MICROSEC
Számítástechnikai Fejlesztő zrt.

e-Szignó Hitelesítés Szolgáltató
Minősített tanúsítvány hitelesítési rendek

Azonosító:	1.3.6.1.4.1.21528.2.1.1.2.4.0, 1.3.6.1.4.1.21528.2.1.1.12.4.0, 1.3.6.1.4.1.21528.2.1.1.38.4.0, 1.3.6.1.4.1.21528.2.1.1.39.4.0, 1.3.6.1.4.1.21528.2.1.1.40.4.0, 1.3.6.1.4.1.21528.2.1.1.41.4.0
Verzió:	4.0
Első verzió hatálybalépése:	2005-04-01
Biztonsági besorolás:	NYILVÁNOS
Jóváhagyta:	Ellbogen András
Jóváhagyás dátuma:	2012-03-30
Hatálybalépés dátuma:	2012-05-01

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: 1.3.6.1.4.1.21528.2.1.1.2	2005-04-01	Berta István Zsolt Belső auditor: Tóth Elemér
2.0	A hatósági szemlét követő módosítások. Az álnevet kizáró és az álneves hitelesítési rend szétválasztása. OID: 1.3.6.1.4.1.21528.2.1.1.*	2005-08-08	Berta István Zsolt Belső auditor: Tóth Elemér
3.0	Módosítás az Általános Szerződési Feltételek megváltozása miatt. OID: 1.3.6.1.4.1.21528.2.1.1.*	2006-11-19	Dr. Berta István Zsolt
3.1	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően. OID: 1.3.6.1.4.1.21528.2.1.1.*.3.1	2006-12-04	Dr. Berta István Zsolt
3.2	Közjegyzői regisztráció megszüntetése. OID: 1.3.6.1.4.1.21528.2.1.1.*.3.2	2007-10-28	Dr. Berta István Zsolt
3.4	A tanúsítványcsere folyamata változott. OID: 1.3.6.1.4.1.21528.2.1.1.*.3.4	2008-12-20	Dr. Berta István Zsolt

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
4.0	A BALE használatát megkövetelő és a BALE nélküli rendek szétválasztása. Természetes és nem természetes személynek kibocsátott tanúsítványok szétválasztása. OID: 1.3.6.1.4.1.21528.2.1.1.*.4.0	2012-05-01	Dr. Berta István Zsolt

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec zrt. által üzemeltetett e-Szignó Hitelesítés Szolgáltató által meghatározott 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 rendek

Jelen dokumentum az alábbi hitelesítési rendeket definiálja:

- Természetes személyek számára kibocsátott minősített tanúsítványokhoz használt, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, álnevet kizáró hitelesítési rend.
  OID: 1.3.6.1.4.1.21528.2.1.1.2.4.0
- Természetes személyek számára kibocsátott minősített tanúsítványokhoz használt, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, álneves hitelesítési rend.
  OID: 1.3.6.1.4.1.21528.2.1.1.12.4.0
- Természetes személyek számára kibocsátott minősített tanúsítványokhoz használt, kriptográfiai hardver eszköz használatát megkövetelő hitelesítési rend.
  OID: 1.3.6.1.4.1.21528.2.1.1.38.4.0
- Természetes személyek számára kibocsátott minősített tanúsítványokhoz használt hitelesítési rend.
  OID: 1.3.6.1.4.1.21528.2.1.1.39.4.0
- Nem természetes személyek számára kibocsátott minősített tanúsítványokhoz használt, kriptográfiai hardver eszköz használatát megkövetelő hitelesítési rend.
  OID: 1.3.6.1.4.1.21528.2.1.1.40.4.0

- Nem természetes személyek számára kibocsátott minősített tanúsítványokhoz használt hitelesítési rend.
  OID: 1.3.6.1.4.1.21528.2.1.1.41.4.0

A természetes személyek számára kibocsátott tanúsítványokra vonatkozó rendek esetén az Aláíró minden esetben természetes személy. A nem természetes személyek számára kibocsátott tanúsítványokra vonatkozó rendek esetén az Aláíró jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, akinek a nevében az őt képviselő természetes személy készíthet aláírást.

