egység	A Bizalmi szolgáltató tanúsítványokat kibocsátó egysége. Létezik végfelhasználói tanúsítványokat kibocsátó egység és ezen egységeket hitelesítő köztes hitelesítő egység, valamint a legfelső szintű gyökér hitelesítő egység, amelyek hierarchiába szervezetten működnek. A láncolt hitelesítő egység alatt Szolgáltatótól független szervezeti egység kezelésében lévő hitelesítő egységet értünk. .
Kezdeti felfüggesztés	A Tanúsítványfelfüggesztés egy speciális esete, amikor a Szolgáltató a tanúsítványt kibocsátása után azonnal felfüggeszti, így megóvva azt a visszaélésektől arra az időszakra, míg a

	Tanúsítvány és a magánkulcs biztonságosan eljut az Ügyfélhez.
Kihelyezett Regisztrációs Egység	A Szolgáltatótól független, önálló szervezet (Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Regisztrációs Egység.
Kikötések és feltételek	Szolgáltató azon dokumentumai, amelyek ismertetik hogy a bizalmi szolgáltatások nyújtásával kapcsolatosan, milyen elvárásoknak, milyen módon felel meg, s ismertetik a többi szereplő kötelezettségeit és jogait. Ide tartozik a Szolgáltató Szolgáltatási kivonata, Hitelesítési rendje, Szolgáltatási szabályzata, ÁSZF-e, szolgáltatási szerződése.
Kritikus szolgáltatások	A Bizalmi szolgáltató tanúsítvány- és kulcselőállítással, az Ügyfelek eszközzel való ellátásával és a visszavonáskezeléssel kapcsolatos szolgáltatásai.
Kulcscsere	Az a folyamat, amikor a Bizalmi szolgáltató egy már regisztrált Végfelhasználó részére bocsát ki új Tanúsítványt és magánkulcsot, annak egy már létező tanúsítványát alapul véve. Az új tanúsítványban a végfelhasználó nyilvános kulcsa megváltozik. Lásd a 4.7 fejezet.
Kulcsgenerálás	Az a folyamat, amikor a tanúsítványhoz tartozó kulcs a vonatkozó jogszabályban előírt tanúsítással rendelkező kriptográfiai modulban (HSM-ben) történik, védett környezetben, megfelelő személyi felügyelet mellett
Kulcsletét szolgáltatás	Olyan szolgáltatása a Bizalmi szolgáltatónak, amely a végfelhasználó magánkulcsának megőrzését és annak végfelhasználó számára történő átadását biztosítja (arra az esetre, ha a végfelhasználó kulcs elveszne, megsemmisülne vagy más okból használhatatlanná válna).
Minősített tanúsítvány	Olyan minősített tanúsítvány, amiről kiejelentésre került, hogy megfelel az eIDAS Annex I, III vagy IV részének vagy a 1999/93/EC direktívának, attól függően mi van érvényben a tanúsítvány kiadásakor. Jelen hitelesítési rend nem tárgyalja a minősített tanúsítványokra vonatkozó elvárásokat.
OV tanúsítvány Organizational Validation Certificate (OVC)	Olyan SSL tanúsítvány, amely ellenőrzött szervezeti adatot tartalmaz a tanúsítványban.
Regisztrációs egység	A Bizalmi szolgáltató azon egysége, amely a végfelhasználók azonosítását végzi. Létezhet a Szolgáltatón belül (mint belső szervezeti egység) vagy kívül (Kihelyezett Regisztrációs Egység)

	egyaránt.
Szolgáltatási Szabályzat	A Szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.
Szolgáltatási szerződés	Szolgáltató által kötött szerződés Előfizetővel és Igénylővel (ha elkülönül) egy vagy több adott Bizalmi szolgáltatás nyújtására és igénybevételére vonatkozóan. Elfogadása a szolgáltatás igénybevételének előfeltétele.
Szolgáltatói partner	Olyan természetes vagy jogi személyek, amelyek a Szolgáltatóval való megállapodás alapján a Szolgáltatás nyújtásában részt vesznek, vagy saját Szolgáltatást nyújtanak.
Szolgáltatói rendszer	Szolgáltató szolgáltatásnyújtást végző rendszereinek együttese.
Szolgáltatói tanúsítvány	Szolgáltató azon tanúsítványa, amelyeket a szolgáltatásnyújtás érdekében használ (pl. Végfelhasználói tanúsítványok aláírására).
Tanúsítvány	Szolgáltató által kibocsátott hiteles igazolás, amely a nyilvános kulcsot az Alanyhoz kapcsolja, és igazolja e Tanúsítványban közzétett adatok valódiságát.
Tanúsítványkezelési eljárás	Olyan eljárás, ami új tanúsítvány kibocsátását eredményezi (pl. kezdeti kibocsátás, megújítás, kulcscsere, módosítás) vagy ami a tanúsítvány álapotát megváltoztatja (pl. visszavonás).
Tanúsítványkibocsátó egység	A bizami szolgáltató tanúsítványibocsátó szerve a tanúsítványkibocsátó egység, amely az előírt eljárási rend szerint a hozzá tartozó regisztrációs egységek kérelme alapján a nem minősített tanúsítványok kiadását, publikálását, visszavonását, felfüggesztését, valamint a Tanúsítvány Visszavonási Lista (a továbbiakban: CRL) publikálását végzi.
Tanúsítványfelfüggesztés	Az a folyamat, amelyben a Bizalmi szolgáltató egy még érvényes Tanúsítvány érvényességét átmenetileg megszünteti az eredetileg tervezett érvényességi idő vége előtt. A tanúsítványfelfüggesztés egy átmeneti állapot, a felfüggesztett Tanúsítvány visszavonható, vagy a Tanúsítvány eredeti érvényességi idejében újra érvényessé tehető. A felfüggesztés visszavonása esetén a Tanúsítvány visszamenőleges hatállyal érvényessé válik, mintha a felfüggesztés meg sem történt volna.
Tanúsítványigénylés	Az a folyamat, amikor Igénylő tanúsítványt igényel, azaz a tanúsítvány elkészítéséhez szükséges adatokat megadja és igazolja a Szolgáltatónak, végül pedig Szolgáltatási szerződés Igénylő és - amennyiben nem egyezik Igénylővel - Előfizető általi aláírásával hitelesíti kérelmét az igényelt tanúsítványra vonatkozóan és ezzel felhatalmazza Szolgáltatót az igényelt tanúsítvány kibocsátására. A Tanúsítványigénylés általában az Ügyfélmenüben végezhető el, Szolgáltató azonban Szolgáltatási szabályzatában meghatározhat

	más módot is a Tanúsítványigénylésre.
Tanúsítványtár (tanúsítványállapot-adatbázis)	Szolgáltató által üzemeltetett nyilvános adatbázis, amelyen keresztül lekérdezhetők a szolgáltató által kiadott nyilvános tanúsítványok és az összes tanúsítvány érvényességi állapota.
Tanúsítvány-visszavonás	Az a folyamat, amelyben a Bizalmi szolgáltató a tanúsítvány érvényességét megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány-visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont tanúsítvány a visszavonás időpontjában érvényességét veszti, s már soha többé nem lehet újra érvényes.
Tanúsítványaktiválás	Felfüggesztett tanúsítvány érvényességének visszaállítása. Aktiválása után a tanúsítvány visszamenőlegesen, azaz a felfüggesztés időtartamára is újra érvényessé válik, mintha a felfüggesztés meg sem történt volna..
Tanúsítványmegújítás	Az a folyamat, amikor a Bizalmi szolgáltató ugyanarra a nyilvános kulcsra, változatlan Alannyal egy új Tanúsítványt állít ki, új érvényességi időszakra. Lásd a 4.6 fejezet.
Tanúsítványmódosítás	Az a folyamat, amikor a Bizalmi szolgáltató egy már regisztrált Igénylő részére bocsát ki új Tanúsítványt egy korábban kibocsátott Tanúsítványa alapján, az abban szereplő nyilvános kulccsal, de megváltozott Alany vagy Szolgáltató adatokkal. Lásd a 4.8 fejezet.
Ügyfél	A bizalmi szolgáltatás ügyfele, aki alatt a tanúsítvány Igénylőjét és Előfizetőjét egyaránt értjük (amíg a szabályzat nem tisztázza, hogy adott helyzetben pontosan kit kell érteni alatta, s amennyiben az adott esetben ezek a szereplők léteznek).
Ügyféleszköz	Olyan biztonságos kriptográfiai eszköz, amely az Végfelhasználó magánkulcsát tartalmazza, azt védi a kompromittálódás ellen, s a kulccsal kriptográfiai műveleteket végez az Végfelhasználó számára. Adott esetben megegyezik az elektronikus aláírást létrehozó eszközzel.
Ügyfélmenü	A Bizalmi szolgáltató ügyfelei számára a tanúsítványokkal és hozzájuk kapcsolódó szolgáltatásokkal kapcsolatos különböző igénylések elvégzésére illetve a folyamatban lévő igénylések állapotának megtekintésére biztosított a Szolgáltató internetes oldalán keresztül elérhető egyedi felület, melybe egyedi felhasználónév és jelszó megadásával lehet belépni (ügyfélmenü regisztrációt követően).
Ügyfélmenü regisztráció	Az a folyamat, amikor egy természetes személy adatai megadásával létrehozza saját Ügyfélmenüjét, illetve az Ügyfélmenübe való bejelentkezéshez szükséges bejelentkező nevét és jelszavát.
Végfelhasználó	Az a természetes személy, aki a tanúsítványban szereplő

	nyilvános kulcs magánkulcs párja felett rendelkezik (kizárólagosan használja vagy a használatáért felelős).
Végfelhasználói tanúsítvány, Végfelhasználói kulcs	Az Előfizetők tanúsítványát és kulcsát jelöli, megkülönböztetve a Szolgáltató saját tanúsítványaitól és kulcsaitól.

1.6.2 Rövidítések

Hivatkozott jogszabályok rövidítései

eIDAS	Az Európai Parlament és Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
eüt.	Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. Évi CCXXII. törvény.
Nytv	A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény.
Szmtv	2007. évi I. törvény a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról.
Harmtv	2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény

Műszaki szakkifejezések rövidítései

CA	Certification Authority
IP	Internet Protocol
IT	Information Technology
TSP	Trust Service Provider
BRG	Baseline Requirements Guidelines
CAB Forum	CA/Browser Forum
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DVC	Domain Validation Certificate

EAL	Evaluation Assurance Level
EV	Extended Validation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
OVC	Organizational Validation Certificate
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSP	Trust Service Provider
QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person
QSCD	Qualified electronic Signature/Seal Creation Device
ASN.1	Abstract Syntax Notation 1
UN	United Nations
IETF	Internet Engineering Task Force
QC	Qualified Certificate
QSCD	Qualified electronic Signature/Seal Creation Device
URL	Uniform Resource Locator

2 Közzétételre és tanúsítványtárra vonatkozó felelősségek

2.1 Adatbázisok és tanúsítványtár

Szolgáltató köteles a tanúsítványokra vonatkozó különböző információk (szabályzatok, tanúsítványok, érvényességi információk) nyilvánosságra hozatalára vonatkozó adatokat a szabályzatában ismertetni, és ezt a szabályzatot közzé tenni.

2.2 A tanúsítványokra vonatkozó információk közzététele

A bizalmi szolgáltató a tanúsítványokat köteles közzétenni az Ügyfelek és Érintett felek számára. Így különösen:

- A tanúsítvány előállítását követően a teljes és pontos tanúsítványt a Végfelhasználó rendelkezésre kell bocsátania.
- A végfelhasználói tanúsítványok csak akkor publikálhatók, amennyiben a végfelhasználó ehhez hozzájárul.
- A tanúsítvány használatával kapcsolatos kikötéseket és feltételeket az érintett felek számára elérhetővé kell tennie nyilvánosan és nemzetközi szinten;
- A tanúsítvány kapcsán alkalmazandó kikötéseknek és feltételeknek azonosíthatónak kell lenniük;
- A publikált tanúsítványokat és a kikötéseket szolgáltatónak folyamatosan elérhetővé kell tennie. Szolgáltatónak mindent meg kell tennie annak érdekében, hogy ezek az információk ne legyenek hosszabb ideig elérhetetlenek, mint ahogy azt a szolgáltatási szabályzatában jelezte.
- SSL tesztelési célokra visszavont, lejárt és érvényes tanúsítványokat

A kikötéseket és feltételeket az RFC 3647 szerinti tartalommal és struktúrában kell közzétenni. A szolgáltatási szabályzat 4.2. fejezetének tartalmaznia kell, hogy a Szolgáltató a CAA Rekordokat felülvizsgálja-e, és ha igen, akkor milyen eljárással dolgozza fel a domain neveket. Szolgáltatónak ezen tevékenységét - ha végez ilyet - naplóznia kell.

2.3 Közzététel időpontja és gyakorisága

Szolgáltatónak a Kikötéseket és feltételeket, illetve azok újabb verzióit a hatályba lépésüket megelőzően közzé kell tennie. A korábbi verziókat az érvényességük végét követően is mindaddig közzé kell tennie, ameddig az az alapján kibocsátott tanúsítványok még érvényben vannak.

A szolgáltatónak legalább évente felül kell vizsgálnia a hitelesítési rendjét és szabályzatait, szükség esetén módosítva azokat.

2.4 Tanúsítványtár elérésének szabályai

A szolgáltatónak a tanúsítványtárát és Kikötéseket és feltételeket nyilvánossan elérhetővé kell tennie olvasási jogosultsággal.

3 Azonosítás és hitelesítés

3.1 Elnevezések

A tanúsítvány Kibocsátó azonosító (Issuer) és Alany azonosító (Subject) mezői feleljenek meg az ITU-T X.509, RFC 5280 és a ETSI EN 319 412 ajánlások név formátum előírásainak.

3.1.1 Névtípusok

Szolgáltatónak a tanúsítványok Subject mezőinek képzése esetében az RFC 5280 szabványnak megfelelően az X.500 distinguished name előírásait kell követni (email címek esetén az RFC-822 előírásait). Ezen belül többfajta névtípust különböztethet meg a végfelhasználói tanúsítványok esetén (lásd az 1.2.1 másodlagos hitelesítési rend Alany attribútumát a névtípusok tekintetében, valamint a Szolgáltatási Szabályzat 7. fejezetét a kitöltésük módjára vonatkozóan).

3.1.2 A nevek értelmezhetősége

Természetes személyek számára kibocsátott tanúsítvány Subject mezőjének a következő adatokat kell tartalmaznia kell:

- countryName (Országkód);
- givenName+surname vagy pseudonym (Vezeték és Családnév vagy Álnév)
- commonName (Név)

Ezen kötelező mezőkből csak egyet szabad feltüntetni. Pseudonym alkalmazása esetén a givenName+surname mezők nem kerülhetnek feltüntetésre.

Jogi személyek számára kibocsátott tanúsítvány Subject mezőjének a következő adatokat tartalmaznia kell:

- countryName (Országkód);
- commonName (Név)

A tanúsítványban szereplő természetes és jogi személy nevét közhiteles nyilvántartásban, annak hiányában hivatalos azonosító dokumentumban, illetve az alapító okiratban szereplő írásmóddal kell feltüntetni.

Amennyiben a tanúsítvány Alanyaként jogi személy kerül feltüntetésre (természetes személy mellett vagy helyett), akkor kötelezően szerepelnie kell az organizationIdentifier mezőnek, a jogi személy egyedi azonosítóját tartalmazva. A mezőben egy hivatalos nemzeti vagy más azonosító rendszerben kapott egyedi azonosító szerepelhet kötött formátumban, amelyet az ETSI EN 319 412-1 5.1.4 definiál (*REFCO-szervezetazonosító* formában szerepel, ahol a REF és CO helyére három és két karakter kerül az alábbiak szerint).

Kitöltése:

1. Ha a szervezet rendelkezik adószámmal, az alapján kell kitölteni a mezőt: magyar adószám esetén "VATHU", EU-s adószám esetében “VATEU” értékkel.
2. Ha előző pont nem alkalmazható, akkor Cégjegyzékszámmal "NTRHU" értékkel.

3. Ha előző pontok nem alkalmazhatók, akkor nemzeti bejegyzett séma alapján "XX:HU" értékkel, amelyben az „XX” a nemzeti vagy EU-s azonosítási séma két karakteres jelölése.
4. Ha előző pontok nem alkalmazhatók, akkor más egyedi hivatalos azonosító is alkalmazható.
5. Ha egyik említett azonosító sem áll rendelkezésre, az alapító okirat azonosítója és az alapító jogszabály megnevezése is kerülhet ide.

Más országok azonosítórendszerei esetében az ISO 3166 szerinti országkód alkalmazandó a HU országkód helyett.

Amennyiben Subject/Serialnumber mező tartalma egy hivatalos (okmány alapján ellenőrzött) nemzeti azonosító, azt szabványos formátumban javasolt kitölteni. A mező az útlevél, személyi igazolvány, jogosítvány, adószám és más, egyedi azonosítórendszerek alapján kerülhet kitöltésre, az ETSI EN 319 412-1 5.1.3-nak megfelelően.

Ezek szerint, amennyiben nemzeti azonosító kerül feltüntetésre, annak kötelező formátuma: <REF>HU-<igazolványszám>, ahol a <REF> helyére három karakter kerül a következők szerint:

- "PAS" útlevélszám esetében
- "IDC" személyi igazolvány vagy jogosítvány számának esetén
- "TIN" adóazonosító jel esetében

Egyedi azonosítórendszerek esetén szintén javasolt a szabvány szerinti forma használata, ahol a <REF> helyére „XX:” formátumú karaktersorozat kerül, amelyben az „XX” a nemzeti vagy EU-s azonosítási séma két karakteres jelölése.

Amennyiben a további serialnumber mező nem a fenti igazolványok alapján kerül kitöltésre, formai előírás nincs, kivéve a külön tárgyalt eseteket.

3.1.3 Álnevek használata

A szolgáltató természetes személyek részére kiadhat álneves tanúsítványt is. Igénylőnek rendelkeznie kell az Előfizető hozzájárulásával az alkalmazott Álnévhez.

Álneves Tanúsítvány esetén a “Common Name” és "Pseudonym" mezők megegyező módon tartalmazzák az álnevet.

A Szolgáltató az egyes személyeket vagy csoportokat esetlegesen sértő (pl. jóízlést, szemérmet, etnikai hovatartozást sértő) álnevek és egyéb adatok alkalmazását elutasíthatja.

3.1.4 A különböző elnevezési formák értelmezési szabályai

Az azonosítók értelmezése tekintetében az Érintett feleknek a jelen dokumentumban leírtak alapján kell eljárniuk (lásd különösen a 7. fejezetet). A Kibocsátó és Alany megkülönböztető név mezőket (Distinguished Name) az X.500 szabvány és az ASN.1 szintaxis szerint kell értelmezni (lásd RFC 2253 and RFC 2616).

A Szolgáltató által természetes személyek számára kibocsátott tanúsítványoknak nem célja, hogy az Alanyaként megjelölt személyt a tanúsítványban feltüntetett adatok alapján azonosítani lehessen. Természetes személyeknek kiadott olyan tanúsítványok esetén, amelyben jogi személy is megjelenítésre került, nem cél, hogy a természetes személy jogi személlyel való viszonyát vagy képviseleti jogosultságát a tanúsítvány igazolja (hacsak egy kifejezetten erre vonatkozó szabványos jelölési forma nem kerül alkalmazásra).

Amennyiben a tanúsítványban foglalt bármely adat értelmezésével kapcsolatban az Érintett félnek segítségre lenne szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot. A Szolgáltató ilyen esetben az Ügyfél egyéb adatairól többlet tájékoztatást – feltéve, hogy jogszabály ezt nem írja elő – nem adhat, csak a Tanúsítványban feltüntetett adatok értelmezését segítő információkat szolgáltathat.

3.1.5 A nevek egyedisége

A Bizalmi szolgáltató tanúsítványtárában minden Alanynak egyedi névvel (Subject mező) kell rendelkeznie, hogy egyértelműen azonosítható legyen. Ennek érdekében a bizalmi szolgáltató minden személynek egy, a Szolgáltató nyilvántartásában egyedi alanyazonosítót (OID alapú permanentID) ad, melyet köteles szerepeltetni a tanúsítvány Subject/Serialnumber mezőjében (ha az Alany egy személy). Ez az azonosító egyedien azonosítsa a tanúsítványban szereplő természetes személyt vagy annak hiányában a benne szereplő jogi személyt, azonban egy ügyfélnek lehessen több azonosítója is. Ezt az azonosítót soha nem kaphatja meg egy másik természetes vagy jogi személy.

Álneves tanúsítványok esetén az egyediséget szintén biztosítani kell, de az itt alkalmazott alanyazonosítónak különböznie kell az Ügyfél nem álneves tanúsítványok esetén alkalmazott alanyazonosítójától.

A Bizalmi szolgáltató e mellett egy további Subject/Serialnumber mezőben más egyedi azonosítót (pl. személyi igazolvány szám, adószám, szervezeten belüli azonosító) is feltüntethet (lásd 3.1.2).

