MICROSEC
Számítástechnikai Fejlesztő zrt.

e-Szignó Hitelesítés Szolgáltató
Nem minősített tanúsítvány hitelesítési rendek

e-SZIGNO

Azonosító	1.3.6.1.4.1.21528.2.1.1.31.3.1, 1.3.6.1.4.1.21528.2.1.1.32.3.1, 1.3.6.1.4.1.21528.2.1.1.33.3.1, 1.3.6.1.4.1.21528.2.1.1.34.3.1, 1.3.6.1.4.1.21528.2.1.1.11.3.1, 1.3.6.1.4.1.21528.2.1.1.10.3.1
Verzió	3.1
Első verzió hatálybalépése	2006-11-19
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Ellbogen András
Jóváhagyás dátuma	2013-12-15
Hatálybalépés dátuma	2014-01-31

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
1031 Budapest, Záhony utca 7. D. épület

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat OID: 1.3.6.1.4.1.21528.2.1.1.10 OID: 1.3.6.1.4.1.21528.2.1.1.11	2006-11-19	Dr. Berta István Zsolt
1.1	Hibák javítása	2006-11-19	Dr. Berta István Zsolt
1.2	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően OID: 1.3.6.1.4.1.21528.2.1.1.10.1.2 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.2	2006-12-04	Dr. Berta István Zsolt
1.3	Közjegyzői regisztráció megszüntetése. OID: 1.3.6.1.4.1.21528.2.1.1.10.1.3 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.3	2007-10-28	Dr. Berta István Zsolt
1.4	Megváltozott a fogyasztóvédelem elérhetősége. OID: 1.3.6.1.4.1.21528.2.1.1.10.1.4 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.4	2008-01-01	Dr. Berta István Zsolt
1.5	Változás a II. hitelesítési osztály követelményeiben. OID: 1.3.6.1.4.1.21528.2.1.1.10.1.5 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.5	2008-12-20	Dr. Berta István Zsolt
1.6	Változás a III. hitelesítési osztály követelményeiben. OID: 1.3.6.1.4.1.21528.2.1.1.10.1.6 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.6	2009-03-09	Dr. Berta István Zsolt
2.0	A természetes személyek és az automatizmusok számára kibocsátott tanúsítványokra vonatkozó, valamint a biztonságos hardver eszközt megkövetelő rendek különválasztása. OID: 1.3.6.1.4.1.21528.2.1.1.*.2.0	2010-10-20	Dr. Berta István Zsolt

Verzió	A változás leírása	Hatálybalépés	Készítette
3.0	Cégforma változása. OID: 1.3.6.1.4.1.21528.2.1.1.*.3.0	2012-05-01	Dr. Berta István Zsolt
3.1	Normatívák változása, kisebb változtatások. OID: 1.3.6.1.4.1.21528.2.1.1.*.3.1	2014-01-31	Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec zrt. által üzemeltetett e-Szignó Hitelesítés Szolgáltató által meghatározott nem minősített hitelesítési rendeket tartalmazza.

1.1. Áttekintés

A *Hitelesítési rend* egy "szabálygyűjtemény, amely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára". A szabályokra vonatkozó követelményeit jelen dokumentum hitelesítési rend formájában határozza meg. A jelen dokumentumnak megfelelően kibocsátott tanúsítványok tartalmazzák azon *Hitelesítési rend* azonosítóját (OID), amelyet az *Érintett felek* arra használhatnak, hogy meghatározzák a tanúsítványok alkalmazhatóságát és megbízhatóságát egy adott alkalmazás tekintetében.

A *Hitelesítési rend* alapvető követelményeket fogalmaz meg a tanúsítványokkal kapcsolatban. Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a *Szolgáltató* által kibocsátott *Szolgáltatási szabályzat* írja le.

1.1.1. *Hitelesítési rend*ek

Jelen dokumentum az alábbi *Hitelesítési rend*eket definiálja:

- „III. hitelesítési osztályba tartozó, természetes személyek számára kibocsátott, kriptográfiai hardver eszköz használatát megkövetelő tanúsítványok kibocsátására vonatkozó hitelesítési rend"
  OID: 1.3.6.1.4.1.21528.2.1.1.31.3.1
- „III. hitelesítési osztályba tartozó, automatizmusok számára kibocsátott, kriptográfiai hardver eszköz használatát megkövetelő tanúsítványok kibocsátására vonatkozó hitelesítési rend"
  OID: 1.3.6.1.4.1.21528.2.1.1.32.3.1
- „III. hitelesítési osztályba tartozó, természetes személyek számára kibocsátott tanúsítványok kibocsátására vonatkozó hitelesítési rend"
  OID: 1.3.6.1.4.1.21528.2.1.1.33.3.1
- „III. hitelesítési osztályba tartozó, automatizmusok számára kibocsátott tanúsítványok kibocsátására vonatkozó hitelesítési rend"
  OID: 1.3.6.1.4.1.21528.2.1.1.34.3.1
- „III. hitelesítési osztályba tartozó tanúsítványok kibocsátására vonatkozó hitelesítési rend"
  OID: 1.3.6.1.4.1.21528.2.1.1.11.3.1

- „II. hitelesítési osztályba tartozó tanúsítványok kibocsátására vonatkozó hitelesítési rend" OID: 1.3.6.1.4.1.21528.2.1.1.10.3.1

Ezen *Hitelesítési rend*ek alapján a *Szolgáltató* olyan tanúsítványokat is kibocsát, amelyek az elektronikus aláírásról szóló 2001. évi XXXV. törvény szerint fokozott biztonságú elektronikus aláírás létrehozására alkalmasak. [1] A fokozott biztonságú elektronikus aláírással ellátott dokumentumok kielégítik az írásba foglaltság követelményét.

A *Szolgáltató* a fenti rendek mindegyike szerint bocsát ki álneves és nem álneves tanúsítványokat is.

A III. hitelesítési osztályba tartozó tanúsítványok esetén a *Szolgáltató* személyes regisztrációt végez, a II. hitelesítési osztályba tartozó tanúsítványok esetén a *Szolgáltató* távoli regisztrációt végez.

A természetes személyek számára kibocsátott tanúsítványokra vonatkozó hitelesítési rendek esetén a *Szolgáltató* a tanúsítvány alanyának nevét tünteti fel a tanúsítványban. Automatizmus számára kibocsátott tanúsítványokra vonatkozó hitelesítési rendek esetén a *Szolgáltató* az automatizmus megnevezését tünteti fel a tanúsítványban, de a tanúsítvány kibocsátása során ekkor is egy természetes személy igénylőt azonosít.

A kriptográfiai hardver eszköz használatát megkövetelő hitelesítési rendek esetén a *Szolgáltató* meggyőződik róla, hogy a tanúsítványhoz tartozó magánkulcs az alábbi tanúsítások legalább egyikével rendelkező vagy velük egyenértékű kriptográfiai hardver eszközön helyezkedik el:

- az Európai Unió valamely tagállamában nyilvántartásba vett tanúsító szervezet által kiadott igazolás szerint „biztonságos aláírás-létrehozó eszköz"
- Common Criteria tanúsítás a CEN SSCD PP szerint, legalább EAL4 szinten
- FIPS 140-2, Level 2 (vagy magasabb)

1.1.2. Hatály

Jelen *Hitelesítési rend* a dokumentum címlapján feltüntetett hatálybalépési dátumtól határozatlan ideig hatályos. A hatályosság megszűnik jelen dokumentum újabb verziójának hatályba lépésekor vagy a dokumentum hatályon kívül helyezésekor.

A *Hitelesítési rend* az 1.4. alfejezetben azonosított közösség minden egyes tagjára – köztük természetes személyekre és jogi személyekre – egyaránt kiterjed.

1.2. A *Szolgáltató*

A jelen *Hitelesítési rend*nek megfelelő tanúsítványokat kibocsátó szolgáltató (a továbbiakban: *Szolgáltató*) adatait, ügyfélszolgálati irodájának elérhetőségét, nyitvatartását, a *Szolgáltató*val

való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a *Szolgáltatási szabályzat* tartalmazza.

1.3. Dokumentum neve és azonosítása

Jelen dokumentum azonosító adatai a dokumentum fedőlapján találhatóak. A jelen dokumentumban leírt *Hitelesítési rend*ek azonosító adatait az 1.1.1. fejezet tartalmazza.

1.4. PKI közösség

A jelen *Hitelesítési rend*ben szereplő PKI közösség az alábbi felekből áll:

- *Szolgáltató*: A jelen *Hitelesítési rend*nek megfelelő tanúsítványokat kibocsátó hitelesítés szolgáltató, amely a tanúsítványok kibocsátásával és menedzsmentjével kapcsolatos műszaki tevékenységeket végzi.
- *Regisztrációs szervezet*: A *Regisztrációs szervezet* szerepét a *Szolgáltató* is ellátja, de e funkciót más szervezet is betöltheti. A *Regisztrációs szervezet* feladata a tanúsítványok kibocsátásával és menedzsmentjével kapcsolatos adminisztratív tevékenység ellátása, különösen a tanúsítványok alanyainak azonosítása, és az adataik rögzítése. Amennyiben a *Regisztrációs szervezet* szerepét nem a *Szolgáltató* látja el, a *Szolgáltató* akkor is felelősséget vállal a *Regisztrációs szervezet* működéséért.
- *Előfizető* : Az *Előfizető* határozza meg az elektronikus aláírás hitelesítés szolgáltatást igénybe vevő *Aláírók* körét. Ugyancsak az *Előfizető* határozza a nem elektronikus aláírásra szolgáló tanúsítványokhoz tartozó Alanyok körét. Az *Előfizető* fizeti meg az ezen szolgáltatások igénybevételével kapcsolatos költségek ellenértékét. Az *Előfizető Szolgáltatási szerződés*t köt a *Szolgáltató*val.
- *Alany*: Nem elektronikus aláírás létrehozására szolgáló tanúsítványok kibocsátása esetén Alanynak nevezzük azt a természetes vagy nem természetes személyt, aki számára a *Szolgáltató* a tanúsítványt kibocsátja.
- *Aláíró*: Az elektronikus aláírás hitelesítés szolgáltatást igénybe vevő fél, aki számára a *Szolgáltató* elektronikus aláírás létrehozására alkalmas tanúsítványt bocsát ki.