Az álnevet kizáró rendek esetén a tanúsítványban az Aláíró valódi neve szerepel, míg az álneves rendek esetén a tanúsítványban minden esetben álnév szerepel. A többi rend valódi nevet és álnevet is megenged a tanúsítványokban.

A biztonságos aláírás-létrehozó eszköz használatát megkövetelő rendek esetén a tanúsítványhoz tartozó magánkulcsot biztonságos aláírás-létrehozó eszköz védi, amely minősített eszköz szolgáltatás keretében kerül kibocsátásra. Az ilyen rendek szerint kibocsátott tanúsítványokra minősített aláírás alapulhat. A minősített aláírással ellátott dokumentum a jogszabályok értelmében teljes bizonyító erejű magánokirat.

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)

Amennyiben egy hitelesítési rend nem követeli meg biztonságos aláírás-létrehozó eszköz használatát, a rend szerint kibocsátott tanúsítványra alapuló aláírás minősített tanúsítványra épülő fokozott biztonságú aláírásnak tekinthető. A minősített tanúsítványra épülő aláírással ellátott dokumentum a polgári perrendtartásról szóló 1952. évi III. törvény 196. §-a értelmében értelmében teljes bizonyító erejű magánokirat.

Az automatikusan, közvetlen személyi felügyelet nélkül készült aláírások esetén készült aláírások olyan informatikai eszköz útján készíthetőek, amelyek megfelelnek az Eat. 10/A §-ában hivatkozott jogszabálynak.

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 rendnek megfelelő tanúsítványokat kibocsátó szolgáltató (a továbbiakban: Szolgáltató) adatait, ügyfélszolgálati irodájának elérhetőségét, nyitvatartását, a Szolgáltatóval 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 rendek azonosító adatait az 1.1.1. fejezet tartalmazza.

1.4. PKI közösség

A jelen hitelesítési rendben szereplő PKI közösség az alábbi felekből áll:

- *Szolgáltató*: A jelen hitelesítési rendnek 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. Az Előfizető fizeti meg az ezen szolgáltatások igénybevételével kapcsolatos költségek ellenértékét. Az Előfizető szolgáltatási szerződést köt a Szolgáltatóval.
- *Aláíró*: Az elektronikus aláírás hitelesítés szolgáltatást igénybe vevő fél, aki számára a Szolgáltató elektronikus aláírás létrehozására alkalmas tanúsítványt bocsát ki.
- *Képviselt Szervezet*: Amennyiben a tanúsítvány az Aláíró 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 Szervezettel 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 Szolgáltatóval. Tevékenységére vonatkozó ajánlásokat a Szabályzat és az abban megnevezett egyéb szabályzatok tartalmazzák. A Szolgáltató az Érintett féllel elsősorban az internetes honlapon keresztül tart kapcsolatot.

1.5. Alkalmazhatóság

Engedélyezett alkalmazási lehetőségek

A kibocsátott végfelhasználói tanúsítványok, illetve a hozzájuk tartozó magánkulcsok kizárólag elektronikus aláírás készítésére használhatóak fel.

Korlátozások

A Szolgáltató korlátozza a tanúsítványokkal kapcsolatos kártérítési kötelezettségét. Ennek részleteit a Szolgáltatási Szabályzat tartalmazza. A tanúsítvánnyal egy alkalommal vállalható pénzügyi kötelezettség legmagasabb mértékét a tanúsítvány tartalmazza.

Tiltott alkalmazási lehetőségek

A kibocsátott tanúsítványokat, illetve a hozzájuk tartozó magánkulcsokat aláírástól 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.

Aláíró (Signatory): Az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult, valamint 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 Aláíró részére, akkor a Képviselt Szervezet a szóban forgó szervezet, amely szintén megjelölésre kerül a tanúsítványban.

Alany (Subject): A tanúsítvány által azonosított személy vagy eszköz. Elektronikus aláírásra szolgáló tanúsítvány esetén az Alany megegyezik az Aláíróval.

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: 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.

Kompromittálódik: 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 személyazonosságát. 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 az 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 személyhez kapcsolja, akinek személyazonosságáról meggyőződött.

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

Tanúsítványkérelem: Az a folyamat, amelynek során az Aláíró 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.

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 elektronikus formában hozza nyilvánosságra a honlapján. A honlapon az érvényben levő dokumentumokon kívül a korábbi verziók is elérhetőek.