3.1.6 Védjegyek elismerése, azonosítása, szerepük

A jogi személyek részére kiállított tanúsítványokban feltüntethető az Ügyfél birtokában lévő DBA vagy Trademark vagy terméknév és termékazonosító is.

Ez szerepelhet a Subject/CN mezőben vagy a subjectAltName/dirname mezőben.

Az adatok ellenőrzésére vonatkozó előírásokat lásd a 3.2.2 fejezetben.

3.2 Kezdeti azonosítás

Amennyiben a Szolgáltató még nem ellenőrizte vagy a korábbi ellenőrzése már nem nyújt elegendő biztonságot, akkor jelen kezdeti azonosítási eljárással ellenőriznie kell az Igénylő személyazonosságát, valamint az Előfizető adatait és az azon adatokat, amiket a tanúsítvány Alanyaként fel kíván tüntetni, illetve amelyeket róluk el kíván tárolni. Az ellenőrzéshez hiteles és érvényes hivatalos okmányokat és/vagy megbízható adatbázisokat kell felhasználnia, amelyek kellő biztonsággal igazolják az adatok valódiságát és érvényességét.

Az ellenőrzés lehet teljeskörű (pl. amennyiben az érintett személy még nem ismert Szolgáltató számára) vagy részleges (amennyiben az érintett egyes adatai szorulnak csak újbóli megerősítésre, pl. egyes dokumentumok érvényességének lejárata miatt).

A Szolgáltatási szabályzatnak és Szolgáltató belső eljárásrendjének meg kell határoznia a részletes eljárást.

A bizalmi szolgáltató a tanúsítványba foglalandó adatokat köteles ellenőrizni, így különösen az Alanyként feltüntetésre kerülő (természetes és/vagy jogi) személy azonosságát, a személyazonosság megállapításához használt azonosító adatok valódiságát és - ha elérhető - közhiteles vagy más központi nyilvántartásban foglalt adatokkal való megegyezőségét, az Igénylő eljárási jogosultságát, a tanúsítványba foglalandó képviseleti jog meglétét, a tanúsítvány által igazolt címtartomány (domain) fölötti rendelkezési jogot, a tanúsítványban feltüntetendő IP-cím fölötti rendelkezési jogot, a tanúsítványba foglalandó szervezeti egység létezését, a tanúsítványba foglalandó szabályozott szakma megnevezése esetén az annak gyakorlására való jogosultságot.

Ha a tanúsítvány Alanya természetes vagy jogi személy az ellenőrzés a következő módon valósulhat meg:

[NCP és NCP+
- a természetes személynek vagy a jogi személy képviseletre jogosult képviselőjének személyes jelenléte útján; vagy
- távolról, olyan elektronikus azonosító eszköz használatával, amely tekintetében biztosították a természetes személynek vagy a jogi személy képviseletre jogosult képviselőjének személyes jelenlétét, és amely megfelel a 2015. évi CCXXII. törvény 8. cikkben a „jelentős”, illetve a „magas” biztonsági szintre vonatkozóan meghatározott követelményeknek, vagy
- fokozott biztonságú elektronikus aláírás vagy fokozott biztonságú elektronikus bélyegző a) vagy b) ponttal összhangban kibocsátott tanúsítványával; vagy
- személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerek alkalmazásával, aminek egyenértékűségét megfelelőségértékelő szervezet igazolja.]

]
[LCP és LCP+: Az Igénylő a Szolgáltatónál távolról (pl. elektronikus úton, levélben, faxon) is eljárhat. A Szolgáltatónak ez esetben is egyértelműen azonosítania kell az Igénylő személyét.]

Szolgáltató korlátozhatja az általa elfogadott elektronikus aláírások és bélyegzők körét.

Ha a tanúsítvány Alanya nem természetes személy, a bizalmi szolgáltató legalább az Alany tanúsítványba foglalt teljes nevét és egyedi azonosító adatát ellenőrzi. Ha a tanúsítvány Alanya Magyarországon bejegyzett személy, a Bizalmi szolgáltató ezen adatok valódiságát és hatályosságát közhiteles nyilvántartás tartalma alapján, vagy ha ilyen közhiteles nyilvántartás nincsen, a bejegyzést igazoló közokirat alapján ellenőrzi.

Ha a tanúsítvány Alany nevében a Bizalmi szolgáltató előtt képviselő jár el, vagy a tanúsítvány teljes vagy részleges képviseleti jogot vagy ekként is értelmezhető jogviszonyt is tartalmaz (a továbbiakban együtt: képviseleti jog), a bizalmi szolgáltató köteles a tanúsítvány kibocsátása előtt a képviseleti jog fennállásáról és annak a tanúsítványból kiolvasható tartalmáról jogszabály, közhiteles nyilvántartás, létesítő okirat vagy ezek hiányában meghatalmazás alapján meggyőződni és az ellenőrzés eredményét rögzíteni.

A szolgáltatás igénybevevője Szolgáltató vagy annak munkatársa, Szolgáltatói partnere csak akkor lehet, ha szolgáltató a szabályzatában ezt kifejezetten lehetővé teszi.

A Szolgáltatónak az adatok ellenőrzésére használt információkat (mint pl. dokumentumok típusa, azonosítószáma, érvényességi ideje), valamint az Előfizető eléréséhez szükséges adatokat (pl. postacím, telefonszám) el kell mentenie. Egyéb, az Ügyfél és Igénylő azonosításához és a kapcsolattartáshoz nem szükséges információkat nem tárorlhat (az adatkezeléssel kapcsolatosan lásd 9.3 és 9.4 fejezeteket).

3.2.1 A magánkulcs birtoklásának igazolása

Amennyiben nem a Bizalmi szolgáltató generálja a végfelhasználói kulcspárt, akkor meg kell győződnie arról, hogy a számára átadott nyilvános kulcshoz tartozó magánkulcsot az Ügyfél birtokolja.

Amennyiben a végfelhasználói kulcspárt Szolgáltató generálta, a magánkulcs Átvevőnek történő átadását és Átvevő azonosítását Szolgáltatónak írásban kell rögzítenie, amennyiben Átvevő és Igénylő eltérő személyek, illetve az Igénylés és az Átvétel időben elválik.

3.2.2 Szervezet azonosságának hitelesítése

Amennyiben a tanúsítványban egy jogi személy kerül feltüntetésre (akár a CN, az O vagy OU vagy más mezőkben), akkor a 3.2 szerint azonosítani kell és ellenőrizni kell az adatait, különös tekintettel a tanúsítványban feltüntetendő nevére és címére. Igénylőnek rendelkeznie kell a jogi személy nevében való eljárási jogosultsággal (képviseleti jog vagy képviselő általi felhatalmazás útján). A képviseleti jogot hiteles okmánnyal vagy megbízható adatbázisban ellenőrizni szükséges.

A jogi személy adatainak ellenőrzésére lehetőség szerint közhiteles adatbázist kell felhasználni. Amennyiben ez nem elérhető, akkor felhasználható más megbízható, rendszeresen frisssített adatbázis vagy a személy székhelyének felkeresése. A cím elenőrzésére bankkivonat, közműszámla, hivatalos adózási okmány vagy más dokumentum is felhasználható.

Amenyiben a tanúsítvány Alanyaként egy eszköz, rendszer vagy termék neve, illetve azonosítója vagy DBA / Védjegy vagy más egyedi elnevezés kerül feltüntetésre (önállóan vagy egy természetes vagy jogi személy mellett), akkor a 3.2-ben írtakon túl meg kell győződni arról, hogy az Ügyfél jogosan birtokolja a nevet és azonosítót, s az nem megtévesztő (amennyiben ezek értelmezhetőek). Az ellenőrzésnek hivatalos dokumentumon, megbízható adatforráson, az azonosítót kezelő hivatalos szervvel való egyeztetésen vagy más megbízható adatforráson kell alapulnia, amely igazolja a névhasználat jogosságát.

Ilyen esetben, amennyiben az Alany adataként ország is megnevezésre kerül, s a mögötte álló természetes vagy jogi személy nem ismert, akkor a szolgáltatónak az országot az eszközhöz tartozó domain név vagy IP cím szerint kell ellenőriznie.

[PTC]
Amennyiben a tanúsítvány Alanyaként (Subject vagy SAN mezők) domain név vagy IP cím kerül feltüntetésre, a Szolgáltatónak ellenőriznie kell, hogy Előfizető a domain név / IP cím felett kontrollal bír.
Amennyiben a domain név wildcard karaktert tartalmaz, akkor az Előfizetői kontrollnak a teljes wildcard feletti domain névre ki kell terjednie. Különös körültekintéssel kell eljárni olyan esetekben, ahol a wildcard közös használatú domain nevekre vonatkozik.
Amennyiben Előfizető nem kontrollálja egyedül a domain nevet, akkor a tanúsítvány kiállítását vissza kell utasítani.

Mielőtt Szolgáltató bármilyen adatforrást megbízható adatforrásként kezd el alkalmazni, értékelnie kell annak megbízhatóságát, pontosságát, és a módosításnak vagy hamisításnak való ellenállását. Szolgáltatónak figyelembe kell venni a következőket az értékelése során:

1. A biztosított információk származási ideje,
2. Az információforrás frissítési gyakorisága,
3. Az adatszolgáltató és az adatgyűjtés célja,
4. Az adatok nyilvános elérhetősége,
5. Az adatok meghamisításának vagy megváltoztatásának relatív nehézsége.

Szolgáltató (vagy tulajdonosa, leányvállalata) által fenntartott adatbázis nem minősül megbízható adatforrásnak, ha az elsődleges célja a 3.2 fejezet szerinti hitelesítési követelmények teljesítése céljából való információgyűjtés.

3.2.3 Természetes személy azonosságának hitelesítése

Amennyiben a tanúsítványban egy természetes személy kerül feltüntetésre, akkor a 3.2 szerint azonosítani kell és ellenőrizni kell az adatait, különös tekintettel az egyértelmű személyazonosító adataira (pl. név, születési adatok, anyja neve).

Amennyiben a természetes személy egy jogi személlyel együtt kerül a tanúsítványban feltüntetésre, akkor a jogi személy képviselőjének hiteles igazolása szükséges a természetes személy szerepeltetéséhez (lásd 3.2.2).

Az eljárásban részt vevő természetes személyek azonosságát személyes megjelenés vagy kapcsolat esetén hivatalos személyazonosító okmány fényképe alapján ellenőrizni kell.

Az Ügyfél, Igénylő és Átvevő által biztosított adatok valódiságát (kézi vagy elektronikus) aláírásukkal el kell ismerniük. Az elfogadott elektronikus aláírások körét Szolgáltató korlátozhatja. Az Ügyfél, Igénylő és Átvevő nyilatkozatain szereplő aláírások valódiságát szolgáltatónak ellenőriznie kell, kézi aláírások esetén hivatalos személyazonosító okmányon szereplő vagy személyesen felvett aláírásminta alapján.

A szolgáltató a tanúsítványban feltüntetésre kerülő természetes személy Alany személyazonosságát az Nytv. hatálya alá tartozó természetes személyek esetében ezt az Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolvány alapján kell elvégezze. Egyúttal köteles a személyazonosság igazolására használt hatósági igazolvány érvényességét és az igazolványban foglalt adatok egyezését a megfelelő közhiteles hatósági nyilvántartásban is ellenőrizni.

Az Nytv. hatálya alá nem tartozó természetes személy esetén a személyazonosságot elsősorban az Szmtv. és a Harmtv. szerinti úti okmány alapján kell ellenőrzni. A személyazonosság megállapítására használt okmány érvényességét (hitelességét), valamint az abban használt adatok és a rájuk vonatkozó központi nyilvántartás egyezőségét ellenőrizni kell. Ha ilyen nyilvántartás nem érhető el, a bizalmi szolgáltató számára nem hozzáférhető vagy a hozzáférés és ellenőrzés költsége aránytalanul magas, a bizalmi szolgáltató ezt a tényt rögzíti, és az egyéb rendelkezésére álló bizonyítékok alapján dönthet arról, hogy az adott tanúsítványt Ügyfél részére kibocsátja-e.

3.2.4 Nem ellenőrzött alany információk

A Bizalmi szolgáltató által kibocsátott Tanúsítvány Alanyaként csak olyan adatok kerülhetnek feltüntetésre, amelyeket a Szolgáltató ellenőrzött, vagy amelyek valódiságáról az Előfizető írásban, büntetőjogi felelősségének tudatában nyilatkozott.

3.2.5 Jogok, felhatalmazások ellenőrzése

Amennyiben Előfizető nem a saját nevében jár el Szolgáltató előtt (pl. Igénylőként vagy Átvevőként), hanem meghatalmazotton keresztül, akkor Szolgáltatónak minden esetben egyértelműen azonosítania kell a meghatalmazott személyét (lásd 3.2.2) és ellenőriznie kell az Előfizető nevében történő eljárási jogosultságát a Szolgáltató előtt, az adott eljárás (pl. tanúsítványigénylés, felfüggesztés, visszaállítás és visszavonás) kapcsán. Jogi személy nevében csak a képviseletre jogosult adhat meghatlamazást képvisletre.

A meghatalmazás hitelességét (lásd 3.2.2) és érvényességét ellenőrizni szükséges. Meghatározott időre adott meghatalmazások esetén minden felhasználás esetén ellenőrizni kell a lejárati időpont meg nem haladását, valamint (jogi személyek esetén) a meghatalmazó képviseleti jogának fennálását.

3.2.6 Együttműködési képességre vonatkozó követelmények

A Bizalmi szolgáltató a szolgáltatásnyújtása során együttműködhet más bizalmi szolgáltatókkal, akik magukra kötelező érvényűnek ismerik el jelen Hitelesítési rend követelményeinek betartását.

A Bizalmi szolgáltatónak közzé kell tennie minden kereszthitelesített tanúsítványt, amely Alanyaként vagy kibocsátójaként szerepel.

3.3 Azonosítás és hitelesítés tanúsítványkezelési eljárás igénylése esetén

Olyan eljárás esetén, ami új tanúsítvány kibocsátását eredményezi az Igénylőt legalább fokozott biztonságú érvényes elektronikus aláírásával vagy felhasználóneve és jelszava

megadásával vagy a 3.2 fejezetben ismertetett Kezdeti azonosítási eljárás szerint kell azonosítania Szolgáltatónak.

Amennyiben az igénylés új aláíró vagy bélyegző nyilvános kulcsot tartalmaz, akkor az Igénylésnek tartalmaznia kell annak bizonyítékát is, hogy a nyilvános kulcs magánkulcs párját a Végfelhasználó birtokolja (pl. aláíró kulccsal történő aláírást).

[DVCP, OVCP, IVCP: Amennyiben Ügyfél vagy Igénylő valamely dokumentuma (ami alapján a tanúsítványba vagy Szolgáltató belső nyilvántartásába került valamely adata, illetve ami alapján azonosítva lett) 39 hónapnál korábban lett ellenőrizve, akkor azt a Szolgáltatónak újra kell ellenőriznie.]

3.3.1 Azonosítás és hitelesítés érvényes tanúsítvány esetén

A még érvényes Tanúsítványra vonatkozó, ahhoz tartozó nem kompromittálódott magánkulccsal aláírt érvényes igényléseket további ellenőrzés nélkül automatikusan elfogadhatja a Bizalmi szolgáltató.

3.3.2 Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Lásd a 3.3 szerinti előírást.

3.4 Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási igénylés esetén

A szolgáltató a visszavonással vagy felfüggesztéssel érintett tanúsítvánnyal aláírt kérelmet nem fogadhat el.

Olyan eljárás esetén, ami a tanúsítvány állapotát megváltoztatja, de új tanúsítvány kibocsátását nem eredményezi az Igénylőt legalább egy kódszóval vagy felhasználóneve és jelszava megadásával kell azonosítani.

4 Tanúsítvány életciklus követelmények

A Bizalmi szolgáltató a Szolgáltatási szabályzatában korlátozhatja a tanúsítvány megújítás, kulcscsere és tanúsítványmódosítás szolgáltatásokkal támogatott tanúsítványtípusok körét.

4.1 Tanúsítványigénylés

Új tanúsítvány kiadásához Igénylőnek Tanúsítványigénylést kell benyújtani Szolgáltató felé. A Tanúsítványigénylés alapján a Bizalmi szolgáltatónak el kell készíteni az Alannyal és Előfizetővel kötendő szolgáltatási szerződést, amit saját vagy képviselője aláírásával hitelesítve el kell juttatni a Szolgáltató számára. A szerződésnek tartalmaznia kell az Igénylő és Előfizető nyilatkozatát arra vonatkozóan, hogy kötelezettségeiket megismerték és azok betartását vállalják. Szolgáltatónak a szerződést nem kell aláírni, a szerződés elfogadását az érintett tanúsítvány kibocsátásával jelzi.

A Bizalmi szolgáltató köteles a szeződést a tanúsítánnyal kapcsolatos adatokkal együtt megőrizni.

A Bizalmi szolgáltatónak a szolgáltatási szerződés megkötését megelőzően tájékoztatnia kell Igénylőt a szolgáltatás nem minősített voltáról, a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről, valamint a kapcsolódó jogszabályokról. A tájékoztatást és a hozzá tartozó dokumentumokat honlapján meg kell jelenítse elektronikusan aláírt formában, valamint a szerződéskötést követően tartós adathordozón elérhetővé kell tennie a szolgáltatási szerződést, a hitelesítési rendet és a szolgáltatási szabályzatot.

4.1.1 Ki nyújthat be tanúsítványigénylést?

Tanúsítványigénylést a Szolgáltató rendszerében regisztrált Igénylők tudnak benyújtani. Amennyiben az Igénylő nem a saját nevében jár el, akkor Előfizető felhatalmazásával kell bírnia.

Szolgáltató kockázatlistát kezelhet azon személyekről, akik esetében a tanúsítványigényléssel kapcsolatos kockázatokat tart nyilván, valamint külső adatforrásokat is felhasználhat kockázatértékeléshez. Szolgáltató a kockázatértékelés alapján visszautasíthatja a tanúsítványigényléseket.

4.1.2 Az igénylés folyamata és a résztvevők felelőssége

Bizalmi szolgáltatónak a 3. fejezetben írtak szerint meg kell győződnie Igénylő személyazonosságáról, eljárási jogáról, valamint az Igénylésben szereplő adatok megfelelőségéről.

Igénylő és Ügyfél adjon meg minden szükséges információt az azonosítási és ellenőrzési eljárások lefolytatásához. A Bizalmi szolgáltatónak nyilvántartásba kell vennie az Igénylő és Ügyfél azonosságára vonatkozó, a szolgáltatás nyújtásához és a kapcsolattartáshoz szükséges minden információt, valamint az Igénylő által aláírt szolgáltatási szerződést.

A nyilvántartásba vett adatokat meg kell őrizni legalább a hatályos jogszabályokban előírt időtartamig.

A szolgáltatási szerződésnek tartalmaznia kell a következőket:

- Igénylő nyilatkozatát arról, hogy a tanúsítványigénylésben megadott adatok teljesek és pontosak;
- Azt, hogy hozzájárul-e a Tanúsítvány közzétételéhez;
- Nyilatkozatát arról, hogy a Tanúsítványban feltüntett adatok jogos felhasználója, s azok más érdekeit nem sértik.

4.2 Tanúsítványigénylések feldolgozása

4.2.1 Azonosítás és hitelesítés

Lásd a 3.2 fejezetet.

Az Azonosítási és hitelesítési feladatokat végrehajthatja a Szolgáltató vagy a Szolgáltató megbízásából eljáró, a Szolgáltató szabályzata szerint működő Regisztrációs Egység. Szolgáltatónak a Regisztrációs Egységet megbízható módon hitelesíteni kell.

A tanúsítványigénylésnek tartalmaznia kell az összes tanúsítványban megjelenő Alany információt, valamint az összes további információt, amire Szolgáltatónak szükséges van annak érdekében, hogy szabályzatainak megfelelően tudja kiadni a tanúsítványt. Abban az esetben, ha a tanúsítványigénylés nem tartalmazza az összes szükséges információt Szolgáltatónak be kell szerezni a hiányzó adatokat az Igénylőtől vagy megbízható, független forrásból, amelyeket Igényőnek meg kell erősíteni.

Szolgáltatónak dokumentált folyamatot kell létrehozni és követni minden a tanúsítványba foglalandó adat ellenőrzésére, továbbá a kiemelt kockázatú tanúsítványkérelmek azonosítására és kiegészítő ellenőrzési eljárására.

[PTC: A tanúsítványigénylésnek tartalmaznia kell legalább egy FQDN-t vagy IP-cím-et, ami a tanúsítvány subjectAltName kiterjesztésébe foglalandó.]

4.2.2 Tanúsítványigénylések elfogadása vagy visszautasítása

A Bizalmi szolgáltatónak vissza kell utasítani azon Tanúsítványigényléseket, amelyek megfelelőségét nem tudja teljeskörűen ellenőrizni.
A Bizalmi szolgáltató saját hatáskörében, külön indoklás nélkül dönthet az igényelt Tanúsítvány kiadásának megtagadásáról, melyről tájékoztatja Igénylőt.