  Jelen dokumentumban olyan *Hitelesítési rend*ek szerepelnek, amelyek szerint egyaránt kibocsáthatóak elektronikus aláírás létrehozására, valamint egyéb célra alkalmas tanúsítványok is. Jelen dokumentumban – elektronikus aláírásra szolgáló tanúsítványok esetén is – Alanynak nevezzük azt a személyt, aki számára a *Szolgáltató* a tanúsítványt kibocsátja.

- Képviselt szervezet: Amennyiben a tanúsítvány az Alany részére egy jogi személy képviseletében történő aláírásra vagy tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra (szervezeti tanúsítvány), akkor a *Képviselt szervezet* a szóban forgó szervezet, amely szintén megjelölésre kerül a tanúsítványban. A *Szolgáltató* a *Képviselt szervezet*tel nem feltétlenül áll szerződéses viszonyban, de a *Szolgáltató* szervezeti tanúsítványt ezen szervezet hozzájárulása nélkül nem bocsát ki. A *Szolgáltató* felfüggeszti, illetve visszavonja a tanúsítványt ezen szervezet kérésére.
- Érintett fél: A tanúsítvány felhasználásával létrehozott elektronikus aláírással ellátott elektronikus dokumentumot befogadó fél, valamint az időbélyegzőt, illetve online tanúsítvány-állapot választ befogadó fél. Az *Érintett fél* nem áll szerződéses viszonyban a *Szolgáltató*val. Tevékenységére vonatkozó ajánlásokat a Szabályzat és az abban megnevezett egyéb szabályzatok tartalmazzák. A *Szolgáltató* az *Érintett fél*lel elsősorban az internetes honlapon keresztül tart kapcsolatot.

1.5. Alkalmazhatóság

Engedélyezett alkalmazási lehetőségek

A kibocsátott végfelhasználói tanúsítványok, illetve a hozzájuk tartozó magánkulcsok kizárólag a tanúsítványban (annak Key Usage mezejében) feltüntetett célra használhatóak fel.

Korlátozások

A *Szolgáltató* korlátozza a tanúsítványokkal kapcsolatos kártérítési kötelezettségét. Ennek részleteit a *Szolgáltatási szabályzat* tartalmazza.

Tiltott alkalmazási lehetőségek

A kibocsátott tanúsítványokat, illetve a hozzájuk tartozó magánkulcsokat a tanúsítványban szereplő kulcshasználattól eltérő célra nem szabad felhasználni.

1.6. Fogalmak és rövidítések

Fogalmak

Aláírás-ellenőrző adat (Signature-Verification Data): Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), amelyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.

Aláírás-létrehozó adat (Signature-Creation Data): Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), amelyet az *Aláíró* az elektronikus aláírás létrehozásához használ.

Aláírás-létrehozó eszköz (ALE): Olyan hardver, illetve szoftver eszköz, amelynek segítségével az *Aláíró* az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Biztonságos aláírás-létrehozó eszköz (BALE): Olyan hardver, illetve szoftver eszköz, amelyet egy erre kijelölt független tanúsító szervezet megvizsgált és a biztonsági és működési követelményeknek megfelelőnek talált. Minősített elektronikus aláírás csak BALE eszköz használatával készíthető.

Aláíró (Signatory):

- az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult;
- az a jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, amely az aláírás-létrehozó eszközt birtokolja, és akinek a nevében az őt képviselő természetes személy az elektronikus aláírást az elektronikus dokumentumon elhelyezi, valamint aki meghatározza, hogy a nevében jogszabályban meghatározott feltételeknek megfelelő informatikai eszköz elektronikus aláírást elektronikusan dokumentumon elhelyezzen.

***Képviselt szervezet*:** Amennyiben a tanúsítvány egy jogi személy képviseletében történő aláírásra vagy tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra az Alany részére, akkor a *Képviselt szervezet* a szóban forgó szervezet, amely szintén megjelölésre kerül a tanúsítványban.

Alany (Subject): A tanúsítvány által azonosított személy, szervezet vagy alkalmazás. Elektronikus aláírásra szolgáló tanúsítvány esetén az Alany megegyezik az *Aláíró*val.

Elektronikus aláírás (Electronic Signature): Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.

Fokozott biztonságú elektronikus aláírás (Advanced Electronic Signature): Elektronikus aláírás, amely megfelel a következő követelményeknek:

- alkalmas az *Aláíró* azonosítására és egyedülállóan hozzá köthető,
- olyan eszközzel hozták létre, amely kizárólag az *Aláíró* befolyása alatt áll,
- a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető.

Hardver kriptográfiai eszköz (HSM: Hardware Security Modul): Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására. Megjegyzés: Lehetséges példák ilyen eszközre: PC bővítő kártya, intelligens kártya, USB token.

***Érintett fél* (Relying Party):** Az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el.

Hatóság: Az elektronikus aláírással kapcsolatos szolgáltatásokat nyújtó szolgáltatókat felügyelő hatóság, a Nemzeti Média- és Hírközlési Hatóság.

Hitelesítési rend: Olyan szabálygyűjtemény, amelyben a *Szolgáltató* valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.

Hitelesítő egység: A hitelesítés szolgáltató rendszerének egy egysége, amely tanúsítványok aláírását végzi. Egy hitelesítő egységhez mindig egy aláírókulcs tartozik. Előfordulhat, hogy egy szolgáltató egyszerre több hitelesítő egységet is működtet.

Időbélyegző (Time Stamp): Egy elektronikus dokumentumhoz hozzárendelt vagy azzal logikailag összekapcsolt adat, amely segítségével igazolható, hogy a dokumentum változatlan az időbélyegző elhelyezésének időpontjában létező állapothoz képest.

Időbélyegzési rend: Olyan szabálygyűjtemény, amelyben a *Szolgáltató* az általa kibocsátott időbélyegzők felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.

Kompromittálódás: Egy kriptográfiai kulcs akkor kompromittálódik, ha illetéktelen személyek is megismerik.

Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ): A 78/2010. Kormányrendeletben meghatározott szervezet.

Kriptográfiai kulcs (Key): Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításához és dekódolásához, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.

Kulcsgondozás (Key Management): A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, szoros kapcsolatban az alkalmazott biztonsági eljárásmóddal.

Minősített elektronikus aláírás (Qualified Electronic Signature): Olyan fokozott biztonságú elektronikus aláírás, amely biztonságos aláírás létrehozó eszközzel készült és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

Minősített hitelesítés-szolgáltató (Qualified Certification Service Provider): Az elektronikus aláírási törvény 3. számú mellékletében foglalt követelményeknek megfelelő, valamint ennek alapján nyilvántartásba vett hitelesítés-szolgáltató.

Minősített tanúsítvány (Qualified Certificate): Az elektronikus aláírási törvény 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített szolgáltató bocsátott ki.

Nyilvános (publikus) kulcsú infrastruktúra (Public Key Infrastructure, PKI): Az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.

Regisztráló szervezet (Registration Authority): Szervezet, amely ellenőrzi a tanúsítvány alanyának adatainak valódiságát. Egy hitelesítés-szolgáltató több ilyen szervezettel is együttműködhet.

Rendkívüli üzemeltetési helyzet: Olyan, a *Szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség;

Szervezeti ügyintéző: Olyan személy, aki jogosult saját szervezete nevében a saját szervezetéhez tartozó tanúsítványokat felfüggeszteni, visszaállítani és visszavonni.

Szolgáltatási szabályzat (Certificate Practice Statement): A hitelesítés-szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.

Tanúsítvány (Certificate): A hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot egy meghatározott *Aláíró*hoz kapcsolja, akinek adatainak valódiságáról meggyőződött.

Tanúsítványigénylés: Az a folyamat, amelynek során az Alany előzetesen megadja az adatait a *Szolgáltató*nak, és felhatalmazza a *Szolgáltató*t az adatok kezelésére. Ezen adatok alapján a *Szolgáltató* elkészíti az Alany aláírás létrehozó eszközét (ha ez szükséges), majd felkészül a tanúsítvány kibocsátására. A tanúsítványigénylésben szereplő adatokat a *Szolgáltató* mindaddig nem tekinti hitelesnek, amíg az Alany egy saját kézzel aláírt tanúsítványkérelemben meg nem erősíti őket. A tanúsítványigénylés távolról is (postán, illetve elektronikusan) beküldhető.

Tanúsítványkérelem: Az a folyamat, amelynek során az Alany saját kezű aláírásával megerősíti a tanúsítványba kerülő adatokat. Minősített és közigazgatási tanúsítványok esetén a tanúsítványkérelem kizárólag személyesen nyújtható be.