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

- tevékenységének befejezése (lásd: 5.7. 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 Aláíró 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 renddel 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 Aláíró 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 Aláíró azonosító (Subject) mezők az RFC 5280 szerinti egyedi név formátum előírásainak felelnek meg. [1] Ezen kívül a Szolgáltató támogatja a kiterjesztések között található Alternatív név mezők (Subject Alternative Names, Issuer Alternative Names) kitöltését is.

A tanúsítványban szereplő Aláíró 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 Aláíró esetén az Aláíró személyazonosító okmányában szereplő neve kerül e mezőbe, magyar írásmód szerint, ékezetesen.

  Nem természetes személy Aláíró esetén az Aláíró valamely közhiteles adatbázisban (cég esetén a cégnyilvántartásban) szereplő neve kerül e mezőbe, ékezetesen. E mező opcionálisan tartalmazhatja még az automatizmus funkcióját is.

  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.

- Pseudonym (PSEUDO) – OID: 2.5.4.65
  Kizárólag álneves tanúsítvány esetén kerül kitöltésre, ekkor e mezőbe kerül az Aláíró álneve. Az álnevet az Aláíró 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 Aláíró egyedi azonosítója az RFC 4043 szerint. [2] A tanúsítványban legalább egy serial number kötelezően szerepel.

- Organization (O) – OID: 2.5.4.10
  Amennyiben az Aláíró 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 Aláíró állandó lakcíme szerinti ország kétbetűs kódja. Kitöltése kötelező.

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

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

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

A jelen hitelesítési rendek szerint kibocsátott tanúsítványok a fentieken túl további Subject DN mezőket is tartalmazhatnak.

Az Aláíró 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 Aláíró 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 Aláíró 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 lenni.
- A tanúsítványban szereplő személynevet a bemutatott személyazonosító okmányban szereplő írásmóddal, ékezethelyesen kell feltüntetni.

Álneves tanúsítvány 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 feleknek a jelen dokumentumban leírtak alapján kell eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett félnek segítségre lenne szüksége, akkor a Szolgáltatóval közvetlen is felveheti a kapcsolatot. A Szolgáltató ilyen esetben az ügyfél egyéb

adatairól többlettájékoztatást – feltéve, hogy jogszabály ezt nem írja elő – nem ad, csak a tanúsítványban feltüntetett adatok értelmezését segítő információt szolgáltatja.

3.1.2. A nevek egyedisége

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

3.1.3. Eljárások a nevekre vonatkozó vitás kérdések megoldására

Az Aláírók 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, Szolgáltatónak jogában áll visszavonni a kérdéses tanúsítványt.

3.1.4. 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

A Szolgáltató személyes találkozás során győződik meg róla, hogy az Aláíró valóban birtokolja a tanúsítványba kerülő 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

Azon hitelesítési rendek esetén, ahol a tanúsítvány alanya természetes személy, a Szolgáltató személyes találkozás során azonosítja az Aláírót valamely okmánya alapján.

Azon hitelesítési rendek esetén, ahol a tanúsítvány alanya jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, a Szolgáltató az Aláíró képviseletére jogosult munkatársát, vagy meghatalmazottját azonosítja az előző bekezdésben leírtakkal megegyező módon.

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 Aláíró előzetes tanúsítványigénylést kell, hogy benyújtson a Szolgáltatónak. Ez történhet a Szolgáltató honlapján keresztül is. A tanúsítványigénylésben az Aláíró megadja a tanúsítványba kerülő adatait, megnevezi, hogy pontosan milyen tanúsítványt igényel, és felhatalmazza a Szolgáltatót az adatok kezelésére.

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

A tanúsítványigényléssel kapcsolatban a Szolgáltatási Szabályzat további megkötéseket tartalmazhat.

4.2. A tanúsítványkérelem benyújtása és feldolgozása

A tanúsítványkérelmet az Aláíró személyesen nyújthatja be a Szolgáltató ügyfélszolgálati irodájában vagy valamely külső regisztrációs szervezet regisztrációs munkatársa előtt.

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 Aláíró személyazonosságának ellenőrzése céljából adategyeztetést végez legalább eggyel a következő szervezetek 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 Aláíró 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.

A Szolgáltató akkor bocsátja ki a tanúsítványt, amikor a hozzá tartozó magánkulcs már az Aláíró birtokában van.