[PTC: Szolgáltatónak vissza kell utasítani azon Tanúsítványigényléseket, amelyek olyan gTLD-khez tartoznak, amelyeket az ICANN megfontolás alatti fázisban tart.]

4.2.3 A tanúsítványigénylés feldolgozásának időtartama

A Bizalmi szolgáltatónak a Szolgáltatási szabályzatban meg kell határoznia, hogy milyen határidőn belül vállalja az elfogadott Tanúsítványigénylések feldolgozását.

4.3 Tanúsítvány kibocsátása

A Bizalmi szolgáltató csak a Tanúsítványigénylés elfogadása után állíthatja ki a Tanúsítványt. A tanúsítványkibocsátási eljárásnak biztonságosan kell kötődnie a regisztrációs, igénylési és életciklus menedzsment eljárásokhoz, beleértve az Ügyfél vagy a Szolgáltató által generált nyilvános kulcs alkalmazását. A kiállított Tanúsítvány csak az Tanúsítványigénylésben megadott és az elbírálás során a Bizalmi szolgáltató által ellenőrzött adatokat tartalmazhat.

A Gyökér hitelesítő egység általi tanúsítványkibocsátás
A Gyökér hitelesítő egység által történő tanúsítványkibocsátás csak a szolgáltatási szabályzat által felhatalmazott szolgáltatói munkatársak két személyes kontrolljával valósulhat meg.

4.3.1 A Bizalmi szolgáltató tevékenysége a tanúsítvány kibocsátás során

A Szolgáltatónak biztosítani kell a tanúsítványok kibocsátásának biztonságát, megakadályozva a tanúsítványok hamisíthatóságát.

A gyökér hitelesítő egység által történő tanúsítványok kibocsátását egy, a Szolgáltató által felhatalmazott természetes személynek kell kezdeményezni.

4.3.2 Értesítés a tanúsítvány kibocsátásáról

A Bizalmi szolgáltató a Tanúsítvány kibocsátásáról értesítse a Végfelhasználót a tanúsítványban megjelölt vagy külön felvett email címen, és tegye lehetővé számára a Tanúsítvány átvételét.

4.4 Tanúsítvány elfogadása

4.4.1 A tanúsítványelfogadás módja

A Szolgáltató által kiállított tanúsítványok tartalmát az Ügyfélnek ellenőrizni kell és el kell azokat fogadnia az első használatot megelőzően. Hibás tanúsítványt az Ügyfélnek - megfelelő indoklással - vissza kell utasítania és annak (illetve a hozzá tartozó magánkulcsnak) a használatát nem szabad megkezdenie. Az elfogadás megvalósulhat direkt és indirekt módon egyaránt.

4.4.2 A tanúsítvány közzététele

Előfizető vagy Igénylő hozzájárulása esetén a kiállított tanúsítványt a szolgáltató köteles nyilvánosságra hozni a nyilvános tanúsítványtárán keresztül.

4.4.3 További szereplők értesítése a tanúsítvány kibocsátásról

Nincs kikötés.

4.5 Kulcspár és tanúsítvány alkalmazhatósága

4.5.1 A magánkulcs és a tanúsítvány használata

Az Végfelhasználó

- a tanúsítványához tartozó magánkulcsát kizárólag a tanúsítványban jelölt felhasználási célnak megfelelően használhatja fel ("kulcshasználat" és "kiterjesztett kulcshasználat" mezők szerint);
- [NCP+: a magánkulcsot kizárólag az Ügyféleszközön alkalmazza]
- lejárt érvényességű, visszavont, vagy felfüggesztett tanúsítványhoz tartozó magánkulcsot nem használhat fel;
- köteles gondoskodni magánkulcsának és az aktiváló adatának megfelelő védelméről, elkerülve azok illetéktelen használatát;
- amenyiben a magánkulcsról másolatot készít, akkor azt ugyanolyan gondossággal kell kezelje, mint az eredeti példányt;
- azonnal értesíti a szolgáltatót, amennyiben az aláíbbi esetek valamelyike bekövetkezik a tanúsítvány érvényességének vége előtt, s egyúttal azonnal beszünteti a magánkulcs alkalmazását, kivéve az adatvisszafejtés műveletet:
    - a magánkulcs elvesztése, ellopása, kompromittálódása,
    - a magánkulcs feletti kizáírólagos kontroll elvesztése, pl. az aktiviálási adat kompromittálódása miatt,
    - a tanúsítványban feltüntetett adatok pontatlansága vagy változása;
- a szolgáltatói kulcs kompromittálódása esetén beszünteti a magánkulcs és a tanúsítvány alkalmazását;
- a magánkulcshoz tartozó tanúsítvány érvényessége végén vagy visszavonása esetén a magánkulcsot, s annak bármilyen másolatát visszaállíthatatan módon törli.

A magánkulcs a Végfellhasználó kizárólagos befolyása alatt kell álljon.

A használat során be kell tartani az 1.4. fejezetben leírt korlátozásokat.

4.5.2 Az Érintett felek nyilvános kulcs és tanúsítvány használata

A Szolgáltatónak a szolgáltatási szabályzatában közzé kell tennie azokat az eljárásokat és feltételeket, amelyek követésével és betartásával az Érintett Felek megbízhatnak a tanúsítványokban.

4.6 Tanúsítványmegújítás

Szolgáltatónak a tanúsítványok egyszerűsített kiadása érdekében Tanúsítványmegújítási szolgáltatást kell nyújtania.

Tanúsítványmegújítást a Bizalmi szolgáltató saját hatáskörben is végrehajthat, valamint az Ügyfél is kezdeményezheti. Az Ügyfél jogosult tanúsítványa megújítását igényelni, amennyiben annak lejárata 30 napon belül esedékes.

4.6.1 A tanúsítványmegújítás körülményei

Az eljárás - Ügyfél igénylése esetén - egy az eljárásra vonatkozó igény Bizalmi szolgáltatóhoz történő beérkezésével kezdődő és egy új végfelhasználói tanúsítvány kibocsátásával, illetve nem megfelelő igénylés esetén az igénylés visszautasításával záródó folyamat.

Amennyiben a Szolgáltató az új tanúsítványt eltérő szabályzatok szerint vagy eltérő kiadóval adja ki, mint amivel az eredeti tanúsítvány készült, akkor intézkedni kell, hogy minden új vagy szigorúbb elvárásnak is megfeleljen az újonnan kiadott tanúsítvány.

A megújított tanúsítvány kibocsátásakor a Bizalmi szolgáltatónak a kezdeti tanúsítványkibocsátás során alkalmazott módon kell eljárnia a Tanúsítvány előállítása, közzététele, az Ügyfél és az érintettek értesítése során.

Az új tanúsítvány kiadását követően a Bizalmi szolgáltató az eredeti tanúsítványt visszavonhatja, az eljárás idejére az eredeti tanúsítványt felfüggesztheti.

4.6.2 Ki igényelheti a tanúsítványmegújítást?

A Tanúsítványmegújítás a Tanúsítványigénylés benyújtásával igényelhető a Szolgáltatónál. Az igénylésre az jogosult, aki a kezdeti tanúsítványigénylésre is jogosult. Az igénylés teljesítését megelőzően az Igénylőt azonosítani kell a 3.3. fejezetben megadottak szerint és tájékoztatni kell a Tanúsítvány használatával kapcsolatos kikötésekről és feltételekről, amiket el kell fogadnia.

A tanúsítvány megújítási igénylésben a Igénylőnek nyilatkoznia kell, hogy a Tanúsítványban szereplő adatok még érvényben vannak.

4.6.3 A tanúsítványmegújítási igénylések feldolgozása

A Bizalmi szolgáltatónak meg kell győződni az Ügyfél által benyújtott Tanúsítványigénylés feldolgozásakor, hogy

- a benyújtott igénylés hiteles (elektronikusan aláírt igénylés esetén érvényes aláírással rendelkezik);
- Igénylő jogosult igénylés benyújtására az Előfizető nevében (kivéve ha az érintett tanúsítványhoz tartozó magánkulccsal van aláírva az igénylés);
- az igénylés teljes (minden kötelező adata kitöltött) és hibátlan;
- az érintett tanúsítvány egyértelműen azonosítható;
- az aktuálisan elérhető információk alapján a kiadandó Tanúsítvány tervezett érvényessége alatt a felhasznált kriptográfiai algoritmusok még használhatók lesznek;
- a tanúsítvány még érvényes (nem járt le, nincs felfüggesztve vagy visszavonva);
- a tanúsítványhoz tartozó magánkulcs nem kompromittálódott (ügyfélnyilatkozat);
- a tanúsítvány igénylése során az adatok ellenőrzésére használt dokumentumok még érvényesek;
- a szolgáltatási szerződés még hatályos;
- a művelet végrehajtható.

Amennyiben a fenti elvárások nem teljesülnek, akkor az igénylést a Szolgáltatónak vissza kell utasítania, az Ügyfél pedig a kezdeti tanúsítványigénylési eljárásban tud új tanúsítványt igényelni.

A szolgáltató korlátozhatja az ugyanazon tanúsítványra vonatkozó megújítások számát, illetve további elvárásokat határozhat meg a megújítás feltételeként.

4.6.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A 4.3.2 fejezet alkalmazandó.

4.6.5 A megújított tanúsítvány elfogadása

A 4.4.1 fejezet alkalmazandó.

4.6.6 A megújított tanúsítvány közzététele

A 4.4.2 fejezet alkalmazandó.

4.6.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A 4.4.3 fejezet alkalmazandó.

4.7 Kulcscsere

Szolgáltatónak a tanúsítványok érvényességi idején belül történő alkalmazhatósága érdekében Kulcscsere szolgáltatást kell nyújtania.

Kulcscserét a Bizalmi szolgáltató saját hatáskörben is végrehajthat, valamint az Ügyfél indoklás nélkül is kezdeményezheti. A Szolgáltatónak hivatalból kell kezdeményeznie a kulcscserét, amennyiben a tanúsítványban szereplő nyilvános kulcs nem felel meg a hatályos jogszabályi követelményeknek, az irányadó szabványleírásoknak vagy a Bizalmi

Felügyelet vonatkozó hatályos határozatának.Kulcscserére sor kerülhet érvényes és érvénytelen (pl. kulcskompromittálódás miatt visszavonásra került) Tanúsítvány esetén egyaránt.

A kulcscsere során kiállított új Tanúsítványban a Végfelhasználó nyilvános kulcsa mellett változnak (például tanúsítvány sorozatszám és érvényességi idő), illetve opcionálisan változhatnak további adatok is (például egyes Szolgáltatói adatok, mint az CRL és OCSP hivatkozások vagy a Tanúsítvány aláírására használt szolgáltatói kulcs), de az Ügyfél a kulcson kívül nem igényelheti más adat módosítását.

Lásd a 6.2.3 fejezetet, valamint a szolgáltatói kulcsok cseréjével kapcsolatosan az 5.6 fejezetet.

4.7.1 A kulcscsere körülményei

A 4.6.1 fejezet alkalmazandó.

4.7.2 Ki igényelheti a kulcscserét

A 4.6.2 fejezet alkalmazandó.

4.7.3 A kulcscsere igénylések feldolgozása

A 4.6.3 fejezet alkalmazandó, azzal a különbséggel, hogy az érintett tanúsítvány érvényessége, illetve a hozzá tartozó magánkulcs kompromittálódás-mentessége nem elvárás (kivéve ha az igénylés azzal lett aláírva).

Amennyiben a Bizalmi szolgáltatónak a kulcscsere eljárás során jut tudomására, hogy a kulcs kompromittálódott, akkor azonnal intézkednie kell annak visszavonásáról, és ennek megfelelően elbírálni az igénylést.

4.7.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A 4.6.4 fejezet alkalmazandó.

4.7.5 A kulcscserével megújított tanúsítvány elfogadása

A 4.6.5 fejezet alkalmazandó.

4.7.6 A kulcscserével megújított tanúsítvány közzététele

A 4.6.6 fejezet alkalmazandó.

4.7.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A 4.6.7 fejezet alkalmazandó.

4.8 Tanúsítványmódosítás

Szolgáltatónak a tanúsítványok folyamatosan hiteles adattartalma és alkalmazhatósága érdekében tanúsítványmódosítási szolgáltatást kell nyújtania.

Tanúsítványmódosítást a Bizalmi szolgáltató saját hatáskörben is végrehajthat, valamint az Ügyfél is kezdeményezheti.

A Bizalmi szolgáltatónak hivatalból kell kezdeményeznie a Tanúsítványmódosítást, amennyiben tudomására jut a Tanúsítványban szereplő adatokban bekövetkezett valamilyen változás, beleértve a Tanúsítványban szereplő valamely saját adatainak vagy bármely más tanúsítványadat megváltozását (pl. jogszabály-, szabvány- vagy szabályzatváltozás következtében). A Bizalmi szolgáltató jogosult a végfelhasználói tanúsítványok kulcscseréjére, ha a Tanúsítványkibocsátásához használt szolgáltatói aláíró kulcsát le kell cserélnie.

A tanúsítványmódosítást az Ügyfél akkor igényelheti, ha a tanúsítványban szereplő adatai megváltoznak.

4.8.1 A tanúsítványmódosítás körülményei

A 4.6.1 fejezet alkalmazandó.

4.8.2 Ki igényelheti a tanúsítványmódosítást

A 4.6.2 fejezet alkalmazandó, azzal a különbséggel, hogy az Alany adatok változatlan voltáról szóló nyilatkozat értelemszerűen nem vonatkozik a megváltozott adatokra.

4.8.3 A tanúsítványmódosítási igénylések feldolgozása

A 4.6.3 fejezet alkalmazandó.

A Bizalmi szolgáltatónak az új Alany adatok valódiságának ellenőrzése során a 3.2 fejezetben ismertetett Kezdeti azonosítási eljárás szerint kell eljárnia.

4.8.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A 4.6.4 fejezet alkalmazandó.

4.8.5 A módosított tanúsítvány elfogadása

A 4.6.5 fejezet alkalmazandó.

4.8.6 A módosított tanúsítvány közzététele

A 4.6.6 fejezet alkalmazandó.

4.8.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A 4.6.7 fejezet alkalmazandó.

4.9 Visszavonás és felfüggesztés

A Bizalmi szolgáltatónak az általa bizalmi szolgáltatás keretében kibocsátott tanúsítványok érvényességének kezelésére Állapotváltoztatási (tanúsítvány-visszavonási, -felfüggesztési és -aktiválási) szolgáltatásokat kell nyújtania. E műveleteket a Bizalmi szolgáltató saját hatáskörben is végrehajthatja, valamint az Ügyfél és Bíróság vagy hatóság is

kezdeményezheti. Az Ügyféligények fogadására a Bizalmi szolgáltatónak folyamatos (7*24 órás) lehetőséget kell biztosítani.

4.9.1 A visszavonást és a felfüggesztést indukáló körülmények

A végfelhasználói tanúsítványok visszavonását vagy felfüggesztését az alábbi körülmények indukálhatják. Az alábbi esetekben a Szolgáltatónak az Igény beérkezését követő legfeljebb 24 órán belül vissza kell vonnia vagy fel kell függesztenie a tanúsítványt:

- Ügyfél szabályos igénylése (Állapotváltoztatási ügyféligény);
- Ügyfél jelzi a szolgáltatónak, hogy az eredeti tanúsítványigénylés nem volt engedélyezett és azt utólag sem engedélyezi;
- Ügyfél kötelezettségeinek be nem tartása;
- a szolgáltató szabályzatai és az ÁSZF által meghatározott egyéb körülmény;
- a tanúsítványban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódása;
- a tanúsítványt hitelesítő szolgáltatói magánkulcs kompromittálódása;
- a tanúsítvány megújítása, módosítása vagy kulcscseréje;
- jogszerűtlen név- vagy adathasználat,
- a tanúsítványban hibásan rögzített adatok vagy az adatok valótlansága, megváltozása, félrevezetésre alkalmassága;
- Ügyfél nem kérte a tanúsítvány aktiválását a felfüggesztési időn belül;
- a tanúsítvány rosszhiszemű felhasználása;
- bíróság vagy hatóság erre vonatkozó jogerős és végrehajtható határozata;
- a tanúsítvány műszaki jellemzői a mértékadó szakmai ajánlások alapján az elfogadhatónál nagyobb kockázatot jelentenek bármely félnek (pl. kulcshossz ajánlottnál kisebb mérete);
- a szolgáltatási szerződés megszegése vagy megszűnése;
- a tanúsítvány nem a vonatkozó szabályzatok szerint lett kibocsátva;
- a szolgáltató tudomására jut, hogy a tanúsítványban szereplő valamely név (pl. FQDN) használatára az Ügyfél nem jogosult;
- a szolgáltató tudomására jut a tanúsítványban feltüntetett képviseleti jogosultság megszűnése;
- amennyiben a tanúsítványra vonatkozó érvényességi információs szolgáltatások fenntartása megszűnik;
- a bizalmi szolgáltatás megszűnése, kivéve, ha a Szolgáltató korábban gondoskodott az általa kibocsátott tanúsítványok vonatkozásában a CRL és OCSP szolgáltatások fenntartásáról;
- jogszabály teszi kötelezővé.

A tanúsítványok felfüggesztésének lehetséges okai:

- a tanúsítvány kiadását követő kezdeti felfüggesztés a szállítás biztonságának növelésére;
- a tanúsítvány visszavonását indukáló bármely körülményre vonatkozó alapos vélelem.

A Szolgáltató legfeljebb 7 napon belül köteles intézkedni a köztes hitelesítő egység tanúsítványának visszavonásáról az alábbi esetekben:

- a köztes hitelesítő egység szabályos, írásbeli igénylése (Állapotváltoztatási ügyféligény);

- a köztes hitelesítő egység jelzi a szolgáltatónak, hogy az eredeti tanúsítványigénylés nem volt hiteles és azt utólag sem hitelesíti, illetve engedélyezi;
- a tanúsítványban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódása;
- a tanúsítványt hitelesítő szolgáltatói magánkulcs kompromittálódása;
- a tanúsítvány rosszhiszemű felhasználása;
- a tanúsítványban hibásan rögzített adatok vagy az adatok valótlansága, megváltozása, félrevezetésre alkalmassága;
- amennyiben a tanúsítványra vonatkozó érvényességi információs szolgáltatások fenntartása megszűnik;
- a tanúsítvány műszaki jellemzői a mértékadó szakmai ajánlások alapján az elfogadhatónál nagyobb kockázatot jelentenek bármely félnek (pl. kulcshossz ajánlottnál kisebb mérete);
- bíróság vagy hatóság erre vonatkozó jogerős és végrehajtható határozata;
- a bizalmi szolgáltatás megszűnése;
- jogszabály teszi kötelezővé;
- a szolgáltató szabályzatai által meghatározott egyéb körülmény.

4.9.2 Állapotváltoztatási ügyféligényre jogosultak

A tanúsítványokra vonatkozó állapotváltozási igény benyújtására az alábbi felek jogosultak:

- Ügyfél;
- Regisztrációs egység;
- Szolgáltató;
- ésszerű ok esetén bármely harmadik fél.

4.9.3 A visszavonási, felfüggesztési és aktiválási eljárás

A Bizalmi szolgáltatónak lehetőséget kell biztosítania az Ügyfelek számára a végfelhasználói tanúsítványok visszavonására illetve felfüggesztésére. A Szolgáltató szabályzatainak tartalmaznia kell a visszavonási, felfüggesztési és a aktiválási folyamat leírását, a tanúsítványállapot-változtatási igénylésére pedig folyamatos (7x24) lehetőséget kell biztosítania.

A Szolgáltató online tájékoztatja az Ügyfeleket a magánkulcs kompromittálódására, Tanúsítvánnyal való visszaélésre vagy más típusú csalásokra vonatkozó feltételezések bejelentésének módjáról.

A visszavonás vagy felfüggesztés vonatkozhat egy végfelhasználói tanúsítványra vagy a szolgáltató valamely köztes hitelesítő egységére.

A Bizalmi szolgáltató nem vonhat vissza vagy függeszthet fel egy tanúsítványt a visszavonás vagy felfüggesztés közzétételét megelőző időre.

A Bizalmi szolgáltató a szabályzataiban vagy szolgáltatási szerződésben rendelkezik a tanúsítvány eredeti érvényességének lejárta előtti visszavonásának illetve felfüggesztésének jogkövetkezményeiről.

A tanúsítvány új státuszának az intézkedést követően haladéktalanul be kell kerülnie a tanúsítványtárba (ún. tanúsítványállapot-adatbázisba), ezzel lehetővé téve a valós idejű

tanúsítványállapot-ellenőrzést. A végfelhasználói tanúsítvány visszavonását vagy felfüggesztését követő legkésőbb 1 órán belül új visszavonási lista (CRL) kiadására is sor kerül, mely ugyancsak tartalmazza a tanúsítvány megváltozott státuszát.