Tanúsítvány típus: Lásd: hitelesítési rend.

Tranzakciós korlát, pénzügyi tranzakciós korlát, tranzakciós limit: A tanúsítványban feltüntetett értékhatár, amely korlátozza, hogy a tanúsítvánnyal legfeljebb mekkora értékű tranzakció írható alá.

1.6.1. Rövidítések

- CA: Certification Authority, Hitelesítés Szolgáltató

- CRL: Certificate Revocation List, Tanúsítvány visszavonási lista
- OCSP: Online Certificate Status Protocol, Online tanúsítvány-állapot protokoll
- NMHH: Nemzeti Média- és Hírközlési Hatóság
- RA: Registration Authority, Regisztráló szervezet
- TSA: Time Stamping Authority, Időbélyegzés Szolgáltató
- CP: Certificate Policy, Tanúsítványtípus, Hitelesítési Rend
- CPS: Certificate Practice Statement, Hitelesítés Szolgáltatási Szabályzat

2. Közzététel és tanúsítványtár

2.1. A szolgáltatói információ közzététele

A *Szolgáltató* szerződéses feltételeit és szabályzatait a honlapján hozza nyilvánosságra elektronikus formában. A honlapon legalább 30 nappal a hatályba lépés előtt publikálásra kerülnek a bevezetésre váró új dokumentumok. A honlapon az érvényben levő dokumentumokon kívül elérhető valamennyi dokumentum összes korábbi verziója is.

A *Szolgáltató* a következő eseményekről hirdetést jelentethet meg egy országos terjesztésű napilapban:

- tevékenységének befejezése (lásd: 5. fejezet),
- valamely, általa működtetett hitelesítő egység magánkulcsának kompromittálódása.

A *Szolgáltató* a szolgáltatói tanúsítványait a honlapján teszi közzé. Legfelsőbb szintű (root) tanúsítványainak lenyomatát egy országos terjesztésű napilapban is közzéteszi.

A *Szolgáltató* a végfelhasználói tanúsítványokat az *Érintett felek* részére közzéteszi honlapján, amennyiben a tanúsítványhoz tartozó Ügyfél ehhez hozzájárul.

A *Szolgáltató* az általa működtetett hitelesítő egységek, valamint az online tanúsítvány-állapot szolgáltatásban részt vevő egységek tanúsítványával kapcsolatos állapot-információkat a következő módszerekkel teszi közzé:

- Gyökér hitelesítő egységei tanúsítványainak állapotváltozásáról egy országos terjesztésű napilapban tesz közzé hirdetést. A gyökér hitelesítő egységek megnevezését, illetve gyökértanúsítványaik lenyomatát a *Szolgáltatási szabályzat* tartalmazza.
- A köztes (nem gyökér) hitelesítő egységek tanúsítványainak állapotváltozását a visszavonási listákon, saját honlapján, valamint az online tanúsítvány-állapot válasz szolgáltatás keretében hozza nyilvánosságra.

- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a *Szolgáltató* – a legjobb nemzetközi gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű tanúsítványt bocsát ki, ezzel kiküszöbölve azt, hogy a tanúsítvány visszavonási állapotát ellenőrizni kelljen. E tanúsítvány visszavonási állapotát a *Szolgáltató* kizárólag olyan módon teszi közzé, hogy kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulcshoz nem kerül kibocsátásra újabb tanúsítvány. A *Szolgáltató* az OCSP válaszadói tanúsítványokat ezt követően új, biztonságos magánkulcshoz bocsátja ki.

A *Szolgáltató* az általa kibocsátott végfelhasználói tanúsítványokkal kapcsolatos állapot-információkat a következő módszerekkel teszi közzé:

- a visszavonási listákon,
- az online tanúsítvány-állapot válasz szolgáltatás keretében.

A végfelhasználói tanúsítvány visszavonását és felfüggesztését a *Szolgáltató* mindig nyilvánosságra hozza, ehhez nem szükséges az Alany hozzájárulása. Az állapot-információk közlésének módszereit illetően lásd még a 4.10. fejezetet.

2.2. A közzététel gyakorisága

2.2.1. Kikötések és feltételek közzétételi gyakorisága

A *Hitelesítési rend*del kapcsolatos új verziók közzététele a 2.1. fejezetben ismertetett eljárásoknak megfelelően történik. A *Szolgáltató* szükség szerint kibocsátja az egyéb szabályzatait, szerződéses feltételeit, illetve azok újabb változatait.

A *Szolgáltató* a rendkívüli információkat késlekedés nélkül közzéteszi a jogszabályi előírásoknak megfelelően, illetve ennek hiányában akkor, amikor arra szükség van.

2.2.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága

A *Szolgáltató* az egyes tanúsítványok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:

- Az általa működtetett gyökér hitelesítő egységek tanúsítványait a szolgáltatás megkezdését követő vagy az új tanúsítvány kibocsátását követő 10 munkanapon belül közzé teszi.
- Az általa működtetett köztes hitelesítő egységek tanúsítványait a kibocsátást követően 5 munkanapon belül hozza nyilvánosságra.
- A *Szolgáltató* a végfelhasználói tanúsítványokat a tanúsítványtárban az előállítást követően haladéktalanul megjeleníti az Alany hozzájárulása esetén.

2.2.3. A megváltozott visszavonási állapot közzétételének gyakorisága

A *Szolgáltató* által kibocsátott végfelhasználói tanúsítványokkal, valamint a végfelhasználói tanúsítványokat kibocsátó egységek tanúsítványaival kapcsolatos állapot-információk az online tanúsítvány-állapot szolgáltatás keretén belül az állapotváltozást követően azonnal elérhetőek.

A tanúsítványok állapotára vonatkozó információk a tanúsítványtárban a tanúsítvány-visszavonási listákon is megjelennek. A tanúsítvány visszavonási listák kibocsátási gyakoriságát a 4.10. fejezet tárgyalja.

2.3. Hozzáférés-ellenőrzések

A *Szolgáltató* által közzétett kikötések és feltételek, rendkívüli információk, tanúsítványok és állapot információk nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közzététel sajátosságainak megfelelően.

A *Szolgáltató* által közölt információkat kizárólag csak a *Szolgáltató* egészítheti ki, törölheti vagy módosíthatja. A *Szolgáltató* különböző védelmi mechanizmusokkal igyekszik megakadályozni az információk jogosulatlan módosítását.

2.4. A tanúsítványtár

A *Szolgáltató* tanúsítványtára a *Szolgáltató* honlapjáról érhető el. A *Szolgáltató* LDAP protokollon keresztül is közzéteszi azon tanúsítványokat, amelyek esetén az ügyfél hozzájárult a tanúsítvány közzétételéhez.

A tanúsítványtár elérhetőségét a *Szolgáltató* folyamatosan (az év minden napján, 0-24 óra között) biztosítja, a karbantartáshoz szükséges idők kivételével. A *Szolgáltató* a tervezett karbantartásokat munkaidőn kívüli időszakokra ütemezi, és ezekről a karbantartás megelőzően 24 órával értesítést tesz közzé a honlapján.

3. Azonosítás és hitelesítés

3.1. Elnevezések

3.1.1. Név típusok

A tanúsítvány alapmezői között található Kibocsátó azonosító (Issuer), illetve Alany azonosító (Subject) mezők az RFC 5280 szerinti egyedi név formátum előírásainak felelnek meg. [2] Ezen kívül a *Szolgáltató* támogatja a kiterjesztések között található Alternatív név mezők (Subject Alternative Names, Issuer Alternative Names) kitöltését is.

A tanúsítványban szereplő Alany megnevezése

Jelen *Hitelesítési rend* a következőket írja elő a tanúsítvány alanyának azonosítójával (Subject mező) kapcsolatban:

- Common Name (CN) – OID: 2.5.4.3
  Természetes személy esetén az Alany személyazonosító okmányában szereplő neve kerül e mezőbe, magyar írásmód szerint, ékezetesen.

  Ha a tanúsítványban álnév szerepel, akkor az "`álneves tanúsítvány`" szöveg (vagy ennek idegen nyelvű megfelelője) szerepel e mezőben, magát az álnevet pedig a pseudonym mező tartalmazza.

  Nem természetes személy (eszköztanúsítvány) esetén az eszköz megnevezése kerül ide.

- Pseudonym (PSEUDO) – OID: 2.5.4.65
  Kizárólag álneves tanúsítvány esetén kerül kitöltésre, ekkor e mezőbe kerül az Alany álneve. Az álnevet az Alany választja, az álnevet a *Szolgáltató* egyáltalán nem ellenőrzi.

  Ha a pseudonym kitöltésre kerül, akkor a CN mezőben szerepelhet arra vonatkozó jelzés, hogy a tanúsítvány álnevet tartalmaz.

- Serial Number – OID: 2.5.4.5
  Az Alany egyedi azonosítója az RFC 4043 szerint. [3] A tanúsítványban legalább egy serial number kötelezően szerepel.

- Organization (O) – OID: 2.5.4.10
  Amennyiben az Alany egy szervezethez kapcsolódik, akkor az „O" mezőbe kerül ezen szervezet rövid neve az alapító okirat vagy valamely közhiteles nyilvántartás szerint ékezetesen. Ha az O mező kitöltésre kerül, akkor ún. szervezeti tanúsítványról beszélünk.