4.4. Tanúsítvány-elfogadás

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

A Szolgáltató értesíti a tanúsítvány kibocsátásáról az Aláírót, az Előfizetőt, illetve a Képviselt Szervezetet.

A Szolgáltatási Szabályzat további előírásokat tartalmazhat.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. Az Aláíró tanúsítvány használata

Az Aláíró a tanúsítványát kizárólag elektronikus aláírás készítésére használhatja.

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

4.5.2. Az Érintett félre vonatkozó ajánlások

Amennyiben egy Érintett fél ésszerűen kíván a tanúsítványra hagyatkozni, a Szolgáltatási Szabályzatnak 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 ügyféllel 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 Aláíró
- 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 ügyfelek a tanúsítványok felfüggesztését kérhetik.

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

Visszavonási kérelmeket a Szolgáltató egy munkanapon belül, de soron kívül dolgoz 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 legkésőbb új CRL-t bocsát ki, illetve a Szolgáltató OCSP szolgáltatásán is meg kell, hogy jelenjen legkésőbb ezen időszak után a megváltozott visszavonási állapot.

A “visszavonási állapot közzététele” szolgáltatás rendelkezésre állása: 99,9%; az eseti szolgáltatás-kiesések nem haladhatják meg a 3 órát. A Szolgáltató által működtetett hitelesítő egységek legfeljebb 24 óránként bocsátanak ki CRL-t.

4.11. Az előfizetés vége

Az ügyféllel kötött szerződés megszűnése esetén a Szolgáltató visszavonja a tanúsítványt.

4.12. Magánkulcs letétbe helyezése és visszaállítása

A tanúsítványhoz tartozó magánkulcs nem helyezhető letétbe.

5. Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

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

5.1. Fizikai óvintézkedések

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

A fizikai óvintézkedések célja a Szolgáltató információjára és 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.

5.2. Eljárásbeli óvintézkedések

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

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] rendelet 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.

5.3. Személyzetre vonatkozó óvintézkedések

A Szolgáltató gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák 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 munkakör esetén a felvételire jelentkezőket biztonsági ellenőrzésnek vetik alá. Minden bizalmi munkakört betöltő alkalmazottnak és külső félnek, akik a Szolgáltató szolgáltatásaival kapcsolatba kerülnek, titoktartási nyilatkozatot kell aláírni.

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

5.4. A biztonsági naplózás folyamatai

Szolgáltató 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. Szolgáltató egyéb 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.

5.5. Adatok archiválása

Szolgáltató informatikai rendszerének biztonsági és egyéb naplózási folyamatait ugyanazon rendszerek végzik, ugyanazon módszerek segítségével. Jelen fejezetben csak Szolgáltató ettől eltérő papír alapú és egyéb speciális archiválási rendszerét ismertetjük.

Szolgáltató regisztrációs szervezete valamennyi regisztrációs eljárás során keletkező iratot tárol és megőriz. Így tárolják:

- a Szolgáltatóhoz benyújtott valamennyi papír alapú kérelmet (tanúsítvány kibocsátás, tanúsítványcsere, tanúsítvány-visszavonás stb.),
- a Szolgáltató és az Ügyfelek között megkötött valamennyi megállapodást.

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

Az iratok biztonságos megőrzéséről és tárolásáról Szolgáltató olyan adattár segítségével gondoskodik, amelyhez a Szolgáltatónak 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 másodpéldányokat tárol, az eredeti példányétól különböző helyszínen, fizikailag elkülönítve.

5.6. Helyreállítás rendkívüli üzemi helyzetek esetén

Szolgáltató katasztrófa elhárítási tervvel rendelkezik, 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 az adott esetekre rendszeresen teszteli. A következő fejezetekben e katasztrófa elhárítási terv irányelveit foglaljuk össze.

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.

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.

5.7. A hitelesítés szolgáltatás leállítása

A Szolgáltató a hitelesítés szolgáltatás leállítása esetén teljesíti a jogszabályban [4], [3] 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 szervezetek), illetve az Aláírók számára) generált magánkulcs biztonságos, és az ipari szabványoknak megfelelő generálásáról.