A Bizalmi szolgáltató valamely hitelesítő egysége magánkulcsának kompromittálódása esetén tegyen meg minden ésszerű erőfeszítést annak érdekében, hogy az eseményről értesítse az Érintett feleket. A szolgáltatói tanúsítványok állapotváltozását hozza nyilvánosságra a honlapján.

4.9.4 Az igénylések feldolgozása

A Bizalmi Szolgáltatónak a tanúsítványállapot-igények feldolgozását átvételük után azonnal el kell kezdenie.

A Bizalmi szolgáltatónak meg kell győződni az Állapotváltoztatási ügyféligény feldolgozásakor, hogy

- a benyújtott igénylés hiteles (elektronikusan aláírt igénylés esetén érvényes aláírással rendelkezik, kivéve ha az érintett tanúsítványhoz tartozó magánkulccsal van aláírva az igénylés);
- Igénylő jogosult igénylés benyújtására az Előfizető nevében;
- az igénylés teljes (minden kötelező adata kitöltött) és hibátlan;
- az érintett tanúsítvány egyértelműen azonosítható;
- a művelet végrehajtható.

Az igénylésre való jogosultság ellenőrzése a *3.4. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási igénylés esetén* fejezetben leírtak szerint történik hiteles forrásból.

Amennyiben a fenti elvárások nem teljesülnek, akkor az igénylést a Szolgáltatónak vissza kell utasítania, egyébként további mérlegelés nélkül intézkednie kell a tanúsítvány visszavonása, felfüggesztése vagy aktiválása érdekében.

A Bizalmi szolgáltató minden végrehajtott és visszautasított felfüggesztési, visszavonási és tanúsítványaktiválási igénylésről e-mailben értesíti az Igénylőt és az Előfizetőt.

4.9.5 Állapotváltozási igények feldolgozásának maximális ideje

Visszavonás vagy felfüggesztés esetén az igény végrehajtását követően a tanúsítvány visszavont vagy felfüggesztett státusza haladéktalanul bekerül a tanúsítványtárba, valamint az igénylést követő legkésőbb 1 órán belül új visszavonási lista (CRL) kiadására is sor kerül, melyen a tanúsítvány státusza

- felfüggesztés esetén “suspended”;
- visszavonás esetén ”revoked” lesz.

Az igényléseket soron kívül a lehető leghamarabb, legkésőbb a beérkezésüket követő 24 órán belül kell elbírálnia.

Visszavonási igényt a visszavonást indukáló körülmény vélelemének tisztázása céljából a Szolgáltató ideiglenesen a tanúsítvány felfüggesztésével is kezelheti.

Felfüggesztett állapotú tanúsítványra vonatkozó aktiválási igény esetén esetén, amennyiben a Bizalmi szolgáltató meggyőződött arról, hogy a felfüggesztést indukáló körülmények megszűntek, az aktiválási igényt haladéktalanul végrehajtja és a tanúsítvány érvényes státusza haladéktalanul bekerül a tanúsítványtárba, valamint az aktiválási igénylést követő legkésőbb 1 órán belül új visszavonási lista (CRL) kiadására is sor kerül, melyen a tanúsítvány már nem szerepel.

4.9.6 Javasolt eljárás az tanúsítványállapot ellenőrzésére

A Tanúsítványban foglalt információk elfogadását és felhasználását megelőzően a Bizalmi szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az Érintett felek megfelelően gondosan járjanak el, így különösen javasolt ellenőrizniük a tanúsítási láncban található valamennyi Tanúsítvány érvényességét a vonatkozó műszaki szabványoknak megfelelően.

Az ellenőrzés terjedjen ki a Tanúsítványok érvényességének ellenőrzésére, a szabályzatok és a kulcshasználat megkötéseire, az egyes Tanúsítványokban hivatkozott CRL vagy OCSP alapú visszavonási státusz információk ellenőrzésére.

4.9.7 A visszavonási lista kibocsátás gyakorisága

A Bizalmi szolgáltató legalább naponta egyszer bocsásson ki új tanúsítvány visszavonási listát a végfelhasználói Tanúsítványokat kibocsátó hitelesítő egységeire. Az ilyen kibocsátott tanúsítvány visszavonási listák érvényességi ideje legfeljebb 25 óra lehet.

A Bizalmi szolgáltató legalább évente egyszer, de visszavonás esetén 24 órán belül bocsásson ki új tanúsítvány visszavonási listát a köztes hitelesítő egységeire. Az ilyen kibocsátott tanúsítvány visszavonási listák érvényességi ideje legfeljebb 12 hónap lehet.

A visszavonási listának tartalmaznia kell az őt követő visszavonási lista kibocsátásának tervezett időpontját, a Bizalmi szolgáltató ugyanakkor ezen időpontot megelőzően is kiadhat új visszavonási listát. A visszavonási listákat a Bizalmi szolgáltató saját elektronikus aláírásával hitelesíti.

4.9.8 A visszavonási lista előállítása és közzététele közötti idő maximális hossza

A visszavonási lista (CRL) előállítása és közzététele között legfeljebb 5 perc telhet el.

4.9.9 Online tanúsítványállapot-ellenőrzés rendelkezésre állása

A Bizalmi szolgáltatónak online (valós idejű) tanúsítványállapotszolgáltatást (OCSP) kell nyújtania a bizalmi szolgáltatások keretében kibocsátott tanúsítványok állapotának ellenőrzéséhez.

A Bizalmi szolgáltató által kibocsátott OCSP válaszoknak meg kell felelniük az RFC2560 és/vagy a RFC5019 ajánlásnak. AZ OCSP válaszokat alá kell írnia

- az ellenőrizendő tanúsítványt kibocsátó a tanúsítványkiadónak (CA),
  vagy

- egy OCSP válaszadónak, amelynek a tanúsítványát az a tanúsítványkiadó (CA) írta alá, mely az ellenőrizendő tanúsítványt kibocsátotta. (Ebben az esetben az RFC2560 alapján az OCSP-t aláíró tanúsítványnak tartalmaznia kell egy “id-pkix-ocsp-nocheck” típusú kiterjesztést.)

4.9.10 Online tanúsítványállapot ellenőrzésre vonatkozó követelmények

A Bizalmi szolgáltatónak támogatnia kell a “GET” paraméterrel érkező OCSP kéréseket.

A Bizalmi szolgáltatónak legalább az alábbi időközönként kell frissítenie az OCSP-vel szolgáltatott információkat:

- végfelhasználói tanúsítványokra legalább 4 naponta;
- köztes tanúsítványkiadói tanúsítványokra alapvetően évente;
- köztes tanúsítványkiadói tanúsítvány visszavonása vagy felfüggesztése esetén 24 órán belül.

A Bizalmi szolgáltató által kibocsátott OCSP válasz csak az adott hitelesítő egység által aláírt, a Bizalmi szolgáltató Tanúsítványtárában szereplő Tanúsítványokra vonatkozóan tartalmazhat "good" állapotinformációt. Egy még ki nem bocsátott tanúsítványra vonatkozó OCSP válasz nem tartalmazhat “good” állapotinformációt. Az OCSP kéréseket a Szolgáltatónak a 6.5 Informatikai biztonsági előírások fejezetben foglaltaknak megfelelően kell ellenőriznie.

A 7.1.5 Névhasználati megkötések fejezeben írtaknak nem megfelelő Tanúsítványkiadói tanúsítványra vonatkozó OCSP válasz nem tartalmazhat “good” állapotinformációt.

4.9.11 A visszavonási hirdetmények egyéb formái

A Bizalmi szolgáltató egyes bizalmi szolgáltatások keretében a visszavonási információkat egyéb módokon is közzéteheti, amennyiben ezt szabályzataiban rögzíti.

4.9.12 A kulcs kompromittálódásra vonatkozó speciális követelmények

Szolgáltató dolgozzon ki megoldást arra, hogy tájékoztassa Ügyfeleit, amennyiben magánkulcsuk veszélybe került (pl. Új sérülékenység felfedezése esetén vagy Szolgáltató saját megállapítása alpján). Amennyiben kulcs kompromittálódás nem vitatott, akkor az érintett Szolgáltatói vagy végfelhasználói tanúsítvány vissavonásáról késedelem nélkül intézkedni kell.

Magánkulcs kompromittálódása esetén az ahhoz tartozó nyilvános kulcs tanúsítványát a 4.9 A visszavonást és a felfüggesztést indukáló körülmények fejezetben írtak szerint a Bizalmi szolgáltatónak fel kell függesztenie vagy vissza kell vonnia.

Szolgáltatói kulcs kompromittálódás esetére lásd az 5.7.3 fejezetet.

4.9.13 A felfüggesztés maximális ideje

[PTC: Tanúsítványfelfüggesztés nem támogatott.]

A felfüggesztett állapot időtartama legfeljebb 30 naptári nap (240 óra lehet). Az időtartam elteltét követően a Bizalmi szolgáltató külön értesítés nélkül jogosult a felfüggesztett

tanúsítvány visszavonására. A felfüggesztési időtartam alatt az Előfizető jogosult a tanúsítvány aktiválását igényelni (Állapotváltoztatási ügyféligény).

4.10 Tanúsítványállapot-szolgáltatások

A Bizalmi szolgáltatónak biztosítania kell az általa bizalmi szolgáltatás keretében kibocsátott tanúsítványok állapotának (érvényes, felfüggesztett vagy visszavont) ellenőrzését biztosító szolgáltatásokat.

4.10.1 Működési jellemzők

A tanúsítványállapot-szolgáltatások működése során a Bizalmi szolgáltatónak az alábbi követelményeket kell teljesítenie:

- A tanúsítványállapot-információkat folyamatosan, napi 24 órában, heti 7 napban kell elérhetővé tenni.
- Biztosítani kell a tanúsítványallapotinformációk sértetlenségét és hitelességét.
- A visszavonási információt legalább a tanúsítvány eredeti érvényességi idejéig kell szerepeltetni a tanúsítványállapotinformációk között.
- Tanúsítványvisszavonási Lista (Certification Revocatuion List - CRL) és Online Tanúsítványállapotellenőrzés (Online Certificate Status Protocoll - OCSP) szolgáltatást egyaránt nyújtani kell;
- A CRL és az OCSP szolgáltatásoknak egymással összhangban kell működniük, egy tanúsítvány állapotának változásáról szóló információnak mindkét szolgáltatásban elérhetőnek kell lennie.
- A tanúsítványvisszavonási információknak nyilvánosnak és nemzetközileg is elérhetőnek kell lenniük.

A tanúsítványállapot-információk között jelenjen meg a visszavont és felfüggesztett Tanúsítványok állapota. A felfüggesztett Tanúsítványok a visszaállítás (tanúsítvány aktiválása) hatására kerüljenek ki a tanúsítványvisszavonási listából (CRL).

Felfüggesztés, aktiválás és visszavonás esetén a folyamat sikeres lezárását követően a Tanúsítvány új állapota azonnal jelenjen meg a Bizalmi szolgáltató tanúsítványállapot-nyilvántartásában. Ettől a pillanattól kezdve a Szolgáltató által nyújtott OCSP válaszok már a Tanúsítvány új állapotát tartalmazzák.

Kulcs kompromittálódás miatti tanúsítvány felfüggesztés vagy visszavonás esetén, az állapotváltozás bejegyzése után a Bizalmi szolgáltató bocsásson ki rendkívüli visszavonási listát (CRL). Más okból kifolyólag történő visszavonás vagy felfüggesztés esetén az állapotváltozás legkésőbb a következő tervezett visszavonási listában kerüljön publikálásra. A Bizalmi szolgáltató más visszavonási állapotváltozás hatására is bocsáthat ki rendkívüli visszavonási listát.

4.10.2 Szolgáltatások elérhetősége

A Bizalmi szolgáltatónak biztosítania kell a Tanúsítványtár, valamint a szolgáltató által kibocsátott Tanúsítványok használatára vonatkozó kikötések és feltételek folyamatos (7X24) elérhetőségét éves szinten legalább 99%-os rendelkezésre állás mellett, ahol az eseti szolgáltatáskiesések maximális időtartama legfeljebb 24 óra.

A Bizalmi szolgáltatónak biztosítania kell a visszavonási nyilvántartások és a visszavonás kezelési szolgáltatás éves szinten legalább 99%-os rendelkezésre állását, ahol az eseti szolgáltatáskiesések időtartama legfeljebb 24 óra.

A Szolgáltatónak képesnek kell lennie a tanúsítványokkal kapcsolatos magas prioritású hibajelentésekre folyamatosan (7x24) reagálni és adott esetben azokat a bűnüldöző szervek felé továbbítani és/vagy az érintett tanúsítványt visszavonni.

A visszavonási nyilvántartások válaszideje normál terhelés esetén legfeljebb 10 másodperc lehet.

4.10.3 További lehetőségek

Nincs előírás.

4.11 Az előfizetés megszűnése

Nincs előírás.

4.12 Kulcsletét és kulcshelyreállítás

4.12.1 A kulcsletét és -helyreállítás rendje és szabályai

A magánkulcsok másolatára ugyanolyan szintű biztosági előírások vonatkoznak, mint az eredeti magánkulcsra.

A magánkulcsokról legfeljebb annyi másolatot szabad készíteni, ami elégséges a szolgáltatás fenntartásához.

Aláíró, autentikációs magánkulcsok éesetében a Bizalmi szolgáltató nem biztosít kulcsletét szolgáltatást. Ez azonban nem zárja ki a kulcsmenedzsment szolgáltatást.

Titkosító magánkulcs esetében a Bizalmi szolgáltató biztosíthat kulcsletét szolgáltatást; ebben az esetben az aláíró és autentikációs kulcshasználatot ki kell zárni.

Kulcsletét szolgáltatás keretében a Szolgáltatónál letétbe helyezett magánkulcsot a Szolgáltatónak titkosítva kell tárolnia, a magánkulcshoz való hozzáférést csak arra jogosult személyeknek biztosíthat.

4.12.2 Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nincs előírás.

5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A bizalmi szolgáltatónak gondoskodnia kell arról, hogy az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazzon.

A bizalmi szolgáltatónak meg kell felenie az alábbi követelményeknek:

- Rendszeresen elvégzett kockázatelemzéssel kell rendelkeznie (ennek részleteit lásd az 5.4.8-ban)
- A szolgáltatónak megfelelő vagyonnyilvántartással (leltár) kell rendelkeznie, beleértve az információs vagyont is. A vagyontárgyak kockázati osztályozását el kell végeznie és az ennek megfelelő védelmi intézkedéseéket kell foganatosítania.
- Menedzsment által elfogadott, dokumentált, implementált és karbantartott információbiztonsági szabályozással kell rendelkeznie, beleértve a biztonsági kontrollok és műveleti eljárásokat a Szolgáltató létesítményei, rendszerei és információs eszközöi számára, melyek a szolgáltatásnyújtást biztosítják. A Szolgáltató az információbiztonsági szabályozást minden érintett minden munkavállalójával.
- Szolgáltató felelősséget visel az információbiztonsági szabályozásában meghatározott eljárások betartásáért, akkor is, ha azokat nem szolgáltató saját személyzete végzi. Szolgáltatónak meg kell határoznia e közreműködők felelősségét, és biztosítania kell, hogy az előírt eljárásokat betartják.
- Az információbiztonsági szabályozást és vagyonnyilvántartást rendszeres időközönként vagy ha jelentős változások történnek felül kell vizsgálni, hogy biztosított legyen azok folyamatos alkalmazhatósága, megfelelősége és eredményessége. Minden változtatást, amely hatással van a biztonsági szintre, jóvá kell hagynia a Szolgáltató menedzsmentjének. A Szolgáltatói rendszerek konfigurációját rendszeresen ellenőrizni kell a biztonsági előírásokat sértő változások kiszűrése érdekében.

5.1 Fizikai óvintézkedések

A Bizalmi szolgáltató gondoskodjon arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások eszközeinek fizikai kockázatát minimalizálják.

A bizalmi szolgáltató biztosítsa az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.
A bizalmi szolgáltató óvintézkedéseket valósítson meg az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

5.1.1 Telephely felépítése

A telephely kiépítése során szolgáltatónak figyelembe kell venni a tűz és vízvédelemre, a folyamatos áramellátásra, légkondicionálásra, a biztonságos zónák kialakítására és a telekommunikációs hálózatok elérhetőségére vonatkozó ajánlásokat és előírásokat.

5.1.2 Fizikai hozzáférés

A bizalmi szolgáltató biztosítson egy egyértelműen meghatározott biztonsági körletet a biztonságos működéséhez kritikus komponensei számára, amelyet a behatolás ellen fizikailag véd, ahova a bejutást ellenőrzi, az illetéktelen behatolást észleli és riasztani képes. Bármely más szervezettel, szervezeti egységgel megosztott rész e körleten kívül essen. Más szolgáltatások e körleten belül csak akkor működtethetők, ha a kritikus szolgáltatások elérésére jogosult személyekkel kiszolgálhatók.

E kritikus szolgáltatások fizikai- és környezetbiztonsági programjai foglalkozzanak a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelem és tűzbiztonság tényezőivel, a támogató eszközök (ezen belül az áram és klíma berendezések) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, katasztrófa utáni helyreállítással.

A bizalmi szolgáltató óvintézkedéseket valósítson meg

- a fizikai és környezetbiztonsági rendszererőforrások, illetve a működésük támogatására használt berendezések megvédése érdekében;
- annak megakadályozására, hogy az elektronikus aláírással kapcsolatos szolgáltatáshoz szükséges berendezés, információ, adathordozó vagy szoftver elvesszen, megsérüljön vagy jogosulatlanul elvigyék a helyszínről.

A bizalmi szolgáltató a kritikus szolgáltatásaival kapcsolatos eszközökhöz történő fizikai hozzáférést megfelelően felhatalmazott egyénekre korlátozza, s az eszközöket olyan környezetben működtesse, amely fizikailag megvédi a szolgáltatásokat attól, hogy a rendszerekhez, illetve adatokhoz történő jogosulatlan hozzáférésen keresztül kompromittálódjanak.

A biztonsági körletbe való belépéseket felügyelni kell, a nem jogosult személyek csak jogosult személyek felügyeletével tartózkodhatnak a körletben. A belépéseket és kilépéseket naplózni kell.

A szolgáltató gyökér kulcsok a normál operációtól elkülönített módon tárolhatók, a hozzáférést csak a bizalmi munkatársakra korlátozva.

5.1.3 Áramellátás, légkondicionálás

A bizalmi szolgáltató szolgáltatási helyszíneire olyan szünetmentes áramellátást kell biztosítani, amely megfelelő teljesítménnyel rendelkezik a rendszerek áramellátásához, rövid idejű kimaradás esetén, és tartós áramszünet esetén saját áramtermelő berendezés segítségével biztosított a rendszerek további működése.

A szolgáltatási helyszínre bejutó levegő tisztaságát megfelelő szűrőrendszerrel kell biztosítani, amely kiszűri a levegőből a különféle szennyeződéseket, tovább biztosítja a szolgáltató munkatársai részére szükséges levegőt. A keringetett levegő nedvesség tartalmát és hőmérsékletét az informatikai rendszerek számára megfelelően kell beállítani.

A légkondicionáló rendszer teljesítménye olyan kell legyen, hogy képes legyen a szükséges hűtést biztosítani az IT rendszerek számára.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A bizalmi szolgáltató szolgáltatási helyszíneit védeni kell a beázástól és az elárasztódástól.

5.1.5 Tűzmegelőzés és tűzvédelem

A bizalmi szolgáltató szolgáltatási helyszíneit védeni kell a tűztől.

Az aktuális tűzvédelmi szabályzásoknak megfelelő tűz és füstérzékelőket, kézi és automata oltó berendezéseket kell felszerelni, jelezni kell a kézi oltó berendezések helyét, a menekülési útvonalat.

5.1.6 Adathordozók kezelése

A Bizalmi szolgáltató az adathordozó eszközöket biztonságosan kezelje a sérülés, ellopás és jogosulatlan hozzáférés és az avulás elleni védelem érdekében. A Bizalmi szolgáltató az összes adathordozó eszközt biztonságosan kezelje az adat-minősítési rendszer követelményeinek megfelelően. A média avulát és és sérülését meg kell akadályozni az adatok teljes megőrzési idejében.

A bizalmi szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztől biztonságosan váljon meg, amennyiben azokra már nincs szükség. A selejtezett eszközök tartalmát - széles körben elfogadott módszerek alapján – véglegesen törölni kell, vagy az eszközt egyéb módon helyreállíthatatlanul tönkre kell tenni.

A bizalmi szolgáltatónak a kritikus adatokról több mentési példánnyal kell rendelkeznie, és egy példányt a szolgáltatói helyszíntől eltérő olyan külső helyszínen kell tárolni, melyben a mentések védelmének szintje azonos a szolgáltatási helyszínével.