- Country (C) – OID: 2.5.4.6
  Szervezeti tanúsítvány esetén az O mezőben szereplő szervezet székhelye szerinti ország kétbetűs kódja. Egyébként az Alany állandó lakcíme szerinti ország kétbetűs kódja. Kitöltése kötelező.

  Magyarország esetében a C mező értéke: "`HU`".

- Title (T) – OID: 2.5.4.12
  Az Alany szerepe, beosztása vagy hivatása. További korlátozásokat tartalmaz a tanúsítvány felhasználhatóságával kapcsolatban.

- E-mail address (EMAIL) – OID: 1.2.840.113549.1.9.1
  Az Alany e-mail címe. Ha kitöltésre kerül, akkor meg kell, hogy egyezzen az Alany alternatív neve mezőben szereplő RFC822name mezőben szereplő e-mail címmel. Létező e-mail címnek kell lennie.

A jelen *Hitelesítési rend*ek szerint kibocsátott tanúsítványok a fentieken túl további Subject DN mezőket is tartalmazhatnak.

Az Alany alternatív nevei

Az Alany alternatív nevei (Subject Alternative Names – OID: 2.5.29.17) mező a következő módon épül fel:

- Subject Alternative Names – OID: 2.5.29.17 (nem kritikus)

  Az Alany kérésére ide (jellemzően a Subject Alternative Names CN mezejébe) kerülhet az Subject DN / Common Name mezőben szereplőtől eltérő írásmóddal írott neve. E név egyaránt szerepelhet ékezetes vagy ékezet nélküli írásmóddal. A *Szolgáltató* jogosult jelölni a feltüntetett név jellegét is.

  A *Szolgáltató* a Subject Alternative Names mezőbe kerülő neveket is ellenőrzi.

  rfc822Name: Az Alany e-mail címe kerül ebbe a mezőbe. Amennyiben a tanúsítványban szerepel e-mail cím, akkor e mező mindenképpen kitöltésre kerül. Ugyanez az e-mail cím opcionálisan megjelenhet a tanúsítvány EMAIL mezejében is.

Igény a nevek értelmezhetőségére

A SubjectDN mezőre a következő szabályok érvényesek:

- Az azonosítónak értelmezhetőnek kell lennie.
- A tanúsítványban szereplő személynevet a közhiteles nyilvántartásban szereplő írásmóddal, ékezethelyesen kell feltüntetni.
- A tanúsítványban szereplő szervezet nevét a közhiteles nyilvántartásban ellenőrizve, egyértelműen azonosítható módon kell feltüntetni.

Álneves tanúsítvány esetén egyedül a Pseudonym mező tartalmaz álnevet, a többi mezőt a *Szolgáltató* a nem álneves tanúsítványoknál alkalmazottal megegyező módon ellenőrzi.

Különböző elnevezési formák értelmezési szabályai

Az azonosítók értelmezése érdekében az *Érintett felek*nek a jelen dokumentumban leírtak alapján kell eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az *Érintett fél*nek segítségre lenne szüksége, akkor a *Szolgáltató*val közvetlenül is felveheti a kapcsolatot. A *Szolgáltató* ilyen esetben az ügyfél egyéb adatairól többlet tájékoztatást – feltéve, hogy jogszabály ezt nem írja elő – nem ad, csak a tanúsítványban feltüntetett adatok értelmezését segítő információt szolgáltatja.

A nevek egyedisége

Az Alany a *Szolgáltató* tanúsítványtárában egyedi névvel rendelkezik. Erről elsődlegesen a Subject DN Serial Number mezőjébe kerülő egyedi azonosító gondoskodik, amely alapértelmezés szerint az Alanynak a *Szolgáltató* nyilvántartásában szerzett egyedi azonosítója (OID). Kérésre más egyedi azonosító (pl. személyi igazolvány szám, adószám, szervezeten belüli azonosító) is feltüntethető.

Eljárások a nevekre vonatkozó vitás kérdések megoldására

Az Alanyok egyedi azonosítóinak (OID) kiosztása a beérkezett tanúsítvány-kérelmek elbírálásának sorrendje szerint történik. A tanúsítványban szereplő Subject mező ezáltal garantáltan egyedi lesz.

A *Szolgáltató* – lehetőségei szerint – ellenőrzi az ügyfél jogosultságát a feltüntetett nevek használatára vonatkozóan. Jogszerűtlen név- vagy adathasználat miatt, amennyiben erre bíróság kötelezi, vagy másik fél megalapozott módon bizonyítani tudja jogosultságát, *Szolgáltató*nak jogában áll visszavonni a kérdéses tanúsítványt.

Márkanevek elismerése, hitelesítése és szerepe

A *Szolgáltató* a szolgáltatása során az "e-Szignó" védjegyet alkalmazza. A védjegy az E-Szignó Bt. tulajdona, a védjegy használatához a tulajdonos hozzájárulását adta.

A *Szolgáltató* által igényelt végfelhasználói tanúsítvány mezőiben is előfordulhatnak védjegyek. Ezek jogos használatát a *Szolgáltató* lehetőségei szerint ellenőrizheti, de nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában.

3.2. Kezdeti azonosítás

3.2.1. A magánkulcs birtoklása

III. hitelesítési osztályba tartozó tanúsítványok esetén a *Szolgáltató* személyes találkozás során győződik meg róla, hogy az Alany valóban birtokolja a tanúsítványba kerülő magánkulcsot.

II. hitelesítési osztályba tartozó tanúsítvány esetén személyes találkozásra nincsen szükség. Ekkor a *Szolgáltató* távolról azonosítja az Alanyt, és ezen azonosítás során győződik meg arról, hogy az Alany valóban birtokolja a magánkulcsot.

3.2.2. A szervezeti azonosság hitelesítése

Szervezeti tanúsítványok esetén a *Képviselt szervezet* neve is feltüntetésre kerül a végfelhasználói tanúsítványokban. Ezekben az esetekben a *Szolgáltató* a tanúsítványt kizárólag a *Képviselt*

szervezet hozzájárulásával bocsátja ki. (Ezen tanúsítványokat a *Szolgáltató* később a *Képviselt szervezet* kérésére felfüggeszti, illetve visszavonja.)

Szervezeti tanúsítványok igénylése esetén az igénylőnek igazolnia kell, hogy jogosult a *Képviselt szervezet* nevében tanúsítványt igényelni.

A részletes eljárásrendet a *Szolgáltatási szabályzat* tartalmazza.

3.2.3. A személyazonosság hitelesítése

III. hitelesítési osztályba tartozó tanúsítványok esetén a *Szolgáltató* személyes találkozás során azonosítja az Alanyt valamely okmánya alapján.

II. hitelesítési osztályba tartozó tanúsítvány esetén személyes találkozásra nincsen szükség, ekkor a *Szolgáltató* távolról azonosítja az Alanyt. Ennek egyik módja, hogy az Alany eljuttatja a *Szolgáltató*nak valamely igazolványának a fénymásolatát.

A *Szolgáltatási szabályzat* tartalmazza a részletes eljárásrendet, valamint az elfogadott igazolványok megnevezését.

3.3. Tanúsítványcsere érvényes tanúsítvány esetén

Az erre vonatkozó eljárásrendet a *Szolgáltatási szabályzat* tartalmazza.

3.4. Tanúsítványcsere érvénytelen tanúsítvány esetén

Az erre vonatkozó eljárásrendet a *Szolgáltatási szabályzat* tartalmazza.

3.5. Felfüggesztési és visszavonási kérelem

Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait az 4.9. fejezet tárgyalja.

4. A tanúsítványok életciklusa

4.1. Tanúsítványigénylés

A tanúsítványkérelem benyújtását megelőzően, az Alany előzetes tanúsítványigénylést kell, hogy benyújtson a *Szolgáltató*nak. Ez történhet a *Szolgáltató* honlapján keresztül is. A tanúsítványigénylésben az Alany megadja a tanúsítványba kerülő adatait, megnevezi, hogy pontosan milyen tanúsítványt igényel, és felhatalmazza a *Szolgáltató*t az adatok kezelésére.

A *Szolgáltató* mindaddig nem tekinti a tanúsítványigénylésben szereplő adatokat hitelesnek, amíg az Alany tanúsítványkérelemben meg nem erősíti azt.

A tanúsítványigényléssel kapcsolatban a *Szolgáltatási szabályzat* további megkötéseket tartalmazhat.

4.2. A tanúsítványkérelem benyújtása és feldolgozása

III. hitelesítési osztályba tartozó tanúsítványok esetén a tanúsítványkérelmet az Alany személyesen nyújthatja be.

II. hitelesítési osztályba tartozó tanúsítványok esetén az Alany postán is elküldheti a *Szolgáltató*nak az aláírt tanúsítványkérelmet. A tanúsítványkérelem a III. hitelesítési osztály szerint személyesen is benyújtható.

A *Szolgáltató* a *Szolgáltatási szabályzat* szerint feldolgozza és jóváhagyja a tanúsítványkérelmet, majd kibocsátja a tanúsítványt.

4.3. A tanúsítvány kibocsátása

Végfelhasználói tanúsítványok kibocsátására a tanúsítványigénylő eljárás lefolytatását követően kerülhet sor. A tanúsítvány elkészítésére a tanúsítványigénylés során megadott, illetve a *Szolgáltató* rendelkezésére álló és a tanúsítványcsere igénylése során érvényesnek elismert adatok alapján kerül sor.