6.1.1. Magánkulcs eljuttatása a tulajdonoshoz

Azon hitelesítési rendek esetén, ahol a magánkulcs biztonságos aláírás-létrehozó eszközön helyezkedik el, a magánkulcs az eszközzel együtt, személyes találkozás során, személyes azonosítást követően kerül az Aláíró birtokába.

A Szolgáltatónak minden esetben biztosítania kell, hogy a magánkulcs az Aláíró kizárólagos birtokába vagy kizárólagos kontrollja alá kerüljön.

A Szolgáltató egyik esetben sem őrizhet meg másolatot a magánkulcsból.

Az ezzel kapcsolatos rendelkezések részleteit a Szolgáltatási Szabályzat tartalmazza.

6.1.2. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Amennyiben a kulcspárt a Szolgáltató generálja, a nyilvános kulcsot nem kell külön eljutatni hozzá.

Amennyiben a kulcspárt az ügyfél generálja, a nyilvános kulcsot olyan módon kell eljuttatni a Szolgáltatóhoz, hogy a Szolgáltató meggyőződhessen róla, hogy az adott nyilvános kulcs mely ügyféltől származik, és illetéktelen fél ne módosíthassa útközben.

Az ezzel kapcsolatos rendelkezések részleteit 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.

A Szolgáltató legalább 2048 bit hosszú RSA kulcsokat vagy más, ezzel legalább egyenértékű biztonságot nyújtó kulcsokat használ rendszereiben.

6.1.5. A nyilvános kulcs paraméterek előállítása

A Szolgáltató tanúsítvány aláírására minden esetben a 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 digitális 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 magánkulcsot kizárólag elektronikus aláírás készítésére szabad használni, és ezt a tényt a tanústvány kulcshasználati mezejében is jelölni kell. Ennek részleteit a Szolgáltatási Szabályzat tartalmazza.

6.2. A magánkulcsok védelme

A Szolgáltató gondoskodik saját magánkulcsainak titkosságáról és sértetlenségéről, valamint az Aláírók magánkulcsainak titkosságáról és sértetlenségéről amíg az Aláírók 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 rendek esetén a Szolgáltató meggyőződik róla, hogy az Aláírók magánkulcsait kriptográfiai hardver eszköz védi. 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 intelligens kártyák aktivizáló adatait.

A Szolgáltató az általa kibocsátott intelligens kártyák aktivizáló adatait műszaki és szervezési intézkedések segítségével védi.

6.5. Számítógépes biztonsági óvintézkedések

A Szolgáltató hitelesítő a Szolgáltatási Szabályzatban 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 jelen dokumentumban leírt tanúsítványprofilok megfelelnek az RFC 5280 és az ETSI TS 101 862 specifikációknak. [1], [5]

A profilok részletes leírását 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 szolgáltást a jelen hitelesítési renddel 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 ügyfelek részére.
- A Szolgáltató pénzügyi felelőssége, valamint a megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében a jogszabályi előírásoknak megfelelő óvadékkal rendelkezik. A Szolgáltató ezen felül, a megbízhatóság biztosítása érdekében a jogszabályi előírásoknak megfelelő felelősségbiztosítással is rendelkezik.

9.1.2. Az Előfizető jogai

- Az Előfizető jogosult a szolgáltatás igénybe vételére a jelen hitelesítési rendben, valamint a Szolgáltatási Szabályzatban 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 Aláíró jogai

- Az Aláíró jogosult tanúsítványt igényelni a Szolgáltatási Szabályzatban leírtak szerint.
- Az Aláíró jogosult saját tanúsítványa visszavonását kérni.
- Amennyiben ezt a vonatkozó hitelesítési rend lehetővé teszi, az Aláíró jogosult tanúsítványának felfüggesztését, illetve visszavonását kérni.

9.1.5. Az Aláíró kötelezettségei

- Az Aláíró köteles a szolgáltatás igénybe vétele előtt megismerni a jelen hitelesítési rendet és a Szolgáltatási Szabályzatot.