5.1.7 Hulladékelhelyezés

Informatikai eszközeinek selejtezése esetén a szolgáltatónak biztonságosan és helyreállíthatatlanul törölnie kell az azon tárolt adatokat, vagy ha ez nem lehetséges legalább az ilyen elemet hordozó alkatrészt fizikai tönkretétellel megsemmisíti, ami annak olvashatóságát megakadályozza.
Iratok selejtezése esetén a személyes adatot tartalmazó iratokat megfelelő eljárással olvashatatlanná kell tenni.

5.1.8 Mentés külső helyszínen

A megőrzendő adatok biztonságos tárolását a szolgáltató elvégezheti csak írható médiával, távoli helyen tárolt mentéssel, vagy több tárolási helyen történő távoli párhuzamos tárolással.

5.2 Eljárásrendi biztonsági intézkedések

A Bizalmi Szolgáltatónak gondoskodnia kell rendszerei biztonságos, szabályszerű, a meghibásodás minimális kockázata melletti üzemelteséről.

5.2.1 Bizalmi munkakörök

Bizalmi munkaköröknek kell tekinteni a következőket:

- Biztonsági tisztviselő: A biztonsági előírások alkalmazásáért felelős személy.
- Rendszergazda: Aki jogosult telepíteni, konfigurálni és karbantartani és helyreállítani a szolgáltató megbízható rendszereit.
- Üzemeltető: A szolgáltató megbízható rendszereinek mindennapi működtetéséért és a rendszermentésért felelős személy..
- Rendszerellenőr: A szolgáltató megbízható rendszereinek archívumának és naplójának megtekintésére jogosult személy.
- Regisztrációs felelős: a végfelhasználói tanúsítványok előállításának, kibocsátásának, állapotváltoztatásának jóváhagyásáért és az ezek kapcsán elvégzendő adatellenőrzésért, azonosításért felelős személy.

Bizalmi munkakört kizárólag a Bizalmi szolgáltatóval munkaviszonyban álló munkatárs tölthet be, a Szolgáltató felső vezetésének formális kinevezését követően. Bizalmi munkakör megbízási szerződés alapján nem tölthető be.

A bizalmi munkakörökről naprakész nyilvántartást kell vezetni, változás esetén a változás tényét haladéktalanul be kell jelenteni a Bizalmi Felügyeletnek.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

Az alábbi tevékenységeket legalább kettő arra kijelölt és közvetlen felhatamazással rendelkező bizalmi munkatárs együttes fizikai jelenlétével, egy fizikailag védett környezetben, más személyek jelenlétét kizárva kell elvégezni:

- köztes kiadó tanúsítványának kibocsátása;
- magánkulcsok mentése, megőrzése és visszaállítása;
- Bizalmi szolgáltató saját szolgáltatói kulcspárjának generálása.

5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelsítés

A Bizalmi Szolgáltató informatikai rendszereihez csak az arra felhatalmazott személyek férhetnek hozzá. A szolgáltató rendszereinek képesnek kell lennie

- az egyes bizalmi munkakörökhöz tartozó jogosultsági szintek Jogosultságkezelő Szabályzat szerinti elkülönítésére;
- a bizalmi munkaköröknek megfelelő folyamatok elkülönítésére;
- a jogosultságok megfelelő időn belül történő módosítására, törlésére.

A személyzetnek azonosítania és hitelesítenie kell magát a a szolgáltatások szempontjából kritikus rendszerek használata előtt, s tevékenységükkel kapcsolatban felelősséggel tartoznak.

5.2.4 Egyes szerepkörök összeférhetetlensége

A szolgáltatói eszközökben, rendszerekben végrehajtott azonosítatlan vagy nem szándékolt módosítások illetve más visszaélések lehetőségének csökkentése érdekében a Bizalmi szolgáltatónak az egymást kizáró feladatokat és felelősségi területeket el kell különíteni.

A feladatkörök elhatárolása végett a biztonsági tisztviselő nem láthatja el a független rendszervizsgáló és az informatikai rendszerért általánosan felelős vezető feladatait, és a

független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető feladatait.

[EVCP: A Bizalmi szolgáltatónak szigorú ellenőrzési eljárásokkal kell biztosítania a regisztrációs feladatok elkülönítését, azaz, hogy a tanúsítvány kibocsátásához szükséges adatok érvényesítését és tanúsítványkibocsátás jóváhagyását ne ugyanaz a bizalmi munkatárs végezze. Az ellenőrzési eljárásoknak auditálhatónak kell lenniük.]

5.3 Személyzeti biztonsági intézkedések

A Bizalmi szolgáltató gondoskodjon arról, hogy alkalmazottai és szerződéses partnerei támogassák a szolgáltatások megbízhatóságát. A Bizalmi szolgáltató bizalmi munkakörben foglalkoztatott személyzetének minden olyan összeférhetetlenségtől mentesnek kell lennie, amely a szolgáltatások nyújtásában végzett tevékenységének pártatlanságát sértheti

A személyzetnek az informatikai biztonsági eljárásokkal összhangban kell végrehajtani az adminisztrációs és menedzsment eljárásokat.

Az információbiztonsági szabályzatban azonosított biztonsági munkaköröket és felelősségeket munakköri leírásokban vagy más az érintettek számára elérhető dokumentációban dokumentálni kell. A bizalmi munkaköröket világosan meg kell határozni, be kell tölteni, és a megbízást el kell fogadnia a menedzsmentnek és az érintett személynek egyaránt.

A személyzetnek (beleértve az állandóan és ideiglenesen foglalkoztatottakat egyaránt) olyan munkaköri leírásokkal kell rendelkezni, amelyek a feladatok szétválasztása és legkevesebb jogosultság elvéből indulnak ki, s a pozíció érzékenységének meghatározása a feladatok, a hozzáférési szintek, a háttér szűrés és az alkalmazott képzése és tudatossága alapján történik.

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

A Bizalmi szolgáltató valamennyi munkatársának rendelkeznie kell a munkaköre ellátásához szükséges végzettséggel, gyakorlattal, megbízhatósággal és szakmai ismeretekkel, tapasztalattal. A Bizalmi szolgáltató bizalmi munkakörben csak büntetlen előélettel rendelkező alkalmazottakat foglalkoztathat, amit a felvételi eljárás során 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni.

A szolgáltató menedzsmentjének megfelelő tapasztalattal kell bírnia a szolgáltató által nyújtott bizalmi szolgáltatások területén, valamint informatikai biztonsági és kockázatkezelési területeken, valamint a biztonságért felelős menedzsereknek a biztonsági eljárások területén, annak érdekében, hogy menedzsment feladataikat elláthassák.

5.3.2 Ellenőrzési eljárások

A Bizalmi szolgáltatónak a bizalmi munkakörben foglalkoztatandó személyek esetében (a szerződéses viszonytól függetlenül) meg kell győződnie e személyek személyazonosságáról fizikai jelenlétük során vagy fényképes személyazonosító okmányaik ellenőrzésével. Valamint meg kell győződniük e személyek megbízhatóságáról, ami magában foglalja a

korábbi munkahelyekre, releváns végzettségekre és szakmai referenciákra vonatkozó információk ellenőzését. Az ellenőrzések lefolytatását megelelőzen nem kaphatnak hozzáférést a szolgáltató rendszereihez.

5.3.3 Képzési követelmények

A szolgáltatónak meg kell bizonyosodni arról, hogy a bizalmi munkakörben dolgozó személyek rendelkeznek a feladataik ellátásához szükséges tudással. Ennek érdekében vizsgát kell tenniük a szükséges ismeretek birtoklását igazolandó. A Szolgáltató bizalmi szolgáltatást nyújtó rendszereihez hozzáférési jogosultságot csak a sikeres vizsgát tevő személyek kaphatnak. A vizsga megtörténtét dokumentálni kell. A szolgáltatónak a vizsgát megelőzően az érintett személyek számára szükség szerinti mértékben támogatni kell a hiányzó ismeretek megszerzését a feladatuk ellátásához szükséges mértékben. A vizsgának és a képzésnek a következőket kell felölelnie:

- PKI alapismeretek;
- hitelesítés és ellenőrzési szabályok és eljárások;
- Biztonsági és adatvédelmi szabályok;
- általános fenyegetések az információhitelesítési eljárásokra (beleértve az adathalász és egyéb social engineering taktikákat);
- jelen Hitelesítési Rend, a Szolgáltatási Szabályzat és egyéb szabályzatok előírásai;
- egyes tevékenységük jogi következményei;
- Szolgáltató informatikai rendszerének sajátosságai és kezelésének módja;

5.3.4 Továbbképzési gyakoriságok és követelmények

A Bizalmi szolgáltatónak gondoskodnia kell róla, hogy a bizalmi munkakört ellátó személyek folyamatosan rendelkezzenek a feladataik ellátásához szükséges tudással, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartania. Így továbbképzést kell tartania, amennyiben a szabályzataiban vagy informatikai rendszerében olyan változás áll be, ami érinti e munkakörök tevékenységét. Legalább 12 havonta tájékoztatni kell a személyzetet az új fenyegetettségekről és az aktuális biztonsági eljárásokról.

A továbbképzést megfelelően dokumentálni kell, amelyből utólag is megállapítható a továbbképzés tematikája és a résztvevők személye.

5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6 Jogosulatlan tevékenységek büntető következményei

A Bizalmi szolgáltatónak megfelelő fegyelmi szankciókat kell alkalmazni szolgáltatói rendszerének nem engedélyezett használata vagy a szolgáltatás nyújtása közben elkövetett hibák, mulasztások, károkozások esetére az azt okozó alkalmazottak vagy közreműködő természetetes és jogi személyek esetében. A lehetséges szankciókról a velük kötött szerződésben rendelkezni kell.

5.3.7 Szerződéses közreműködőkre vonatkozó követelmények

A Bizalmi szolgáltató által szerződéses viszonyban közreműködő személyekre ugyanúgy vonatkoznak a szabályzatok elvárásai, mint az alkalmazottaira.

5.3.8 A személyzet számára biztosított dokumentációk

A Bizalmi szolgáltatónak folyamatosan biztosítania kell a szolgáltatásnyújtásban közreműködő személyek részére a szerepkörük ellátásához szükséges aktuális szabályzatok és dokumentációk elérhetőségét.

5.4 Naplózási eljárások

A Szolgáltatónak rögzíteni és egy meghatározott ideig folyamatosan hozzáférhetővé kell tenni - a tevékenységének megszűnése utáni időszakban is - minden lényeges információt beleértve a kiadott és fogadott adatokat, különösen a bírósági eljárásokban bizonyítékként való felhasználás érdekében, valamint a szolgáltatásfolyamatosság biztosítása céljából és a megfelelőségértékelés számára.

A naplóbejegyzések mellett el kell tárolni

- az bejegyzés (és ha eltér az esemény) dátumát és időpontját;
- az esemény típusát;
- az eseményvégrehajtás sikerességét illetve sikertelenségét;
- a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.

Amennyiben naplózó és naplóelemző rendszer működésében komoly rendellenesség lép fel, a Bizalmi szolgáltató működését fel kell függeszteni az üzemzavar elhárításáig.

Az események mellett rögzített időinformációt legalább naponta szinkronizálni kell hiteles időforrással.

5.4.1 A tárolt események típusai

Az automatikusan és manuálisan rögzített naplóállományokban az alábbi eseményeket el kell tárolni:

1. Biztonsági események
    a. Biztonsági profil változások
    b. Rendszer indítása és leállítása
    c. Tűzfal és router tevékenységek
    d. Szolgáltatói rendszer hozzáférési kísérletek módja és eredménye (sikeres és sikertelen)
    e. Szolgáltatói létesítménybe történő belépések és kilépések
2. Szolgáltatói rendszer beállításai
    a. Rendszer telepítése
    b. Rendszerkonfiguráció változásai (pl. frissítések, foltozások, beállítások)
    c. Tanúsítvány és CRL profil megváltoztatása;
    d. Rendszer vagy rendszeradatok mentése és visszaállítása
3. Szolgáltatói és végfelhasználói kulcsok életciklus műveletei
    a. Kulcsgenerálás, másolatkészítés, tárolásvisszaállítás, achiválás és megsemmisítés
    b. Kriptográfiai eszközök életciklus műveletei
4. Tanúsítványok életciklus műveletei
    a. Igénylések, megújítások, kulcscserék, felfüggesztés, aktiválás, visszavonás
    b. Életciklus műveleteket érintő ellenőrzési események
    c. Igénylések elfogadása és visszautasítása

   d. Tanúsítványkiadások
   e. Visszaonási listák generálása
5. Pontos időt érintő események
   a. Óraszinkronizációs események
   b. Előírt időpontossági küszöb túllépése
6. Naplózási események
   a. Naplózó rendszer leállítása, újraindítása;
   b. Naplózási beállítás módosítása
   c. Naplózási adatok archiválása-törlése;
7. Felhasználómenedzsment műveletek (Szolgáltatói rendszerek tekintetében)
   a. Felhasználók felvétele, törlése
   b. Szerepkörök vagy jogosultságok kiosztása, visszavonása
   c. Státuszváltozások (pl. zárolás, tiltás, engedélyezés)
   d. Előírt azonosítási módszer beállításai
   e. Hitelesítési adat (pl. jelszó) cseréje
8. Rendellenes vagy veszélyt jelentő események
   a. Rendszerösszeomlás és a hardver hibák;
   b. Bármilyen szoftverművelet hibája;
   c. Szoftverintegritás hiba;
   d. Hálózati támadási kísérletek;
   e. Elektromos hálózati üzemzavar;
   f. Szünetmentes tápegység hiba;
   g. Kommunikációs üzemzavar.

Az ügyféligénylések és tanúsítvány műveletek kapcsán az alábbi információk rögzítése szükséges:

- A műveletek dátuma és pontos ideje;
- A bemutatott dokumentumok típusai és azonosító adatai
- A bemutatott dokumentumok és az aláírt szolgáltatási szerződés másolatai és a másolat tárolási helyes
- Az ügyfél által végzett bármilyen választás a szolgáltatás tekintetében (pl. szolgáltatási szerződésben)
- Az Ügyféligényt feldolgozó személy azonosítója
- A dokumentumok ellenőrzésének módszere - amennyiben több módszer is alkalmazható
- A feldolgozásban közreműködő hitelesítői és regisztrációs egységek azonosítói;
- Az ellenőrzés ideje, az ellenőrzéshez felkeresett személy adatai (pl. telefonszáma)

5.4.2 A naplófájl feldolgozásának gyakorisága

A Bizalmi szolgáltatónak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését. A naplóállományokban rögzített bejegyzéseket a keletkezésüktől számított legkésőbb 1 héten belül ki kell értékelni a megfelelő szakértelemmel és jogosultságokkal rendelkező Rendszerellenőrnek. A kiértékeléshez szoftvereszközök is igénybe vehetők.

A kiértékelés során meg kell győződni a vizsgált naplóállományok hitelességéről és sértetlenségéről.

A kiértékelés során elemezni kell

- a rendszerek által generált hibaüzeneteket,
- a forgalmi adatokban bekövetkezett jelentős változásokat,
- a szokványostól eltérő bármilyen rendkívüli mintákat,
- gyanús aktivitásokat.

A kiértékelés tényét, eredményeit és az esetlegesen feltárt problémák és kockázatok elhárítása érdekében meghozott intézkedéseket dokumentálni kell.

Az automatikus kiértékelő eljárásoknak riasztani kell a személyzetet a biztonságkritikusnak tűnő események észlelése esetén.

5.4.3 A naplófájl megőrzési időtartama

A naplóállományokban rögzített információkat meg kell őrizni az érintett tanúsítványok megőrzési idejéig, de legalább 7 évig (a Szolgáltatói rendszerben vagy archivált formában).
A Rendszerellenőr számára bármikor elérhetővé kell tenni a naplózott információkat.

5.4.4 A naplófájl védelme

Gondoskodni kell arról, hogy a naplóállományok, illetve a benne rögzített információk ne legyenek egyszerűen törölhetők vagy megsemmisíthetők. A rögzített információk bizalmasságát és integritását (beleértve a még nem és már archivált eseményeket is) fenn kell tartani a megőrzési idő végéig. A naplóállományokhoz csak az arra jogosultak – elsősorban a Rendszerellenőrök – férhessenek hozzá. Jogi eljárás esetén az érintett információkat elérhetővé kell tenni az eljárásban érintett és erre feljogosított személyek számára. .

5.4.5 A naplófájl mentési eljárásai

A naplóállományokat 2 példányban, fizikailag elkülönülő helyeken kell tárolni. Amennyiben a naplóbejegyzés egy helyen keletkezik, akkor legkésőbb 24 órán belül gondoskodni kell arról, hogy egy másik helyszínen is létrejöjjön róla másolat. Lásd az *5.1.6 Adathordozók kezelése* és *5.1.8. Mentés külső helyszínen* fejezeteit.

5.4.6 A naplózás adatgyűjtési rendszere

Nincs előírás.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

Nincs előírás.

5.4.8 Sebezhetőség felmérése

A Bizalmi szolgáltatónak évente kockázatértékelés kell végeznie, amely segítségével

- Azonosítja az előrelátható belső és külső fenyegetettségeket, amelyek lehetővé tehetik a tanúsítványadatok vagy a tanúsítványkezelési folyamatok jogosulatlan elérését, nyilvánosságra hozatalát, megváltoztatását megsemmisítését vagy más visszaélést.
- Feltérképezi ezen fenyegetettségek bekövetkezésének valószínűségét és a bekövetkezés esetén várható kárt is.

- Értékeli a feltárt fenyegetettségek elhárítására alkalmazott folyamatok, védelmi intézkedések és informatikai rendszerek megfelelőségét.

5.5 Adatok archiválása

A Bizalmi szolgáltató a bizalmi szolgáltatásokkal kapcsolatos adatokat - ide értve a személyes adatokat is - az eüt. 84. §-nak megfelelő módon őrizni meg.

5.5.1 Az archiválandó adatok típusa

A Bizalmi szolgáltatónak egyes tanúsítványokkal kapcsolatosan rendelkezésére álló információkat - beleértve az azok előállításával összefüggőket is - és az ahhoz kapcsolódó személyes adatokat meg kell őriznie. Így például:

- a tanúsítványigénylési eljárás során bekért és beszerzett információkat és dokumentációt (4.1 Tanúsítványigénylés);
- a tanúsítványállapot-változtatási eljárás során közzétett információkat (4.9.3 A visszavonási, felfüggesztési és aktiválási eljárás);
- a jelen Hitelesítési Rend szerint naplózott információkat (5.4 Naplózási eljárások).

5.5.2 Archiválási időtartam

A Bizalmi szolgáltató a jelen Hitelesítési rend szerint az egyes tanúsítványokkal kapcsolatban archivált adatokat az alábbi időtartamokig köteles megőrizni:

- a tanúsítvány érvényességének lejáratától számított 10 évig;
- A tanúsítványba foglalt adat valódiságával vagy érvényességével kapcsolatosan megindult jogvita esetén a szolgáltató a jogvita jogerős lezárásáig.

5.5.3 Az archívum védelme

Az 5.4.4. A naplófájl védelme fejezetben írtak szerint kell eljárni.

5.5.4 Az archívum mentési folyamatai

Az 5.4.5. A naplófájl mentési eljárásai fejezetben írtak szerint kell eljárni.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Az archiválandó adatokat időadattal, vagy időbélyeggel látja el.

5.5.6 Az archívum gyűjtési rendszere

Nincs előírás.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

Nincs előírás.

5.6 Kulcscsere

Szolgáltatónak le kell cserélnie kulcsát amennyiben valamely saját szolgáltatói tanúsítványa lejár, illetve, amennyiben alkalmazott kulcsai elavulnak, továbbá saját belátása szerint egyéb esetben is dönthet kulcscsere mellett.

Az új kulcscsal kiállított új tanúsítvány esetében annak profilját és adatait az aktuális előírásokhoz és legjobb gyakorlathoz kell igazítani.

5.7 Katasztrófaelhárítás és helyreállítás

Szolgáltatónak megfelelő technikai és szervezeti intézkedéseket kell végrehajtani az általuk nyújtott bizalmi szolgáltatások biztonságát fenyegető kockázatok kezelése érdekében. Ezen intézkedésekkel – figyelembe véve a legújabb technológiai fejleményeket – biztosítani kell, hogy a biztonsági szint arányos legyen a kockázat mértékével. Intézkedéseket kell végrehajtani különösen a biztonsági események megelőzése és azok hatásának minimálisra csökkentése, valamint az érdekeltek bármely esemény káros hatásairól való tájékoztatása érdekében.

Szolgáltatónak indokolatlan késedelem nélkül, de minden esetben az esetről való értesüléstől számított 24 órán belül értesíteni kell a felügyeleti szervet és adott esetben más érintett szerveket, például az információbiztonságért felelős nemzeti szervet vagy az adatvédelmi hatóságot a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről, amennyiben az jelentős hatást gyakorol a bizalmi szolgáltatásra vagy az annak keretében tárolt személyes adatokra.

Amennyiben a biztonság megsértése vagy az adatok sértetlenségének megszűnése vélhetőleg hátrányosan érintheti azt a természetes vagy jogi személyt, aki bizalmi szolgáltatást vett igénybe, a bizalmi szolgáltató a természetes vagy jogi személyt is indokolatlan késedelem nélkül értesíti a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről.