A tanúsítvány kibocsátása előtt a *Szolgáltató* ellenőriz minden olyan adatot, amelyet a tanúsítványban feltüntet. A *Szolgáltató* az Alany személyazonosságának ellenőrzése céljából adategyeztetést végez legalább eggyel a következő közhiteles nyilvántartások közül: személyi adat- és lakcímnyilvántartás, úti okmány nyilvántartás, gépjárművezetői nyilvántartás, valamint az aláírási jogosultság ellenőrzése céljából adategyeztetést végez a cégnyilvántartással.

A tanúsítványigénylés során megadott adatok, valamint az Alany nyilvános kulcsa a *Szolgáltató* információs rendszerébe kerülnek. A hitelesítő szervezet aláírja a tanúsítványt saját magánkulcsával, és visszaküldi azt a regisztráló szervezetnek. A hitelesítő szervezet a tanúsítványt nyilvános tanúsítványtárában a kibocsátást követően haladéktalanul közzéteszi – amennyiben az ügyfél ehhez hozzájárult.

4.4. Tanúsítvány-elfogadás

Az Alanynak a tanúsítvány használatba vétele előtt ellenőriznie kell a benne szereplő adatokat.

A *Szolgáltató* értesíti a tanúsítvány kibocsátásáról az Alanyt, az *Előfizető*t, illetve a *Képviselt szervezet*et.

A *Szolgáltatási szabályzat* további előírásokat tartalmazhat.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. Az Alany tanúsítvány használata

Az Alany a tanúsítványát kizárólag a tanúsítványban szereplő kulcshasználatnak megfelelően használhatja.

A használat során be kell tartani az 1.5. fejezetben leírt korlátokat.

4.5.2. Az *Érintett fél*re vonatkozó ajánlások

Amennyiben egy *Érintett fél* ésszerűen kíván a tanúsítványra hagyatkozni, a *Szolgáltatási szabályzat*nak megfelelően célszerű eljárnia a tanúsítványok felhasználása során. Ekkor – a Szabályzatban foglaltak betartása mellett – a lehető legnagyobb gondossággal és körültekintéssel kell eljárnia, amely az összes rendelkezésre álló információ alapján történő ésszerű mérlegelést jelenti. Ennek részleteit a *Szolgáltatási szabályzat* tartalmazza.

Amennyiben az *Érintett fél* nem az ott leírtaknak megfelelően jár el, az ebből következő károkért a *Szolgáltató* nem vállal felelősséget.

4.6. Tanúsítványcsere érvényes tanúsítvány esetén

Ennek eljárásrendjét a *Szolgáltatási szabályzat* tartalmazza.

4.7. Tanúsítványcsere visszavont tanúsítvány esetén

Ennek eljárásrendjét a *Szolgáltatási szabályzat* tartalmazza.

4.8. Tanúsítványban szereplő adatok megváltoztatása

Amennyiben a *Szolgáltató* tudomására jut, hogy a tanúsítványban szereplő valamely adat megváltozott, a *Szolgáltató* az *Ügyfél*lel egyeztetett ütemben visszavonja a tanúsítványt.

Ennek eljárásrendjét a *Szolgáltatási szabályzat* tartalmazza.

4.9. Tanúsítvány felfüggesztése és visszavonása

A következő felek kezdeményezhetik a tanúsítványok felfüggesztését és visszavonását:

- az Alany,
- az *Előfizető*,
- a *Képviselt szervezet*,

- a *Szolgáltató*.

A *Szolgáltató* visszavonja a tanúsítványt, ha tudomására jut, hogy a tanúsítványban szereplő adatok nem felelnek meg a valóságnak, vagy hogy a tanúsítványhoz tartozó magánkulcs illetéktelen kezekbe került.

A *Szolgáltató* 24 órás ügyeletet tart fent, amelyen keresztül az *Ügyfel*ek a tanúsítványok felfüggesztését kérhetik.

A *Szolgáltató* minden megérkező felfüggesztési kérelmet soron kívül, haladéktalanul – jellemzően néhány másodperc alatt – feldolgoz, és az esetleg megváltozott visszavonási állapot a feldolgozást követően azonnal megjelenik a *Szolgáltató* visszavonási nyilvántartásában. A *Szolgáltató* biztosítja, hogy ez a művelet legfeljebb 5 percen belül lezajlik, azaz a megváltozott visszavonási állapot a felfüggesztési kérelem megérkezésétől számítva legfeljebb ennyi időn belül közzétételre kerül.

A visszavonási kérelmeket a *Szolgáltató* egy munkanapon belül dolgozza fel.

A kérelmek benyújtásának módját a *Szolgáltatási szabályzat* tartalmazza.

4.10. A visszavonási állapot közzététele

Tanúsítványok állapotának lekérdezésére a *Szolgáltató* a következő lehetőségeket biztosítja:

- OCSP – online tanúsítvány visszavonási állapot lekérdezési szolgáltatás,
- CRL – visszavonási lista.

A visszavonási listában a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok visszaállítás hatására kikerülnek a listából. A tanúsítványok a tanúsítvány lejárta után törlődnek a listából. Felfüggesztés, visszaállítás és visszavonás esetén a folyamat sikeres lezárását követően a tanúsítvány új állapota azonnal megjelenik a *Szolgáltató* visszavonási nyilvántartásában. Ettől a pillanattól kezdve a *Szolgáltató* által nyújtott OCSP válaszok már a tanúsítvány új visszavonási állapotát tartalmazzák. Felfüggesztés, visszaállítás és visszavonás esetén a 4.9 fejezetben leírt időszakot követően a *Szolgáltató* azonnal új CRL-t bocsát ki, illetve a *Szolgáltató* OCSP szolgáltatásán is meg kell, hogy jelenjen a megváltozott visszavonási állapot.

A "visszavonási állapot közzététele" szolgáltatás rendelkezésre állása: 99%; az eseti szolgáltatáskiesések maximális időtartama 24t. A *Szolgáltató* által működtetett hitelesítő egységek legfeljebb 24 óránként bocsátanak ki CRL-t.

4.11. Az előfizetés vége

Az *Ügyfél*lel kötött szerződés megszűnése esetén a *Szolgáltató* visszavonja a tanúsítványt.

4.12. Magánkulcs letétbe helyezése és visszaállítása

Elektronikus aláírás létrehozására, valamint authentikációra szolgáló tanúsítványok esetén a magánkulcs nem helyezhető letétbe.

Titkosításra szolgáló tanúsítványok esetén a *Szolgáltató* letétbe-helyezés szolgáltatást is nyújt a tanúsítványokkal kapcsolatban. A letétbe helyezés szolgáltatás igénybe vétele opcionális. A Szolgáltatás igénybe vételének módját, és feltételeit a *Szolgáltatási szabályzat* írja le.

5. Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A *Szolgáltató* széles körben elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmaz.

Fizikai előírások

A *Szolgáltató* gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások eszközeit érintő fizikai kockázatát minimalizálja.

A fizikai óvintézkedések célja a *Szolgáltató* által birtokolt információra illetve fizikai zónáira irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a *Szolgáltató* rendszerében. A biztosított védelem arányban áll a *Szolgáltató* által végzett kockázat elemzésben megállapított kockázatokkal.

Eljárásbeli előírások

A *Szolgáltató* gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse.

Az eljárásbeli óvintézkedések célja, hogy a bizalmi szerepkörök kijelölésével és elkülönítésével, az egyes szerepkörök felelősségének dokumentálásával, az egyes feladatokhoz szükséges személyzeti létszámok, a kizáró szerepkörök, valamint az egyes szerepkörökben elvárt azonosítás és hitelesítés meghatározásával kiegészítse, egyúttal fokozza a fizikai és személyzetre vonatkozó óvintézkedések hatásosságát. A *Szolgáltató* által – a 3/2005. (III. 18.) IHM rendelet [4] szerint meghatározott – bizalmi szerepköröket a *Szolgáltatási szabályzat* ismerteti részletesen.

A *Szolgáltató* belső irányítási rendszere biztosítja a jogszabályoknak és belső szabályzatainak megfelelő működést. Rendszerében minden rendszerelemhez és minden folyamathoz egyértelműen hozzárendelhető az adott rendszerelemért, vagy folyamatért felelős személy. A *Szolgáltató* rendszerében élesen elkülönülnek egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a *Szolgáltató* belső ellenőrzése biztosítja.

Személyzetre vonatkozó előírások

A *Szolgáltató* gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlata fokozza és támogassa a *Szolgáltató* működésének megbízhatóságát. A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a visszaélések kockázatának csökkentése.

Ennek érdekében a *Szolgáltató* a személyi biztonsággal már a felvételi szakaszban foglalkozik, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi szerepkör esetén a felvételire jelentkezőknek erkölcsi bizonyítvánnyal kell rendelkezniük. Minden bizalmi szerepkört betöltő alkalmazottnak és külső félnek, akik a *Szolgáltató* szolgáltatásaival kapcsolatba kerül, titoktartási nyilatkozatot kell aláírni.

A *Szolgáltató* egyúttal biztosítja valamennyi munkakör betöltéséhez a szükséges közös, általános, illetve az egyes munkakörök betöltéséhez szükséges speciális szakmai ismeretek megszerzését, illetve továbbfejlesztését.

A biztonsági naplózás folyamatai

A *Szolgáltató* informatikai rendszere széleskörű naplózási tevékenységet folytat a tanúsítványokra vonatkozó műveletek és az ezek során felhasznált adatok megőrzése érdekében. A naplóbejegyzések a bejegyzés pontos idejét, a tevékenység időpontját (ha az a bejegyzés idejétől eltér) és végrehajtóját is tartalmazzák.