- Az Aláíró köteles a Szolgáltató által kért, a szolgáltatás igénybe vételéhez szükséges adatokat hiánytalanul megadni, valamint köteles a valóságnak megfelelő adatokat szolgáltatni.
- Az Aláíró köteles a Szolgáltatót haladéktalanul írásban értesíteni, amennyiben tudomására jut, hogy az általa megadott, a szolgáltatás igénybe vételéhez szükséges adat – különösen valamely tanúsítványban is szereplő adat – megváltozott.
- Az Aláíró köteles a szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a hivatkozott szabályzatokban, a hivatkozott dokumentumokban foglaltaknak megfelelően használni.
- Az Aláíró köteles biztosítani, hogy a szolgáltatás igénybe vételéhez szükséges adatokhoz és eszközökhöz (jelszavakhoz, titkos kódokhoz, intelligens kártyákhoz) illetéktelen személyek ne férhessenek hozzá.
- Az Aláíró köteles a Szolgáltatót haladéktalanul írásban értesíteni, amennyiben valamely, a szolgáltatással kapcsolatos elektronikus aláírással, illetve tanúsítvánnyal kapcsolatban jogvita indul.
- Az Aláíró köteles a tanúsítvány kiadásához szükséges adatok ellenőrzése érdekében a Szolgáltatóval együttműködni, és mindent megtenni azért, hogy az ellenőrzés a lehető leghamarabb befejeződhessen.
- Amennyiben az Aláíró magánkulcsa, intelligens kártyája vagy a kártya aktiválásához szükséges titkos kódok illetéktelen kezekbe kerültek vagy megsemmisülnek, az Aláíró köteles e tényt haladéktalanul írásban jelenteni a Szolgáltatónak, illetve köteles kezdeményezni az eszközhöz tartozó tanúsítványok felfüggesztését, illetve visszavonását.
- Az Aláíró köteles tudomásul venni, hogy az Előfizető jogosult a tanúsítvány visszavonását, illetve felfüggesztését kérni.
- Az Aláíró köteles tudomásul venni, hogy a Szolgáltató a tanúsítványt a Szolgáltatási Szabályzatban leírt meghatározott módon, az ott leírt ellenőrzési lépések elvégeztével bocsátja ki. Az Aláíró 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 Aláíró 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 Aláíró szervezeti tanúsítványt igényel, köteles tudomásul venni, hogy a Szolgáltató a tanúsítványt kizárólag a Képviselt Szervezet hozzájárulása esetén bocsátja ki.
- Amennyiben az Aláíró szervezeti tanúsítványt igényel, köteles tudomásul venni, hogy a Képviselt Szervezet jogosult a tanúsítvány visszavonását kérni.
- A Szolgáltatási Szabályzat további kötelezettségeket tartalmazhat az Aláíró 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 ügyféllel 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 Szabályzatban 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 Ügyféllel megkötött szolgáltatási szerződésekben 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 Szabályzatban, 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.

A minősített tanúsítványok tartalmazzák a tanúsítvánnyal egy alkalommal vállalható kötelezettség legmagasabb mértékét.

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 Aláírók 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 Aláírók 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 Aláíró felelőssége

Az Aláíró 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 Aláíró 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 Aláíró kártérítési felelősséggel tartoznak a Szolgáltatónak 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 Aláíró, 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 Aláíró, 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 Aláíróról. A Szolgáltató kizárólag olyan esetben adja át harmadik félnek az Aláíró adatait, ha ezt jogszabály előírja vagy ha az Aláíró ebbe írásban beleegyezett.

A Szolgáltató – a szolgáltatási szerződésnek megfelelően – nyilvánosságra hozza az Aláírók tanúsítványban szereplő adatait és a tanúsítványra vonatkozó visszavonási információt. A tanúsítványban a Szolgáltató feltünteti az Aláíró 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 ügyfélről 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 Szerződéshez 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 Szabályzatban 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 [4] 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 [4] 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 [4] törvény 16. § 2. bekezdése szerint.

9.8. Leírás-adminisztráció

A Szolgáltató rendelkezik hitelesítési renddel és szolgáltatási szabályzattal, amelyek mind honlapján, mind az ügyfélszolgálati irodájában elérhetőek. Szolgáltatón 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] RFC 5280 (Internet X.509 Nyilvános kulcsú infrastruktúra - tanúsítvány és tanúsítvány visszavonási lista profil).

[2] RFC 4043 Permanent Identifier.

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

[4] 2001. évi XXXV. törvény az elektronikus aláírásról (a 2004. évi módosításokkal).

[5] ETSI TS 101 862 Qualified Certificate Profile V1.3.3 (2006-01).