5.7.1 Incidens- és kompromittálódáskezelési eljárások

Az informatikai rendszerekbe való belépésekre, azok felhasználóira és a szolgáltatásigénylésekre vonatkozó rendszertevékenységeket a Bizalmi szolgáltatónak folyamatosan ellenőrznie kell, az alábbi szempontokat figyelembe véve:

1. A tevékenységek ellenőrzésénél figyelemmel kell lenni a begyűjtött és elemzett adatok érzékenyégére.
2. A potenciális biztonsági sérülésre utaló rendellenes rendszertevékenységet (beleértve a szolgáltatói hálózatba való behatolást is), a Bizalmi szolgáltatónak azonosítania és jelentenie kell.
3. A szolgáltatói informatikai rendszereknek az alábbi eseményeket kell ellenőrzinie:
    a. a naplózózási funkciók indítását és leállítását;
    b. a bizalmi szolgáltatások rendelkezésreállását és működőképességét.
4. A Bizalmi szolgáltatónak rövid időn belül és összehangoltan kell eljárnia a káreseményre való minél gyorsabb reagálás és a biztonsági sérülés hatásainak korlátozása érdekében. A Szolgáltatónak meg kell jelölnie azon riasztásokat és potenciálisan kritikus eseményeket, melyeket a bizalmi személyzetnek nyomon kell követnie és melyekről a belső szabályzatok szerint jelentést kell tennie.
5. Szolgáltató eljárásokat határoz meg az érintettek értesítése érdekében a biztonságát vagy integritását sértő azon eseményekről, melyek jelentős hatással vannak a bizalmi szolgáltatásra vagy az abban kezelt személyes adatokra.
6. Szolgáltató egy korábban nem ismert kritikus sebezhetőség felfedezése után ésszerű időn belül helyreállítja a biztonságos működést. Ha ez nem lehetséges, akkor

létrehoz és életbe léptet egy tervet, amivel a kritikus sebezhetőség veszélyét enyhítheti, illetve a tényszerűen dokumentálja, hogy a biztonsági rés nem igényel ilyen lépéseket.

7. Incidensjelentési és reagálási eljárásokat léptet életbe, melyekkel a biztonsági incidensek és zavarok okozta károk minimálisra csökkenthetők.

A Szolgáltatónak rendelkeznie kell Incidenskezelési és Katasztrófa-helyreállítási tervvel.

A Szolgáltató az üzletfolytonossági és katasztrófa-helyreállítási tervében dokumentálja azokat az eljárásokat amivel értesíti és lehetőség szerint megvédi az Ügyfelekt és az érintett feleket katasztrófa, biztonsági kompromittálódás vagy üzleti kudarc esetén. Szolgáltató nem köteles nyilvánosságra hozni üzletfolytonossági és katasztrófa-helyreállítási tervét, de elérhetővé teszik őket a Rendszerellenőrök kérésre. Szolgáltatónak évente tesztelni, felülvizsgálni, és frissítenie kell ezeket az eljárásokat.

Az üzletfolytonossági tervnek tartalmaznia kell:

1. A tervben foglalt intézkedések aktiválásának feltételei,
2. Vészhelyzeti eljárások,
3. Üzemszüneti eljárások,
4. Újraindulási eljárások,
5. A terv karbantartási ütemezése,
6. Tudatosító és oktatási követelményeknek,
7. Egyéni felelősségek,
8. Helyreállítási idő célkitűzés (RTO),
9. A készenléti tervek rendszeres vizsgálata,
10. Szolgáltató terve az üzleti tevékenységének fenntartására vagy helyreállítására kritikus üzleti folyamatainak sérülése vagy megszakadása esetén,
11. A kritikus kriptográfiai eszközök (kulcsok, kulcstároló eszközök, aktiváló kódok) eltérő helyen való tárolása;
12. Elfogadható kiesési és helyreállítási idő
13. A fontos üzleti információkról és szoftverekről történő biztonsági másolatotok készítésének gyakorisága,
14. A helyreállító létesítmények távolsága az elsődleges üzletiviteli helyszíntől,
15. A berendezések biztosítására szolgáló eljárások katasztrófa után és a helyreállítás előtt az eredeti, vagy egy távoli helyszínen.

5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása

A Bizalmi szolgáltató informatikai rendszereit megbízható hardver és szoftver komponensekből kell felépíteni.

A Bizalmi szolgáltató olyan gyakorisággal készítsen teljes rendszermentést, amely biztosítja, hogy abból katasztrófa esetén a teljes szolgáltatás helyreállítható legyen.

A Szolgáltató üzletfolytonossági terve tartalmazzon előírásokat a kritikus rendszerelemek meghibásodása esetén végrehajtandó feladatokra.

A Bizalmi szolgáltató a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb indítsa újra a szolgáltatásait. A helyreállítása során elsőbbséget kell élvezzenek a tanúsítványállapot információkat szolgáltató rendszerelemek.

Adatmentés és helyreállítás

- Szolgáltató működésének helyreállításához szükséges adatokat menteni szükséges, és biztonságos, lehetőleg távoli helyen kell tárolni, ami alkalmas arra, hogy lehetővé tegye a Szolgáltató működésének helyreállítását incidens vagy katasztrófa esetén.
- A fontos üzleti információkról és szoftverekről rendszeresen biztonsági másolatotok kell készíteni. Megfelelő biztonsági mentési eszközöket kell biztosítani annak érdekében, hogy minden lényeges információt és szoftvert helyre lehessen állítani katasztrófa vagy médiasérülés után. A mentési rendszert rendszeresen tesztelni kell az üzletfolytonossági tervnek való megfelelés biztosítása érdekében.
- A biztonsági mentési és helyreállítási funkciókat 5.3 pontban meghatározott, releváns megbízható szerepkörrel rendelkező személyzetnek kell elvégezni.
- Amennyiben az előírások kettős kontrollt követlenek meg adott kezeléséhez, akkor ezek helyreállításához is ketős kontrollt kell alkalmazni.

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

Végfelhasználói kulcs kompromittálódás

Lásd a 4.9.12 A kulcs kompromittálódásra vonatkozó speciális követelmények fejezetet.

Szolgáltatói kulcs kompromittálódás

- Szolgáltató üzletfolytonossági tervének (vagy katasztrófa-helyreállítási tervének) ki kell térni a Szolgáltatói kulcs kompromittálódás vagy annak gyanúja - mint katasztrófahelyzet - esetére, és tervezett folyamatokkal kell készülnie erre a helyzetre.
- A katasztrófát követően Szolgáltatónak lépéseket kell tennie a katasztrófa megismétlődésének elkerülése érdekében.

Szolgáltatói kulcs kompromittálódása esetén a Szolgáltatónak legalább:

- Tájékoztatnia kell az Ügyfeleit, Szolgáltatói partnereit, az Érintett feleket és a bizalmi felügyeletet.
- Jeleznie kell, hogy az érintett szolgáltatói kulcscsal kibocsátott tanúsítványok és visszavonási állapot információ már nem érvényesek; és
- Vissza kell vonni az érintett Szolgáltatói tanúsítványt.

Amennyiben bármelyik algoritmus (vagy a kapcsolódó paraméterek) amiket a Szolgáltatón vagy a Végfelhasználók alkalmaznak nem felel meg az elvárásoknak a fennmaradó tervezett felhasználási időtartamra, akkor a Szolgáltató köteles:

- Tájékoztatnia kell az Ügyfeleit, Szolgáltatói partnereit, az Érintett feleket és a bizalmi felügyeletet; és
- Vissza kell vonnia mindegyik érintett tanúsítványt.

5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után

Katasztrófa esetén (beleértve a Szolgáltatói kulcs vagy hitelesítési adat kompromitálódását vagy a szolgáltató rendszer kritikus elemeinek meghibásodását) a normál üzletemenet a lehető leghamarabb helyreállítandó Ennek érdekében a szolgáltatónak egy üzletfolytonossági tervet kell készíteni és karbantartani, amit katasztrófa esetén életbe léptethet.

5.8 A tanúsítványkibocsátó vagy regisztrációs egység megszűnése

Ha a szolgáltató meg kívánja szüntetni szolgáltatásának nyújtását, erről legkésőbb a tevékenység megszüntetésekor értesítenie kell az Ügyfeleit, Szolgáltatói partnereit, az Érintett feleket és a bizalmi felügyeletet. Ezt követően szolgáltató nem bocsáthat ki az adott bizalmi szolgáltatás kapcsán új tanúsítványt.

A Szolgáltatás megszűnéséből fakadó esetleges zavarokat minimalizálnia kell a Szolgáltatónak. Ennek érdekében:

- Rendelkeznie kell egy megszüntetési tervvel.
- Meg kell szüntetnie minden Szolgáltatói partnerének a felhatalmazását, ami a tanúsítványkiadási tevékenységben való közreműködésre vonatkozik.
- Köteles gondoskodni kötelezettségeinek ellátásáról és a tanúsítványok ellenőrzéséhez szükséges adatok folyamatos elérhetőségéről, és a tárolt adatainak kezeléséről - beleértve a regisztrációs adatokat és a napló állományokat - ezt követően is (saját maga vagy másik bizalmi szolgáltatónak átadva azokat).
- A szolgáltatói magánkulcsokat (beleértve azok biztonsági mentéseit is) visszaállíthatalan módon meg kell semmisítenie.
- A tevékenység megszüntetését legalább húsz nappal megelőzően köteles az általa kibocsátott és még vissza nem vont tanúsítványokat visszavonni.
- A megszüntetés költségeinek a fedezetét Szolgáltatónak biztosítani kell arra az esetre is, amennyiben csődbe menne vagy egyéb okok miatt nem tudná fedezni a költségeket önerőből.
- Tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést kell készítenie. A mentett adatállományokat védenie kell a jogosulatlan módosítástól, és a jogosulatlan hozzáféréstől, s biztosítania kell, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára legyenek csak hozzáférhetőek és értelmezhetők.

Lásd bővebben az eüt 88.§ -át.

6 Műszaki biztonsági óvintézkedések

6.1 Kulcspár generálás és telepítés

A Szolgáltatónak megfelelő biztonsági kontrollokat kell alkalmazni a kriptográfiai kulcsok és eszközök kezelésére, azok teljes életcikplusában.

6.1.1 Kulcspár előállítása

Szolgáltatónak a kulcsokat védett módon kell generálni és a magánkulcsok bizalmasságáról gondoskodnia kell.

A szolgáltatói kulcsok generálására vonatkozóan az alábbiakat kell követni:

- A szolgáltatói kulcsok generálását és a nyilvános kulcs tanúsítását fizikailag védett könrnyezetben kell megvalósítania bizalmi munkakörben foglalkoztatott munkatársaknak, legalább kettős kontroll alatt. E műveletre feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a szabályzatokkal összhagban kell zajlani.
- A szolgáltatói kulcsok generálásánál csak olyan algoritmus és kulcshosszúság használható, amely megfelel (a CA aláíró kulcsokra vonatkozó) szabványoknak, illetve a Nemzeti Média- és Hírközlési Hatóságnak engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának.
- A ténylegesen alkalmazott algoritmusokat a Szolgáltatási szabályzatban fel kell tüntetni.
- A szolgáltatói kulcsok generálására csak olyan kriptográfiai modulok alkalmazhatók, amelyek megfelelnek a szolgáltató szabályzataiban nyilvánosságra hozott műszaki és egyéb követelményeknek.
- A végfelhasználói tanúsítványok aláírását ellátó szolgáltatói tanúsítványok lejáratát megelőzően a szolgáltatónak új tanúsítványt kell generálnia, s mindent el kell követnie annak érdekében, hogy a tanúsítvány cseréje ne okozzon zavart az érintett felek számára.
- Ezeket a műveleteket úgy kell elvégezni, a megfelelő időtartam álljon rendelkezésre minden szolgáltatói partner és érintett fél számára az átállási feladatok végrehajtására. Ez nem vonatkozik arra az esetre, amikor a Szolgáltató befejezi a tevékenységét.
- Szolgáltatónak dokumentált eljárásokkal kell rendelkeznie a szolgáltatói kulcsok generálására, aminek legalább a következőket kell tartalmaznia:
    - Munkakörök, akik részt vesznek az eljárásban (akár belső, akár külcső résztvevőről van szó);
    - A munkakörök által végrehajtandó feladatok az egyes fázisokban;
    - Felelősségek az eljárás során és azt követően;
    - Az eljárás során végrehajtandó adminisztrációs feladatok (amik bizonyítékul is szolgálnak a későbbiekben a megfelelésre).
- A szolgáltatónak az eljárás során egy olyan riportot kell előállítania, ami bizonyítja, hogy az megfelelt a szabályozásnak, és a kulcspár integritása és bizalmassága biztosított volt. A riportot alá kell írnia:
    - Gyökér hitelesítő egység esetén az a bizalmi munkakört betöltő személynek, aki felelős a kulcsgenerálásért és egy a szolgáltató menedzsmentjétől független auditornak, aki az eljárást követve biztosítja, hogy a riport hűen dokumentálja a végrehajtott eljárást.
    - Köztes hitelesítő egység esetén az a bizalmi munkakört betöltő személy, aki felelős a kulcsgenerálásért és aki az eljárást követve biztosítja, hogy a riport hűen dokumentálja a végrehajtott eljárást.

Amennyiben a végfelhasználói kulcsokat a szolgáltató állítja elő:

- A szolgáltatói által generált végfelhasználói kulcsok esetén olyan algoritmusok alkalmazhatók, amelyek a tanúsítvány érvényességi ideje alatt megfelelnek a hitelesítési rend szerinti felhasználási célra.
- A végfelhasználói kulcsok generálásánál csak olyan algoritmus és kulcshosszúság használható, amely megfelel a hitelesítési rend szerinti felhasználási célravonatkozó szabványoknak, illetve a Nemzeti Média- és Hírközlési Hatóságnak engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának a tanúsítvány érvényességi ideje alatt.
- A szolgáltatónak vissza kell utasítani azon igényléseket, amelyek nem felelnek meg a 6.1.5 és 6.1.6 fejezetekben közzétett kulcselvárásoknak.
- A szolgáltatói által generált végfelhasználói kulcsokat biztonságos módon kell előállítani és megőrizni, amíg a szolgáltató kezelésében vannak.

6.1.2 Magánkulcs eljuttatása Végfelhasználóhoz

A végfelhasználó magánkulcsa olyan módon juttatandó el a végfelhasználó eszközére, illetve a bizalmi szolgáltatóhoz, aki azt kezelni fogja, ami biztosítja a bizalmasságát és integritását. Amennyiben a magánkulcs nem annak Átvevőjéhez kerülne eljuttatásra, akkor a magánulcshoz tartozó összes tanúsítványt vissza kell vonnia Szolgáltatónak.

Szolgáltatónak a végfelhasználói magánkulcs minden példányát törölnie kell az Átvevőhöz való eljuttatást követően, kivéve a 4.12 Kulcsletét és kulcshelyreállítás fejezetben megadott eseteket.

[NCP+: Szolgáltatónak a gondoskodnia kell az Ügyféleszköz biztonságáról annak elkészítése, tárolása és Átvevőhöz juttatás során.]

6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A szolgáltatói aláírások ellenőrzésére szolgáló nyilvános kulcsokat az érintett felek számára olyan módon kell biztosítani, ami garantálja azok integritását és hitelességét.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

A szolgáltatónak a szolgáltatói nyilvános kulcsot Interneten elérhetővé kell tennie.

6.1.5 Kulcsméretek

Lásd a 6.1.1 fejezetet.

6.1.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

Nincs előírás.

6.1.7 A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)

A Gyökér Hitelesítő Egység kulcsa kizárólag a következő célokra alkalmazható:

- Gyökér Hitelesítő Egység tanúsítványának aláírása (Önaláírt tanúsítvány)
- Köztes Hitelesítő Egység tanúsítványának aláírása és kereszthitelesítés
- Belső Szolgáltatói tanúsítványok aláírása (pl. OCSP válaszadó)

- Tesztelési célra, amennyiben az Éles felhasználáshoz a Gyökér Hitelesítő Egység aláírása szükséges

A kulcspárok előállítására, generálásrára, telepítésére, továbbítására eltérő szabályok vonatkoznak szolgáltatói és végfelhasználói tanúsítványok esetén melyet a következő táblázat ír le.

		Végfelhasználói tanúsítvány				**Kiadói tanúsítvány**	
		Ügyfél generálja LCP, NCP	Eszköz szolgáltatás-sal NCP+	Kulcs-vissza-állítással LCP, NCP	Kulcsmene dzsment NCP+	Köztes CA, OCSP, Timestamp	Root CA
1	Ki végzi a kulcspár genárálást?	Ügyfél végzi	Tanúsítvány kiadó RA jogosultságú munkatársa védett zónán belül	Ügyfél kérésére HSM-en belül jön létre	Ügyfél kérésére HSM-en belül jön létre	Bizalmi jogkörrel rendelkező felhasználók kettős kontrollal, védett zónán belül	
2	Szoftveres vagy hardveres?	Ügyfél rendelkezik róla csak információ-val	Hardveres, SSCD kártyán belül	Hardveres, HSM-en belül, védett zónán belül	Hardveres, HSM-en belül, védett zónán belül	Hardveres, HSM-en belül jön létre, védett zónán belül	
3	Hogyan jut el a privát kulcs a felhasználóhoz?	Ügyfélnél jön létre	Második csatornán keresztül	HTTPS kapcsolaton keresztül, ügyfél által megadott jelszóval titkosított állományban	Nem jut el.	Bizalmi jogkörrel rendelkező felhasználók kettős kontrollal kezelik	
4	Hogyan jut el a publikus kulcs a CA-hoz?	Online	Kulcspár generálásakor jön szolgáltatónál jön létre.			Bizalmi jogkörrel rendelkező felhasználók kettős kontrollal kezelik	
5	A CA publikus kulcsa hogyan jut el az értintett felekhez?	-	-	-	-	Szabványos módon AIA:CAIssuer mezőkön keresztül Online	Alkalmazásba szerződéses bekerüléssel
6	Kulcsméretek	RSA 2048 bit+	RSA 2048 bit+	RSA 2048 bit+	RSA 2048 bit+	RSA 2048 bit+	RSA 2048 bit+
7	A publikus kulcs paramétereket ki adja meg?	Ügyfél	Szolgáltató, rendszer konfiguráción keresztül			Szolgáltató, rendszer konfiguráción keresztül	

8	A publikus kulcs paraméterek ellenőrzésre kerülnek-e?	Igen, ismétlődésre és Debian gyenge kulcs listával szemben			
9	Milyen célokra használhatók a kulcsok	Aláírásra, bélyegzésre, titkosításra, Kódaláírásra, SSL kommunikáció titkosításra, a belefoglalt X509v3 biteknek megfelelően.	Aláírásra, bélyegzésre	OCSP: ocsp válaszadásra Timestamp: Időbélyegzésre, Köztes kiadó: Végfelhasználói és köztes kiadói tanúsítványok kiadására	Root: Köztes kiadók kiadására, idélyegző és ocsp tanúsítvány kiadására.
10	Milyen célokra tiltott a kulcsok használata	Minden egyéb célra használatuk tiltott.		Minden egyéb célra használatuk tiltott.	

6.2 Magánkulcs védelem és kriptográfiai modul előírások

A szolgáltatónak olyan fizikai és logikai védelmeket kell implenetálni, amelyek megakadályozzák a jogosulatlan tanúsítványkiadást.

6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások

A szolgáltatói kulcspár generálásnak és a magánkulcs tárolásának és felhasználásának egy biztonságos kritográfiai eszközön kell megvalósulni, amely:

- Legalább EAL4 tanúsítással rendelkezik az ISO/IEC 15408 vagy ezzel ekvivalens IT biztonsági elvárásrendszer szerint; vagy
- Megfelel az ISO/IEC 19790 vagy a FIPS PUB 140-2 [12] level 3 elvárásainak.

A kritográfiai eszköz esetében gondoskodni kell a hamisítás elleni védelemről a szállítás és a tárolás során is, és biztosítani kell a helyes működését. Az eszköz megsemmisítése esetén gondoskodni kell a rajta tárolt magánkulcsok megsemmisítéséről (ez nem vonatkozik a kulcs összes példányára, csak az eszközön lévőre).

6.2.2 Magánkulcs többszereplős (n-ből m) használata

Nincs előírás

6.2.3 Magánkulcs letétbe helyezése

Lásd a 4.12 fejeztet.

6.2.4 Magánkulcs mentése

A szolgáltatói magánkulcs mentése és visszaállítása csak bizalmi munkaörökben lévő munkatársak által, kettős kontroll alatt végezhető fizikailag védett környezetben. E műveletre feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a szabályzatokkal összhagban kell zajlani. A szolgáltatói magánkulcs számára a kritográfiai eszközön kívül is az eszköz által biztosított védelmi szintet kell biztosítani. A kulcs titkosítása

során olyan algoritmust és kulcsméretet kell alkalmazni, ami annak teljes hátralévő idejében biztosítja a védelmet. A szolgáltatói magánkulcs nem üzemben lévő másolatait legalább a produktív kulccsal azonos szintű biztonsági eljárásokkal kell védeni.