A *Szolgáltató* pontos időt biztosító egysége legfeljebb 1 másodperces eltérést engedélyez a valódi időhöz képest. Az esetleges ennél nagyobb eltérések szintén naplózásra kerülnek.

A *Szolgáltató* egyéb informatikai rendszerei szintén naplóznak, e naplózások tulajdonságai az adott alkalmazások függvényei. A naplózások elemei elkülönülten keletkeznek a különböző modulokban. Operatív szinten az egyes rendszerek üzemeltetési leírásai, valamint a *Szolgáltató* biztonsági szabályzata szabályozzák a napló adatok kezelését.

Adatok archiválása

Szolgáltató informatikai rendszerének biztonsági és egyéb naplózási folyamatait egymástól független, a szolgáltatásokat nyújtó informatikai rendszerrel azonos biztonsági szintű rendszerek végzik. Jelen fejezetben csak *Szolgáltató* ettől eltérő papír alapú és egyéb speciális archiválási rendszerét ismertetjük.

*Szolgáltató Regisztrációs szervezet*e valamennyi, a regisztrációs eljárás során keletkező iratot tárolja és megőrzi. Így tárolja:

- a *Szolgáltató*hoz benyújtott valamennyi papír alapú vagy elektronikus kérelmet (tanúsítvány kibocsátás, tanúsítványcsere, tanúsítvány-visszavonás stb.),

- a *Szolgáltató* és az *Ügyfel*ek között megkötött valamennyi megállapodást.

A *Szolgáltató* megőriz minden (papíralapú vagy elektronikus) iratot és hangfelvételt a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított 10 évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig.

Az iratok biztonságos megőrzéséről és tárolásáról *Szolgáltató* olyan adattár segítségével gondoskodik, amelyhez a *Szolgáltató*nak csak meghatározott munkatársai rendelkeznek hozzáférési engedéllyel. A *Szolgáltató* a jogszabályok szerint archiválandó adatállományokat minősített időbélyegzővel és fokozott biztonságú elektronikus aláírással látja el.

A *Szolgáltató* a papíron tárolt adatairól a hiteles elektronikus másolatkészítés szabályainak [5] megfelelően másolatot készít.

Kulcs csere

Helyreállítás rendkívüli üzemi helyzetek esetén

A *Szolgáltató* rendelkezik katasztrófa elhárítási tervvel, mely részletesen szabályozza a különböző sérülések és katasztrófahelyzetek (beleértve valamely szolgáltatói magánkulcs kompromittálódását, vagy kritikus hardver/szoftver elem meghibásodását is) esetén követendő eljárásokat. A katasztrófa elhárítási terv a rendkívüli üzemi helyzetekre helyreállítási terveket tartalmaz. E terveket a *Szolgáltató* rendszeresen teszteli. A következő fejezetekben e katasztrófa elhárítási terv irányelveit foglaljuk össze.

A *Szolgáltató* megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik, a hardver- és szoftver meghibásodások valamint az adatsérülések minimalizálása érdekében. A szolgáltatások helyreállíthatóságát *Szolgáltató* háttérszerződései és saját tartalék eszközei garantálják.

A szolgáltatói nyilvános kulcsok visszavonásáról *Szolgáltató* az 2.1. fejezetnek megfelelően értesítést tesz közzé.

A *Szolgáltató* katasztrófa elhárítási terve a szolgáltatói magánkulcsok kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik valamennyi *Érintett fél* értesítéséről, megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet és a kompromittálódás által érintett végelhasználókat.

A hitelesítés szolgáltató vagy regisztrációs szervezet leállítása

A *Szolgáltató* a hitelesítés szolgáltatás leállítása esetén teljesíti a jogszabályban [1], [4] meghatározott követelményeket.

Az ezzel kapcsolatos rendelkezéseket a *Szolgáltatási szabályzat* tartalmazza.

6. Műszaki biztonsági óvintézkedések

A *Szolgáltató* módosítás ellen védett, megbízható rendszereket és termékeket használ. Megbízható, biztonságtechnikailag értékelt és minősített termékekből álló, egységes informatikai rendszert használ szolgáltatásai nyújtásához. Mind a *Szolgáltató*, mind a rendszert szállító és kivitelező vállalkozók hitelesítés-szolgáltatás kiépítésében jelentős tapasztalatokkal rendelkeznek és nemzetközileg elismert technológiát alkalmaznak.

6.1. Kulcspár előállítás és telepítés

A *Szolgáltató* gondoskodik valamennyi általa (saját maga, egyes szervezeti egységei (pl. tanúsítványtár, *Regisztrációs szervezet*ek), illetve az Alanyok számára) generált magánkulcs biztonságos, és az ipari szabványoknak megfelelő generálásáról.

6.1.1. Magánkulcs eljuttatása a tulajdonoshoz

Az ezzel kapcsolatos rendelkezéseket a *Szolgáltatási szabályzat* tartalmazza.

6.1.2. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Az ezzel kapcsolatos rendelkezéseket a *Szolgáltatási szabályzat* tartalmazza.

6.1.3. A szolgáltatói nyilvános kulcs közzététele

Lásd: 2.1. fejezet.

6.1.4. Kulcs méretek

Az egyes kulcsok hosszát a *Szolgáltatási szabályzat* tartalmazza.

6.1.5. A nyilvános kulcs paraméterek előállítása

A *Szolgáltató* tanúsítvány aláírására minden esetben a Nemzeti Média- és Hírközlési Hatóság Eat. 18. § szerint kibocsátott határozata értelmében biztonságosan felhasználható algoritmust használ.

Az RSA algoritmussal van aláírva a rendszer által kibocsátott minden tanúsítvány, és ezt az algoritmust használják a rendszeren belül is a letagadhatatlanság (tranzakciók aláírása, a *Regisztrációs szervezet* által archivált adatok aláírása stb.) biztosítására. A végfelhasználók számára kibocsátott tanúsítványok aláíró algoritmusa is az RSA.

A rendszerben használt valamennyi elektronikus aláírás esetén a lenyomatképző függvény az SHA-2.

A *Szolgáltató* a későbbiekben további lenyomatképző függvényt is bevezethet.

6.1.6. A paraméterek megfelelőségének ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

- a paraméterekhez felhasznált véletlen szám generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),
- a paraméterekre vonatkozó előírások teljesülésének ellenőrzése.

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

A *Szolgáltatási szabályzat* tartalmazza.

6.2. A magánkulcsok védelme

A *Szolgáltató* gondoskodik saját magánkulcsainak titkosságáról és sértetlenségéről, valamint az Alanyok magánkulcsainak titkosságáról és sértetlenségéről amíg az Alanyok kulcsai a *Szolgáltató* birtokában vannak.

A *Szolgáltató* a végfelhasználók kulcsait a kulcsok átadása előtt fizikailag biztonságos helyszínen tárolja.

A kriptográfiai hardver eszköz használatát megkövetelő *Hitelesítési rend*ek esetén a *Szolgáltató*

- meggyőződik róla, hogy az Alanyok magánkulcsait kriptográfiai hardver eszköz védi, vagy
- elfogadhatja az Alanyok ilyen értelmű írásos nyilatkozatát.

Ennek részleteit a *Szolgáltatási szabályzat* tartalmazza.

6.3. A kulcspár gondozásának egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

A *Szolgáltató* minden, a hitelesítő szervezete által előállított tanúsítványt archivál az érvényesség lejártától számított 10 évig.

6.3.2. A nyilvános és magánkulcsok használatának periódusa

A *Szolgáltatási szabályzat* tartalmazza.

6.4. Aktivizáló adatok

A *Szolgáltató* biztonságosan, véletlen szám generátor segítségével, fizikailag biztonságos körülmények között állítja elő az általa kibocsátott biztonságos aláírás létrehozó eszközök aktivizáló adatait. A *Szolgáltató* az általa kibocsátott biztonságos aláírás létrehozó eszközök valamint a *Szolgáltató* által üzemeltetett HSM modulokban tárolt kulcsok aktivizáló adatait műszaki és szervezési intézkedések segítségével védi.

6.5. Számítógépes biztonsági óvintézkedések

A *Szolgáltató* a *Szolgáltatási szabályzat*ban leírt megbízható informatikai rendszereket és megoldásokat alkalmazza. Ennek megfelelően megbízható technológiákat alkalmaz, és rendszerét redundánsan alakította ki.

6.6. Életciklusra vonatkozó műszaki óvintézkedések

Annak érdekében, hogy az e-Szignó Hitelesítés Szolgáltató valamennyi rendszerfejlesztési projektjében a biztonsági követelmények magas színvonalon biztosítottak legyenek, a teljes fejlesztés során (már a tervezési és követelmény-meghatározási fázisban is) figyelembe kell venni a fokozott követelményeket.

A hitelesítés szolgáltatás nyújtásához használt termékek életciklusra vonatkozó biztonsági szempontok figyelembevételével kerültek alkalmazásra.

A *Szolgáltató* hitelesítő szervezete és ügyfélszolgálati irodája (valamint a mobil regisztrációs egységek) közötti kommunikáció (belső hálózat) védett a bizalmasság, sértetlenség és letagadhatatlanság szempontjából.

7. Tanúsítvány, CRL, OCSP profilok

7.1. Tanúsítvány profil

A *Szolgáltatási szabályzat* tartalmazza.