A szolgáltatói magánkulcs nem lehet elérhető a kritográfiai eszközön kívül.

6.2.5 Magánkulcs archiválása

Nincs előírás

6.2.6 Magánkulcs bejuttatása kriptográfiai modulba, vagy onnan történő exportja

Lásd a 6.2.4 fejezetet.

6.2.7 Magánkulcs tárolása kriptográfiai modulban

Lásd a 6.2.1 fejezetet.

6.2.8 A magánkulcs aktiválásának módja

Nincs előírás

6.2.9 A magánkulcs deaktiválásának módja

Nincs előírás

6.2.10 A magánkulcs megsemmisítésének módja

A lejárt vagy használaton kívül helyezett szolgáltatói magánkulcsok minden (éles, mentett vagy archivált) példányát meg kell megsemmisíteni, olyan módon hogy az ne legyen visszaállítható.

6.2.11 A kriptográfiai modulok értékelése

Lásd a 6.2.1 fejezetet.

6.3 A kulcspárkezelés további szempontjai

A Szolgáltatónak megfelelő módon kell használnia az aláíró / bélyegző kulcsokat, s nem használhatja őket az érvényességük végét követően.

- A tanúsítványokat és érvényességi információkat aláíró / bélyegző kulcsok nem használhatók semmilyen más célra.
- A tanúsítványokat aláíró / bélyegző kulcsok csak fizikailag védett helyszínen használhatók.
- A Szolgáltatói magánkulcsnak kompatibilisnek kell lenni a 6.1.1 fejezettel összhangban a tanúsítványok aláírására alkalmazott hash és aláíró eljárásokkal és kulcshosszakkal.
- Amennyiben a Szolgáltató önaláírt tanúsítványt bocsát ki, a tanúsítvány atribútumainak az ITU-T X.509 szerint meg kell felelni a meghatározott kulcshasználatnak.

6.3.1 Nyilvános kulcs archiválása

Nincs előírás.

6.3.2 A tanúsítványok és kulcspárok használatának periódusa

[DVCP, OVCP, IVCP: A végfelhasználói tanúsítványok érvényességi ideje nem lehet 39 hónapnál hosszabb.]

6.4 Aktiváló adat

Az aktiváló adattal kapcsolatos kérdéseket az alábbi fejezetek írják le.

A Szolgáltatói kulcspár telepítése és helyreállítása a kriptográfiai eszközön kizárólag bizalmi munkakörben foglalkoztatott munkatársak, legalább kettős kontrollja alatt valósulhat meg.

6.4.1 Aktiváló adat generálás és telepítés

Az Ügyféleszköz / magánkulcs aktiválási adatát biztonságosan kell előállítani és az eszköztől függetlenül kell eljuttatni a végfelhasználóhoz.

6.4.2 Aktiváló adat védelme

A végfelhasználói aktiválási adatát kizárólag a végfelhasználó ismerheti meg.

6.4.3 Egyéb aktiváló adattal kapcsolatos előírások

A végfelhasználók részére kibocsátott kriptográfiai eszközök aktiválásának és deaktiválásának biztonságosan kell megvalósulni.

6.5 Informatikai biztonsági előírások

A szolgáltatónak a rendszerei elérését csak az arra jogosult személyek számára kell korlátozni. Ennek érdekében:

- Tűzfalakkal védi a belső zónák határát a jogosulatlan hozzáférés megakadályozása érdekében (beleértve az Ügyfelek és Érintett felek átali eléréseket is).
- Az érzékeny adatokat védeni kell az adathordozók újrafelhasználása során történő feltárástól.

Az egyes tevékenységekre a következő követelmények vonatkoznak:

Tanúsítvány generálás

- A helyi hálózati eszközöknek fizikailag és logikailag is biztonságos helyre kerülni, konfigurációjukat rendszeresen felül kell vizsgálni az Szolgáltatói előírásaival szemben.

Közzététel

- A tanúsítványtárhoz tanúsítványok hozzáadása, törlése és a kapcsolódó információk módosítása csak az arra jogosultak számára legyen lehetséges.

Tanúsítvány visszavonás

- A visszavonási információk módosítása csak csak az arra jogosultak számára legyen lehetséges.

Tanúsítvány kiadás és visszavonás kezelés

- A szolgáltató folyamatosan monitorozó és riasztó eszközöket biztosítson annak érdekében, hogy észlelhesse, rögzíthesse és időben reagálhasson bármilyen az erőforrásait érintő jogosultalan vagy szokatlan hozzáférési probálkozásra.

6.5.1 Speciális informatikai biztonsági műszaki követelmények

Szolgáltatónak multifaktoros azonosítást kell megkövetelnie minden tanúsítványkiadásra jogosult felhasználó esetében.

6.5.2 Az informatikai biztonság értékelése

Nincs előírás.

6.6 Életciklusra vonatkozó biztonsági előírások

6.6.1 Rendszerfejlesztési előírások

A biztonsági követelmények elemzését el kell végezni a - Szolgáltató által vagy az ő megbízásából végzett - rendszerfejlesztési projektek tervezési és követelménymeghatározási szakaszában, annak érdekében, hogy a biztonság be legyen építve az informatikai rendszerekbe.

Változáskezelési eljárásokat kell alkalmazni a Szolgáltatói szoftver új verzióinak kiadásai, a szoftvermódosítások és szoftverjavítások esetén, valamint a konfigurációváltozásokra, amelyek a Szolgáltató biztonsági szabályait érintik. Az eljárások között szerepelni kell a dokumentáció aktualizálásának is.

6.6.2 Biztonságkezelési előírások

A Szolgáltatónak megbízható rendszereket és termékeket kell használnia, amelyek védettek a módosítás ellen és biztosítják az ellátott műveletek műszaki biztonságát és megbízhatóságát.

- A Szolgáltatói rendszereket és információkat védeni kell a vírusok, a rosszindulatú és a nem engedélyezett szoftverektől.
- Eljárásokat kell megállapítani és végrehajtani az összes megbízható és adminisztratív szerepkörre, amelyek hatással vannak a szolgáltatások nyújtására.
- Szolgáltatónak eljárásokat kell meghatározni és alkalmazni biztosítandó, hogy:
    - a biztonsági javítások ésszerű időn belül (legfeljebb 6 hónapon belül) alkalmazásra kerülnek, miután azok megjelentek;
    - A biztonsági javítások nem alkalmazhatók, ha azok olyan plusz biztonsági réseket tartalmaznak vagy instabilitást okozhatnak, amelyek hátrányosabbak, mint a kínált javítás; és a nem alkalmazás okai dokumentálásra kerültek.

6.6.3 Életciklusra vonatkozó biztonsági előírások

Szolgáltatónak monitoroznia kell a kapacitáskihasználtságát és előrejelzéseket kell készíteni a kapacitáskövetelmények várható alakulásáról, biztosítandó, hogy elegendő tár- és feldolgozási kapacitás áll majd rendelkezésre a jövőben is.

6.7 Hálózati biztonság

A bizalmi szolgáltatónak a következő hálózati biztonsági feltételeknek kell megfelelni:

- A szolgáltatói rendszereknek legalább biztonságos zónán belül kell elhelyezkednie, s a szolgáltatónak biztonsági eljárással kell szavatolnia ezen rendszerek valamint a nagy biztonságú zónával való kommunikáció biztonságát.
- A szolgáltatói rendszerek esetében a szolgáltatásnyújtáshoz nem használt felhasználói fiókokat, alkalmazásokat szolgáltatásokat, kapcsolatokat, protokollokat és portokat tiltani kell vagy el kell távolítani. A meghatározott szabályokat rendszeresen felül kell vizsgálni.
- A szolgáltató a biztonságos zónához és a nagy biztonságú zónához csak megbízható szerepkörrel rendelkező munkatársnak adhat hozzáférést.
- A szolgáltatónak kockázatértékelés alapján különböző hálózatokba vagy zónákba kell szegmentálnia a rendszereit, figyelembe véve a megbízható rendszerekkel és szolgáltatásokkal való funkcionális logikai és fizikai kapcsolatokat.
- A szolgáltatói rendszerek számára külön hálózatot kell biztosítani. A információbiztonsági szabályzat érvényesítésére használt rendszereket más célra nem szabad használni. A produktív rendszereknek el kell különülni a fejlesztési, teszt és egyéb felhasználású rendszerektől.
- A különböző megbízható rendszerek közötti kommunikációnak megbízható csatornán kell folynia, ami logikailag elkülönül az egyéb kommunikációs csatornáktól, s biztosítja a végpontok megbízható azonosítását és a forgalmazott adatok bizalmasságát és sértetlenségét.
- Amennyiben a szolgáltatáshoz nagy rendelkezésre állású külső elérés szükséges, akkor a hálózati kapcsolatnak redundánska kell lennie, hogy biztosítsa a szolgáltatás elérését amennyiben valamelyik kapcsolat kiesik.
- Szolgáltatónak rendszeresen sebezhetőségi ellenőrzést kell végeznie a nyilvános és privát IP címein és rögzítenie kell annak bizonyítékait, hogy a vizsgálatot olyan független, a megfelelő ismeretekkel, tapasztalattal és eszközökkel bíró személy vagy szervezet végezte, amely megbízható riportot eredményez. Az ellenőrzést negyedévente vagy szignifikáns hálózati változás esetén kell elvégezni.
- A szolgáltatói rendszeren rendszeresen betörési ellenőrzést kell végezni és rögzítenie kell annak bizonyítékait, hogy a vizsgálatot olyan független, a megfelelő ismeretekkel, tapasztalattal és eszközökkel bíró személy vagy szervezet végezte, amely megbízható riportot eredményez. Az ellenőrzést évente vagy szignifikáns infrstuktuális változás, alkalmazásmódosítás esetén kell elvégezni.

6.8 Időbélyegzés

Az időbélyegzéssel kapcsolatos előírásokat és megfelelőségeket Szolgáltató Időbélyegzés Hitelesítés Rendjének és Szolgáltatási szabályzatának kell tartalmaznia.

7 Tanúsítvány, CRL és OCSP profilok

7.1 Tanúsítványprofil

A Bizalmi szolgáltató által kibocsátott Tanúsítványok feleljenek meg az RFC 5280, RFC 6818 és az ITU-T X.509 specifikációknak.

7.1.1 Verzió szám(ok)

A Bizalmi szolgáltató az X.509 specifikáció szerinti "V3" tanúsítványokat bocsásson ki.

7.1.2 Tanúsítvány kiterjesztések

A Bizalmi szolgáltató az X.509 specifikáció szerinti tanúsítványkiterjesztéseket használhat, a kritikus mezők szükség szerinti jelzésével.

7.1.3 Az algoritmus objektum azonosítója

A tanúsítványban jelezni kell annak az algoritmusnak a megnevezését és paramétereit, amellyel a tanúsítvány hitelesítésre került.

7.1.4 Névformák

Az Alany névfomái tekintetében lásd a 3.1.1. Névtípusok fejezetet.

A tanúsítvány "Issuer" mezőjében szereplő értéknek meg kell egyeznie a kibocsátó Tanúsítványának "Subject" mezőjében szereplő értékkel.

7.1.5 Névhasználati megkötések

A Bizalmi szolgáltatónak az alkalmazott névhasználati megkötéseket a "nameConstraints" mezőben kell jeleznie, a mezőt kritikusnak megjelölve.

7.1.6 A Hitelesítési rend azonosítója

A Bizalmi szolgáltatónak a jelen Hitelesítési rendek alapján kibocsátott Tanúsítványokba fel kell vennie a nem kritikus Hitelesítési Rend kiterjesztést, jelezve benne az alkalmazott Hitelesítési rend OID alapú azonosítóját.

7.1.7 A szabályzati korlátozás kiterjesztés használata

Nincs előírás.

7.1.8 Szabályzatminősítő szintaxis és szemantika

A Bizalmi szolgáltató a Hitelesítési rend (Certificate Policy) kiterjesztés Szabályzatminősítő (Policy Qualifier) mezejében rövid információt helyezhet el a Tanúsítvány felhasználhatóságával kapcsolatban. A mezőnek tartalmaznia kell a Szolgáltatási szabályzat on-line elérhetőségét is (URI).

7.1.9 A kritikus Hitelesítési rend kiterjesztés feldolgozása

Nincs megkötés.

7.2 Tanúsítványvisszavonási profil

7.2.1 Verziószám(ok)

A Szolgáltató által kibocsátott tanúsítványvisszavonási listák feleljenek meg az RFC 5280 és ITU-T X.509 specifikáció szerinti "V2" verziójú tanúsítványvisszavonási listának.

7.2.2 Tanúsítvány visszavonási lista kiterjesztések

A Bizalmi szolgáltató a CRL sorozatszám (CRL number) nem kritikus visszavonási lista kiterjesztést támogassa a visszavonási listák egyesével növekvő sorozatszámának megadásával.

7.3 Online tanúsítvány-állapot szolgáltatás (OCSP) profil

A Bizalmi szolgáltatónak az RFC 6960 szerinti online tanúsítvány-állapot szolgáltatást kell üzemeltetnie.

7.3.1 Verziószám(ok)

A Bizalmi szolgáltató az RFC 6960 szerinti "V1" verziójú online tanúsítványállapot kéréseket és válaszokat támogassa.

7.3.2 OCSP kiterjesztések

Nincs megkötés.

8 A megfelelőség vizsgálata

A Bizalmi szolgáltatónak tevékenységét összhangban kell végeznie

- a vonatkozó és hatályos Európai Uniós és hazai szabályozással,
- jelen Hitelesítési rend követelményeivel, valamint
- a működési helye szerinti Bizalmi felügylet Bizalmi szolgáltatások nyújtására vonatkozó nyilvántartásában szereplnie kell.

A Szolgáltató külső megfelelőségértékeléséhez végzett vizsgálat során az alábbiakat kell betartani:

- figyelembe kelle venni Bizalmi Szolgáltató összes értékelendő bizalmi szolgáltatás sajátosságát;
- biztosítani kell, hogy a vizsgálat tárgyához tartozó minden szolgáltatói tevékenyéget lefedjen a vizsgálat;
- a vizsgálatot vonatkozó szabványok, nyilvánosan hozzáférhető specifikációk és/vagy jogszabályi követelmények alapján kell végezni.

8.1 Az ellenőrzések körülményei és gyakorisága

[PTC: Amíg a Bizalmi szolgáltató tanúsítványkibocsátási szolgáltatást nyújt, legalább évente köteles a jogszabályi és szabványmegfelelőséget belső és külső auditok elvégzésével vizsgálni.

A Bizalmi Szolgáltatónak legalább évente ellenőriznie kell a Kihelyezett Regisztrációs Egységek működését is, kivéve, ha a Kihelyezett Regisztrációs Egység a vonatkozó szabványoknak való megfelelősséget igazoló éves külső audit jelentéssel rendelkezik. A Kihelyezett Regisztrációs Egységekre ugyanazon követelmények vonatkoznak, mint a Szolgáltató belső Regisztrációs egységére.]

A Bizalmi szolgáltató köteles foylamatosan ellenőrizni jelen Hitelesítési rendjében és Szolgáltatási szabályzataiban foglaltak betartását valamint szigorú ellenőrzés alatt kell tartania szolgáltatásai minőségét önellenőrzések végrehajtásával. Ennek cél megvalósulása érdekében a Bizalmi szolgáltatónak évente egyszer belső audit kell tartania.

8.2 Az értékelő és szükséges képesítése

A belső auditokat olyan szakembernek kell végeznie, aki felsőfokú képesítéssel és legalább 5 éves szakmai gyakorlattal rendelkezik szabályozási, informatikai rendszeraudit vagy bizalmi szolgáltatási területen.

[DVCP, OVCP: A külső megfelelőségértékeléseket olyan természetes vagy jogi személynek avagy természetes személyek csoportjának kell végeznie, aki vagy amely

- képes a *8 A megfelelőség vizsgálata* fejezetben megadott szabványokra vonatkozó audit elvégzésére;
- megfelel a *8.3 Az auditor és az auditált rendszerelem kapcsolata* fejezetben megadott követelménynek;

- megfelelő jártassággal bír vagy bírnak a Publikus Kulcsú Infrastruktúra (PKI), az IT illetve IT biztonsági megoldások, technológiák és auditok terén valamint Kihelyezett Regisztrációs Egységnél végzett audit során annak funkcióival kapcsolatban;
- ETSI szabványok alapján végzett auditok esetén rendelkezik vagy rendelkeznek
    - az ETSI EN 319 403 szerinti akkreditációval, *vagy*
    - egy ezzel egyenértékű nemzeti szabvány szerinti akkreditációval, *vagy*
    - a Nemzeti Akkreditációs Hatóság által ISO 27001 szerint végrehajtott ISO 27006 szerinti akkreditációval;
- WebTrust audit végzése esetén rendelkezik vagy rendelkeznek WebTrust audit elvégzéséhez szükséges engedéllyel;
- tevékenységét vagy tevékenységüket jogszabályok vagy szakmai etikai kódex szabályozza;
- rendelkezik az auditor tevékenység végzéséből eredő mulasztások, hibák esetére szóló, legalább egymillió USD fedezetű biztosítással.]

8.3 Az auditor és az auditált entitás kapcsolata

A Bizalmi szolgáltató a belső megfelelőségértékeléseket a Rendszerellenőr szerepkörrel felruházott bizalmi alkalmazottai segítségével is elvégezheti.
A külső megfelelőségértékeléseket olyan értékelő végezheti, aki vagy amely a Szolgáltatótól független.

8.4 Az értékelés által lefedett területek

Szolgáltató belső megfelelőségértékelésének az alábbi területeket kell lefednie:

- szabályzatok hatályos jogszabályoknak és szabványoknak való megfelelése;
- az alkalmazott folyamatok szabályzatoknak való megfelelősége.

Külső megfelelőségértékelés esetén a Megfelelőségértékelőnek az adott értékelési rendszer által meghatározott követelmények és kritériumok teljesülését kell értékelnie.

8.5 A hiányosságok kezelése

[PTC: A belső és külső megfelelőségértékelések eredményét egy értékelésjelentésben kell összefoglalni, amely kitér a vizsgált rendszerelemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben rögzíteni kell a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket.]

8.6 Az eredmények közzététele

A Bizalmi szolgáltató nem köteles a belső megfelelőségértékelés-jelentés publikálására, az abban foglaltakat bizalmas információként kezelheti.

[DVCP, OVCP: A Bizalmi szolgáltatónak az auditidőszakot követő három (3) hónapon belül nyilvánosságra kell hoznia az auditjelentést. A Szolgáltató nem köteles nyilvánosságra hozni az auditjelentés azon általános megállapításait, melyek nincsenek hatással az audit eredményére.]

9 Egyéb üzleti és jogi tudnivalók

9.1 Díjak

A Bizalmi szolgáltató köteles elérhetővé tenni az Előfizetők részére a szolgáltatások kapcsán alkalmazott díjakat.

A Bizalmi szolgáltató az alábbi szolgáltatások szabályzatokban leírt módon való igénybevételéért nem számíthat fel díjat:

- online tanúsítványtár használata;
- tanúsítványállapot-szolgáltatások (CRL és OCSP).

9.1.1 A tanúsítványkiadás és -megújítás díjai

A Bizalmi szolgáltató a tanúsítványkiadás és -megújítás szolgáltatások igénybevételéért a nyilvános árlista alapján számíthat fel díjat, illetve attól Előfizetővel való előzetes egyeztetés alapján eltérhet.

9.1.2 Tanúsítvány hozzáférési díjak

A Bizalmi szolgáltató a tanúsítványtár szabályzatokban leírt módon való on-line igénybevételéért nem számíthat fel díjat.

9.1.3 A tanúsítványállapot-változtatási és tanúsítványállapot-szolgáltatás díjai

A Bizalmi szolgáltató a tanúsítványállapot-változtatási és tanúsítványállapot-szolgáltatások szabályzatokban leírt módon való igénybevételéért nem számíthat fel díjat.

9.1.4 Egyéb szolgáltatások díjai

A Bizalmi szolgáltató az egyéb szolgáltatások igénybevételéért a nyilvános árlista vagy egyedi megállapodás alapján számíthat fel díjat.

9.1.5 Visszatérítési politika

Nincs megkötés.

9.2 Pénzügyi felelősség

A Bizalmi szolgáltatónak teljesítenie kell az eüt. szerinti rendeletben foglalt pénzügyi megfelelőséget (lásd eüt. 106. § a)).

A Bizalmi Szolgáltató a mindenkor hatályos polgári törvénykönyvben meghatározott szerződésszegésért való felelősség szabályai szerint a mindenkor hatályos bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló rendeletben meghatározott mértékig felel a kibocsátott tanúsítvánnyal okozott kárért.