7.2. Tanúsítvány visszavonási lista (CRL) profil

A *Szolgáltatási szabályzat* tartalmazza.

7.3. Online tanúsítvány-állapot válasz (OCSP) profil

A *Szolgáltatási szabályzat* tartalmazza.

8. A megfelelőség vizsgálata

A *Szolgáltatási szabályzat* tartalmazza.

9. Üzleti és jogi tudnivalók

9.1. Jogok és kötelezettségek

9.1.1. A *Szolgáltató* kötelezettségei

A *Szolgáltató* alapvető kötelezettsége, hogy a hitelesítés szolgáltatást a jelen *Hitelesítési rend*del és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a vállalati és biztonsági belső szabályzatokkal összhangban nyújtsa; ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi, szabályozási, anyagi, szerződéses stb. keretek megteremtése,
- magas színvonalú és biztonságos szolgáltatás nyújtása a vonatkozó szabályzatok szerint,
- a szolgáltatáshoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése,
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése,
- a szolgáltatás biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket,
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az Interneten keresztül,
- a jogszabályban előírt tájékoztatás nyújtása az *Ügyfel*ek részére,

9.1.2. Az *Előfizető* jogai

- Az *Előfizető* jogosult a szolgáltatás igénybe vételére a jelen *Hitelesítési rend*ben, valamint a *Szolgáltatási szabályzat*ban leírtak szerint.

Az *Előfizető* további jogait a *Szolgáltatási szabályzat* tartalmazza.

9.1.3. Az *Előfizető* kötelezettségei

Az *Előfizető* kötelessége a *Szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a hitelesítés szolgáltatás felhasználása során, beleértve a tanúsítványok és magánkulcsok igénylését és alkalmazását. Az *Előfizető* kötelezettségeit a jelen *Hitelesítési rend*, a *Szolgáltatási szerződés* és annak mellékletei – különösen az általános szerződési feltételek és a *Szolgáltatási szabályzat* írja le.

9.1.4. Az Alany jogai

- Az Alany jogosult tanúsítványt igényelni a *Szolgáltatási szabályzat*ban leírtak szerint.
- Az Alany jogosult saját tanúsítványa visszavonását kérni.
- Amennyiben ezt a vonatkozó *Hitelesítési rend* lehetővé teszi, az Alany jogosult tanúsítványának felfüggesztését, illetve visszavonását kérni.

9.1.5. Az Alany kötelezettségei

- Az Alany köteles a szolgáltatás igénybe vétele előtt megismerni a jelen *Hitelesítési rend*et és a *Szolgáltatási szabályzat*ot.
- Az Alany köteles a *Szolgáltató* által kért, a szolgáltatás igénybe vételéhez szükséges adatokat hiánytalanul megadni, valamint köteles a valóságnak megfelelő adatokat szolgáltatni.
- Az Alany köteles a *Szolgáltató*t haladéktalanul írásban értesíteni, amennyiben tudomására jut, hogy az általa megadott, a szolgáltatás igénybe vételéhez szükséges adat – különösen valamely tanúsítványban is szereplő adat – megváltozott.
- Az Alany köteles a szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a hivatkozott szabályzatokban, a hivatkozott dokumentumokban foglaltaknak megfelelően használni.
- Az Alany köteles biztosítani, hogy a szolgáltatás igénybe vételéhez szükséges adatokhoz és eszközökhöz (jelszavakhoz, titkos kódokhoz, intelligens kártyákhoz) illetéktelen személyek ne férhessenek hozzá.
- Az Alany köteles a *Szolgáltató*t haladéktalanul írásban értesíteni, amennyiben valamely, a szolgáltatással kapcsolatos elektronikus aláírással, illetve tanúsítvánnyal kapcsolatban jogvita indul.
- Az Alany köteles a tanúsítvány kiadásához szükséges adatok ellenőrzése érdekében a *Szolgáltató*val együttműködni, és mindent megtenni azért, hogy az ellenőrzés a lehető leghamarabb befejeződhessen.

- Amennyiben az Alany magánkulcsa, intelligens kártyája vagy a kártya aktiválásához szükséges titkos kódok illetéktelen kezekbe kerültek vagy megsemmisülnek, az Alany köteles e tényt haladéktalanul írásban jelenteni a *Szolgáltató*nak, illetve köteles kezdeményezni az eszközhöz tartozó tanúsítványok felfüggesztését, illetve visszavonását.
- Az Alany köteles tudomásul venni, hogy az *Előfizető* jogosult a tanúsítvány visszavonását, illetve felfüggesztését kérni.
- Az Alany köteles tudomásul venni, hogy a *Szolgáltató* a tanúsítványt a *Szolgáltatási szabályzat*ban leírt meghatározott módon, az ott leírt ellenőrzési lépések elvégeztével bocsátja ki. Az Alany köteles tudomásul venni, hogy a *Szolgáltató* a kibocsátott tanúsítványokban kizárólag a valóságnak megfelelő adatokat szerepeltet. Ennek megfelelően a *Szolgáltató* a tanúsítványba kerülő adatokat a *Szolgáltatási szabályzat* szerint ellenőrzi, és ha valamely, a tanúsítványban szereplő adat megváltozik, a *Szolgáltató* a tanúsítványt a *Szolgáltatási szabályzat* szerint visszavonja.
- Az Alany köteles tudomásul venni, hogy a *Szolgáltató* jogosult a szolgáltatás során kibocsátott tanúsítványt felfüggeszteni, illetve visszavonni, amennyiben az *Előfizető* nem fizeti meg határidőre a Szolgáltatások díját.
- Amennyiben az Alany szervezeti tanúsítványt igényel, köteles tudomásul venni, hogy a *Szolgáltató* a tanúsítványt kizárólag a *Képviselt szervezet* hozzájárulása esetén bocsátja ki.
- Amennyiben az Alany szervezeti tanúsítványt igényel, köteles tudomásul venni, hogy a *Képviselt szervezet* jogosult a tanúsítvány visszavonását kérni.
- A *Szolgáltatási szabályzat* további kötelezettségeket tartalmazhat az Alany számára.

9.1.6. A *Képviselt szervezet* jogai

- A *Szolgáltató* kizárólag a *Képviselt szervezet* hozzájárulásával bocsát ki olyan tanúsítványt, amelyben a *Képviselt szervezet* neve is feltüntetésre kerül.
- A *Képviselt szervezet* jogosult azon tanúsítványokat felfüggeszteni és visszavonni, amelyekben a *Képviselt szervezet* neve is feltüntetésre került.

9.2. Felelősség

A *Szolgáltató* felelősségét a jelen *Hitelesítési rend*, a *Szolgáltatási szabályzat*, valamint az *Ügyfél*lel kötött szerződés és annak mellékletei tartalmazzák.

9.2.1. A *Szolgáltató* általános felelőssége

- A *Szolgáltató* felelősséget vállal az általa támogatott hitelesítési rendekben, és a *Szolgáltatási szabályzat*ban leírt eljárásoknak való megfelelésért, még abban az esetben is, amikor a *Szolgáltató* egyes tevékenységeit alvállalkozók végzik.
- A *Szolgáltató* a vele szerződéses jogviszonyban álló ügyfelekkel szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésszegésért való felelősség szabályai szerint felelős.
- A *Szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik féllel (ilyen az *Érintett fél*) szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésen kívüli károkozásról szóló szabályai (Ptk. 339. §) szerint felelős.
- A *Szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött *Szolgáltatási szerződés*ekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása).

Felelősség korlátozása

- A *Szolgáltató* nem felelős az olyan károkért, amelyek abból adódnak, hogy az *Érintett fél* a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és a *Szolgáltató* szabályzatai szerint járt el, illetve nem úgy járt el, ahogyan az az adott helyzetben elvárható.
- A *Szolgáltató* a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helyt állni.
- A *Szolgáltató* nem felelős az abból adódó károkért, amikor az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.
- A *Szolgáltató* tevékenységét a Nemzeti Média- és Hírközlési Hatóság által elfogadott kriptográfiai algoritmusok segítségével végzi, és a kibocsátott intelligens kártyák is a Hatóság által elfogadott kriptográfiai algoritmusokat használnak. A *Szolgáltató* nem felelős ezen kriptográfiai algoritmusok hibájából, illetve gyengeségeiből eredő károkért.
- A *Szolgáltató* kizárólag azért vállal felelősséget, hogy a Szolgáltatásokat a *Szolgáltatási szabályzat*ban, illetve az abban meghivatkozott dokumentumokban (hitelesítési , szabványok, ajánlások) leírtaknak, valamint saját belső szabályzatainak megfelelően nyújtja.

Pénzügyi felelősség korlátozása

A *Szolgáltató* a kártérítés felső határát tanúsítványonként és összességében is (az összes tanúsítvánnyal és káreseménnyel kapcsolatban) korlátozza. Ezen korlátozás mértékét a *Szolgáltatási szabályzat* tartalmazza.

A hitelesítő szervezet felelőssége

Az e-Szignó Hitelesítés *Szolgáltató* felelős:

- az általa kibocsátott tanúsítványok hitelességéért, pontosságáért
- az általa kibocsátott szabályzatokért, azok jogszabályi megfelelőségéért és betartásáért,
- az általa generált kulcspárok megfelelőségéért, a magánkulcs-nyilvános kulcs és a tanúsítvány összetartozásáért,
- az intelligens kártyát aktivizáló kód és az eszközre töltött kulcsok összetartozásáért,
- általában a kötelezettségei betartásáért.