9.2.1 Biztosítási fedezet

A Bizalmi szolgáltatónak rendelkeznie kell megfelelő erőforrással vagy felelősségbiztosítással az Ügyfelek és érintett felek kártalanításhoz az eIDAS vonatkozó rendelkezései alapján. A szolgáltató korlátozhatja a felelősségvállalása értékét, az Ügyfeleket és Érintetteket a weboldalán keresztül vagy a tanúsítványban tájékoztatva.

A bizalmi szolgáltató köteles megbízhatóság érdelében felelősségbiztosítással rendelkezni. A felelősségbiztosításnak ki kell terjedni a szolgáltató által nyújtott bizalmi szolgáltatásokkal összefüggésben okozott károkra és költségekre:

- a bizalmi szolgáltatási ügyfélnek a bizalmi szolgáltatási szerződés megszegésével összefüggésben okozott károkra,
- a bizalmi szolgáltatási ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,
- az az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvényben foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, a bizalmi szolgáltatások általános szabályairól szóló törvény szerinti költségekre, és
- az eIDAS Rendelet vonatkozó rendelkezései alapján a bizalmi felügyelet által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.

A szolgáltatónak biztosítania kell, hogy az általa kötött biztosítási szerződés kifejezetten nevesítse, hogy a szerződés kiterjed a fentiekre.

A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem lehet alacsonyabb, mint 3 000 000 forint.

9.2.2 Egyéb eszközök

Nincs megkötés.

9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák

A szolgáltató tegye közzé, hogy az általa nyújtott garanciák és biztosítások mennyiben terjednek ki más felek által okozott károkra.

A Bizalmi Szolgáltató a mindenkor hatályos polgári törvénykönyv rendelkezései szerint felel a vele szerződésben nem álló érintett feleknek okozott károkért.

9.3 Bizalmas üzleti információk kezelése

A Bizalmi Szolgáltató köteles az információs önrendelkezési jogról és az információszabadságról szóló jogszabály rendelkezéseinek megfelelően tárolni és kezelni a birtokába jutott bizalmas adatokat.

9.3.1 A bizalmas információk köre

A Bizalmi szolgáltatónak bizalmas információnak kell tekintenie minden az egyes Ügyfelekre vonatkozó adatot, amik nem szerepelnek a 9.3.2 fejezetben.

9.3.2 A bizalmas információk körén kívül eső adatok

A Bizalmi szolgáltatónak nem kell bizalmas információnak tekintenie azon adatokat, amiket személyes jellegüktől megfosztott (pl. anonimizálással), valamint azokat amelyeket a szolgáltatása részeként hoz nyilvánosságra a tanúsítványtárán keresztül (tanúsítvány adatok és tanúsítvány állapot információk).

A Szolgáltatónak a szolgáltatási szabályzatban nyilvánosságra kell hozni minden további olyan szolgáltatási információt, melyet nem tekint bizalmasnak.
A nem bizalmas adatokat Szolgáltató nyilvánosságra hozhatja, megoszthatja partnereivel, illetve nyilvánosságra kerülésükért nem tartozik felelősséggel.

9.3.3 A bizalmas információk védelme

A Bizalmi szolgáltató a bizalmas adatok kezelésére voatkozó szabályokataz elektronikus ügyintézési törvény vonatkozó rendelekzései taralmazzák.

A Bizalmi szolgáltató felelősséggel tartozik az általa kezelt bizalmas adatok védelméért. Ezeket az adatokat csak azon munkatársai és partnerei ismerhetik meg, amelyek munkájához ezen adatok ismerete szükséges. Más személyek hozzáférését ki kell zárni jogi úton és lehetőség szerint műszaki-biztonsági óvintézkedésekkel.

Minden a bizalmas adathoz hozzáférő személyt szerződésben vagy titoktartási nyilatkozat aláírásával kell kötelezni a bizalmasság megőrzésére.

A Bizalmi szolgáltatónak a szolgáltatási szabályzatban nyilvánosságra kell hozni, mely esetekben és kik számára fedheti fel a bizalmas adatokat.

9.4 Személyes adatok kezelése

A Bizalmi szolgáltatónak gondoskodnia kell az általa kezelt személyes adatok védelméről az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseinek megfelelően. A szolgáltató csak a szolgáltatás nyújtásához szükéges személyes adatokat igényelheti, a 95/46/EK Adatvédelmi Direktívának megfelelően.

A Bizalmi szolgáltató köteles az Ügyfélről és a tanúsítványokkal kapcsolatosan rendelkezésére álló nyilvántartott személyes adatokat és információkat - a személyes adatokat is beleértve - a jogszabályi előírások alapájn szerint megőrizni (lásd eüt. 84. § (1)).

A bizalmi szolgáltató nyilvánosnak tekint minden olyan adatot, amely nem szerepel a bizalmas adatok felsorolásában a Szolgáltatási szabályzatban.

9.4.1 Adatkezelési szabályok

A Bizalmi szolgáltatónak rendelkeznie kell adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a személyes információk kezelésére. Az Adatkezelési szabályzatot nyilvánosságra kell hozni a Bizalmi szolgáltató honlapján.

9.4.2 Személyes adatok

A bizalmi szolgáltató csak olyan személyes adatokat gyűjt, amelyek szolgáltatásainak nyújtásához szükségesek vagy a szolgáltatásnyújtás hatékonyságát növelik, s melyek kezeléséről az érintetteket tájékoztatja. A bizalmi szolgáltatónak bizalmas adatként kell kezelnie minden személyes adatot, kivéve a 9.3.2-ben és 9.4.3-ban megadott személyes adatokat.

9.4.3 Személyes adatnak nem minősülő információk

A bizalmi szolgáltató az Ügyfél írásbeli hozzájárulása alapján nyilvánosságra hozza a tanúsítvány Alanyaként feltüntetett személyes és szervezeti adatokat, továbbá nyilvánosságra hozza a tanúsítványok állapotinformációit.

9.4.4 Személyes adatok védelme

A bizalmi szolgáltató köteles biztonságosan tárolni és védeni a tanúsítványkiadással kapcsolatos és a Tanúsítványban nem szereplő személyes adatokat. Az adatokat megfelelő intézkedésekkel védeni kell a jogosulatlan hozzáférés és a megváltoztatás ellen, különösen az Ügyfél és a szolgáltató egyes egységei között történő továbbítás során. Továbbá védeni kell őket, az adatvesztés, a károsodás és a nem engedélyezet feldolgozás ellen. Lásd még a 6.2.2, 6.3.2, 6.3.4, 6.4.3, 6.4.5 és 6.5.6 fejezeteket.

9.4.5 Személyes adatok felhasználása

A bizalmi szolgáltató a tanúsítványokkal kapcsolatos személyes adatokat az 5.5.2 szerinti időtartamban megőrzi.

9.4.6 Adatkezelés

A bizalmi szolgáltató csak a jogszabályok által meghatározott esetekben adhatja ki az Ügyfélről tárolt személyes adatokat az Ügyfél értesítése nélkül.

A bizalmi szolgátlató az információs önrendelkezési jogról és az információszabadságról szóló törvény adatkezlési szabályait köteles betartani.

A bizalmi szolgáltató személyes adatokat az ügyfél előzetes hozzájárulása alapján kezel, amennyiben az előzetes hozzájárulás beszerzése lehetetlen vagy aránytalan többlet kötelezettséggel vagy aránytalan költséggel járna, és a személyes adat kezelése a bizalmi szolgáltatóra vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy bizalmi szolglтató vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

9.4.7 Egyéb adatvédelmi követelmények

Nincs előírás.

9.5 Szellemi tulajdonjogok

A Bizalmi szolgáltató által ügyfelei részére kibocsátott magán- és nyilvános kulcs tulajdonosa az Előfizető, teljes jogú felhasználója pedig a Végfelhasználó. A Bizalmi szolgáltató által ügyfelei részére kibocsátott tanúsítvány tulajdonosa a Szolgáltató, teljes jogú felhasználója pedig a Végfelhasználó.

A Bizalmi szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat a benne szereplő nyilvános kulccsal és egyéb adatokkal együtt közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.

A Bizalmi szolgáltató tulajdonát képezi a tanúsítványvisszavonási állapotinformáció, amit nyilvánosságra hozhat. A Bizalmi szolgáltató által az Ügyfelek részére kibocsátott egyedi azonosító (OID) a szolgáltató tulajdonát képezi.

A jelen Hitelesítési rend a NetLock kizárólagos tulajdonát képezi. Az Ügyfelek, Végfelhasználók és egyéb Érintett felek a dokumentumot csak a Hitelesítési rend előírásainak megfelelően jogosultak felhasználni, minden egyéb (pl. kereskedelmi) célú felhasználás szigorúan tilos.

A Hitelesítési rend szabadon terjeszthető, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A Hitlesítési rendben és/vagy tanúsítványokban található védett nevek felett a jogtulajdonosuk rendelkezik.

A Hitelesítési rendben hivatkozott művek (szabványok, jogi források) szerzői joga a jog tulajdonosáé.

A bizalmi szolgáltató működése során nem sértheti meg harmadik személyek szellemi tulajdonjogait.

A szolgáltatási tevékenység során alkalmazott összes név, termék, szabályzat, CRL a Szolgáltató tulajdonát képezi, a szoftver és hardver komponensek a Szolgáltató tulajdonát képezik vagy azokat jogszerűen használja.

9.6 Felelősség és garanciák

A bizalmi szolgltató köteles a felelősség és garanciák tekintetében jelen Hitelesítési Rend 5.1 fejezetében foglaltakat betartani.

9.6.1 A tanúsítványkibocsátó egység felelőssége

A bizalmi szolgáltató felel a jelen Hitelesítési rendben, a vonatkozó Szolgáltatási szabályzatában, valamint az Ügyféllel kötött szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan teljesítéséért.

A bizalmi szolgáltató sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért.

A bizalmi szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a mindenkor hatályos Polgári Törvénykönyv általános felelősségi szabálya szerint, a vele szerződésben álló természetes vagy jogi személynek okozott kárért a szerződésszegésért való felelősség szabályai szerint felelős, az elektronikus aláírással, illetve az elektronikusan aláírt elektronikus dokumentummal okozott kárért eIDAS-ban meghatározottak szerint felel.

A nem minősített bizalmi szolgáltató szándékosságát vagy gondatlanságát annak a természetes vagy jogi személynek kell bizonyítania, aki/amely állítása szerint az említett kár megtérítését követeli.

A bizalmi szolgáltató előzetesen tájékoztatja az ügyfeleit az általa nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, úgy a bizalmi szolgáltató nem felelős a szolgáltatások igénybevételéből eredő károkért.

9.6.2 A regisztrációs egység felelőssége

A bizalmi szolgáltató megköveteli a vele együttműködő Regisztráló szervezetektől a jelen Hitelesítési rend és a vonatkozó Szolgáltatási szabályzat előírásainak maradéktalan betartását.

A Regisztráló szervezet felelőssége:

- az Igénylők és az Alanyként feltötüntetett entitások (személy-) azonosságának megállapítása, a szolgátlató rendelkezésére bocsátott adatok ellenőrzése;
- a Képviselt szervezet szervezeti azonosságának, a Képviselt szervezet nevében eljáró személy személyazonosságának és képviseleti jogosultságának megállapítása, ellenőrzése;
- a felvett regisztrációs adatok valódiságának garantálása;
- a szolgáltatási szerződés megkötését megelőzően a szolgáltatások igénybe vevőjének tájékoztatása a Hitelesítési rend és a Szolgáltatási szabályzat tartalmáról és elérhetőségéről, a szolgáltatás igénybevételének feltételeiről;
- általános kötelezettségeinek maradéktalan betartása.

9.6.3 Ügyfelek felelőssége és kötelezettségei

Ügyfélnek haladéktalanul tájékoztatni kell a Bizalmi szolgáltatót

- a következő adatok változásáról: az azonosításához szükséges, a tanúsítványban feltüntetett személyazonosító adatok, más személy képviseletével összefüggésben kiállított tanúsítvány esetén a képviseletre jogosult személy és a képviselt személy adatai, a tanúsítványban feltüntetett egyéb adatok;
- a bizalmi szolgáltatással vagy a tanúsítvánnyal kapcsolatban észlelt, a külön jogszabályban, szolgáltatási szerződésben illetve szolgáltatási szabályzatban meghatározott rendellenességről vagy más, a bizalmi szolgáltatást érintő eseményről, így különösen arról, ha a bizalmi szolgáltatás használatához szükséges, a bizalmi szolgáltató által biztosított Ügyféleszközt jogosulatlan személy használhatta;
- a bizalmi szolgáltatással kapcsolatos jogvita megindulásáról.

9.6.4 Más érintett felek felelőssége

Az Érintett felek saját belátásuk és/vagy szabályzataik alapján dönthetnek az egyes Tanúsítványok elfogadásáról és a felhasználás módjáról. Az érvényesség vizsgálata során a bizalmi szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az Érintett fél megfelelő körültekintéssel járjon el.

9.6.5 Egyéb résztvevők felelőssége

Amennyiben a szervezet képviselője nem személyesen jár el a tanúsítvány igénylése során, úgy a képviselt szervezet felelősséggel tartozik az általa kiadott igazolásokért, különös tekintettel azon igazolásokra, amelyben azt igazolja, hogy az Igénylő jogosult a Szervezet nevét is tartalmazó Tanúsítvány igénylése, állapotváltoztatása, megújítása stb. kapcsán eljárni.

9.7 Szavatosság kizárása

A bizalmi szolgáltató kizárja felelősségét, amennyiben:

- az Érintett fél nem körültekintően jár el a tanúsítványok felhasználása vagy ellenőrzése során, azaz nem a jelen Hitelesítési rend, a Szolgáltatási szabályzat vagy a hatályos jogszabályok szerint jár el;
- az Ügyfelek nem tartják be az Ügyféleszköz illetve a kulcs kezelésével kapcsolatos előírásokat;
- az Érintett felek vagy mások által kibocsátott szabályzatok nem felelnek meg a jelen Hitelesítési rendnek vagy a Szolgáltatási szabályzatnak;
- a bizalmi szolgáltató az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Felügyeleti szerv által jóváhagyott kriptográfai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

A bizalmi szolgáltató korlátozhatja a kártérítési felelősségét az alábbiak szerint:

- a tanúsítvánnyal egy alkalommal vállalható kötelezettség legmagasabb mértékében (tranzakciós limit),
- összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban.

9.9 Kártérítés, kártalanítás

A Bizalmi Szolgáltató felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okozott a vállat kötelezettségének megszegéséből eredően.

A nem minősített bizalmi szolgáltató szándékosságát vagy gondatlanságát annak a természetes vagy jogi személynek kell bizonyítania, aki/amely állítása szerint az említett kár megtérítését követeli.

Amennyiben a bizalmi szolgáltató előzetesen megfelelően tájékoztatja ügyfeleit az általuk nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a bizalmi szolgáltató nem felelős a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.

Minden egyéb esetben a mindenkori hatályos polgári törvénykönyv vonatkozó rendlekezései az irányadóak.

9.10 Hatály

A Hiteleítési rend aktuális verziójának időbeli hatálya a feldlapon jelzett hatálybalépés dátumával kezdődik és határozatlan időre szól.

A Hitelesítési rend személyi hatálya a Szolgáltatóra, annak a Szolgáltatásokban közreműködő munkatársaira, valamint az Ügyfelekre terjed ki.

A Hitelesítési rend tárgyi hatálya kiterjed a bizalmi szolgáltató átla nyújtott Szolgáltatásokra, illetve ezek keretében kibocsájtott tanúsítványokra, valamint Szolgáltatónak a fenti Szolgáltatásokkal kapcsolatban álló összes objektumára és tárgyi eszközére.

9.10.1 Érvényesség

A Hitelesítési rend adott verziója hatályba lépésének napja a Hitelesítési rend fedlapján kerül meghatározásra

9.10.2 Megszűnés

A Hitelesítési rend érvényessége megszűnik egy újabb szabályzat verzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor.

9.10.3 A megszűnés következményei

A Hitelesítési rend visszavonása esetén a bizalmi szolgáltató honlapján teszi közzé a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket. A bizalmi szolgáltató vállalja, hogy a Hitelesítési rend visszavonása esetén is érvényben maradnak a mindenkor hatályos vonatkozó jogzsabályokban meghatározott bizalmas adatok védelmére vonatkozó előírások.

9.11 Egyedi értesítések és a résztvevők közti kommunikáció

A bizalmi szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát, telefonos ügyfélszolgálatot működtet.

9.12 Módosítások

A bizalmi szolgáltató a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén megváltoztatja a Hitelesítési rendjét, a vonatkozó szabályzatait. Rendkívüli esetben a változások azonnali hatállyal is életbe léptethetők.

9.12.1 A módosítási eljárás

A Szolgáltatón belül Szabályzatelfogadó Egység (a továbbiakban: SzEE) működik, amely a Hitelesítési rend és a szabályzatok karbantartásáért felelős. A változtatási igényeket SzEE gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti. A változtatásokat gyűjtve az egység belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső

felülvizsgálaton esnek át. Szolgáltató a változásokat kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A bizalmi szolgáltató elfogadás előtt megvizsgálja a Hitelesítési Rend formai megfelelését az RFC 3647 szabványnak. A hitelesítési rend elfogadására vagy esetlegesen a Felügyelet által már nyilvántartásba vett hitelesítési rendre voantkozóan a bizalmi szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd egyetértés esetén a Felügyelet nyilvántartásba veszi a bizalmi szolgáltató által jóváhagyott és bejelentett Hitelesítési Rendet.

A Szolgáltató jóváhagyás előtt megvizsgálja a Hitelesítési Rendet és a szolgáltatási szabályzatokat, hogy tartalmilag és formailag megfelel-e hatályos jogszabályi követlményeknek. A hitesítési rend és a szabályzatok jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd bejelentés után a hitesítési rendet és a szabályzatokat a Felügyelet nyilvántartásba veszi.

A módosított hitelesítési rend és szabályzatok változatai mindig új verziószámmal kerülnek nyilvánosságra. A hitelesítési rend és a szabályzatok valamint a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente történik. A szabályzatok rendkívüli felülvizsgálatára és módosítására a jogszabályi változások esetén kerül sor. A hitelesítési rend és a szabályzatok felülvizsgálatát a bizalmi szolgáltató a működése során szerzett gyakorlati tapasztalatok alapján is elvégzi.

9.12.2 Az értesítések módja és határideje

A Szolgáltató az Ügyfeleit és Érintett feleket a szabályzat módosításának hatálybalépése előtt 30 nappal tájékoztatja, az új szabályzat tervezetének weboldalon való közzétételével.

9.12.3 A dokumentumazonosító változása

Minden módosítás megváltoztatja a Szabályzat verziószámát és objektumazonosítóját. Azt a módosított szabályzatot, amely csak az újonnan kibocsátásra kerülő tanúsítványokra vonatkozik (de a már kibocsátottakra nem), a Szolgáltató az előző főbb verziótól eltérő Internet címen teszi közzé, így csak az újonnan kibocsátott tanúsítványok mutatói fognak rá hivatkozni, amennyiben a tanúsítványban van ilyen mutató.

,

A bizalmi szolgáltató a Hitelesítési rend változtatása esetén is új verziószámot ad a dokumentumnak, így az az OID változását is eredményezi egyben, vagyis a két eltérő tartalmú dokumentumnak nem lehet azonos OID azonosítója.

9.13 Vitás kérdések rendezése

A bizalmi szolgáltató köteles biztosítani a panaszok bejelentésének elérhetőségét, a panaszok kezelését, valamint köteles tájékoztatni a szolgáltatással összefüggő jogviták peres és peren kívüli kezdeményezésének lehetőségéről, annak feltételeiről, a békéltető testülethez való fordulás jogalapjáról, az eljárásra jogosult hatóságok és békéltető testület vagy más vitarendező szervezetek megnevezéséről, elérhetőségeiről.

9.14 Irányadó jog

A bizalmi szolgáltató tevékenységét a mindenkor hatályos magyar és európai uniós jogszabályoknak megfelelően végzi. A bizalmi szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

9.15 A hatályos jogszabályoknak való megfelelés

Szolgáltatónak bizalmi szolgáltatásait a mindenkor hatályos európai uniós és magyarországi szabályozásnak megfelelően kell nyújtania. A vonatkozó jogszabályokat és az azoknak való megfelelés módját Szolgáltató szolgáltatási szabályzataiban adja meg.

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs megkötés.

9.16.2 Átruházás

A jelen Hitelesítési rendnek megfelelően működő szolgáltató csak a előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3 Részleges érvénytelenség

A jelen Hitelesítési rend egyes rendelkezéseinek bármilyen okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 Igényérvényesítés

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

9.16.5 Vis maior

A bizalmi szolgáltató nem felelős a Hitelesítési rendben és a Szolgáltatási szabályzatban megfogalmazott követelmények hibás vagy késedelmes teljesítéséért, ha a hiba vagy késedelem oka a bizalmi szolgáltató ellenőrzési körén kívül eső, előre nem látható körülmény volt.

9.16.6 Egyéb rendelkezések

Nincs megkötés.