A regisztráló szervezet felelőssége

Az ügyfélszolgálati iroda felelős:

- az Alanyok személyazonosságának megállapításáért és a *Képviselt szervezet* szervezeti azonosságának megállapításáért, és ez utóbbi esetben a *Képviselt szervezet* nevében eljáró személy képviseleti jogosultságának megállapításáért is,
- a felvett regisztrációs adatok valódiságáért,
- a szolgáltatások igénybe vevőjének tájékoztatásáért a Szabályzat tartalmáról és elérhetőségéről, és a szolgáltatás igénybevételének feltételeiről a Szolgáltatói Szerződés megkötését megelőzően,
- általában kötelezettségei betartásáért.

Az e-Szignó Hitelesítés Szolgáltató nem felelős:

- az Alanyok magánkulccsal, illetve intelligens kártyával kapcsolatos tevékenységeiért,
- az *Érintett felek* tanúsítvány ellenőrzési és felhasználási tevékenységeiért,
- az *Érintett felek* vagy mások által kibocsátott szabályzatokért.

9.2.2. A *Szolgáltató* felelőssége a tanúsítványok ellenőrzésével kapcsolatban

A *Szolgáltató* kizárja felelősségét, amennyiben az *Érintett fél* nem körültekintően jár el a tanúsítványok felhasználása vagy ellenőrzése során, azaz nem jelen *Hitelesítési rend*, nem a *Szolgáltatási szabályzat*, illetve nem a hatályos jogszabályok szerint jár el.

9.2.3. Az Alany felelőssége

Az Alany felelős:

- a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért,
- az adataiban bekövetkezett változások haladéktalan bejelentéséért,
- magánkulcsának és intelligens kártyájának a szabályzatoknak megfelelő felhasználásáért,
- magánkulcsának és aktivizáló kódjának biztonságáért,
- az intelligens kártyája biztonságáért,
- a *Szolgáltató* haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben,
- általában a kötelezettségei betartásáért.

9.2.4. A *Képviselt szervezet* felelőssége

A *Képviselt szervezet* kizárólag az általa kiadott igazolásokért felel. Különösen azon igazolásokért, amelyben igazolja, hogy az Alany a *Képviselt szervezet* munkatársa.

9.2.5. Az *Előfizető* felelőssége

Az *Előfizető* felelősségét a *Szolgáltatási szerződés* és annak mellékletei (köztük az általános szerződési feltételek) határozzák meg.

9.2.6. Kártérítés a *Szolgáltató* számára

Az *Előfizető*, illetve az Alany kártérítési felelősséggel tartoznak a *Szolgáltató*nak azokért a veszteségekért és károkért, amelyeket kötelezettségeik és a rájuk vonatkozó ajánlások be nem tartásával okoznak számára.

9.2.7. Adminisztratív folyamatok

A *Szolgáltató* a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) a naplóadatokat.

9.3. Értelmezés és érvényesítés

9.3.1. Irányadó jog

A *Szolgáltató* tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A *Szolgáltató* szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

- 2001. évi XXXV. törvény az elektronikus aláírásról (a 2004. évi módosításokkal).
- 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról
- 7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről.
- 45/2005 (III. 11) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól.
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
- 1959. évi IV. törvény a Polgári Törvénykönyvről.

9.3.2. Vitás kérdések megoldására vonatkozó eljárások

A *Szolgáltatási szabályzat* tartalmazza.

9.4. Díjak és árak

A *Szolgáltatási szabályzat* tartalmazza.

9.5. Szellemi tulajdonjogok

A *Szolgáltató* által ügyfelei részére kibocsátott tanúsítvány és az ennek megfelelő kulcspár tulajdonosa az *Előfizető*, a tanúsítványok teljes jogú felhasználója pedig az Alany, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

- A *Szolgáltató* az általa kibocsátott végfelhasználói tanúsítványokat a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.
- A visszavonási információ a *Szolgáltató* tulajdonát képezi.
- A *Szolgáltató* által az ügyfelek részére kibocsátott egyedi azonosító a *Szolgáltató* tulajdonát képezi.
- A tanúsítványban szereplő azonosító (amely a tanúsítvány alanyát azonosítja) használatára a megnevezett Alany, illetve *Ügyfél* jogosult.
- A *Szolgáltató* szabályzatai, szerződéses feltételei a *Szolgáltató* tulajdonát képezik.

9.6. Az ügyfelek adatainak kezelése

A *Szolgáltató* nyilvántartásában azonosító adatokat, tanúsítványban szereplő adatokat és elérhetőséggel kapcsolatos adatokat és a szolgáltatás nyújtásával kapcsolatos adatokat tárol az Alanyról. A *Szolgáltató* kizárólag olyan esetben adja át harmadik félnek az Alany adatait, ha ezt jogszabály előírja vagy ha az Alany ebbe írásban beleegyezett.

A *Szolgáltató* – a *Szolgáltatási szerződés*nek megfelelően – nyilvánosságra hozza az Alanyok tanúsítványban szereplő adatait és a tanúsítványra vonatkozó visszavonási információt. A tanúsítványban a *Szolgáltató* feltünteti az Alany személyéhez rendelt egyedi azonosítót (OID-et).

A *Szolgáltató* online tanúsítvány-állapot szolgáltatások előfizetőiről kizárólag a szolgáltatás igénybevételéhez, a hitelesítéshez, valamint a szerződéskötéshez és számlázáshoz szükséges információkat tárolja.

A *Szolgáltató* naplóz minden olyan eseményt, amely kapcsolatos tanúsítványok igénylésével, felfüggesztésével, visszaállításával vagy visszavonásával, illetve kapcsolatos a Szolgáltatások nyújtásával.

A *Szolgáltató* az általa tárolt adatokat és információkat a jogszabályi előírásoknak megfelelően megőrzi. A *Szolgáltató* az *Ügyfél* kérésére az *Ügyfél*ről nyilvántartott személyes adatokat a jogszabályi előírásoknak megfelelően törli adatbázisából.

9.7. Bizalmasság

A *Szolgáltató* az ügyfelek adatait a jogszabályoknak megfelelően kezeli. A *Szolgáltató* rendelkezik adatkezelési szabályzattal, amely a személyes adatok kezelésével kiemelten foglalkozik.

9.7.1. Nem bizalmasnak tekintett információ típusok

A *Szolgáltató* nem bizalmas információként kezeli mindazon adatokat, amelyet a tanúsítványba belefoglal. Ezek az adatok a *Szolgáltatási szerződés*hez kapcsolódó tanúsítványkérelem űrlapon egyértelmű jelöléssel szerepelnek.

9.7.2. Tanúsítvány visszavonási állapotának közzététele

A *Szolgáltató* az általa kibocsátott tanúsítványok visszavonását és felfüggesztését a tanúsítvány-visszavonási listában teszi közzé, a tanúsítvány sorszámának és opcionálisan a visszavonás okának a jelölésével. Bővebb információ a *Szolgáltatási szabályzat*ban található.

9.7.3. Információszolgáltatás a hatóságok részére

A *Szolgáltató* bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat az [1] törvény 11.§ (2) bekezdése szerinti körben.

A *Szolgáltató* rögzíti az előző pontbeli adatátadás tényét, de arról nem tájékoztatja az érintett ügyfeleket.

9.7.4. Információszolgáltatás polgári eljárás keretében

A *Szolgáltató* a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során – az érintettség igazolása esetén – az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas felhasználói információkat, illetőleg azokat közölheti a megkereső bírósággal az [1] törvény 11.§ (3) bekezdése szerinti körben.

A *Szolgáltató* rögzíti az előző pontbeli adatátadás tényét, és arról tájékoztatja az érintett ügyfelet.

9.7.5. A tulajdonos kérésére történő felfedés

A *Szolgáltató* az *Ügyfél* személyes kérése vagy az általa hivatalosan, írásban adott felhatalmazása alapján tárja fel a rá vonatkozó bizalmas felhasználói információkat harmadik fél részére a

személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény rendelkezéseinek megfelelően.

9.7.6. Egyéb információ-közzétételt eredményező körülmények

A *Szolgáltató* a nyilvántartásait (a jogszabályban meghatározott bizalmas felhasználói adatokkal együtt) a tevékenysége befejezésekor átadja más – azonos besorolású – szolgáltató részére az [1] törvény 16. § 2. bekezdése szerint.

9.8. Leírás-adminisztráció

A *Szolgáltató* rendelkezik hitelesítési renddel és *Szolgáltatási szabályzat*tal, amelyek mind honlapján, mind az ügyfélszolgálati irodájában elérhetőek. *Szolgáltató*n belül olyan csoport működik, amely a szabályzatok és dokumentációk karbantartásáért felelős. Az ezen csoport működésével és a *Szolgáltató* nyilvános szabályzatainak adminisztrációjával kapcsolatos további előírásokat a *Szolgáltatási szabályzat* tartalmazza.

A. Hivatkozások

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

[1] 2001. évi XXXV. törvény az elektronikus aláírásról.

[2] RFC 5280: X.509 Internet Public Key Infrastructure – Certificate and Certificate revocation List (CRL) Profile, May 2008.

[3] RFC 4043: Internet X.509 public Key Infrastructure - permanent Identifier, May 2005.

[4] 3/2005. (III.18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

[5] 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól.