MICROSEC
Számítástechnikai Fejlesztő Kft.

e-Szignó Hitelesítés Szolgáltató nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó szolgáltatási szabályzat

Azonosító:	1.3.6.1.4.1.21528.2.1.1.21.2.2
Verzió:	2.2
Első verzió hatálybalépése:	2006-11-19
Biztonsági besorolás:	NYILVÁNOS
Jóváhagyta:	Ellbogen András
Jóváhagyás dátuma:	2009-08-29
Hatálybalépés dátuma:	2009-10-01

MICROSEC Számítástechnikai Fejlesztő Kft.
1022 Budapest, Marcibányi tér 9.

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat	2006-11-19	Dr. Berta István Zsolt
1.1	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően OID: 1.3.6.1.4.1.21528.2.1.1.21.1.1	2006-12-04	Dr. Berta István Zsolt
1.2	Közjegyzői regisztráció megszüntetése. Változás a láncolt hitelesítés szolgáltatásban. OID: 1.3.6.1.4.1.21528.2.1.1.21.1.2	2007-10-28	Dr. Berta István Zsolt
1.3	A fogyasztóvédelem elérhetősége megváltozott. OID: 1.3.6.1.4.1.21528.2.1.1.21.1.3	2008-01-01	Dr. Berta István Zsolt
1.4	Nem lépett hatályba. OID: 1.3.6.1.4.1.21528.2.1.1.21.1.4	2008-10-01	Dr. Berta István Zsolt
1.5	A tanúsítvány-kibocsátás és a tanúsítványcsere folyamata változott. OID: 1.3.6.1.4.1.21528.2.1.1.21.1.5	2008-12-20	Dr. Berta István Zsolt
1.6	A telefonos felfüggesztésre vonatkozó határidők pontosítása. OID: 1.3.6.1.4.1.21528.2.1.1.21.1.6	2009-03-09	Dr. Berta István Zsolt
2.0	Az SHA-256 alapú hierarchia bevezetése. OID: 1.3.6.1.4.1.21528.2.1.1.21.2.0	2009-06-01	Dr. Berta István Zsolt
2.1	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően. OID: 1.3.6.1.4.1.21528.2.1.1.21.2.1	2009-07-19	Dr. Berta István Zsolt
2.2	Az ingyenes OCSP szolgáltatás leírásának pontosítása. OID: 1.3.6.1.4.1.21528.2.1.1.21.2.2	2009-10-01	Dr. Berta István Zsolt

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a MICROSEC Számítástechnikai Fejlesztő Kft. (továbbiakban: Szolgáltató) által üzemeltetett e-Szignó Hitelesítés Szolgáltató nem minősített hitelesítés és időbélyegzés szolgáltatására vonatkozó Szolgáltatási Szabályzata (továbbiakban: Szabályzat).

A Szolgáltató szolgáltatásait a vele szerződéses viszonyban álló ügyfelek részére biztosítja.

Jelen Szabályzat a fenti szolgáltatások nyújtásának kereteit, a részletes eljárási és egyéb működési szabályokat tartalmazza, és ajánlásokat fogalmaz meg a szolgáltatások segítségével létrehozott elektronikus aláírások és időbélyegzők ellenőrzésében érintett felek számára.

Jelen Szabályzat az RFC 3647 [1] nemzetközi ajánlás alapján készült, tartalmában és felépítésében követi annak előírásait.

1.1. Áttekintés

1.1.1. A Szabályzat

Jelen Szabályzat célja, hogy összefoglalja mindazokat az információkat, amelyeket a Szolgáltatóval kapcsolatba kerülő ügyfeleknek tudniuk érdemes. Ezzel elő kívánja segíteni, hogy ügyfelei és leendő ügyfelei minél könnyebben megismerhessék a Szolgáltató által kínált szolgáltatások részleteit, feltételeit és a szolgáltatás nyújtásának gyakorlati hátterét; hogy átláthassák a Szolgáltató működését, és ennek révén minél könnyebben eldönthessék, hogy a szolgáltatások megfelelnek-e, illetve az egyes szolgáltatások melyik típusa felel meg igényeiknek, elvárásaiknak.

Jelen dokumentum feladata továbbá, hogy segítségével a Szolgáltató által kibocsátott tanúsítványok, tanúsítvány visszavonási listák, online tanúsítvány-állapot válaszok és időbélyegzők használói és elfogadói egyértelműen meg tudják állapítani azok kezelésének módját, az általuk garantált biztonság mértékét, valamint a rájuk vonatkozó technikai, üzleti és pénzügyi garanciákat és jogi felelősségvállalásokat.

Felhívjuk a végfelhasználók figyelmét, hogy az igénybe vett szolgáltatással kapcsolatos tevékenységükre vonatkozó előírásokat jelen Szabályzaton kívül az általános szerződési feltételek, a szolgáltatóval kötött szolgáltatási szerződés, a Szolgáltató által alkalmazott hitelesítési rendek (lásd: 1.2.2. fejezet), az Időbélyegzési Rend [2], illetve egyéb, a Szolgáltatótól független szabályzat illetve dokumentum is tartalmazhat.

1.1.2. A Szabályzat hatálya

Tárgyi hatálya: A Szabályzat az 1.1.4. fejezetben ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.

Időbeli hatálya: A Szabályzat jelen verziója a dokumentum címlapján feltüntetett hatálybalépési dátumtól határozatlan ideig hatályos. A hatályosság megszűnik a Szabályzat újabb verziójának hatályba lépésekor vagy a szolgáltatások beszüntetésekor.

Személyi hatálya: A Szabályzat személyi hatálya a Szolgáltatóra, az Előfizetőre és az Aláíróra terjed ki.

Területi hatálya: A Szabályzat területi hatálya Magyarország területe. A Szolgáltató működésére vonatkozóan a mindenkori magyar jogszabályok az irányadóak.

A jelen Szabályzat szerint elektronikusan nyújtott szolgáltatások az egész világon elérhetőek. A jelen Szabályzat szerint létrejött elektronikus aláírások és időbélyegzők érvényessége független attól, hogy mely földrajzi helyen készültek, illetve mely földrajzi helyen használják őket.

1.1.3. A Szolgáltató

A Szolgáltató adatai

Név:	MICROSEC Számítástechnikai Fejlesztő Kft.
Cégjegyzékszám:	01-09-078353, Fővárosi Bíróság, mint Cégbíróság
Székhely:	1022 Budapest, Marcibányi tér 9.
Telephely:	1031 Budapest, Záhony u. 7, Graphisoft Park, D épület
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	`http://www.microsec.hu`, `http://www.e-szigno.hu`
Minősítések:	ISO 9001, ISO 27001

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 9:00-12:00 és 14-16:30 között
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda e-mail címe:	`info@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`http://www.e-szigno.hu`
Panaszok bejelentésének helye:	MICROSEC Számítástechnikai Fejlesztő Kft. 1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Illetékes fogyasztóvédelmi felügyelőség:	NFH Közép-magyarországi Regionális Felügyelősége 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 270. tel.: (+36-1) 318-2681 fax: (+36-1) 318-1639

A Szolgáltató bemutatása

A Microsec Kft. 2002. május 30. óta szerepel a Nemzeti Hírközlési Hatóság (korábban Hírközlési Felügyelet) nyilvántartásában nem minősített szolgáltatóként a 2001. évi XXXV. törvényben meghatározott elektronikus aláírás hitelesítés szolgáltatás, időbélyegzés és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatás (a továbbiakban eszköz szolgáltatás) vonatkozásában. Regisztrációs szám: MH 6834 1/2002.

A Microsec Kft. 2005. május 15. óta minősített szolgáltatóként is szerepel a Nemzeti Hírközlési Hatóság nyilvántartásában elektronikus aláírás hitelesítés szolgáltatás, időbélyegzés és eszköz szolgáltatás vonatkozásában.

A Microsec Kft. minősített elektronikus archiválás szolgáltatást nyújtó szolgáltatóként is szerepel a Nemzeti Hírközlési Hatóság nyilvántartásában. (A nyilvántartásba vételről szóló határozat ügyiratszáma: HL-3549-2/2007.) Az elektronikus archiválás szolgáltatás indításának időpontja 2007. február 1.

Minőség és információbiztonság

A Microsec Kft. kiemelten fontosnak tartja ügyfelei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a Szolgáltató ISO 9001[1] szabványnak megfelelő minőségbiztosítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance ellenőrizte. A Microsec Kft. nagy figyelmet szentel az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein az ISO 27001-nek (korábbi nevén BS 7799) megfelelő információbiztonság-irányítási rendszert üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance ellenőrizte. A Szolgáltató önkéntes akkreditációs rendszer keretében nem lett tanúsítva, mert ilyen rendszer Magyarországon még nem működik.

1.1.4. Szolgáltatások

A Szolgáltató az alábbi szolgáltatásokat nyújthatja az Előfizető számára jelen Szabályzat keretében:

- elektronikus aláírás hitelesítés szolgáltatás [3],
- aláírás-létrehozó eszközön az aláíró adat elhelyezése [3], a továbbiakban eszköz szolgáltatás,
- online tanúsítvány-állapot szolgáltatás (amely segítségével a kibocsátott tanúsítványok visszavonási állapota kérdezhető le),
- időbélyegzés szolgáltatás [3].

Az elektronikus aláírás hitelesítés szolgáltatást, az eszköz szolgáltatást és az időbélyegzés szolgáltatást a Szolgáltató jelen Szabályzat keretében nem minősített szolgáltatóként nyújtja. Az online tanúsítvány-állapot szolgáltatás segítségével a nem minősített szolgáltatóként kibocsátott tanúsítványok visszavonási állapota kérdezhető le. Az egyes szolgáltatások külön-külön is igénybe vehetők. A Szerződés keretében nyújtott fenti szolgáltatások együttes elnevezése: *Szolgáltatások*.

Elektronikus aláírás hitelesítés szolgáltatás esetén a Szolgáltató az Előfizető által megnevezett *Aláírók* számára bocsát ki tanúsítványokat. A Szolgáltató az Aláíróval a Szolgáltatások igénybe vételére külön szerződést köt. Az Előfizető és a hozzá tartozó összes Aláíró együttes elnevezése: *Ügyfél*.

[1] A Szolgáltató vállalja, hogy minőség- és információbiztonság-irányítási rendszereit a hivatkozott szabványok mindenkori legfrissebb verziói szerint működteti.

Elektronikus aláírás hitelesítés szolgáltatás

A Szolgáltató elektronikus aláírás hitelesítés szolgáltatás keretében a Szolgáltató az Előfizető által meghatározott Aláírókkal *aláírói szerződést* köt, és e szerződés keretében elektronikus aláírás létrehozására alkalmas tanúsítványt bocsát ki. A tanúsítvány hitelesen összekapcsolja az azonosított Aláíró adatait és az általa birtokolt aláírás-létrehozó adathoz tartozó nyilvános aláírás-ellenőrző adatot. Egy aláírói szerződés keretében a Szolgáltató egy tanúsítványt bocsát ki, az aláírói szerződés időtartama a tanúsítvány érvényességének ideje. A tanúsítvány megújításával a szerződés időtartama meghosszabbításra kerül.

A jelen Szolgáltatási Szabályzat alapján létrehozott fokozott biztonságú elektronikus aláírással hitelesített dokumentum megfelel az írásba foglalás követelményének.

Elektronikus aláírás hitelesítés szolgáltatás esetén az érvényes előfizetéssel rendelkező Aláíró a következő műveleteket kezdeményezheti:

- Az Aláíró elektronikus aláírás létrehozására alkalmas tanúsítványt (és hozzá aláírás-létrehozó eszközt) igényelhet a Szolgáltatótól. A tanúsítvány kibocsátása a valamely hitelesítési rend vagy rendek szerint történik.
- Az Aláíró kérheti a tanúsítványa visszavonását.
- Az Aláíró kérheti tanúsítványa felfüggesztését, illetve visszaállítását, amennyiben a tanúsítványhoz tartozó hitelesítési rendek lehetővé teszik a felfüggesztés és visszaállítás műveleteket.

Az Előfizető is kérheti a hozzá tartozó Aláíró tanúsítványának visszavonását (illetve felfüggesztését, visszaállítását). Ezen műveleteket az Előfizető által erre feljogosított és a Szolgáltatónál bejelentett ún. szervezeti ügyintéző is kérheti.

A Szolgáltató a kibocsátott tanúsítványok visszavonási állapotát tartalmazó visszavonási listákat nyilvánosan elérhetővé teszi. A Szolgáltató magát a tanúsítványt is nyilvánosságra hozza, amennyiben az Aláíró ehhez hozzájárul. A visszavont, a felfüggesztett és a lejárt tanúsítvány érvénytelen. Az érvénytelen tanúsítvány alapján létrehozott aláíráshoz nem fűződik semmilyen joghatás.

A szolgáltató a rendszerének tesztelése céljából teszttanúsítványokat is kibocsát. A teszttanúsítványokhoz nem fűződik semmilyen joghatás.

A nem minősített szolgáltatóként nyújtott elektronikus aláírás hitelesítés szolgáltatásra vonatkozó visszavonás-kezelés, visszavonási állapot közzététele és tanúsítványtár közzététele rendelkezésre állása éves szinten 99%, és az eseti kiesések nem haladhatják meg a 24 órát.

A Szolgáltató a tanúsítványokat a hozzájuk tartozó hitelesítési rend (lásd 1.2.2. fejezet) szerint bocsátja ki.

Eszköz szolgáltatás

A szolgáltató olyan szolgáltatást is nyújt, melynek keretében aláírás-létrehozó eszközön aláírás-létrehozó adatot helyez el, és az eszközt az Aláíró rendelkezésére bocsátja. Ezen szolgáltatás a hitelesítés szolgáltatással együttesen is, és külön is igénybe vehető.

Időbélyegzés szolgáltatás

A Szolgáltató az időbélyegzés szolgáltatás keretében a szerződéses viszonyban álló Előfizetők részére időbélyegzőket bocsát ki. Az időbélyegző hitelesen összekapcsolja az Előfizető által az időbélyegző kérésben eljuttatott dokumentum lenyomatot a kérés feldolgozásának pontos, hiteles időpontjával, amellyel így harmadik fél előtt is bizonyítható, hogy a dokumentum az adott formában az adott időpontban létezett. Az időbélyegek kéréséhez az Előfizetőnek a Szolgáltatónál létrehozott egyedi azonosítót, illetve authentikációs tanúsítványt kell használnia.

Az időbélyegzés szolgáltatás a következő elemekből áll:

- Időbélyegző kérés fogadása, amely során a Szolgáltató rendszere azonosítja az Előfizetőt és fogadja a kérését.
- Időbélyegző előállítás, amely során a Szolgáltató rendszere előállítja az időbélyegzés kérésnek megfelelő, az aktuális, hiteles időpontot tartalmazó időbélyegzőt.
- Időbélyegző kibocsátás, amely során a Szolgáltató eljuttatja az Előfizetőnek a kérése alapján számára előállított időbélyegzőt.

A nem minősített szolgáltatóként nyújtott időbélyegzés szolgáltatás rendelkezésre állása 99%, az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

Online tanúsítvány-állapot szolgáltatás

A Szolgáltató az online tanúsítvány-állapot szolgáltatás keretében a szerződéses viszonyban álló Előfizetői – természetes és jogi személyek – részére online tanúsítvány-állapot válaszokat bocsát ki.

Az online tanúsítvány-állapot válasz hiteles információt nyújt az Előfizető által a tanúsítvány-állapot kérésben meghatározott tanúsítványnak a kérés feldolgozásának időpontjában levő visszavonási állapotára vonatkozóan. Ennek segítségével később, harmadik fél előtt, külső szolgáltató igénybe vétele nélkül is bizonyítható az adott tanúsítvány adott időpontra vonatkozó visszavonási állapota. Az online tanúsítvány-állapot válaszok kéréséhez az Előfizetőnek a Szolgáltatónál létrehozott egyedi azonosítóját, illetve authentikációs tanúsítványt kell használnia.

Az online tanúsítvány-állapot szolgáltatás a következő elemekből áll:

- Online tanúsítvány-állapot kérés fogadása, amely során a Szolgáltató rendszere azonosítja az Előfizetőt és fogadja a kérését.
- Online tanúsítvány-állapot válasz előállítás, amely során a Szolgáltató rendszere előállítja a kérésben hivatkozott tanúsítvány aktuális visszavonási állapotára vonatkozó információkat hitelesen tartalmazó választ.
- Online tanúsítvány-állapot válasz kibocsátás, amely során a Szolgáltató eljuttatja az Előfizetőnek a kérése alapján számára előállított online tanúsítvány-állapot választ.

Az online tanúsítvány-állapot szolgáltatásra a visszavonási állapot közzétételére vonatkozó rendelkezésre állási követelmények vonatkoznak.

1.1.5. Szabványok és előírások

Jelen Szabályzat megfelel az „RFC 3647 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)" [1] nemzetközi szabványnak.

A Szabályzat tartalmi vonatkozásokban eleget tesz a vonatkozó hazai jogszabályok [3], [4] előírásainak és ajánlásainak, továbbá a hitelesítés szolgáltatásra vonatkozóan felhasználja az ETSI TS 102 024 [5] specifikációt, valamint a „Nyilvános kulcs és attribútum tanúsítvány keretrendszer" című (ITU-T) ajánlást [6]. Jelen Szolgáltatási Szabályzathoz szervesen kapcsolódik – és ezzel összhangban került kialakításra – a Szolgáltató által kibocsátott tanúsítványok felhasználásának feltételeit előíró „e-Szignó Hitelesítés Szolgáltató nem minősített hitelesítési rendek" című dokumentum [7].

A jelen dokumentumban leírtak szerint kibocsátott tanúsítványok, visszavonási listák, illetve a jelen dokumentumban leírtak szerint nyújtott szolgáltatások az alábbi szabványoknak, illetve ajánlásoknak felelnek meg:

- International Telecommunication Union X.509 „Információ technológia – Nyílt rendszerek kapcsolódása – Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer" ajánlás 3. verziója,
- RFC 3280: Certificate and Certificate Revocation List (CRL) Profile (az RFC 2459 újabb változata),
- ETSI TS 102 280: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons (v1.1.1; 2004-03),
- A CWA 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures,
- Az ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates,

- Az Informatikai és Hírközlési Minisztérium által kibocsátott [8], [9], [10], [11] ajánlások (a közigazgatási területen használható tanúsítványokkal kapcsolatban),
- Az RFC 3161: Time-Stamp Protocol (TSP) [12],
- Az RFC 2560: Online Certificate Status Protocol (OCSP) [13].

1.1.6. Tanúsítványfajták, hitelesítési rendek

Jelen Szabályzat kizárólag a Szolgáltató által üzemeltetett e-Szignó Hitelesítés Szolgáltató önálló üzleti egysége által kibocsátott tanúsítványokról szól. A jelen Szabályzatban támogatott hitelesítési rendeket az 1.2.2. fejezetben mutatjuk be. Az alkalmazott hitelesítési rend azonosítója minden esetben feltüntetésre kerül a tanúsítvány Certificate Policies mezejében.

Az e-Szignó Hitelesítés Szolgáltató több különböző tanúsítványfajtát ajánl ügyfelei részére, amelyek főképp az általuk hitelesen az Aláíróhoz kötött adatok és tulajdonságok körében térnek el.

- Szervezeti tanúsítványról beszélünk, ha a tanúsítvány az Aláíró valamely szervezethez való tartozását mutatja. Ilyen esetben a tanúsítvány „O” mezejében a szervezet neve feltüntetésre kerül. Az Aláíró a tanúsítványt ekkor kizárólag az adott szervezet által meghatározott módon használhatja. Szervezeti tanúsítvány esetén a „Title” mezőben további korlátozások szerepelhetnek a tanúsítvány használhatóságával kapcsolatban.
- Hivatáshoz kapcsolódó tanúsítványról akkor beszélünk, ha a tanúsítvány „Title” mezeje – jellemzően természetes személy esetén – tartalmazza az Aláíró hivatását vagy titulusát.
- Személyes tanúsítványról is jellemzően természetes személy esetén beszélhetünk, ha a tanúsítvány sem „O”, sem „Title” mezőt nem tartalmaz.

Az e-Szignó Hitelesítés Szolgáltató által kibocsátott tanúsítványok egyaránt lehetnek személyes, szervezeti, illetve hivatáshoz kapcsolódó tanúsítványok.

1.2. Dokumentum neve és azonosítása

1.2.1. A Szabályzat azonosítása

A Szolgáltatási Szabályzat egyértelmű azonosítására szolgáló adatok megtalálhatóak a dokumentum címlapján. A Szolgáltatási Szabályzat hivatalos és aktuális verziója elérhető a következő címen: `https://www.e-szigno.hu/ASZSZ/`

Emellett a Szolgáltatási Szabályzat megtekinthető a Szolgáltató ügyfélszolgálati irodájában is.

1.2.2. Támogatott hitelesítési és időbélyegzési rendek

A Szolgáltató az alábbi hitelesítési rendek szerint bocsát ki tanúsítványokat:

- „III. hitelesítési osztályba tartozó tanúsítványok kibocsátására vonatkozó hitelesítési rend”
  OID: 1.3.6.1.4.1.21528.2.1.1.11
  (Az e rend szerint kibocsátott tanúsítványok esetén a Szolgáltató személyes regisztrációt végez.)

- „II. hitelesítési osztályba tartozó tanúsítványok kibocsátására vonatkozó hitelesítési rend”
  OID: 1.3.6.1.4.1.21528.2.1.1.10
  (Az e rend szerint kibocsátott tanúsítványok esetén a Szolgáltató távoli regisztrációt végez.)

A Szolgáltató mindkét rend szerint bocsát ki álneves és nem álneves tanúsítványokat. A közigazgatásban használható III. hitelesítési osztályba tartozó tanúsítványokban nem szerepelhet álnév.

A fenti, a Szolgáltató által definiált hitelesítési rendek mellett a Szolgáltató harmadik fél által definiált hitelesítési rendek szerint is bocsát ki tanúsítványokat.

Az ilyen hitelesítési rendek szerint kibocsátott tanúsítványban a hitelesítési rend harmadik fél által meghatározott azonosítója szerepel. A Szolgáltató a tanúsítványok kibocsátása során alkalmazott folyamatait úgy alakította ki, hogy azok nemcsak a saját hitelesítési rendjei szerinti, hanem az alábbiakban felsorolt hitelesítési rendek szerinti tanúsítványok kibocsátására is alkalmasak. A harmadik féltől származó hitelesítési rendek szerint kibocsátott tanúsítványokat a Szolgáltató a saját hitelesítési rendjei szerint kibocsátott tanúsítványokhoz hasonlóan kezeli, a hitelesítési rendet kibocsátó féltől származó többletkorlátozásokat is érvényesíti, illetve a hitelesítési rendet kibocsátó fél által meghatározott többletszolgáltatásokat is nyújtja.

A Szolgáltató az alábbi, harmadik fél által definiált hitelesítési rendeket támogatja. E hitelesítési rendek leírását a közigazgatás által közzétett [11] dokumentum tartalmazza.

- „Közigazgatási, ügyfélhez kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend, (1.0)”
  0.2.216.1.100.42.101.3.2.1
  (Az e rend szerint kibocsátott tanúsítványokhoz viszontazonosítás szolgáltatás is kapcsolódik.)

- „Közigazgatási, köztisztviselőhöz kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend”, (1.0)
  0.2.216.1.100.42.101.4.2.1

- „Közigazgatási, ügyfélhez kapcsolódó, egységesített hitelesítési rend, (1.0)”
  0.2.216.1.100.42.101.5.2.1
  (Az e rend szerint kibocsátott tanúsítványokhoz viszontazonosítás szolgáltatás is kapcsolódik.)

- „Közigazgatási, ügyfél által működtetett automatizmushoz kapcsolódó, egységesített hitelesítési rend, (1.0)”
  0.2.216.1.100.42.101.6.2.1

- „Közigazgatási, köztisztviselőhöz kapcsolódó, egységesített hitelesítési rend, (1.0)”
  0.2.216.1.100.42.101.7.2.1

- „Közigazgatási, közigazgatást képviselő automatizmushoz kapcsolódó, egységesített hitelesítési rend, (1.0)”
  0.2.216.1.100.42.101.8.2.1

A Szolgáltató viszontazonosítás szolgáltatást is nyújt a közigazgatási hitelesítési rendeknek megfelelő, a közigazgatás ügyfelei számára kibocsátott tanúsítványokkal kapcsolatban. (4.14. fejezet)

Amennyiben a Szolgáltató harmadik féltől származó hitelesítési rendnek megfelelő tanúsítványt bocsát ki, úgy a Szolgáltató ezen hitelesítési rend szerint jár el, valamint a hitelesítési rend a Szolgáltató és az Ügyfél közötti szerződés mellékletét képezi.

Nem minősített időbélyegzők kibocsátásra vonatkozó időbélyegzési rend

A jelen Szabályzat hatáskörébe a következő időbélyegzési rend tartozik:

- „e-Szignó Hitelesítés Szolgáltató – nem minősített időbélyegzési rend” [2], OID: 1.3.6.1.4.1.21528.2.1.1.23

Az időbélyegzési rend mindenkori aktuális változata elérhető a Szolgáltató honlapján keresztül.

1.2.3. Teszttanúsítványok

A Szolgáltató – egyrészt saját rendszerének tesztelése céljából, másrészt azért, hogy harmadik felek tesztelhessék a Szolgáltatásokat – teszttanúsítványokat is kibocsát. A teszttanúsítványokhoz semmilyen joghatás nem tartozik, és a Szolgáltató sem kibocsátásukért, sem felhasználásukért, sem a hozzájuk kapcsolódó szolgáltatások rendelkezésre állásáért nem vállal felelősséget. A Szolgáltató a következő módon jelöli meg a teszttanúsítványokat:

- A Szolgáltató vagy az 1.3.6.1.4.1.21528.2.1.1.9 OID-et tünteti fel a tanúsítványban a hitelesítési rendként, vagy
- a Szolgáltató semmilyen hitelesítési rendet nem tüntet fel a tanúsítványban.

1.3. PKI közösség

A jelen Szabályzat keretei között nyújtott Szolgáltatásokat alkalmazó közösség az alábbiakból áll:

- a Microsec e-Szignó Hitelesítés Szolgáltató,
- a Microsec Kft-vel szerződéses kapcsolatban álló regisztrációs szervezetek,
- a végfelhasználók.

1.3.1. Hitelesítő szervezet

A tanúsítványok előállítása és menedzsmentje központosítottan történik, amelyet a Szolgáltató szervezetén belül működő önálló üzleti egység, az e-Szignó Hitelesítés Szolgáltató lát el.

Ugyancsak ezen szervezeti egység keretein belül történik a tanúsítványtár és tanúsítvány visszavonási-állapot információk közzététele és az intelligens kártyák menedzselése és rendelkezésre bocsátása is, valamint az online tanúsítvány-állapot és időbélyegzés szolgáltatást is ez a szervezeti egység nyújtja. A szabályzatok menedzselésével kapcsolatos feladatokat is ez a szervezeti egység látja el.

Hitelesítő egységek

Az alábbiakban az e-Szignó Hitelesítés Szolgáltató rendszerében megjelenő hitelesítő egységeket mutatjuk be. A hitelesítő egységek két nagy csoportra oszthatóak. A Szolgáltató hitelesítő egységeinek egyik része SHA-1 alapú, míg a másik része SHA-256 alapú tanúsítványokkal működik. Az SHA-256 alapú tanúsítványok tekintetében a Szolgáltató külön hitelesítő egységeket, és külön gyökértanúsítványt hozott létre. Az SHA-1 alapú tanúsítvánnyal rendelkező hitelesítő egységek szerepét az SHA-256 alapú tanúsítvánnyal rendelkező egységek veszik majd át.

A Szolgáltató alábbi hitelesítő egységei rendelkeznek SHA-1 alapú tanúsítvánnyal:

- „Microsec e-Szigno Root CA” (önhitelesített) – Gyökér hitelesítési egység, SHA-1 alapú tanúsítványokat bocsát a Szolgáltató hitelesítő egységei számára. E hitelesítő egység önhitelesített tanúsítvánnyal (SHA-1 alapú) rendelkezik.

- „Advanced e-Szigno CA3” – Ezen egység kizárólag a III. hitelesítési osztály szerint bocsát ki tanúsítványokat, természetes személyek és automaták részére. Ezen egység nem bocsát ki álneves tanúsítványt. A Microsec e-Szigno Root CA hitelesíti felül.

- „Advanced e-Szigno CA2” – Ezen egység a II. hitelesítési osztály szerint bocsát ki tanúsítványokat, természetes személyek és automaták részére. Ezen egység bocsátja ki a III. hitelesítési osztályba tartozó álneves tanúsítványokat is. A Microsec e-Szigno Root CA hitelesíti felül.

- „Signature e-Szigno CA6” – Ezen egység kizárólag közigazgatási hitelesítési rendeknek megfelelő nem minősített tanúsítványokat bocsát ki, ezen egységet a Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) hitelesíti felül.

- „Microsec e-Szigno Server CA”, a gyökér hitelesítő egység, illetve a KGYHSZ hitelesíti felül. Ezen hitelesítő egység hitelesíti felül az időbélyegző egységeket, illetve közigazgatási hitelesítési rendeknek megfelelő tanúsítványokat bocsát ki automaták számára.

- Időbélyegző egységek, amelyeket a Microsec e-Szigno Server CA hitelesít felül. Az e-Szignó Hitelesítés Szolgáltató ezen egységek magánkulcsaival bocsátja ki az SHA-1 alapú nem minősített időbélyegzőket. Az időbélyegző egységek tanúsítványai timeStamping kiterjesztett kulcshasználatot tartalmaznak.

- „e-Szigno OCSP CA” (önhitelesített) – Az OCSP válaszadó tanúsítványát kibocsátó hitelesítő egység.

- „Advanced e-Szigno OCSP Responder” – OCSP válaszadó – az e-Szigno OCSP CA hitelesíti felül.

A Szolgáltató alábbi hitelesítő egységei rendelkeznek SHA-256 alapú tanúsítvánnyal:

- „Microsec e-Szigno Root CA 2009” – Gyökér hitelesítő egység, amely SHA-256 alapú tanúsítványokat bocsát ki a Szolgáltató hitelesítő egységei részére. E hitelesítő egység önhitelesített tanúsítvánnyal (SHA-256 alapú) rendelkezik.

- Időbélyegző egységek, amelyeket a Microsec e-Szigno Root CA 2009 hitelesít felül. Az e-Szignó Hitelesítés Szolgáltató ezen egység magánkulcsával bocsátja ki az SHA-256 alapú nem minősített időbélyegzőket. Ezen egység egyáltalán nem bocsát ki SHA-1 alapú időbélyeget. Az időbélyegző egységek tanúsítványai timeStamping kiterjesztett kulcshasználatot tartalmaznak.

- „Advanced Class 3 e-Szigno CA 2009” – Ezen egység kizárólag a III. hitelesítési osztály szerint bocsát ki tanúsítványokat, természetes személyek és automaták részére.

A Microsec e-Szigno Root CA 2009 hitelesíti felül. Ezen egység nem bocsát ki álneves tanúsítványt.

- „Advanced Class 2 e-Szigno CA 2009" – Ezen egység a II. hitelesítési osztály szerint bocsát ki tanúsítványokat, természetes személyek és automaták részére. A Microsec e-Szigno Root CA 2009 hitelesíti felül. Ezen egység nem bocsát ki álneves tanúsítványt.

- „Advanced Pseudonymous e-Szigno CA 2009" – Ezen egység a II. és a III. hitelesítési osztály szerint bocsát ki tanúsítványokat, természetes személyek és automaták részére. A Microsec e-Szigno Root CA 2009 hitelesíti felül. Ezen egység álneves tanúsítványokat is kibocsát.

- OCSP válaszadók; minden SHA-256 alapú tanúsítvánnyal rendelkező hitelesítő egység külön, dedikált OCSP válaszadó egységet hitelesít felül, amely az adott hitelesítő egység által kibocsátott tanúsítványok visszavonási állapotára vonatkozóan ad választ. Az OCSP válaszadó egységek neve az adott hitelesítő egység neve mögött az „OCSP Responder" szöveget tartalmazza. Az OCSP válaszadók tanúsítványában ocspSigning kiterjesztett kulcshasználat szerepel.

A fentiek közül a „Microsec e-Szigno Root CA" és az „e-Szigno OCSP CA" tanúsítványának lenyomatát a Szolgáltató a Magyar Nemzet 2005. július 21-ei számában tette közzé. A Szolgáltató a Microsec e-Szigno Root CA 2009 tanúsítványának lenyomatát a Magyar Hírlap 2009. június 22-ei számában teszi közzé. Az alábbiakban ezen önhitelesített gyökértanúsítványok lenyomatát ismertetjük. Ezen tanúsítványok az e-Szignó Hitelesítés Szolgáltató honlapján keresztül is elérhetőek.

- A Microsec e-Szigno Root CA tanúsítványának SHA-1 lenyomata:
  `23 88 c9 d3 71 cc 9e 96 3d ff 7d 3c a7 ce fc d6 25 ec 19 0d`,
  ugyanezen tanúsítvány SHA-256 lenyomata:
  `32 7a 3d 76 1a ba de a0 34 eb 99 84 06 27 5c b1 a4 77 6e fd ae 2f df 6d 01 68 ea 1c 4f 55 67 d0`

- Az e-Szigno OCSP CA tanúsítványának SHA-1 lenyomata:
  `56 2c 85 5b 9c d9 be 0e 64 e6 f7 95 86 24 95 a1 09 3e f1 68`,
  ugyanezen tanúsítvány SHA-256 lenyomata:
  `15 a9 45 a5 e4 92 c8 6c 3e 4e 0e a5 81 4c 9c 43 b0 4f 2e a6 83 1a 64 6c 37 8c d2 b1 82 05 aa 89`

- A Microsec e-Szigno Root CA 2009 tanúsítványának SHA-1 lenyomata:
  `a6 5c b4 73 3d 94 a5 c8 65 a8 64 64 7c 2c 01 27 2c 89 b1 43`,
  ugyanezen tanúsítvány SHA-256 lenyomata:

```
8e 8c 6e bf 77 dc 73 db 3e 38 e9 3f 48 03 e6 2b 6b 59 33 be b5 1e e4 15
2f 68 d7 aa 14 42 6b 31
```

A Szolgáltató Microsec e-Szigno Root CA gyökértanúsítványával részt vesz a „Microsoft Root Certificate Program”-ban, így ezen tanúsítványt a Microsoft termékek tanúsítványtárai tartalmazzák, illetve terjesztik.

A Szolgáltató többi saját tanúsítványa az önhitelesített gyökértanúsítványok alapján ellenőrizhető, ezért ezen tanúsítványokat a Szolgáltató csak a honlapján teszi közzé. Amennyiben – jogszabály, vagy hitelesítés szolgáltatók közötti szerződés vagy kölcsönös megegyezés keretében – a Szolgáltató egyes hitelesítő egységei számára más hitelesítés szolgáltató is bocsát ki tanúsítványt, a Szolgáltató ezen tanúsítványokat is közzéteheti honlapján. A Szolgáltató számára ilyen módon kibocsátott tanúsítványok esetén a Szolgáltató vállalja, hogy a Szolgáltatót felül- vagy kereszthitelesítő másik szolgáltató hitelesítési rendjét betartja, és az ezen tanúsítvánnyal kapcsolatban benne foglaltakat magára nézve kötelezőnek ismeri el. Ennek megfelelően, a Szolgáltató betartja a Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) hitelesítési rendjét [14], és az abban foglaltakat magára – mint első szintű hitelesítés szolgáltatóra – nézve kötelezőnek ismeri el.

1.3.2. Láncolt hitelesítés szolgáltatás

A Szolgáltató jogosult láncolt hitelesítés szolgáltatást nyújtani, amelynek keretében a Szolgáltató valamely hitelesítő egysége tanúsítványt bocsát ki egy másik hitelesítés szolgáltató (továbbiakban: felülhitelesített hitelesítés szolgáltató) irányítása alatt álló hitelesítő egység számára.

A Szolgáltató az alábbi hitelesítő egységeket jogosult láncolt hitelesítés szolgáltatásra használni:

- „Microsec e-Szigno Root CA”
- „Microsec e-Szigno Root CA 2009”
- „Microsec e-Szigno Server CA”

Ezen felülhitelesítés a következő feltételekkel történik:

- A felülhitelesített hitelesítés szolgáltatóval a Szolgáltató szerződést köt, a felülhitelesítés pontos feltételeit e szerződés szabályozza. A felülhitelesített hitelesítés szolgáltató maga köt szerződést a hozzá tartozó ügyfelekkel, e szerződésben a felülhitelesített hitelesítés szolgáltató jelenik meg hitelesítés szolgáltatóként.
- A Szolgáltató teljes felelősséget vállal a láncolt hitelesítés szolgáltató tevékenységéért.

- A felülhitelesített hitelesítés szolgáltató kizárólag valamely jól definiált kör részére bocsáthat ki tanúsítványt.
- A felülhitelesített hitelesítés szolgáltatónak nyilvánosságra kell hoznia a hitelesítési rendjét, és e hitelesítési rend szerint kell működnie. A Szolgáltató jogosult rendszeresen ellenőrizni a felülhitelesített szolgáltató működését.
- A Szolgáltató visszavonja a felülhitelesítés során kibocsátott tanúsítványt, amennyiben a felülhitelesített hitelesítés szolgáltató nem felel meg saját hitelesítési rendjének, vagy amennyiben a felülhitelesített hitelesítés szolgáltató jelzi, hogy a felülhitelesített szolgáltatói kulcsa kompromittálódott.
- A felülhitelesített hitelesítés szolgáltató – ezen felülhitelesítés alapján – közigazgatási hitelesítési rend szerint nem bocsáthat ki tanúsítványt.
- Amennyiben a Szolgáltató más hitelesítés szolgáltató számára bocsát ki szolgáltatói tanúsítványt, ezt bejelenti a Nemzeti Hírközlési Hatóságnak. Amennyiben a felülhitelesített szolgáltató belföldi és nyilvános körben használható tanúsítványokat bocsát ki, a felülhitelesített szolgáltató köteles a felülhitelesítést bejelenteni a Nemzeti Hírközlési Hatóságnak, és köteles kérni a nyilvántartásba vételét (amennyiben még nem szerepel a Hatóság nyilvántartásában). Más, alárendelt szolgáltatásként nyújtott elektronikus aláírással kapcsolatos szolgáltatásokra (pl. időbélyegzés) is ennek megfelelő szabályok vonatkoznak.

1.3.3. Regisztráló szervezet

A Szolgáltató a regisztrációt és a tanúsítványok kibocsátásával kapcsolatos egyéb feladatokat, valamint a további tanúsítvány menedzsment feladatokat központilag, a saját szervezetén belül működő ügyfélszolgálati iroda keretében valósítja meg.

Az iroda feladatai:

- a végfelhasználói tanúsítványokban feltüntetett Aláíró regisztrációja,
- a tanúsítványok és intelligens kártyák kibocsátásához kapcsolódó adminisztrációs és regisztrációs tevékenység,
- az ügyfelekkel való kapcsolattartás (kérdések, bejelentések, kérelmek és panaszok fogadása és feldolgozásának kezdeményezése),
- tanúsítvány műveletek (visszavonás, felfüggesztés, visszaállítás, tanúsítványcsere) elvégzése,

- az online tanúsítvány-állapot és időbélyegzés szolgáltatáshoz kapcsolódó adminisztrációs tevékenység.

A Szolgáltató által üzemeltetett ügyfélszolgálati iroda fogadja a különböző tanúsítvány műveletekre (tanúsítványcsere, visszavonás, felfüggesztés, visszaállítás) vonatkozó kérelmeket és kezdeményezi azok feldolgozását. A Szolgáltató a felfüggesztés és a visszaállítás kezdeményezésére folyamatosan – a nap 24 órájában, a hét minden napján – rendelkezésre álló ügyeletet tart fenn.

A regisztráló szervezet a következő helyeken végezhet regisztrációs tevékenységet:

- A Szolgáltató ügyfélszolgálati irodájában;
- A regisztráló szervezet munkatársai kiszállhatnak az ügyfelekhez, és a helyszínen mobil regisztrációs tevékenységet végezhetnek a Szolgáltató belső szabályzatai szerint.

A Szolgáltató a későbbiekben egyéb szervezetekkel is szerződést köthet külső regisztrációs irodák létrehozására, amelyek a központi iroda egyes feladatait külső helyszínen látják el. A külső regisztrációs irodák ezen szabályzat alapján működési rendet és saját szabályzatot dolgoznak ki, amelyet a Szolgáltató elfogad.

1.3.4. Végfelhasználók

A Szolgáltató által nyújtott Szolgáltatások végfelhasználói a következők:

- *Előfizető*: Az Előfizető határozza az elektronikus aláírás hitelesítés szolgáltatást igénybe vevő Aláírók körét, és az Előfizető fizeti meg az elektronikus aláírás hitelesítés szolgáltatás igénybe vételével kapcsolatos költségek ellenértékét is. Az Előfizető az online tanúsítvány-állapot és időbélyegzés szolgáltatást igénybe vevő fél, aki a Szolgáltatásokkal kapcsolatos költségek ellenértékét megfizeti. Az Előfizető szolgáltatási szerződést köt a Szolgáltatóval.
- *Aláíró*: Az elektronikus aláírás hitelesítés szolgáltatást igénybe vevő fél, aki a kibocsátott tanúsítvány segítségével elektronikus aláírást hozhat létre. Az Aláíró (nem természetes személy Aláíró esetén a nevében eljáró fél) aláírói szerződést köt a Szolgáltatóval.
- *Képviselt Szervezet*: Amennyiben a tanúsítvány egy jogi személy képviseletében történő aláírásra vagy tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra az Aláíró részére (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.

1.4. Alkalmazhatóság

A hitelesítés szolgáltatás keretében rendelkezésre bocsátott magánkulcsok, tanúsítványok és tanúsítvány visszavonási listák, az időbélyegzés szolgáltatás keretében kibocsátott időbélyegzők, valamint az online tanúsítvány-állapot szolgáltatás keretében kibocsátott online tanúsítvány-állapot válaszok alkalmazhatóságára a következő alapszabályok érvényesek:

Engedélyezett alkalmazási lehetőségek

A kibocsátott végfelhasználói tanúsítványokhoz kapcsolódó magánkulcsok elektronikus aláírások készítésére, míg a hozzájuk kapcsolódó, a tanúsítványban is szereplő nyilvános kulcs, maga a tanúsítvány, a tanúsítvány visszavonási listák, az időbélyegzők és az online tanúsítvány-állapot válaszok az elektronikus aláírások ellenőrzésére használhatóak fel. Az időbélyeg további felhasználási célja annak ellenőrzése, hogy az időbélyegzett dokumentum az időbélyegzés pillanatában létezett.

Korlátozások

A Szolgáltató korlátozza a Szolgáltatásokkal kapcsolatos kártérítési kötelezettségét. Ezen korlátozás mértéke a III. hitelesítési osztályba tartozó, illetve közigazgatási hitelesítési rendeknek megfelelő tanúsítványokkal, valamint a nem minősített szolgáltatóként kibocsátott időbélyegekkel kapcsolatban káreseményenként 100 000 forint. A II. hitelesítési osztályba tartozó tanúsítványokkal kapcsolatban a Szolgáltató nem vállal kártérítési felelősséget. Több, azonos okból bekövetkező kár egy káreseménynek minősül.

Azon ügyfelek, illetve Érintett felek számára, akik számára ezen korlátozás nem megfelelő, a Szolgáltató a minősített Szolgáltatóként nyújtott szolgáltatásainak igénybe vételét javasolja, amelyekhez nagyobb szolgáltatói felelősségvállalás tartozik.

Tiltott alkalmazási lehetőségek

Elektronikus aláírásra használható tanúsítványokat kizárólag elektronikus aláírásra szabad felhasználni. Egyéb más célra – különösen titkosításra, felhasználó-hitelesítésre – nem szabad őket használni.

1.5. Kapcsolattartás

1.5.1. Ügyfélszolgálati iroda

A szolgáltatásokkal kapcsolatos kérdésekkel, problémákkal a végfelhasználók az Ügyfélszolgálati irodához fordulhatnak. Az ügyfélszolgálati iroda adatait és elérhetőségét és nyitvatartási idejét az 1.1.3. fejezet tartalmazza.

Az ügyfélszolgálati iroda egyes funkcióit a Szolgáltató mobil regisztrációs munkatársai is ellátják.

A Szolgáltató telefonos felfüggesztés szolgáltatást működtet, amely napi 24 órában elérhető a következő telefonszámokon:

- (36-1) 505-4446
- (36-1) 505-4447

1.5.2. Hitelesítő szervezet

A hitelesítő szervezet elérése az Ügyfélszolgálati irodán, illetve a mobil regisztrációs munkatársakon keresztül történik.

1.5.3. Illetékes fogyasztóvédelmi felügyelőség

Lásd: 1.1.3. fejezet.

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 adat 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.

Képviselt Szervezet: Amennyiben a tanúsítvány egy nem természetes 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 a 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): Lásd: 1.3.4. fejezet.

Hatóság: Az elektronikus aláírással kapcsolatos szolgáltatásokat nyújtó szolgáltatókat felügyelő hatóság, a Nemzeti 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 194/2005 Kormányrendeletben meghatározott szervezet.

Kriptográfiai Kulcs (Key): Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításhoz és dekódoláshoz, 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.

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 a saját szervezete nevében a saját szervezetéhez tartozó tanúsítványokat felfüggeszteni, visszaállítani és visszavonni.

Szolgáltatási szabályzat (Certificate Practice Statement): Jelen szabályzat, amely a hitelesítés- és időbélyegzés szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.

Tanúsítvány (Certificate): A hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot az elektronikus aláírásról szóló törvény szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.

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, 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. III. hitelesítési osztályba tartozó és közigazgatási hitelesítési rendnek megfelelő tanúsítványok esetén a tanúsítványkérelem kizárólag személyesen nyújtható be.

Tanúsítvány típus: Lásd: hitelesítési rend.

Rövidítések

- CA: Certification Authority, Hitelesítés Szolgáltató
- CRL: Certificate Revocation List, Tanúsítvány visszavonási lista
- OCSP: Online Certificate Status Protocol, Online tanúsítvány-állapot protokoll
- NHH: Nemzeti 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

2.1.1. Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában (PDF formátumban) hozza nyilvánosságra a honlapján. A honlapon az érvényben levő dokumentumokon kívül a korábbi verziók is elérhetőek.

2.1.2. Rendkívüli információk közzététele

A Szolgáltató hirdetést jelentet meg egy országos terjesztésű napilapban, amennyiben szolgáltatásainak megszüntetésére készül, vagy valamely, általa működtetett hitelesítő egység – beleértve a gyökér és a köztes hitelesítő egységeket és az időbélyegző egységeket is – magánkulcsa kompromittálódott. A fent említett esetekben a Szolgáltató mindenképpen megjelenteti a hirdetést.

Az előbbi esetben a hirdetést legalább 60 nappal a szolgáltatások megszüntetése előtt teszi közzé. (5.7. fejezet) Szolgáltatói magánkulcs kompromittálódása esetén a hirdetést

haladéktalanul közzéteszi, illetve haladéktalanul közzéteszi a magánkulcsokhoz tartozó tanúsítványok megváltozott visszavonási állapotát is.

2.1.3. Tanúsítványok nyilvánosságra hozatala

A szolgáltatói tanúsítványok nyilvánosságra hozatalának módját az 1.3.1. fejezet tartalmazza.

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

2.1.4. A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala

A Szolgáltató az általa működtetett hitelesítő egységek, valamint az online tanúsítvány-állapot és időbélyegzés 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. Az önhitelesített tanúsítványok esetében ez az egyetlen módszer tekinthető hivatalos formának (lásd: 1.3.1. fejezet).
- 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 nemzetközi legjobb gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű (legfeljebb 1 napig érvényes) tanúsítvány kerül kibocsátásra, ezzel kiküszöbölve azt, hogy a tanúsítvány visszavonási állapotát ellenőrizni kelljen. A legfeljebb 1 napig érvényes 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. Az OCSP válaszok ellenőrzését bővebben az 4.5.2. fejezet tartalmazza.

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 (amennyiben a vonatkozó hitelesítési rend ezt lehetővé teszi).

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

2.2.2. Rendkívüli információk közzétételi gyakorisága

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

2.2.3. 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 teszi közzé.
- 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.

2.2.4. A megváltozott visszavonási állapot közzétételének gyakorisága

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokkal, valamint a végfelhasználói tanúsítványokat és időbélyegeket kibocsátó egységek tanúsítványaival kapcsolatos állapot-információkat visszavonási listákon ás az online tanúsítvány-állapot szolgáltatás keretén belül hozza nyilvánosságra.

A visszavonási listák közzétételének gyakoriságát és az online tanúsítvány-állapot szolgáltatás által szolgáltatott visszavonási információ frissítésének 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 http lekérdezésekkel érhető el a Szolgáltató honlapjáról. A Szolgáltató LDAP protokollon keresztül is közzéteszi azon tanúsítványokat, amelyek esetén az ügyfél hozzájárult a tanúsítvány közzétételéhez.

A tanúsítványtár a következő címen érhető el:

`https://www.e-szigno.hu/?lap=tanusitvanytar`

A tanúsítványtár elérhetőségét a Szolgáltató folyamatosan (az év minden napján, 0-24 óra között) biztosítja, a karbantartáshoz szükséges idők kivételével.

3. Azonosítás és hitelesítés

3.1. Elnevezések

3.1.1. Név típusok

A tanúsítvány alapmezői között található Kibocsátó azonosító (Issuer), illetve az Aláíró azonosító (Subject) mezők a [15] szerinti egyedi név formátum előírásainak felelnek meg. Ezen kívül a Szolgáltató támogatja a kiterjesztések között található Alternatív név mezők (Subject Alternative Names, Issuer Alternative Names) kitöltését is.

A tanúsítványt kibocsátó hitelesítő egység megnevezése

A tanúsítványok kibocsátójának azonosítója (Issuer mező) a következő módon épül fel:

- Common Name (CN) – OID: 2.5.4.3
  A tanúsítványt kibocsátó hitelesítő egység angol nyelvű megnevezése (lásd: 1.3.1. fejezet).
- Organization (O) – OID: 2.5.4.10
  `"Microsec Ltd."`
  (A Szolgáltató neve angolul, ékezet nélkül.)

- Organizational unit (OU) – OID: 2.5.4.11
  "e-Szigno CA"
  (A Szolgáltató szervezeti egységének neve ékezet nélkül.)
- Locality (L) – OID: 2.5.4.7
  "Budapest"
  (A Szolgáltató székhelye szerinti város neve ékezet nélkül.)
- Country (C) – OID: 2.5.4.6
  "HU"
  (A Szolgáltató székhelye szerinti ország kétbetűs rövidítése.)

A végfelhasználói tanúsítvány kibocsátójának tanúsítványában, az alany azonosító mezőben ugyanezen adatok szerepelnek.

A tanúsítványt kibocsátó hitelesítő egység alternatív nevei

A végfelhasználói tanúsítványokban a kibocsátó alternatív nevei (Issuer Alternative Names) mező nem kerül kitöltésre. Az SHA-1 alapú szolgáltatói tanúsítványokban az aláíró (azaz a hitelesítési egység) alternatív nevei mező kitöltésre kerül a következők szerint:

- Subject Alternative Names – OID: 2.5.29.17 (nem kritikus)
  CN = (a kibocsátó hitelesítő egység magyar nyelvű megnevezése, lásd: 1.3.1. fejezet)
  O = "Microsec Kft."
  OU = "e-Szignó HSZ"
  L = "Budapest"
  C = "HU"
  rfc822Name = "info@e-szigno.hu"

Az SHA-256 alapú szolgáltatói tanúsítványok esetén az alternatív név mezőben csak az e-mail cím (rfc822Name) kerül kitöltésre.

A tanúsítványban szereplő Aláíró megnevezése

A tanúsítvány alanyának azonosítója (a Subject mező tartalma) a következő módon épül fel:

- Common Name (CN) – OID: 2.5.4.3
  Az Aláíró személyazonosító okmányában szereplő neve kerül e mezőbe, magyar írásmód szerint, ékezetesen.

  Eszköztanúsítvány esetén az eszköz megnevezése kerülhet ide.

- Surname – OID: 2.5.4.4
  E mezőbe az Aláíró vezetékneve kerül, ahol a vezetéknevet a Szolgáltató a CN mezőben szereplő teljes névből a mellékletben szereplő szabály szerint képzi. (B melléklet) E mezőt a Szolgáltató kizárólag akkor tölti ki, ha a tanúsítványra vonatkozó valamely hitelesítési rend ezt megköveteli. (Ilyenek például a közigazgatás által közzétett hitelesítési rendek.)

  Ha a tanúsítványban szereplő Aláíró nem természetes személy, akkor a Szolgáltató nem tölti ki ezt a mezőt.

- 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 minden esetben az "`álneves tanúsítvány`" szöveg szerepel.

- Serial Number – OID: 2.5.4.5
  Egy tanúsítványban egyszerre több serial number mező is szerepelhet. Az egyik serial number mezőbe az Aláíró egyedi azonosítója (OID) kerül.

  Az OID formája:
  "`1.3.6.1.4.1.21528.2.2.x.y`"

  A fenti OID-ben x azt a regisztrációs egységet jellemzi, amely a tanúsítvány alanyhoz tartozó regisztrációs adatokat rögzítette, y pedig az Aláíró egyedi sorszáma.

  Az Aláíró minden esetben jogosult friss (még ki nem osztott) OID-et kérni. Álneves tanúsítványt a Szolgáltató kizárólag friss OID-hez bocsát ki. A Szolgáltató kizárólag akkor ad két tanúsítványnak azonos OID-et, ha biztosítja, hogy a két tanúsítványhoz tartozó Aláíró azonos.

  További serial number mezők (Érték:Név) párokat tartalmaznak. Például:
  "`Szig.szam:AAAAAA`"

  A serial number mezőben a Szolgáltató – a szabványoknak megfelelően – nem tüntet fel ékezeteket.

  Eszköztanúsítványok esetén a kitöltése opcionális. Közigazgatási hitelesítési rend szerint kibocsátott eszköztanúsítványok esetén nem kerül kitöltésre.

- 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 (pl. cégnyilvántartás) szerint, ékezetesen. Ha az O mező kitöltésre kerül, akkor ún. szervezeti tanúsítványról beszélünk (lásd: 1.1.6). A közigazgatás képviseletére szolgáló

tanúsítványok esetén itt a képviselt közigazgatási szerv neve szerepel; közigazgatás képviseletére szolgáló tanúsítványok esetén e mező mindig kitöltésre kerül.

- Organizational unit (OU) – OID: 2.5.4.11
  Kizárólag szervezeti tanúsítványok esetén tölthető ki az O mezőben szereplő szervezet által kibocsátott igazolás vagy nyilatkozat alapján.

- 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.

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

- Locality (L) – OID: 2.5.4.7
  Az Aláíró állandó lakcíme, illetve a szervezet székhelye szerinti város. Kitöltése opcionális.

- Title (T) – OID: 2.5.4.12
  Az Aláíró szerepe, beosztása vagy hivatása.

  Szervezeti tanúsítvány esetén az O mezőben szereplő szervezet által kiállított igazolás alapján kerül kitöltésre. Nem szervezeti tanúsítvány esetén valamely az Aláírótól független szervezet által kiállított igazolás alapján kerül kitöltésre, amelyet a Szolgáltató ellenőriz.

  Tekintve, hogy a „Title” mező az Aláíró szerepét tartalmazza, további korlátozásokat tartalmazhat azzal kapcsolatban, hogy a tanúsítvány mire használható.

- 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.

  E mező kitöltése opcionális.

Az alábbi felsorolás azt tartalmazza, hogy az egyes tanúsítványok Subject mezői milyen elemeket tartalmazhatnak. A kötelező mezők zárójel nélkül szerepelnek, az opcionális mezők zárójelben, a szervezeti tanúsítványok esetén kitölthető mezők pedig / jelek között.

- III. hitelesítési osztály, és közigazgatási hitelesítési rendek természetes személyek számára
  CN, (surname[2]), serialNumber, (TITLE), (EMAIL) /O/, /OU/, (L), C

[2] A közigazgatási hitelesítési rendek esetén a surname mező mindig kitöltésre kerül.

- III. hitelesítési osztály, és közigazgatási hitelesítési rendek automaták személyek számára
  CN, (serialNumber[3]), (TITLE), /O/, /OU/, (L), C

- II. hitelesítési osztály
  CN, (serialNumber), (TITLE), (EMAIL), /O/, /OU/, (L), C

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 Aláíró személyazonosító okiratában 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, a nevekről egyedi elbírálás alapján dönt. A döntést az alapján hozza meg, hogy az ügyfél által kért elnevezés valóban az Aláíró neve-e, illetve nem vezethet-e félre másokat. Amennyiben az Aláíró a hivatása gyakorlása során nem a személyazonosításra használt okmányában szereplő nevét használja, akkor kérheti, hogy a Szolgáltató a Subject Alternative Names mezőben ezen alternatív elnevezést szerepeltesse.

  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.

3.1.2. 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.

3.1.3. Különböző elnevezési formák értelmezési szabályai

Az azonosítók értelmezése érdekében az Érintett feleknek a jelen Szolgáltatási Szabályzatban leírtak alapján ajánlott eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt

[3]Közigazgatási hitelesítési rendek szerint kibocsátott tanúsítványok esetén nem kerül kitöltésre.

adatok értelmezésével kapcsolatban az Érintett félnek segítségre lenne szüksége, akkor a Szolgáltatóval közvetlenül 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.

A Szolgáltató viszontazonosítás szolgáltatást nyújt a tanúsítvánnyal kapcsolatban, amennyiben a Szolgáltató olyan hitelesítési rend szerint bocsátotta ki a tanúsítványt, amely a viszontazonosítás szolgáltatást megköveteli. A viszontazonosítás szolgáltatást a 4.14. fejezet írja le.

3.1.4. 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.

3.1.5. 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, a Szolgáltatónak jogában áll visszavonni a kérdéses tanúsítványt.

3.1.6. Márkanevek elismerése, hitelesítése és szerepe

A Szolgáltató a szolgáltatása során az „e-Szignó” megnevezést alkalmazza. Az E-Szignó Bt. hozzájárulását adta a megnevezés használatához.

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 a következő lehetőségek valamelyikével győződik meg arról, hogy a tanúsítványhoz tartozó magánkulcsot valóban az Aláíró birtokolja.

- Amennyiben a tanúsítvány a Szolgáltató áltla biztosított intelligens kártyán kerül kibocsátásra, akkor a Szolgáltató saját szervezetén belül maga generálja a tanúsítványhoz tartozó magánkulcsokat, és az intelligens kártyán adja át az Aláíró részére.

- Amennyiben a Szolgáltató nem biztosít a tanúsítványhoz intelligens kártyát, és a tanúsítványhoz tartozó nyilvános és magánkulcsot az Aláíró generálja, az Aláíró a nyilvános kulcsot PKCS#10 formátumú tanúsítványkérelembe foglalja, e PKCS#10 tanúsítványkérelmet aláírja. Az Aláíró a nyilvános kulcsot tartalmazó PKCS#10 tanúsítványkérelemmel együtt egy jelszót is eljuttat a Szolgáltatóhoz. (E folyamatot az Aláíró a Szolgáltató honlapján keresztül végezheti el a legegyszerűbben.) Regisztrációkor ugyanezen jelszót kell megadnia, ezzel igazolja, hogy a nyilvános kulcsot tartalmazó PKCS#10 tanúsítványkérelmet is ő nyújtotta be.

- Amennyiben a Szolgáltató nem biztosít a tanúsítványhoz intelligens kártyát, és a tanúsítványhoz tartozó nyilvános és magánkulcsot a Szolgáltató generálja, a Szolgáltató vagy a személyes regisztráció során, vagy más, biztonságos csatornán juttatja el a magánkulcsot az Aláíró részére. A magánkulcsból a Szolgáltató nem őriz meg másolatot. Ezen lehetőség közigazgatási területen használható, közigazgatási hitelesítési rendnek megfelelő tanúsítványok esetén nem alkalmazható.

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.)

A regisztráció és a tanúsítványcsere során az ügyfélnek adatokat és bizonyítékokat kell nyújtani a következőkről:

- a szervezet teljes és rövid neve, székhelye

- a szervezeten belüli szervezeti egység neve, ha kérik ennek feltüntetését a tanúsítványban,

- az Aláírónak a szervezetben betöltött szerepe,

- a szervezet hivatalos azonosító adatai,

- igazolás arra vonatkozóan, hogy a szervezet nevében a Szolgáltatási Szerződést aláíró személy jogosult-e az aláírás megtételére,

- amennyiben a Képviselt Szervezet közigazgatási szerv, és az adott tanúsítvány esetén ezt valamely hitelesítési rend megköveteli, úgy a közigazgatási szervet képviselő természetes személynek a regisztrációhoz magával kell vinnie egy, az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a Képviselt Szervezet képviseletében a Szolgáltatónál előforduló ügyekben eljárjon,
- amennyiben a Képviselt Szervezet nem közigazgatási szerv, de a közigazgatás területén is használható tanúsítványt igényel, akkor regisztrációhoz magával kell vinnie az adott szervezet nevében aláírásra jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a Képviselt Szervezet képviseletében a Szolgáltatónál előforduló ügyekben eljárjon,
- igazolás arra vonatkozóan, hogy a szervezet valóban létező szervezet.

A tanúsítvány-igényléshez csatolni kell a Képviselt Szervezet nevében aláírásra jogosult személy aláírási címpéldányát vagy más az aláírási címpéldánnyal egyenértékű hivatalos dokumentumot, mely a szervezet aláírásra jogosult vezetőinek nevét és aláírását tartalmazza. Csatolni kell továbbá a szervezet azonosságát is hitelesítő dokumentumot is. Cégbíróságon bejegyzett cégek esetében a fenti iratokat a Szolgáltató is beszerezheti.

A Szolgáltató a bemutatott iratok és okmányok érvényességét és hitelességét közhiteles adatbázisokban ellenőrzi. A Szolgáltató a tanúsítvány kibocsátását visszautasítja, amennyiben:

- az átadott adatok hiányosak,
- a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a személy szervezethez tartozása nem egyértelmű,
- a szervezet azonossága nem állapítható meg minden kétséget kizáróan,
- a közhiteles adatbázisokkal végzett adategyeztetés során kétely merül fel a fentiekkel kapcsolatban,
- nem egyértelmű a szervezet felhatalmazása a tanúsítvány kibocsátására, és az igénylő a Szolgáltató által megadott határidőn (hiánypótlási határidő) belül nem pótolta, illetve nem helyesbítette a szolgáltatói felhívásban szereplő adatokat, dokumentumokat.

3.2.3. A személyazonosság hitelesítése

A III. hitelesítési osztályba tartozó és a közigazgatási hitelesítési rendeknek megfelelő tanúsítványok esetén az Aláírónak személyesen meg kell jelennie a Szolgáltató regisztrációs munkatársa előtt. Amennyiben az Aláíró személyazonosságát a Szolgáltató regisztrációs munkatársa hitelesíti, úgy e hitelesítés általában a Szolgáltató ügyfélszolgálati irodájában történik, de a Szolgáltató ezzel minden esetben egyenértékűnek ismeri el, ha ezen hitelesítést a Szolgáltató mobil regisztrációs munkatársa külső helyszínen végzi el.

A Szolgáltató az alábbi okmányokat fogadja el a személyazonosság hitelesítéséhez:

- személyi igazolvány,
- útlevél,
- jogosítvány.

Az Aláírónak a személyazonosságát a fentiek közül legalább egy igazolvánnyal kell igazolnia. Amennyiben az alkalmazott hitelesítési rend további igazolványok (pl. lakcímkártya) bemutatását is megköveteli, úgy a Szolgáltató ezen igazolványokat is elkéri az igénylőtől.

A bemutatott dokumentumoknak eredetinek, valódinak és érvényesnek kell lenniük. A dokumentumokat a Szolgáltatónak az okmányok ellenőrzésére kiképzett regisztrációs munkatársai a megfelelő módszerekkel ellenőrzik, valamint az adatokat a személyi adat- és lakcímnyilvántartással, az útiokmány nyilvántartással és a gépjárművezetői nyilvántartással történő adategyeztetéssel ellenőrzik.

Regisztrációkor az Aláíró saját kezű aláírásával erősíti meg a felvett adatok helyességét. A regisztrációt végző személy saját aláírásával igazolja, hogy a bemutatott hatósági igazolványon szereplő fénykép megfeleltethető az Aláíró arcának, és az Aláíró saját kezű aláírása megfeleltethető a hatósági igazolványban szereplő aláírásnak.

A tanúsítvánnyal kapcsolatban a Szolgáltató később viszontazonosítás szolgáltatást nyújt (lásd: 4.14), amennyiben a tanúsítványban feltüntetett valamely hitelesítési rend megköveteli ezt.

Közigazgatási szerv képviseletére alkalmas tanúsítvány esetén a Szolgáltató értesíti a Képviselt Szervezetet a tanúsítvány kibocsátásának tényéről – az Aláíró adatainak megadása nélkül.

A II. hitelesítési osztályba tartozó tanúsítványok esetén az Aláíró el kell, hogy juttassa valamely igazolványa fénymásolatát. (Amennyiben az Aláíró nem szeretné, hogy igazolványának a másolata a Szolgáltató birtokába kerüljön, akkor a III. hitelesítési osztály szerint is igazolhatja személyazonosságát.) A Szolgáltató az alábbi igazolványokat fogadja el:

- személyi igazolvány,

- útlevél,
- jogosítvány

A Szolgáltató fenntartja a jogot, hogy II. hitelesítési osztályba tartozó tanúsítványok esetén más igazolványokat is elfogadjon. A Szolgáltató a II. hitelesítési osztályba tartozó tanúsítványok esetén is végez adategyeztetést közhiteles nyilvántartásokkal.

A Szolgáltató külföldi állampolgárok személyazonosságát is útlevél, vagy más, személyazonosításra alkalmas okmány segítségével ellenőrzi, illetve ekkor az adott ország megfelelő nyilvántartásaival végez adategyeztetést. A külföldi okmány megfelelő biztonsággal történő ellenőrzése, illetve a külföldi nyilvántartáshoz való hozzáféréshez további lépések – esetleg az okmány diplomáciai felülhitelesítése, illetve az adott ország nagykövetségével való kapcsolatfelvétel – is szükségesek lehetnek; az ezekkel kapcsolatos szabályokat és irányelveket a Szolgáltató belső szabályzatai határozzák meg. A Szolgáltató nem állítja ki a tanúsítványt, amennyiben belső szabályzatai alapján úgy ítéli meg, hogy nem képes a külföldön kiállított okmányt vagy a külföldi személy adatait megfelelő biztonsággal ellenőrizni.

3.3. Tanúsítványcsere esetén

Tanúsítványcseréről akkor beszélünk, ha egy, a regisztráción, azaz a 3.2.3. fejeztben leírt folyamaton átesett Aláíró meglévő tanúsítványa helyett új tanúsítványt igényel.

Tanúsítványcsere esetén az Aláírónak, illetve a Képviselt Szervezetnek írásban – például elektronikus aláírással ellátva – nyilatkoznia kell róla, hogy az új tanúsítványba kerülő adatok helyesek. Ekkor vagy megerősíti, hogy az Aláíró új tanúsítványába a korábbi tanúsítványában szereplő adatai kerüljenek, vagy megjelöli, hogy pontosan mely adatok megváltoztatását kéri.

Attól függően, hogy a tanúsítványcserére miért kerül sor, a tanúsítványcseréhez különböző folyamatok tartozhatnak:

- Ha az Aláíró meglévő tanúsítványa még érvényes, de hamarosan le fog járni, és az ügyfél olyan tanúsítványt igényel, amelybe az Aláíró korábbi tanúsítványában lévőkkel megegyező adatok kerülnek, és a két tanúsítvány ugyanazon nyilvános kulcshoz kerül kibocsátásra, akkor *megújításról* beszélünk, amelynek részeleteit a 4.6. fejezet írja le.
- Ha a Szolgáltató az új tanúsítványt új nyilvános kulcshoz bocsátja ki, a folyamatot *kulcscserének* nevezzük, amelyet a 4.7. fejezet ír le. Kulcscserére jellemzően akkor kerül sor, ha az Aláíró tanúsítványa már nem érvényes (például, ha visszavonásra került), de még érvényes tanúsítvány esetén is történhet kulcscsere (például, ha a régi kulcsok mérete már nem megfelelő).

- Ha az Aláíró új tanúsítványa még érvényes, de az Aláíró a tanúsítványban szereplő adatok megváltoztatását kéri, *adatváltozásról* beszélünk, amelyet a 4.8. fejezet ír le. Adatváltozás esetén a Szolgáltató ellenőrzi az új adatok helyességét.

A tanúsítványcsere kizárólag akkor bonyolítható le távolról, személyes megjelenést nem igénylő módon, ha az új tanúsítványhoz tartozó magánkulcs már az Aláíró birtokában van, és erről a Szolgáltató személyes találkozás során, az első tanúsítvány kibocsátásakor alkalmazott folyamatokkal egyenszilárdságú biztonságú módon győződött meg, azaz az új tanúsítvány magánkulcsa személyes találkozás során került az Aláíró birtokába. Amennyiben e feltétel teljesül, a tanúsítványcsere távolról is lebonyolítható; ez megtörténhet megújítás, kulcscsere (visszavont vagy lejárt tanúsítvány esete) és adatváltozás esetén is.

A Szolgáltató minden egyes tanúsítványcsere esetén – attól függetlenül, hogy megújításról, kulcscseréről vagy adatváltozásról van-e szó – ismételt egyeztetést végez a közhiteles adatbázisokkal.

Adatváltozás és kulcscsere esetén a Szolgáltató jogosult az első tanúsítvány kibocsátásakor alkalmazott folyamat megismétlését kérni, beleértve a személyes találkozást is. A személyes találkozás megismétlése kötelező, amennyiben a megváltozott adatok természete miatt nem állapítható meg, hogy az új tanúsítványba kerülő, megváltozott adatok ugyanazon személy adatai-e, amint akihez a Szolgáltató a korábbi tanúsítványt kapcsolta.

Kulcscsere esetén a személyes találkozást kötelező megismételni, ha a korábbi tanúsítvány már legalább 2 hónapja érvénytelen, és az Aláíró erről nem egyeztetett előzetesen a Szolgáltatóval.

Közigaztatásban használható tanúsítványok esetén további szabály, hogy a tanúsítvány csak egyszer újítható meg, azt követően már kulcscserére van szükség.

A II. hitelesítési osztályba tartozó tanúsítványok cseréje kizárólag új tanúsítvány igénylésével, az első tanúsítvány kibocsátásakor alkalmazott folyamattal végezhető el.

3.4. Felfüggesztési és visszavonási kérelem

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

4. A tanúsítványok életciklusa

4.1. Tanúsítványigénylés

Tanúsítványkérelmet azok az ügyfelek nyújthatnak be, akik előzetesen a Szolgáltatóval szerződéses kapcsolatot létesítettek. Az Előfizető képviseletében meghatalmazott, többek között a tanúsítványkérelemben szereplő Aláíró is eljárhat.

A Szolgáltató a szerződéses kapcsolat létesítése előtt tájékoztató kiadványokban tájékoztatja ügyfeleit a tanúsítványok használatával kapcsolatos kikötésekről és feltételekről. Ezen

tájékoztatás egyrészt a Szolgáltató honlapja, az ott elérhető nyilvános dokumentumok, valamint egy külön erre a célra szolgáló tájékoztató kiadvány segítségével történik. A fenti tájékoztató kiadvány letölthető a Szolgáltató honlapjáról, illetve megtekinthető a Szolgáltató ügyfélszolgálati irodájában, vagy elkérhető a Szolgáltató mobil regisztrációs munkatársaitól. Amennyiben az Aláíró nem azonos az Előfizetővel, úgy a Szolgáltató az ő számára is megadja a fenti tájékoztatást.

III. hitelesítési osztályba tartozó, illetve a közigazgatási rendeknek megfelelő tanúsítványra vonatkozó tanúsítványkérelem kizárólag személyesen nyújtható be a Szolgáltató ügyfélszolgálati irodájában vagy a Szolgáltató mobil regisztrációs munkatársainál.

A tanúsítványkérelmet megelőzően az ügyfeleknek előzetes tanúsítványigénylést is be kell nyújtaniuk a Szolgáltatóhoz, amelyben jelzik a Szolgáltatónak, hogy milyen tanúsítványt milyen feltételekkel szeretnének. E lépés történhet személyesen vagy elektronikusan, a Szolgáltató honlapján keresztül, illetve történhet tetszőleges levélben, amely a tanúsítványkérelem lapon szereplő információkat tartalmazza. E levelet az Aláíró küldheti elektronikusan és postai úton is, elektronikus esetben a Szolgáltató minősített, fokozott biztonságú vagy egyszerű elektronikus aláírással hitelesített leveleket is elfogad.

II. hitelesítési osztályba tartozó tanúsítványok esetén a tanúsítványkérelem postán nyújtható be. Ekkor is be kell nyújtani egy előzetes tanúsítványigénylést a Szolgáltató honlapján keresztül.

4.2. A tanúsítványkérelem benyújtása és feldolgozása

III. hitelesítési osztályba tartozó, valamint a közigazgatási hitelesítési rendeknek megfelelő új végfelhasználói tanúsítvány a Szolgáltató ügyfélszolgálati irodájában, vagy valamelyik külső regisztrációs szervezeténél igényelhető. A Szolgáltató a személyes regisztrációval minden esetben egyenértékűnek tekinti azt az esetet, amikor nem az Aláíró jelenik meg a Szolgáltató előtt, hanem a Szolgáltató regisztrációs munkatársa keresi fel az Aláírót.

Az igénylési eljárás lépései a következők:

- Az Előfizető tájékozódik a Szolgáltató által támogatott hitelesítési rendekről és tanúsítványfajtákról, és a szolgáltatás igénybevételének feltételeiről. Ezt a Szolgáltató honlapján vagy az ügyfélszolgálati irodájában teheti meg.
- Az Előfizető szolgáltatási szerződést köt a Szolgáltatóval, amelyben megadja, hogy mely Aláírók jogosultak a szerződés keretében kibocsátott tanúsítványokban szerepelni.
- Az Előfizető meghatározza, hogy mely Aláíró mely hitelesítési rend szerinti tanúsítványt jogosult igényelni.

- Az Aláíró is tájékozódik a Szolgáltató tanúsítványtípusairól és a szolgáltatás igénybevételének feltételeiről. Ezt a Szolgáltató honlapján vagy ügyfélszolgálati irodájában teheti meg.
- Az Aláíró jelzi a Szolgáltatónak, hogy tanúsítványt szeretne, eljuttatja adatait a Szolgáltató ügyfélszolgálati irodájának, és felhatalmazza a Szolgáltatót, hogy adatait a tanúsítvány kibocsátásának céljából kezelje.
- A Szolgáltató ellenőrzi a megadott információkat, különösen azokat, amelyeket a tanúsítványban is szerepeltetnie kell.
- Amennyiben az Aláíró e-mail címet tartalmazó tanúsítványt igényel, a Szolgáltató a tanúsítvány kibocsátása előtt ellenőrzi a tanúsítványba kerülő e-mail címet. Meggyőződik róla, hogy az valóban létező e-mail cím, valamint ellenőrzi, hogy az e-mail cím valóban az Aláíró e-mail címe.
- A Szolgáltató adategyeztetést végez közhiteles adatbázisokkal (például a lakcímnyilvántartással vagy a cégnyilvántartással). Amely adatbázisok esetén ez megoldható, ott a Szolgáltató az adategyeztetést elektronikusan végzi.
- Szervezeti tanúsítvány esetén a Szolgáltató olyan igazolást is kér, amelyet a Képviselt Szervezet arról állított ki, hogy az Aláíró – a megjelölt szerepkörben – jogosult a Képviselt Szervezet tanúsítványában szerepelni. Amennyiben az igazolás nem közvetlenül a Képviselt Szervezettől érkezik, a Szolgáltató értesíti róla a Képviselt Szervezetet, hogy ilyen igazolást kapott.
- A Szolgáltató tájékoztatási kötelezettségét olyan módon teljesíti, hogy egy tájékoztató kiadványt bocsát az Aláíró rendelkezésére. Az Aláírónak módja van a kiadvány áttanulmányozására és konzultációra. A kiadvány tartalma és a tanúsítványkérelem űrlap megtalálható a Szolgáltató honlapján is, így előzetesen is megtekinthető.
- Az Aláírónak regisztrációkor személyesen meg kell jelennie a Szolgáltató vagy egy külső regisztrációs szervezete regisztrációs munkatársa előtt. A regisztrációs munkatárs azonosítja az Aláírót a 3.2.3. fejezetben leírtak szerint.
- Az előző lépéssel minden esetben egyenértékű, ha a Szolgáltató (vagy egy külső regisztrációs szervezete) kiszáll az Aláíróhoz, és a személyes azonosítást az Aláíró által meghatározott helyen, a Szolgáltató biztonsági előírásainak megfelelően hajtja végre.
- A Szolgáltató azonosítja a Képviselt Szervezetet a 3.2.2. fejezetben leírtak szerint.
- A Szolgáltató meghatározza az Aláíró egyedi nevét, ennek keretében globálisan egyedi azonosítót (OID) rendel az Aláíróhoz. Ez a 3.1.1. fejezetben tárgyaltaknak megfelelően történik.

- Az Aláíró aláírói szerződést köt a Szolgáltatóval.
- A Szolgáltató archiválja a szerződéseket, a tanúsítványkérelem űrlapot és valamennyi igazolást, amelyet az Aláíró vagy a Képviselt Szervezet benyújtottak.
- E lépéseket megelőzően az igénylő szóban is jelezheti tanúsítványigényét. A szolgáltatás nyilvános dokumentumainak helyszíni tanulmányozására is lehetősége van, valamint szóban történő tájékoztatást is kaphat a szolgáltatással kapcsolatban.
- Regisztrációkor az Aláíró saját kezű aláírásával igazolja, hogy a tanúsítványkérelem űrlapon megadott adatai helyesek, és azt, hogy igazolványa a regisztráció pillanatában érvényes volt. A Szolgáltató (vagy a külső regisztrációs szervezet) regisztrációs munkatársa aláírásával igazolja, hogy az Aláíró igazolványán szereplő arckép megfeleltethető az Aláíró arcának és az igazolványban szereplő aláírás megfeleltethető az Aláíró aláírásának.
- Amennyiben az Aláíró személyazonossága vagy a Képviselt Szervezethez való tartozása nem állapítható meg minden kétséget kizáróan, vagy valamely, a tanúsítványkérelem űrlapon feltüntetett adat nem helyes, akkor az igénylési eljárás félbeszakad. Ekkor az ügyfélnek lehetősége van a megadott adatokat korrigálni, illetve a hiányzó igazolásokat átadni.
- A Szolgáltató nyilvántartásba vesz minden, az Aláíró és a Képviselt Szervezet azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat is.
- Az Aláíró nyilatkozik róla, hogy tájékoztatást kapott a szolgáltató feltételeiről, kikötéseiről és saját kötelezettségeiről, valamint elfogadja ezen feltételeket, kikötéseket és kötelezettségeket. Az Aláíró hozzájárul, hogy a Szolgáltató nyilvántartásba vegye azon információkat, amelyeket az Aláíró a regisztráció során megadott, és tudomásul veszi, hogy a Szolgáltató ezen információt a szerződésben és mellékleteiben – köztük jelen Szolgáltatási Szabályzatban – leírtak szerint kezeli. Az Aláíró egyúttal igazolja, hogy
  - vállalja a magánkulcs, illetve az intelligens kártya használatát, védelmét,
  - igazolja és garantálja feltüntetett adatainak valódiságát, és
  - az adatok későbbi változásairól a Szolgáltatót értesíti.

A Szolgáltató haladéktalanul feldolgozza a tanúsítványkérelmet.

Ha az Aláíró külső regisztrációs szervezet előtt nyújtja be a tanúsítványkérelmet, akkor a Szolgáltató 14 munkanapon belül vállalja a kérelem feldolgozását és a tanúsítvány kibocsátását.

II. hitelesítési osztályba tartozó tanúsítvány esetén az Aláíró postán juttatja el a fenti (a III. hitelesítési osztály esetén leírt) iratokat a Szolgáltatónak, aki az ott leírtak szerint dolgozza fel. II. hitelesítési osztályba tartozó tanúsítvány esetén az Aláírónak nem kell személyesen megjelenni a Szolgáltató munkatársa előtt.

Amennyiben a tanúsítványhoz tartozó magánkulcsot az Aláíró generálja, nyilvános kulcsát a tanúsítványigényléssel együtt, egy PKCS#10 formátumú adatblokkban juttatja el a Szolgáltatónak. Amennyiben a tanúsítványhoz tartozó magánkulcsot a Szolgáltató generálja, a nyilvános kulcs már eleve rendelkezésre áll a Szolgáltató számára.

4.3. A tanúsítvány kibocsátása

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

A tanúsítványigénylés során megadott adatok, valamint az Aláíró nyilvános kulcsa a Szolgáltató információs rendszerébe kerülnek. A hitelesítő szervezet létrehozza a tanúsítványt – aláírja a saját magánkulcsával – és visszaküldi azt a regisztráló szervezetnek.

A tanúsítványkérelem benyújtását követően a Szolgáltató kibocsátja a tanúsítványt, azaz a 4.4. fejezetben leírtak szerint átadja az Aláíró részére, majd – amennyiben az ügyfél ehhez hozzájárult – haladéktalanul közzéteszi a tanúsítványt a nyilvános tanúsítványtárában.

4.4. Tanúsítvány-elfogadás

A III. hitelesítési osztályba tartozó, valamint a közigazgatási hitelesítési rendeknek megfelelő tanúsítványok esetén az Aláíró csak akkor veheti át tanúsítványát, illetve a magánkulcsát tartalmazó intelligens kártyát, ha a Szolgáltató (vagy a külső regisztrációs szervezet) ügyfélszolgálati munkatársa azonosította őt.

Intelligens kártyához kapcsolódó tanúsítvány esetén, amennyiben a kártya átvétele nem közvetlenül a regisztrációt követően történik, akkor az Aláíró olyan személyes azonosítás során veheti át a kártyát, amely során személyazonosításra alkalmas igazolvánnyal kell azonosítania magát. Az átadó fél ellenőrzi, hogy az Aláíró arcképe megfelel-e az igazolványában szereplő arcképnek, és az Aláíró aláírása megfelel-e az igazolványában szereplő aláírásának.

Az intelligens kártya átvétele előtt az Aláírónak ellenőriznie kell a kártyára kerülő tanúsítványban szereplő adatokat. A kártya átvételével egyidejűleg az Aláíró megkapja az aktiválásához szükséges kódokat. E kódokat zárt borítékban kapja meg, amelyet átvételkor köteles felnyitni és ellenőrizni, hogy a kódok olvashatóak-e. Az Aláíró meg kell, hogy változtassa az alapértelmezés szerinti ötjegyű kódot, egy hatjegyű kódra. Azzal, hogy az

eredeti kód ötjegyű volt, az Aláíró megbizonyosodhat róla, hogy az eszközt korábban nem használták. Az eszköz átvételét követően az Aláíró a Szolgáltató ügyfélszolgálati irodájában kipróbálhatja a kártyáját. Az eszköz átvételét követően az Aláírónak (kézzel) alá kell írnia, hogy átvette a kártyáját és a hozzá tartozó aktiváló kódokat.

Amennyiben a tanúsítványhoz tartozó magánkulcsot nem a Szolgáltató generálta, az Aláíró a tanúsítvány letöltésével és használatba vételével fogadja el a tanúsítványt.

Mindkét esetre igaz, hogy a tanúsítvány használatba vétele előtt az Aláírónak meg kell bizonyosodnia a tanúsítványban szereplő adatok helyességéről. Amennyiben az Aláíró helytelen adatot talál a tanúsítványban, köteles haladéktalanul jelezni ezt a Szolgáltatónak, illetve köteles kezdeményezni a tanúsítvány felfüggesztését.

A Szolgáltató a tanúsítvány kibocsátásáról és elfogadásáról értesíti az Aláírót, az Előfizetőt, illetve a Képviselt Szervezetet. A Képviselt Szervezetnek küldött értesítés tartalmazza a Képviselt Szervezet által kibocsátott azon igazolás iktatószámát, amely alapján a Szolgáltató a tanúsítványt kibocsátotta, amennyiben az igazolás rendelkezett iktatószámmal. Az Előfizetőnek és a Képviselt Szervezetnek küldött értesítés nem tartalmazza az Aláíró személyes adatait.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. Az Aláíró tanúsítvány használata

Az Aláíró a tanúsítványát kizárólag a tanúsítványban szereplő kulcshasználatnak megfelelően használhatja. (6.1.9) A tanúsítványokat kizárólag fokozott biztonságú elektronikus aláírás létrehozására szabad használni. (Más célra, különösen titkosításra és hitelesítésre nem szabad őket felhasználni.) A használat során be kell tartani az 1.4. fejezetben leírt korlátokat.

4.5.2. Az Érintett félre vonatkozó ajánlások

Amennyiben egy Érintett fél ésszerűen kíván egy tanúsítványra hagyatkozni, a jelen Szolgáltatási Szabályzatnak megfelelően javasolt eljárnia a számára nyújtott szolgáltatások igénybevétele során, így különösen a tanúsítványok érvényességének ellenőrzése során. Ekkor – a Szolgáltatási Szabályzatban foglaltak betartása mellett – a lehető legnagyobb gondossággal és körültekintéssel javasolt eljárnia, amely az összes rendelkezésre álló információ alapján történő ésszerű mérlegelést jelenti az alábbiakban leírt módon.

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

A tanúsítványra vonatkozó ellenőrzéseket az Érintett félnek célszerű elvégeznie a teljes tanúsítványláncra vonatkozóan.

Az itt leírtakhoz képest a vonatkozó hitelesítési és időbélyegzési rend további ajánlásokat is tartalmazhat az Érintett fél számára. Az itt leírt lépések a hatályos jogszabályokból, a nemzetközi szabványokból és ajánlásokból levezethetőek, hozzájuk képest további követelményt nem tartalmaznak. E lépések a jogszabályokban, szabványokban, ajánlásokban felsorolt követelményeket fejtik ki.

Elektronikus aláírás ellenőrzése esetén, ha az ellenőrzendő elektronikus aláírás, a hozzá kapcsolódó tanúsítvány vagy a tanúsítványlánc bármely adata a művelet érvénytelenségére utal, illetve ha az az adott kontextusban nem elfogadható, akkor az elektronikus aláírást és a tanúsítvány elfogadását az Érintett félnek célszerű elutasítania.

Ha egy Érintett fél ésszerűen kíván egy elektronikus aláírásra hagyatkozni, a következő lépéseket javasolt elvégeznie:

1. Az aláírás és az aláírói tanúsítvány összetartozásának ellenőrzése.

2. A tanúsítvány érvényességi idejének ellenőrzése az aláírás megbízható (pl. időbélyegből megállapítható) időpontjára vonatkozóan, azaz annak vizsgálata, hogy az aláírás időpontja a tanúsítvány érvényességi idején belülre esik-e.

3. A tanúsítvány adott célra való alkalmasságának vizsgálata. Javasolt megvizsgálni, hogy aláírásra szolgáló tanúsítványról van-e szó. Szervezeti tanúsítványok esetén azt is javasolt megvizsgálni, hogy az aláíró a tanúsítvány alapján megállapítható (pl. a Title mezőben feltüntetett) szerepe szerint jogosan írta-e alá az adott dokumentumot.

4. A tanúsítvány visszavonási állapotának ellenőrzése az aláírás időpontjára vonatkozóan. Ez visszavonási lista (CRL) vagy online tanúsítvány-állapot válasz (OCSP) alapján tehető meg. Bármelyik megoldást választja az Érintett fél, az alábbiakat célszerű figyelembe vennie:

   Mind a Szolgáltató által közzétett legfrissebb CRL, mind a Szolgáltató által adott friss OCSP válaszok a Szolgáltató visszavonási nyilvántartásában szereplő aktuális állapotot tükrözik. A Szolgáltató visszavonás kezelését úgy alakította ki, hogy ügyfeleinek lehetősége van olyan módon kérni a tanúsítványok felfüggesztését, hogy a megváltozott visszavonási állapot a bejelentés befogadásának pillanatától számítva haladéktalanul – jellemzően néhány másodperc alatt – megjelenik a Szolgáltató CRL-jeiben, illetve OCSP szolgáltatásában. A Szolgáltató visszavonási nyilvántartása a tanúsítványok visszavonási állapotának lekérdezésére szolgál, amennyiben egy tanúsítvány a Szolgáltató visszavonási nyilvántartása szerint egy adott időpontban érvényes, a visszavonási nyilvántartás a későbbiekben is ugyanazon választ fogja adni ugyanazon időpont vonatkozásában[4].

[4]Eat. 14. § (3)

A fentiek alapján a Szolgáltató azt javasolja, hogy az Érintett fél a közvetlenül az aláírás megbízható (pl. időbélyeggel igazolható) időpontja után létrejött CRL-ek és OCSP válaszok alapján állapítsa meg a tanúsítvány aláírás pillanatában vett visszavonási állapotát. Egy tanúsítványnak a Szolgáltató visszavonási nyilvántartásában szereplő aktuális visszavonási állapotának lekérdezésére a Szolgáltató friss OCSP válasz beszerzését, vagy a legfrissebb CRL letöltését javasolja.

A CRL és az OCSP alapján történő ellenőrzés között az jelenti a fő különbséget, hogy CRL esetén előfordulhat, hogy az aláírás megbízható időpontját követő pozitív (a tanúsítvány érvényességét megerősítő) CRL csak a következő periodikus CRL kibocsátása esetén gyűjthető be, míg a Szolgáltató ügyfelei által igénybe vehető OCSP szolgáltatás esetén tetszőleges időpontban – akár rögtön az aláírás létrehozását követően – lekérdezhető a friss pozitív válasz. A Szolgáltató több különböző módon nyújt OCSP szolgáltatást, ezekről a 4.10. fejezetben található bővebb információ. A Szolgáltatóval szerződéses viszonyban nem lévő Érintett fél is találkozhat aláírásokhoz csatolt (és esetleg időbélyeggel ellátott) OCSP válaszokkal, valamint igénybe veheti az OCSP szolgáltatás nyilvánosan és ingyenesen elérhető változatát is.

Megjegyzés: A vonatkozó szabványok és specifikációk mind a CRL, mind az OCSP technológiák esetén lehetővé teszik ezek merőben más módon történő alkalmazását, így a fenti megállapítások, ajánlások más szolgáltatók esetén nem feltétlenül alkalmazhatóak.

5. A tanúsítványt kibocsátó hitelesítő egység tanúsítványának, illetve a rajta lévő aláírásnak ellenőrzése a fenti pontok szerint.

Amennyiben a fentiek közül bármelyik ellenőrzés sikertelen, az aláírást célszerű elutasítani.

Az Érintett félnek célszerű mérlegelnie, hogy a tanúsítvány biztonsági szintje megfelel-e az adott célra. A Szolgáltató által meghatározott kártérítési korlátot meghaladó esetekben az Érintett félnek célszerű az aláírást elutasítania, és magasabb (például minősített) biztonsági szintet megkövetelni. A Szolgáltató felhívja a figyelmet, hogy a fenti leírtakon kívül egyéb szempontok is befolyásolhatják egy aláírás érvényességét, így az érintett félnek ajánlott az adott helyzetben elvárható gondossággal eljárnia és az összes rendelkezésre álló információ alapján döntenie.

Ha egy Érintett fél ésszerűen kíván OCSP válaszra hagyatkozni, a következőket célszerű tennie:

Tanúsítvány-állapot válasz (OCSP válasz) ellenőrzésekor javasolt megvizsgálni a válaszon lévő aláírás érvényességét, valamint azt, hogy a válasz valóban az e-Szignó Hitelesítés Szolgáltató válaszadójától (e-Szignó OCSP Responder) származik-e. A válaszadó tanúsítványát kibocsátó hitelesítő egység (e-Szigno OCSP CA) tanúsítványa a `www.e-szigno.hu` honlapról elérhető. Emellett azt is javasolt ellenőriznie, hogy az OCSP válaszadó tanúsítványa az OCSP lekérdezés időpontjában érvényes volt-e.

OCSP választ kizárólag akkor javasolt érvényesnek tekinteni, ha igazolható, hogy az OCSP válasz kibocsátásának pillanatában a válaszadó érvényes tanúsítvánnyal rendelkezett. Ez akkor igaz, ha:

- A válaszadó tanúsítványa még érvényes.
- A válaszadó tanúsítványa már nem érvényes, de – például időbélyeg alapján – igazolható, hogy az OCSP válaszadó tanúsítványa a válasz kibocsátása pillanatában érvényes volt.

Ha a fentiek egyike sem teljesül, az OCSP választ célszerű elutasítani.

Ha egy Érintett fél időbélyegre kíván hagyatkozni, a következőket célszerű tennie:

Időbélyeg ellenőrzésekor célszerű megvizsgálni, hogy az időbélyeg valóban a lebélyegzett dokumentumhoz tartozik-e, valamint azt, hogy az időbélyegző egység tanúsítványa nem járt-e le, illetve nem vonták-e vissza. Ha az időbélyegző egység tanúsítványát azért vonták vissza, mert az időbélyegző egységhez tartozó aláírás-létrehozó adat illetéktelen kezekbe jutott (vagy a visszavonás oka nem megállapítható), akkor célszerű minden, e tanúsítvány alapján kibocsátott, időbélyeget (visszamenőleg is) érvénytelennek tekinteni. (Lásd: RFC 3161, 4. fejezet, 1. és 2. pont) Vitás esetben az egyes időbélyegek érvényessége a Szolgáltató biztonságos naplófájljai segítségével lehet bizonyítható.

Ha az időbélyegző egység tanúsítványát más okból vonták vissza, akkor csak a visszavonást követően kibocsátott időbélyegeket célszerű érvénytelennek tekinteni. (Lásd: RFC 3161, 4. fejezet, 1. és 2. pont)

Az időbélyegző egység tanúsítványát a végfelhasználói tanúsítványokéval megegyező módon célszerű ellenőrizni. A fentiek miatt, amikor egy érintett fél időbélyegre kíván hagyatkozni, minden egyes alkalommal ellenőriznie célszerű az időbélyegző tanúsítványának visszavonási állapotát. (Lásd: CWA 14171, 5.4.7.3. fejezet, RFC 3161, 2.2. és 4. fejezet)

4.6. Tanúsítványcsere érvényes tanúsítvány esetén

Tanúsítványcsere alatt azt a folyamatot értjük, amikor egy már regisztrált (a regisztrációs folyamaton átesett) Aláírónak a már érvényes szerződése keretében korábbi tanúsítványa helyett másik tanúsítványt kell kibocsátani. A tanúsítványcsere minden esetben új tanúsítvány kibocsátását jelenti. Ha ilyenkor az Aláíró korábbi tanúsítványa még érvényes, azt – az Ügyféllel egyeztetett ütemben – vissza kell vonni. A tanúsítványcserére a következő szabályok vonatkoznak:

- A tanúsítvány cseréjét az Aláíró kezdeményezheti.
- Ha az Aláíró korábbi tanúsítványa a tanúsítványcsere előtt visszavonásra került, az új tanúsítványt a Szolgáltató csak új kulcshoz bocsátja ki a 4.7. fejezetben leírtak szerint.

- Amennyiben valamely, a tanúsítványban is szereplő adat megváltozik, akkor a Szolgáltató a 4.8. fejezeben leírtak szerint jár el.
- Az új tanúsítvány kibocsátása előtt a Szolgáltató ellenőrzi, hogy a régi tanúsítvány létezett-e, valamint, hogy az új tanúsítványba kerülő minden új adat helyes és érvényes. A tanúsítványban szereplő szervezet vagy személy nevében bekövetkező változás esetén a Szolgáltató megismétli a közhiteles adatbázissal történő egyeztetést.
- A tanúsítványcsere során alkalmazott azonosítás és hitelesítés módját a 3.3. fejezet írja le.

4.7. Tanúsítványcsere visszavont tanúsítvány esetén

Amennyiben a régi tanúsítvány visszavonásra került, a Szolgáltató az új tanúsítványt új kulcshoz bocsátja ki. A Szolgáltató ekkor is biztosítja a 4.6. fejezetben leírt feltételeket. A Szolgáltatónak a tanúsítvány kibocsátása előtt ekkor is meg kell győződnie róla, hogy az új kulcs az Aláíró birtokában van, illetve, hogy a tanúsítványba kerülő adatok érvényesek.

4.8. Tanúsítványban szereplő adatok megváltoztatása

Ha az Aláírónak valamely olyan adata változik meg, amely a tanúsítványában szerepel, akkor a Szolgáltató az ügyféllel egyeztetett ütemben visszavonja a tanúsítványát. A régi tanúsítvány a 4.7. fejezetben leírtak szerint cserélhető le.

Adatváltozás esetén az ügyfélnek – a kezdeti regisztrációkor lefolytatott eljárásnál alkalmazottal megegyező módon – igazolnia kell az új adatok érvényességét. A Szolgáltató ekkor is biztosítja a 4.6. fejezetben leírt feltételeket.

4.9. Tanúsítvány felfüggesztése és visszavonása

A Szolgáltató mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatást nyújt. A tanúsítvány visszavonása a tanúsítvány-állapotát végérvényesen érvénytelenre állítja. A felfüggesztett tanúsítvány mindaddig, míg felfüggesztett állapotban van, ugyanúgy érvénytelenként kezelendő, mint a visszavont. Egy tanúsítvány egyfolytában legfeljebb 5 napig lehet felfüggesztett állapotban. Ha a tanúsítvány ezen idő elteltével sem kerül visszaállításra, a Szolgáltató a tanúsítványt visszavonja.

A visszavont és felfüggesztett tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. A visszavont tanúsítványhoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges.

Felelősségi szabályok a felfüggesztéssel és visszavonással kapcsolatban:

- A visszavonási/felfüggesztési kérelem Szolgáltatóhoz történő megérkezéséig az Aláíró, illetve az Előfizető a felelős a felmerülő károkért.
- Azon pillanattól kezdve, amikor a Szolgáltató a felfüggesztés vagy visszavonás bejelentést elfogadja, a Szolgáltató felel a felmerülő károkért. A Szolgáltató a kérelem elfogadását követően haladéktalanul közzéteszi a tanúsítvány megváltozott visszavonási állapotát.
- Amennyiben a Szolgáltató már közzétette a tanúsítvány érténytelen visszavonási állapotát, a Szolgáltató semmilyen felelősséget nem vállal azért, ha az Érintett fél ekkor mégis érvényesnek tekinti a tanúsítványt.

Az Aláírónak (vagy az Előfizető nevében eljáró szervezeti ügyintézőnek) lehetősége van telefonon, személyesen vagy elektronikusan aláírva felfüggeszteni a tanúsítványt. A telefonos felfüggesztés a hét minden napján, a nap 24 órájában működik. Személyesen és elektronikusan aláírt elektronikus levélben felfüggeszteni kizárólag nyitvatartási időben lehet. Tanúsítvány visszavonására vonatkozó kéréseket a Szolgáltató kizárólag írásban (személyesen és papíron, postai levélben vagy elektronikusan aláírva) fogad.

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 Szolgáltató belső folyamatai biztosítják, 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 személyesen vagy telefonon érkező kérelmek esetén a megérkezés időpontja az, amikor az ügyfél megad minden, a felfüggesztéshez/visszavonáshoz szükséges adatot. A postán vagy elektronikus levélben küldött kérelmek esetén a megérkezés időpontja az, amikor a levél nyitvatartási időben a Szolgáltató ügyfélszolgálatához, vagy a Szolgáltató szerverén lévő postafiókba ér. A nyitvatartási időn kívül érkező levelek a legközelebbi nyitvatartási idő kezdetén tekinthetőek megérkezettnek. A Szolgáltató kizárólag az 1.1.3. fejezetben megjelölt címekre küldött kérelmekre vállalja e követelmények teljesítését, más csatornákon vagy címekre – különösen a Szolgáltató egyes munkatársainak közvetlenül – küldött kérelmek feldolgozásával kapcsolatban semmilyen rendelkezésre állást nem vállal.

Ha az ügyfél vissza kívánja vonni a tanúsítványát, és a visszavonás sürgős, vagy az ügyfél nem képes személyesen bemenni a Szolgáltató ügyfélszolgálati irodájába, a Szolgáltató azt javasolja, hogy a visszavonásig az ügyfél a telefonos ügyelet segítségével függessze fel a tanúsítványt. A felfüggesztett tanúsítvány visszavonásáról elég később gondoskodni.

Amennyiben az ügyfél sürgősen fel kívánja függeszteni a tanúsítványát, a Szolgáltató akkor is a telefonos ügyelet használatát javasolja.

Az Aláíró csak a saját tanúsítványát függesztheti fel, kivéve a szervezeti ügyintézőket és az adott szervezet nevében aláírásra jogosultakat, akik a saját előfizetésükhöz (vagyis, ugyanazon Előfizetőhöz) tartozó összes tanúsítványt felfüggeszthetik, visszaállíthatják, visszavonhatják. (A szervezet nevében aláírásra jogosultak csak személyesen vagy elektronikusan aláírva függeszthetnek fel tanúsítványokat, telefonon nem.) Mivel telefonon a felfüggesztési jogosultság ellenőrzése (vagyis az Aláíró azonosítása) jelszó alapján történik, a Szolgáltató csak a jelszó helyességét tudja ellenőrizni. A Szolgáltató mindenkitől elfogadja a felfüggesztést, aki meg tudja adni a helyes felfüggesztési jelszót. A Szolgáltató minden felfüggesztési, visszaállítási és visszavonási kérelmet naplóz. Felfüggesztés és visszaállítás esetén a Szolgáltató e-mailben értesíti az Aláírót és az Előfizetőt ennek tényéről.

4.9.1. Felfüggesztés telefonon

A telefonos felfüggesztés a hét 7 napján, a nap 24 órájában működik. A Szolgáltató ügyfelei ezen ügyelet segítségével jelezhetik a Szolgáltatónak, ha kártyájuk vagy magánkulcsuk illetéktelen kezekbe került. A telefonos felfüggesztés szolgáltatás rendelkezésre állása 99% (vagyis egy év perceinek 99%-ában folyamatosan működik), az eseti szolgáltatás-kiesések nem haladhatják meg a 3 órát. A telefonon megérkező kérelmeket a Szolgáltató soron kívül dolgozza fel és haladéktalanul teljesíti.

A telefonos kérelemre a Szolgáltató ügyeletes munkatársa válaszol. A Szolgáltató jogosult hangfelvételt készíteni az ügyelethez megérkező felfüggesztések és visszaállítások során elhangzott párbeszédekről.

A Szolgáltató ügyeletes munkatársa a következő információkat mindenképpen elkéri a kérelmezőtől:

- a kérelmező nevét,
- azon Aláíró nevét, akinek a tanúsítványát fel kell függeszteni,
- az Aláíró születési dátumát vagy a tanúsítványában szereplő OID-jének utolsó három számát (szervezeti felfüggesztés esetén az OID-et kötelező megadni),
- a felfüggesztési jelszót, amely lehet:
  - az Aláíró felfüggesztési jelszava vagy
  - szervezeti felfüggesztési kérelem esetén a szervezeti felfüggesztési jelszó.

A fenti adatok mellett az ügyeletes további – a regisztráció során megadott – személyes adatokat is kérhet a kérelmezőtől.

Amennyiben a kérelmező nem adja meg a fenti listában szereplő kötelező adatok valamelyikét, vagy nem a helyes jelszót adja meg, a Szolgáltató elutasítja a felfüggesztési kérelmet.

Amint a Szolgáltató munkatársa a telefonbeszélgetés során sikeresen megállapította a kérelmező felfüggesztési jogosultságát, közli, hogy a kérelmet a Szolgáltató elfogadta, és megkezdte annak feldolgozását. E pillanattól a Szolgáltató felelősséget vállal a tanúsítvány elfogadásából eredő károkért, amíg a tanúsítvány új visszavonási állapota meg nem jelenik a Szolgáltató visszavonási nyilvántartásában.

Amennyiben a Szolgáltató tudomására jut, hogy valamely ügyfél kártyája illetéktelen kezekbe került, akkor a Szolgáltató a kártyára kibocsátott összes tanúsítványt felfüggeszti.

A felfüggesztési jelszó a Szolgáltató ügyfélszolgálati irodáján keresztül módosítható.

Amennyiben a Szolgáltató tudomására jut, hogy valamely Aláíró szoftveres (azaz nem intelligens kártyán kibocsátott) tanúsítványához tartozó magánkulcsa illetéktelen kezekbe került, akkor az Aláíró összes szoftveres tanúsítványát felfüggeszti.

4.9.2. Felfüggesztés személyesen vagy elektronikusan aláírva

A Szolgáltató felfüggeszti az Aláíró tanúsítványát, ha az ügyfél ezt kéri. A felfüggesztési kérelem a Szolgáltató honlapjáról letölthető „felfüggesztési/visszaállítási kérelem” űrlap formájában is benyújtható. Ezen űrlap használata nem kötelező, de a Szolgáltató pontosan meg kell, hogy tudja állapítani, hogy a kérelmező pontosan melyik tanúsítvány felfüggesztését kéri. A kérelem benyújtására lehetőség van személyesen, a Szolgáltató ügyfélszolgálati irodájában vagy elektronikus levélben, elektronikusan aláírva. A regisztrációs munkatárs e-mailben értesítést küld az Aláírónak és az Előfizetőnek.

Szervezeti felfüggesztési kérelem esetén a szervezeti ügyintézőnek (vagy a szervezet nevében aláírásra jogosult személynek) „szervezeti felfüggesztési / visszaállítási kérelem” űrlapot kell kitöltenie, egyébként e folyamat pontosan úgy zajlik, mint a nem szervezeti felfüggesztés esetében.

4.9.3. Felfüggesztés és visszavonás a Szolgáltató kezdeményezésére

A Szolgáltató is kezdeményezheti egy tanúsítvány felfüggesztését a következő okok esetén:

- Ha az Előfizető a fizetési határidőig nem fizet.
- Ha a Szolgáltató valószínűsíti, hogy a tanúsítványban szereplő adatok nem felelnek meg a valóságnak, azaz az Eat. 14. §-a (1), (2) bekezdés b), c), e), illetve f) pontjaiban meghatározott valamely körülmények esetén. Amennyiben a Szolgáltató e körülményekről tudomást szerez, kezdeményezi a tanúsítvány felfüggesztését vagy visszavonását.
- Ha a Szolgáltató valószínűsíti, hogy a tanúsítványhoz tartozó magánkulcs nem az Aláíró birtokában van, és ezt megalapozott bizonyítékok alátámasztják. Amennyiben

a Szolgáltató tudomására jut, hogy egy intelligens kártya illetéktelen kezekbe került, akkor a Szolgáltató a rajta lévő összes tanúsítványt felfüggeszti.

A Szolgáltató visszavonja a tanúsítványt, ha a Hatóság az Eat. 18. § szerinti határozata értelmében a tanúsítvány aláírására használt algoritmus már nem biztonságos, illetve nem alkalmas tanúsítványok aláírására.

4.9.4. Visszaállítás

A tanúsítvány visszaállítása azt a folyamatot jelenti, amelynek során a felfüggesztett tanúsítvány újra érvényes állapotba kerül. Visszaállítási kérelmet az Aláíró kizárólag személyesen, az Előfizető képviselője pedig kizárólag személyesen vagy szervezeti ügyintéző által elektronikusan aláírva nyújthat be a Szolgáltatónak.

Ha ugyanarra a tanúsítványra több féltől is érkezik felfüggesztési kérelem, akkor a Szolgáltató csak akkor állítja vissza a tanúsítványt, ha mindegyik felfüggesztő fél kéri a visszaállítást is.

4.9.5. Visszavonás

Visszavonás kizárólag írásban (papíron vagy elektronikusan aláírva) történhet. Visszavonási kérelmeket a Szolgáltató egy munkanapon belül[5](de soron kívül) dolgoz fel. Visszavonási kérelmeket személyesen leadni kizárólag az ügyfélszolgálati iroda nyitvatartási ideje alatt lehet. Amint a visszavonási kérelem feldolgozásra került, a Szolgáltató értesíti erről az Aláírót, annak szervezetét (vagy harmadik felet, aki a tanúsítványt visszavonta).

Ha az Aláíró írásban, „visszavonási kérelem” űrlapon kéri, a Szolgáltató visszavonja a tanúsítványát. Az Előfizető is jogosult a tanúsítvány visszavonását személyesen vagy elektronikusan aláírva kérni a „szervezeti visszavonási kérelem” űrlap kitöltésével. A visszavonást vagy szervezeti ügyintézői tanúsítvánnyal rendelkező személy kérheti, vagy olyan személy, aki egyébként is jogosult az Előfizető nevében aláírni. A fenti űrlapok használata nem kötelező, de a Szolgáltató pontosan meg kell, hogy tudja állapítani, hogy pontosan ki, pontosan melyik tanúsítvány visszavonását kéri, és milyen jogcímen. Ha a tanúsítványt a Szolgáltató harmadik féltől származó dokumentum alapján állította ki (e dokumentumban harmadik fél igazolta az Aláíró valamely szerepét), és e harmadik fél ezen igazolást írásban visszavonja (pl. mert az Aláírónak e szerepe megszűnt), a Szolgáltató a tanúsítványt visszavonja.

A Szolgáltató akkor kezdeményez visszavonást, ha a szolgáltatási szerződés megszűnik, vagy

- ha az Előfizető a fizetési határidőig nem fizet;

[5]Ennél gyorsabb – azonnali – visszavonás-kezelés a felfüggesztés segítségével érhető el. Az ügyfél a 4.9.1. fejezetben leírt telefonos ügyeleten keresztül kérheti a felfüggesztést, amelyet a Szolgáltató azonnal, a telefonos beszélgetés során végrehajt. Az ügyfél ezt követően kérheti írásban a tanúsítvány visszavonását.

- ha a Szolgáltató bizonyítottnak látja, hogy a tanúsítványban szereplő adatok nem felelnek meg a valóságnak.

Visszavonáskor meg kell adni a visszavonás okát. Amennyiben a visszavonást az Ügyfél kéri, és a visszavonás okát nem adja meg, a Szolgáltató úgy tekinti, hogy a visszavonás oka az, hogy az Aláíró a tanúsítványt a továbbiakban nem kívánja használni. A Szolgáltató a visszavonást ilyenkor is teljesíti.

4.10. A visszavonási állapot közzététele

A tanúsítványok visszavonási állapotának lekérdezésére a Szolgáltató a következő lehetőségeket biztosítja:

- OCSP (online tanúsítvány visszavonási állapot lekérdezési szolgáltatás)
- CRL (visszavonási lista)

A visszavonási listában a visszavont és a felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok visszaállítás hatására kikerülnek a listából. Felfüggesztés, visszaállítás és visszavonás esetén a folyamat sikeres lezárását követően a tanúsítvány új állapota haladéktalanul – lásd: 4.9. fejezet – megjelenik a Szolgáltató visszavonási nyilvántartásában. Ettől a pillanattól kezdve a Szolgáltató által nyújtott OCSP válaszok már a tanúsítvány új visszavonási állapotát mutatják. Felfüggesztés, visszaállítás és visszavonás esetén a Szolgáltató haladéktalanul – lásd: 4.9. fejezet – új CRL-t bocsát ki.

A visszavonási állapot közzététele szolgáltatás rendelkezésre állása: 99%, és az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

4.10.1. Visszavonási listák

A Szolgáltató egyes hitelesítő egységei az alábbi gyakorisággal bocsátnak ki visszavonási listát:

- A Szolgáltató által működtetett produktív (nem gyökér) hitelesítő egységek 24 óránként bocsátanak ki CRL-t.
- A Microsec e-Szigno Root CA 2009 gyökér hitelesítő egység 24 óránként bocsát ki CRL-t.
- A Microsec e-Szigno Root CA gyökér hitelesítő egység havonta bocsát ki CRL-t.
- Az e-Szigno OCSP CA gyökér hitelesítő egység 24 óránként bocsát ki CRL-t[6].

[6]Az e-Szigno OCSP CA által kibocsátott CRL egyetlen tanúsítványra sem vonatkozik, mindig üres, mert az ezen egység által kibocsátott rövid lejáratú OCSP válaszadói tanúsítványok ocspNoCheck kiterjesztést tartalmaznak.

Az egyes tanúsítványokra vonatkozó visszavonási listák az alábbi címeken érhetőek el:

- Microsec e-Szigno Root CA által kibocsátott tanúsítványok esetén:
  `http://www.e-szigno.hu/RootCA.crl`
- Microsec e-Szigno Root CA 2009 által kibocsátott tanúsítványok esetén:
  `http://crl.e-szigno.hu/rootca2009.crl`
- e-Szigno OCSP CA által kibocsátott tanúsítványok esetén:
  `http://www.e-szigno.hu/OCSPCA-Crl`
- Microsec e-Szigno Server CA által kibocsátott tanúsítványok esetén:
  `http://www.e-szigno.hu/SCA-Crl`
- Signature e-Szigno CA6 által kibocsátott tanúsítványok esetén:
  `http://www.e-szigno.hu/ca6.crl`
- Advanced e-Szigno CA3 által kibocsátott tanúsítványok esetén:
  `http://www.e-szigno.hu/ACCA3.crl`
- Advanced e-Szigno CA2 által kibocsátott tanúsítványok esetén:
  `http://www.e-szigno.hu/ACCA2.crl`
- Advanced Class 3 e-Szigno CA 2009 által kibocsátott tanúsítványok esetén:
  `http://crl.e-szigno.hu/a3ca2009.crl`
- Advanced Class 2 e-Szigno CA 2009 által kibocsátott tanúsítványok esetén:
  `http://crl.e-szigno.hu/a2ca2009.crl`
- Advanced Pseudonymous e-Szigno CA 2009 által kibocsátott tanúsítványok esetén:
  `http://crl.e-szigno.hu/apca2009.crl`

A visszavonási listák hatályba lépésének időpontja (thisUpdate) egyúttal azt az időpontot is jelöli, amikor a hitelesítő egység a visszavonási listát összeállította, és aláírását megkezdte. Ezt követően a visszavonási lista publikálásáig hosszú visszavonási listák esetén egy vagy két perc is eltelhet. A következő visszavonási lista megjelenése (következő frissítés, nextUpdate) azt az időpontot jelzi, amikortól kezdve a következő lista a nyilvánosság számára elérhető. Ennek megfelelően a visszavonási lista hatályba lépési időpontja és a következő visszavonási lista megjelenési időpontja között a fenti időintervallumoknál hosszabb időintervallumok is megjelenhetnek, ez nem befolyásolja azt, hogy a visszavonási listák megjelenése között legfeljebb 24 óra, illetve egy hónap telik el.

Tekintetbe véve, hogy a felkínált szolgáltatások közül OCSP segítségével állapítható meg egy tanúsítvány érvényessége a leggyorsabban és legegyszerűbben, a Szolgáltató az OCSP használatát javasolja ügyfelei részére.

4.10.2. Online tanúsítvány-állapot szolgáltatás (OCSP)

A Szolgáltató a tanúsítványok visszavonási állapotát OCSP szolgáltatás segítségével is közzéteszi. E szolgáltatáson keresztül, a legfrissebb CRL-en elérhető állapottal megegyező információ érhető el. A két technológiát a 4.5.2. fejezet hasonlítja össze.

Az SHA-1 alapú tanúsítványok tekintetében a Szolgáltató az RFC 2560 szerinti „trusted responder" elv szerint nyújtja az OCSP szolgáltatást, azaz OCSP válaszadói külön tanúsítvány-hierarchiában helyezkednek el. Az SHA-256 alapú tanúsítványok tekintetében a Szolgáltató az RFC 2560 szerinti „authorized responder" elv szerint nyújtja az OCSP szolgáltatást, így minden egyes hitelesítő egysége külön OCSP válaszadót hitelesít felül, amely az adott hitelesítő egység által kibocsátott tanúsítványok állapotára vonatkozóan nyújt információt (1.3.1. fejezet).

A Szolgáltató két különböző módon nyújt OCSP szolgáltatást, az alábbiakban e két változat jellemzőit mutatjuk be.

Ügyfelek részére nyújtott OCSP szolgáltatás.

- Az OCSP szolgáltatás e változatát kizárólag a Szolgáltató ügyfelei vehetik igénybe, OCSP szolgáltatásra vonatkozó szolgáltatási szerződés keretében. A Szolgáltató lekérdezéskor tanúsítvány vagy felhasználónév-jelszó páros alapján azonosíthatja az ügyfelet. Az SHA-1 alapú tanúsítványokban szereplő OCSP URL-en, tanúsítvány-alapú authentikáció szükséges.
- Az OCSP szolgáltatás e változata minden tanúsítvány tekintetében elérhető, a válaszok mindig a Szolgáltató visszavonási nyilvántartásában szereplő aktuális információt tartalmazzák.
- A kibocsátott OCSP válasz mindig a lekérdezés időpontjának pillanatában készül. Az OCSP válaszban szereplő thisUpdate és producedAt időpontok megegyeznek a lekérdezés időpontjával.
- A válaszban szereplő nextUpdate időpont vagy nincsen kitöltve, vagy a válaszadói tanúsítvány lejáratánál nem későbbi időpontot tartalmaz.
- Az Ügyfelek részére nyújtott OCSP szolgáltatás segítségével mindig beszerezhető olyan bizonyíték, amely később harmadik fél felé is igazolja a tanúsítványnak a Szolgáltató nyilvántartásában szereplő visszavonási állapotát, a lekérdezés időpontjára vonatkozóan.

Nyilvánosan és ingyenesen nyújtott OCSP szolgáltatás.

- Az OCSP szolgáltatás e változata nyilvánosan és ingyenesen érhető el, a visszavonási listákhoz hasonlóan bármely Érintett fél igénybe veheti. Lekérdezéskor nincsen szükség authentikációra.
- Az OCSP szolgáltatás e változata kizárólag az SHA-256 alapú tanúsítványok tekintetében érhető el, az ezen tanúsítványokban feltüntetett URL-eken.
- Az RFC 2560 „Response Pre-production" eljárása alapján, a kibocsátott OCSP válasz a lekérdezést megelőzően is létrejöhet, és nem feltétlenül tartalmaz „nonce" elemet. A Szolgáltató egyazon választ több lekérdezésre is visszaadhatja. Az OCSP válaszban szereplő thisUpdate és producedAt időpontok megegyeznek, de ezek megelőzhetik a lekérdezés időpontját.
- A válaszban szereplő nextUpdate időpont vagy nincsen kitöltve, vagy a válaszadói tanúsítvány lejáratánál nem későbbi időpontot tartalmaz.
- Az OCSP válaszok mindig a Szolgáltató visszavonási nyilvántartásában szereplő aktuális információt tartalmazzák. Azonban, ha az OCSP válasz thisUpdate időpontja korábbi, mint az az időpont, amelyre nézve az ellenőrzést végezzük — amely vagy korábbi vagy egybeesik a lekérdezés időpontjával -–, akkor az OCSP válasz nem egyértelmű bizonyíték harmadik fél számára a tanúsítvány visszavonási állapotára vonatkozóan.

Az OCSP szolgáltatás fenti két változatában jelzett különbözőségek következtében, a nyilvánosan és ingyenesen nyújtott szolgáltatás csak a következő esetekben tekinthető egyenértékűnek az ügyfelek számára nyújtott szolgáltatással:

- Ha nincsen szükség az OCSP válaszok tárolására, hanem azokat prompt, azonnali döntések meghozatalánál használjuk. Ekkor elfogadható, hogy az OCSP válasz utólag nem igazolja egyértelműen harmadik fél számára a tanúsítvány adott időpontban vett érvényességét.
- Ha az OCSP lekérdezés időpontja között és azon időpont között, amelyre nézve az ellenőrzést végezzük, eltelt idő nagyobb, mint a tárolt OCSP válasz nextUpdate és thisUpdate időpontjainak különbsége (amely legfeljebb az OCSP válasz aláírására használt válaszadói tanúsítvány érvényességi ideje lehet). Ekkor a nyilvánosan és ingyenesen nyújtott szolgáltatás által biztosított OCSP válaszok is egyértelmű bizonyítékként fogadhatóak el harmadik fél számára, mert a bennük szereplő thisUpdate időpont már garantáltan későbbi lesz, mint az az időpont, amelyre nézve az ellenőrzést végezzük.

- Ha az ellenőrző fél nem maga kérdezi le az OCSP választ (hanem pl. egy archív aláíráshoz csatolt OCSP választ használ fel), nem szükséges vizsgálnia, hogy az OCSP válasz eredetileg mely forrásból származik. Elegendő azt vizsgálnia, hogy az OCSP válaszban szereplő thisUpdate időpont későbbi-e, mint amely időpontra nézve végzi az ellenőrzést.

Az OCSP szolgáltatás fenti két változatát a Szolgáltató azonos rendelkezésre állással nyújtja.

4.11. Időbélyeg kibocsátás

Az időbélyegzés szolgáltatás igénybevétele során az Előfizető egy dokumentum lenyomatát adja meg, amelyre a Szolgáltató aláírt időbélyeget ad vissza. Az időbélyegzés szolgáltatás igénybevétele felhasználónév és jelszó vagy authentikációs tanúsítvány alapján történik. Az időbélyegzés szolgáltatás rendelkezésre állása 99%, az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

A Szolgáltató az Interneten keresztül nyújt időbélyegzés szolgáltatást, de a Szolgáltató jogosult egyes ügyfelek számára – különösen nagy, ipari mennyiségű időbélyeg kibocsátása esetén – más csatornán keresztül (például bérelt vonalon) is időbélyegeket biztosítani.

4.12. Az előfizetés vége

Az ügyféllel kötött szerződés megszűnése esetén a Szolgáltató visszavonja a szerződés keretében kibocsátott tanúsítványokat.

4.13. Magánkulcs letétbe helyezése és visszaállítása

Az elektronikus aláírásra szolgáló tanúsítványokhoz tartozó magánkulcsokból a Szolgáltató nem tart meg másolatot, ezen magánkulcsok letétbe helyezése nem megengedett.

4.14. Viszontazonosítás

A Szolgáltató viszontazonosítás szolgáltatást nyújt minden olyan tanúsítvánnyal kapcsolatban, amely esetén a tanúsítványra vonatkozó valamely hitelesítési rend előírja azt. A Szolgáltató a viszontazonosítást a [8] dokumentumban leírtak szerint nyújtja a következő kiegészítésekkel:

- A hivatkozott dokumentum nem definiálja azon lenyomatképző algoritmusok körét, amelyek szerint az érintett tanúsítvány lenyomata megadható. A szolgáltató SHA-1 algoritmussal képzett lenyomatokat fogad.
- A hivatkozott dokumentum nem definiálja, hogy az érintett tanúsítvány lenyomata milyen módon szerepel a viszontazonosítás kérdésben. A szolgáltató a base64 kódolású bináris adatként megadott lenyomatot fogadja el.

- A hivatkozott dokumentum nem definiálja, hogy a lenyomatot milyen formátumú tanúsítványról kell képezni. A szolgáltató a DER és a PEM formátumból képzett lenyomatokat egyaránt elfogadja.
- A hivatkozott dokumentum nem definiálja, hogy a (pl. születési) dátumot milyen módon kell megadni a viszontazonosítás kérdésben. A szolgáltató az YYYY-MM-DD (év, hó, nap) és az YYYY (év) formátumú adatokat fogadja el.
- A hivatkozott dokumentum közvetlenül nem definiálja, hogy az érintett természetes személy állampolgárságát milyen módon kell megadni. A Szolgáltató az <ALLAMPOLGARSAG> XML tagben várja az állampolgárságot.
- A hivatkozott dokumentum nem definiálja, hogy a természetes személy nemét milyen formátumban kell megadni. A Szolgáltató a "`férfi`" és a "`nő`" stringeket fogadja el.
- A Szolgáltató a hivatkozott dokumentumban megadott, a település nevére vonatkozó összehasonlító szabályokat a település magyar nevére alkalmazza.

A Szolgáltató által nyújtott viszontazonosítás szolgáltatás a következő címen érhető el:
`https://viszontazonositas.e-szigno.hu/`

4.14.1. A viszontazonosítási kérések fogadásáról szóló szabályzat

A Szolgáltató kétoldalú, tanúsítvány alapú authentikációt követően kiépített SSL kapcsolaton keresztül fogadja a viszontazonosítás kéréseket. Az authentikációhoz a viszontazonosítást kérő félnek közigazgatási területen használható authentikációs tanúsítvánnyal kell rendelkeznie, azaz:

- A tanúsítvány a benne feltüntetett kulcshasználat (Key Usage és Extended Key Usage) alapján authentikációs tanúsítványnak kell lennie.
- A tanúsítványt vissza kell, hogy lehessen vezetni a Közigazgatási Gyökér Hitelesítés Szolgáltató tanúsítványára. A viszontazonosítás kérést a kérelmezőnek elektronikus aláírással kell ellátnia, amelyhez közigazgatási területen használható aláíró tanúsítványt kell használnia. E tanúsítványra a következő feltételek érvényesek:
  - A benne feltüntetett kulcshasználat alapján aláíró tanúsítvány kell, hogy legyen.
  - A tanúsítvány visszavezethető kell legyen a Közigazgatási Gyökér Hitelesítés Szolgáltató tanúsítványára.
  - A benne feltüntetett hitelesítési rendek alapján alkalmas legyen a közigazgatás képviseletére.

A kérelmet a kérelmező nem köteles sem időbélyeggel, sem időjelzéssel ellátni. Amennyiben a kérelem mégis tartalmaz időbélyeget, az időbélyeg érvényes és ellenőrizhető kell, hogy legyen. A Szolgáltató minden kérelmet minősített időbélyeggel lát el, ilyen módon archiválja őket.

4.14.2. A viszontazonosítás válaszok kiállításáról szóló szabályzat

A Szolgáltató a választ a kérés beküldésére használt SSL csatornán keresztül küldi el.

A válaszon a Szolgáltató – közigazgatási felhasználásra alkalmas – automata aláíró tanúsítványával készített aláírás szerepel. Az aláírás minősített időbélyeget tartalmaz.

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 kockázatelemzésben megállapított kockázatokkal.

- A hitelesítő szervezet védett számítógéptermében valósítják meg a leginkább veszélyeztetett szolgáltatásokat. Ez a számítógépterem speciálisan erre a célra lett tervezve és kialakítva, s tervezésénél sok, különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés /beléptetés ellenőrzése és felügyelete/, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, stb.) egységes érvényesítésére került sor.

- A Szolgáltató ügyfélszolgálati irodája úgy lett kialakítva, hogy a fenti szempontoknak szintén megfeleljen alacsonyabb kialakítási és fenntartási költségek mellett. A szolgáltató ügyfélszolgálati irodája úgy lett kiválasztva, hogy reális költségek mellett képesek legyenek kielégíteni a regisztrációs szolgáltatásokkal szemben támasztott követelményeket. A Szolgáltató úgy alakította ki mobil regisztrációs egységeit,

hogy szintén megfeleljenek a regisztrációs szolgáltatásokkal szemben támasztott követelményeknek.

- A Szolgáltató a külső regisztrációs szervezetek irodáival szemben azt várja el, hogy biztonságuk egyenszilárdságú legyen a Szolgáltató regisztrációs irodáinak biztonságával. Ennek feltételeit és a Szolgáltató ezzel kapcsolatos elvárásait a Szolgáltató a külső regisztrációs szervezettel kötött szerződésben rögzíti.
- A hitelesítő szervezet valamennyi kritikus szolgáltatását egy külön biztonsági zónában valósítja meg, és az ehhez szükséges valamennyi eszközt egy a biztonsági zóna részét képező védett számítógépteremben helyezte el.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A hitelesítő szervezet egy elkülönített biztonsági zónában lévő ablaktalan helyiségben helyezkedik el. A zónát vastag és elektromágneses sugárzást át nem engedő falak veszik körül. A hitelesítő szervezet másodlagos telephelye az elsődleges telephelytől távol helyezkedik el egy védett szerverteremben.

5.1.2. Fizikai hozzáférés

A hitelesítő szervezet védett számítógépterme úgy lett kialakítva, hogy illetéktelen személyek nehezen juthassanak be. A biztonsági zóna integráltan megvalósított behatolás jelző (riasztó) és beléptető rendszerrel van ellátva. A biztonsági zónát 24 órás videó kamerás megfigyelő rendszer is védi. A védett számítógépterembe az ott dolgozó bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és felügyelet mellett léphetnek be.

Az ügyfélszolgálati irodába önállóan csak az erre feljogosított személyek léphetnek be, egy beléptető rendszer felügyelete alatt.

5.1.3. Áramellátás, légkondicionálás

A Szolgáltató védekezik a nem megfelelő hőmérsékletből vagy áramellátásból eredő hibák és adatvesztések ellen.

Áramellátás

A hitelesítő szervezet védett számítógéptermének zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében. Ez a következő – egységes tervezéssel megalapozott, a vonatkozó szabványoknak megfelelő – védelmi megoldások együttműködésével biztosított:

- akkumulátoros szünetmentes energiaellátás,
- dízelmotoros generátoregység,
- villamos zavar-, villám- és túlfeszültség-védelem,
- A háttérrendszeren működő szerverterem folyamatos áramellátását
  - akkumulátoros szünetmentes energiaellátás és
  - villamos zavar-, villám- és túlfeszültség-védelem,

  biztosítják.

Légkondicionálás

A hitelesítő szervezet védett számítógépterme hűtésigényének kiszolgálását két klímaberendezés együttes működése biztosítja. A klímaberendezések elhelyezésének módja biztosítja, hogy azok karbantartása ne okozzon zavart gépterem működésében.

5.1.4. Beázás és elárasztás veszélyeztetettsége

A hitelesítő szervezet biztonsági zónájának kialakítása során fontos szempont volt a beázás és elárasztódás veszélyének minimalizálása. A biztonsági zóna teljes területe mentes a vizesblokkoktól, illetve a közelben nincs sem csatorna sem vízvezeték. A védett számítógépteremben a fenti biztonságot tovább növeli az álpadló alkalmazása.

5.1.5. Tűzmegelőzés és tűzvédelem

A hitelesítő szervezet géptermében tűzvédelmi rendszer működik, melyet az illetékes tűzoltó parancsnokság jóváhagyott.

5.1.6. Adathordozók tárolása

A hitelesítő szervezet operátori helyiségében egy kódzáras tűzálló páncélszekrény gondoskodik az adathordozók biztonságos tárolásáról. Az ügyfélszolgálati irodában is páncélszekrény szolgál az adathordozók biztonságos tárolására.

5.1.7. Selejt kezelése és megsemmisítése

A hitelesítő szervezet biztonsági zónájában a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat még tartalmuk törlése után sem használják fel nem bizalmas minősítésű adatok tárolására. A feleslegessé vált, bizalmas minősítésű adatokat

tartalmazó adathordozókat – a Szolgáltató selejtezési szabályzatának megfelelően – fizikailag megsemmisítik:

- a papíralapú dokumentumokat zúzógéppel felaprítják;
- a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprítják;
- a merevlemezeket összetörik;
- az optikai lemezeket összetörik.

5.1.8. Fizikailag elkülönítetten őrzött mentési példányok

A hitelesítő szervezet biztonság-kritikus szolgáltatásaira vonatkozó adatok mentési példányait a háttérrendszer biztonsági zónájában tárolják.

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 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 ellenőrének ellenőrzési tevékenysége biztosítja.

5.2.1. Bizalmi szerepkörök

A Szolgáltató a következő bizalmi szerepköröket határozza meg az alábbi felelősségkörökkel:

A Szolgáltató informatikai rendszeréért átfogóan felelős vezető: Az e-Szignó Hitelesítés Szolgáltató igazgatója.

Biztonsági tisztviselő: Biztonságtechnikai főmunkatárs, a szolgáltatás biztonságáért általánosan felelős személy.

Rendszeradminisztrátor: Infrastruktúra adminisztrátor. Feladata a Szolgáltató rendszereinek telepítése, konfigurálása, karbantartása. Felelős a rábízott rendszerelemek megbízható és folyamatos működéséért, valamint a technológia fejlődésének nyomon követéséért, az egyes rendszerelemekben való biztonsági rések felderítéséért és megoldási javaslatok kidolgozásáért.

Regisztrációs felelős: A végfelhasználói tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy;

Perszonalizáció területén tevékenykedő tisztviselő: Feladata az intelligens kártyák gondozása, megszemélyesítése, valamint a tanúsítványkérelmek összeállítása.

Független rendszervizsgáló: A szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

Operátor: Rendszerüzemeltető, az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.

Ügyeletes tisztviselő: Feladata a 24 órás ügyelet biztosítása. Felelős az ügyelet elérhetőségéért, valamint azért, hogy a megérkező felfüggesztési és visszaállítási kérelmeket haladéktalanul feldolgozza a Szolgáltató biztonsági szabályzata szerint.

A fenti bizalmi munkakörökben dolgozó személyek a Szolgáltatóval munkaviszonyban állnak, megbízhatóságukról a Szolgáltató a biztonsági szabályzatában leírtak szerint bizonyosodott meg. A Szolgáltató biztonsági szabályzata meghatározza, hogy mely bizalmi szerepkörök olyanok, hogy egyazon dolgozó nem töltheti be őket. A bizalmi szerepkörök összeférhetetlenségével kapcsolatban a Szolgáltató teljesíti a 3/2005. IHM rendelet 7. § és 20. § (1) szerinti követelményeket, azaz:

- Az informatikai rendszerért általánosan felelős vezető nem lehet: biztonsági tisztviselő, független rendszervizsgáló.
- A biztonsági tisztviselő nem lehet: az informatikai rendszerért általánosan felelős vezető, rendszeradminisztrátor, független rendszervizsgáló.
- A rendszeradminisztrátor nem lehet: biztonsági tisztviselő, független rendszervizsgáló.
- A független rendszervizsgáló nem lehet: az informatikai rendszerért általánosan felelős vezető, biztonsági tisztviselő, rendszeradminisztrátor, regisztrációs felelős.
- A regisztrációs felelős nem lehet: független rendszervizsgáló.

A fentieken túl, a Szolgáltató a bizalmi szerepkörök teljes szétválasztására törekszik. [16]

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

Általánosan teljesül a hitelesítő szolgáltató egészére, hogy minden munkatárs csak a saját munkakörének megfelelő funkciókat aktivizálja. Két bizalmi munkakört betöltő személy együttes jelenléte szükséges a következő feladatok elvégzéséhez:

- a Szolgáltató magánkulcsának generálása,
- a Szolgáltató magánkulcsának biztonsági mentése (egy titkosított adatállományba),
- a Szolgáltató magánkulcsának visszaállítása,
- tanúsítvány kibocsátásához két személy, egy regisztrációs tisztviselő és egy perszonalizáció területén tevékenykedő regisztrációs tisztviselő szükséges

A Szolgáltató rendszerében minden bizalmi szerepkörhöz egyszerre legalább két munkatárs kell, hogy tartozzon.

5.2.3. Az egyes munkakörökben elvárt azonosítás és hitelesítés

Az informatikai rendszer minden felhasználója és az adminisztratív folyamatok minden szereplője személy szerint kerül azonosításra. Fizikai és logikai hozzáférés ellenőrzéshez a Szolgáltató intelligens kártyára épülő technológiát használ. Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani. A Szolgáltató minden munkatársa pontosan annyi hozzáférési jogosultsággal rendelkezik, amennyi a feladatköre ellátásához elengedhetetlenül szükséges.

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. A Szolgáltató fontosnak tartja dolgozói folyamatos

képzését. E képzés egy része az új szabványok, jogszabályok folyamatos tanulmányozása és nyomon követése, egy másik része formális képzés.

Felvételi követelményként a Szolgáltató minden dolgozója számára legalább középfokú végzettséget ír elő, de a Szolgáltató a továbbiakban is gondot fordít arra, hogy dolgozói megfelelő képzésben részesüljenek. Közvetlenül a felvételt követően a Szolgáltató új dolgozóit képzésben kell részesíteni, melynek keretében el kell sajátítania a munkája elvégzéséhez szükséges ismereteket. Regisztrációs tisztviselő szerepkört csakis olyan munkatárs tölthet be, aki olyan tanfolyamot végzett, amelyen elsajátította a Szolgáltató által elfogadott igazolványok (személyi igazolvány, útlevél és jogosítvány) felismerését. A Szolgáltató általában támogatja a dolgozók szakmai fejlődését, de el is várja, hogy a dolgozók saját szakterületükön önállóan fejlesszék tudásukat. A Szolgáltató bizonyos dolgozóinak munkaköri kötelessége a technikai és üzleti újdonságok felderítése és összegyűjtése, rendszerezése, és ezen ismeretek megosztása munkatársaikkal.

5.3.1. Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között kötelezően nem valósul meg.

5.3.2. A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs esetén, a munkakörbe kinevezéskor a foglalkoztatási dokumentumok részeként

- írásos tájékoztatást kapott jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról,
- munkaköri leírást kapott, mely tartalmazta az őt érintő biztonsági feladatokat,
- titoktartási nyilatkozatot írt alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is megfogalmazódtak.

Mindezek tartalmazzák azokat a munkajogi vagy büntető következményeket, melyek a különböző fegyelem- munkaköri kötelezettség- vagy törvénysértést szankcionálják. Amennyiben egy munkatárs (gondatlanságból fakadóan vagy szándékosan) megsérti a fenti szabályokat, ellene büntető intézkedéseket hoznak (melyek az elkövetés módjától és következményétől függően a jutalom megvonástól fegyelmi eljárás indításán és kártérítésen át, egészen a hatósági feljelentésig terjedhet).

5.3.3. A szerződéses alkalmazottakra vonatkozó követelmények

A Szolgáltató bizalmi munkakörben csak vele munkaviszonyban álló személyt alkalmaz.

Az egyéb feladatok ellátására, alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket (külső munkavállalókat és ideiglenes alkalmazottakat egyaránt) a Szolgáltató lehetőleg a korábban már minősített beszállítók listájáról választ. A beszállítókkal a Szolgáltató olyan írásos szerződést köt, melyben beszállító elfogadta a Szolgáltató biztonságpolitikájának a beszállító tevékenységére vonatkozó részeit.

Valamennyi szerződő fél – még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismerendő üzleti/vállalati titkokat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is. A külső munkavállalók és ideiglenes alkalmazottak szakmai kiképzésben, továbbképzésben nem részesülnek, erre nem kötelezettek.

5.3.4. A személyzet számára biztosított dokumentációk

Minden bizalmi munkakört betöltő munkatárs, írásban megkapja a következő dokumentumokat:

- A Szolgáltató szervezeti biztonsági szabályzata,
- aláírt titoktartási nyilatkozat,
- egyéni munkaköri leírás,
- a tervezett és rendkívüli továbbképzések alkalmával megkapja az adott oktatási formához tartozó oktatási segédanyagokat is.

A szervezeti biztonsági szabályzatban bekövetkező változásokról írásos értesítők formájában mindenki tájékoztatást kap.

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. A 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.

5.4.1. A tárolt események típusai

A hitelesítési rendszer által a hitelesítő és a regisztráló egységekhez történő valamennyi hozzáférés és tevékenység naplózásra kerül. Így naplózásra kerül:

- valamennyi regisztrációval kapcsolatos esemény,
- a tanúsítványok életciklusával kapcsolatos összes esemény,
- a kulcsok életciklusával kapcsolatos események,
- az intelligens kártyák elkészítésével, megszemélyesítésével kapcsolatos valamennyi esemény,
- viszontazonosítás kérelmek és válaszok,
- az esetleges hibaesemények.

5.4.2. A napló állomány feldolgozásának gyakorisága

A Szolgáltató naplóbejegyzéseinek átvizsgálása minden munkanapon megtörténik. A Szolgáltató hálózati védelmi riasztás funkciókkal is rendelkezik az erőforrásokhoz történő jogosulatlan hozzáférés észlelésének jelzésére. Ilyen riasztási esetekben a naplóbejegyzéseket soron kívül átvizsgálják. Rendellenességek észleléskor, reklamáció esetén, vagy egyéb megkeresések kapcsán szintén sor kerülhet a napló adatok rendkívüli átvizsgálására.

5.4.3. A napló-állomány megőrzési időtartama

Az adatokat egyszer írható médiára archiválják, és a napló-állományok archív adathordozóit biztonságosan megőrzik a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított 10 évig, illetőleg a velük kapcsolatban esetleg felmerült jogvita jogerős lezárásáig.

Ezen időtartamig a Szolgáltató biztosítja az archivált adatok olvashatóságát. A Szolgáltató megőrzi az ehhez szükséges szoftver és hardver eszközöket.

5.4.4. A napló állomány védelme

Szolgáltató hitelesítési rendszerének naplóbejegyzéseit a Szolgáltató időbélyeggel látja el, a naplóbejegyzések törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A napló állományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében Szolgáltató gondoskodik az adatok bizalmas tárolásáról. A napló állományokhoz való hozzáférésre csak azok jogosultak, akiknek

erre munkakörük folytán szükségük van. A Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a Szolgáltató biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

5.4.5. A napló állomány mentési folyamatai

A naplóállományok minden munkanapon (az átvizsgálást megelőzően) mentésre kerülnek egyszer írható médiára aláírt formában. A média elzárva és fizikailag is elkülönítetten megőrzésre kerül.

A mentés operatív folyamatait Szolgáltató mentési szabályzatai írják le részletesen.

5.4.6. A napló gyűjtési rendszere

A naplóbejegyzéseket az alkalmazások automatikusan gyűjtik és tárolják a napló állományokban. A mentett médiákat Szolgáltató napi rendszerességgel begyűjti. A médiákat a Szolgáltató saját munkatársai szállítják a megőrzési helyre.

5.4.7. Az eseményeket kiváltó ügyfelek értesítése

A naplóbejegyzéseket kiváltó személyeket, szervezeteket és alkalmazásokat a Szolgáltató nem értesíti, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában közreműködő ügyfeleknek (az Aláírónak és az Előfizetőnek) ilyen esetben kötelessége a Szolgáltatóval való együttműködés.

5.4.8. Sebezhetőség felmérése

A naplóbejegyzések feldolgozása során Szolgáltató a naplózott események alapján a sebezhetőségre vonatkozó felméréseket végez. A napi rendszerességgel végzett feldolgozáson túl Szolgáltató szakemberei havonta áttekintik a rendkívüli eseményeket és ezek alapján a sebezhetőségre vonatkozó elemzéseket végeznek. Ezen elemzések alapján Szolgáltató lépéseket tesz a rendszer biztonságának javítására.

5.5. Adatok archiválása

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

5.5.1. A tárolt események típusai

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.

5.5.2. Az archívum megőrzési időtartama

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.

5.5.3. Az archívum védelme

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.

5.5.4. Az archívum mentési folyamatai

A Szolgáltató a papíron tárolt adatairól másodpéldányokat tárol, az eredeti példányától különböző helyszínen, fizikailag elkülönítve.

5.5.5. A rekordok időbélyegzésére vonatkozó követelmények

Lásd: 5.5.3. fejezet.

5.5.6. Az archívum gyűjtési rendszere

A regisztráció során keletkezett papíralapú iratokat a Szolgáltató által működtetett adattárban tárolják és őrzik.

5.5.7. Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés az ügyfelek számára a rájuk vonatkozó adatokhoz lehetséges, más feleknek a 9. fejezetben leírtak szerint.

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.

5.6.1. Sérült számítási erőforrások, szoftverek és/vagy adatok

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.

5.6.2. A szolgáltatói egység nyilvános kulcsának visszavonása

A szolgáltatói nyilvános kulcsok visszavonásáról Szolgáltató az 1.3.1. fejezetnek megfelelően értesítést tesz közzé.

5.6.3. Egy szolgáltatói egység kulcsának kompromittálódása

Szolgáltató katasztrófa elhárítási terve a szolgáltatói magánkulcsok kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs és a hozzá tartozó tanúsítvány 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 Szolgáltató valamely hitelesítő egység kulcsának kompromittálódása esetén haladéktalanul megszünteti az adott kulcs használatát.

Amennyiben az adott hitelesítő egység számára – jogszabály vagy hitelesítés szolgáltatók közötti szerződés vagy megegyezés alapján – másik hitelesítés szolgáltató is bocsátott ki tanúsítványt, és felül- vagy kereszthitelesítette a Szolgáltató ezen hitelesítő egységét, a Szolgáltató az adott kulcs kompromittálódása esetén haladéktalanul értesíti ezen másik hitelesítés szolgáltatót, és kezdeményezi az érintett kulcshoz tartozó tanúsítvány visszavonását. A közigazgatási területen felhasználható tanúsítványokat kibocsátó hitelesítő egységek kulcsának kompromittálódása esetén ez a Közigazgatási Gyökér Hitelesítés Szolgáltató értesítését jelenti.

5.6.4. Helyreállás természeti vagy más katasztrófát követően

Szolgáltató elsődleges működési helyszínein kívül másodlagos helyszínnel is rendelkezik. Természeti vagy más katasztrófát követően, illetve Szolgáltató berendezéseinek olyan mértékű meghibásodását illetően, mely az elsődleges rendszeren nem kezelhető, Szolgáltató a másodlagos helyszínen is képes szolgáltatásainak beindítására.

Ilyen esetekben Szolgáltató a következő szolgáltatások legfeljebb 24 órán belüli elindítását vállalja

- a tanúsítványtár közzététele szolgáltatás;
- a felfüggesztés és visszavonás kezelés szolgáltatás;
- a visszavonási állapot közzététele szolgáltatás;
- az időbélyegzés szolgáltatás.

elérhetőségének biztosítását.

5.7. A szolgáltatások leállítása

A Szolgáltató a Szolgáltatások valamelyikének tervezett megszüntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Hatóságot.

A hitelesítés szolgáltatás és online tanúsítvány-állapot szolgáltatás leállítása

A Szolgáltató a szolgáltatás leállítására vonatkozó bejelentéssel egyidejűleg leállítja a következő szolgáltatásait:

- regisztráció
- tanúsítvány-előállítás,
- tanúsítvány-kibocsátás,
- intelligens kártyák megszemélyesítése,
- tanúsítványcsere.

A Szolgáltató a tervezett megszűnés előtt legalább 20 nappal intézkedik a végfelhasználói tanúsítványok visszavonásáról. Ezzel egyidejűleg leállítja a következő szolgáltatásait:

- tanúsítvány visszavonás/felfüggesztés kezelés,

A megszűnés időpontjával egyidejűleg a Szolgáltató a következő szolgáltatásokat állítja le:

- információ szolgáltatás,
- tanúsítvány közzététel,
- tanúsítvány visszavonási állapot közzététele,
- online tanúsítvány-állapot szolgáltatás.

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait, a bizalmas felhasználói adatokkal együtt a 9.3 fejezet szerint mindenképpen átadja egy ilyen szolgáltatónak, egyéb szolgáltatásait a tárgyalások eredményétől függően.

A szolgáltatói tanúsítványok visszavonásáról (és a magánkulcsok megsemmisítéséről) – a tárgyalások eredményétől függően – a Szolgáltató fokozatosan intézkedik a 60 napos időszakban.

A Szolgáltató a tárgyalások végeredményéről tájékoztatja a végfelhasználókat és a Hatóságot. A Szolgáltató az Ügyfeleket elektronikus levélben, az Érintett feleket a honlapján történő közzététel útján tájékoztatja. A Szolgáltató a Microsec e-Szigno Root CA, Microsec e-Szigno Root CA 2009 és az e-Szigno OCSP CA tanúsítványának visszavonását 5 nappal megelőzően a 2.1. fejezetnek megfelelően hirdetményt tesz közzé.

Amennyiben egy gyökér hitelesítő egység tanúsítványának érvénytelenné válásával valamely időbélyegző egység tanúsítványa is érvénytelenné válik, vagy más CA által kiadott tanúsítványról kell gondoskodni az időbélyegző egység számára, vagy az időbélyegzés szolgáltatást is meg kell szüntetni.

A Szolgáltató a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített időbélyegzővel ellátott mentést készít.

A Szolgáltató biztosítja, hogy a visszavont, illetőleg felfüggesztett tanúsítványok nyilvántartásában szereplő adatokat szükség esetén az arra jogosult harmadik felek értelmezhessék.

A Szolgáltató – annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak – az adatokat az új szolgáltató által fogadóképes médián és formátumban helyezi el vagy biztosítja az új szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, amelyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

Az időbélyegzés szolgáltatás leállítása

A Szolgáltató a szolgáltatás tervezett megszüntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Hatóságot.

A Szolgáltató az időbélyegzés szolgáltatási tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített időbélyegzővel ellátott mentést készít.

A szolgáltatás leállításakor az időbélyegzők tanúsítványait vissza kell vonni. A Szolgáltató a tanúsítvány visszavonását 5 nappal megelőzően hirdetményt tesz közzé. (2.1. fejezet)

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. Kulcspár előállítás

A Szolgáltató az alábbi kulcspárokat használja:

- A Szolgáltató gyökér hitelesítő egységének kulcsai 2048 bitesek.
- A Szolgáltató köztes hitelesítő egységeinek (köztük a végfelhasználói tanúsítványokat kibocsátó hitelesítő egységek) kulcsai 2048 bitesek.
- A szolgáltató időbélyegző egységeinek kulcsa 2048 bites.
- A Szolgáltató OCSP válaszadóinak tanúsítványát aláíró hitelesítő egységek kulcsa 2048 bites.
- Az SHA-1 alapú tanúsítványokra vonatkozó OCSP válaszokat aláíró kulcsok 1024 bitesek.
- Az SHA-256 alapú tanúsítványokra vonatkozó OCSP válaszokat aláíró kulcsok 2048 bitesek.
- Az SSL protokollhoz felhasznált kulcsok 2048 bitesek.
- A Szolgáltató belső folyamataiban felhasznált kulcsok 2048 bitesek.
- A végfelhasználók tanúsítványaiban szereplő kulcsok 1024 vagy 2048 bitesek.

A tanúsítványok és időbélyegzők kibocsátására használt szolgáltatói kulcsokat a Szolgáltató biztonságos hardvermodulban generálja, e magánkulcsok a (6.2.4. fejezetben részletezett) mentést leszámítva, teljes életciklusukat a kriptográfiai hardver modulokban töltik, megsemmisítésükig soha sehová nem kell őket továbbítani.

Amennyiben a végfelhasználók tanúsítványaihoz használt kulcspárait a Szolgáltató generálja, akkor erre fizikailag biztonságos környezetben kerül sor. A kulcs ezt követően intelligens kártyára kerül, és a végfelhasználókhoz való továbbítása magának az intelligens kártyának a végfelhasználóhoz történő továbbítását jelenti.

Amennyiben a végfelhasználók tanúsítványaihoz használt kulcspárait nem a Szolgáltató generálja, az alkalmazott kulcsméret a Szolgáltató által generált, azonos célra szolgáló, kulcsméretnél ekkor sem lehet kisebb.

6.1.2. Magánkulcs eljuttatása a tulajdonoshoz

Mivel a Szolgáltató valamennyi kulcspárja helyben generálódik, így azok magánkulcsait nem kell sehová továbbítani.

Amennyiben a végfelhasználó magánkulcsát a Szolgáltató generálja, akkor a magánkulcs védett tárolását és felhasználását biztosító intelligens kártyával együtt a regisztrációs ponton személyesen megjelenő Aláíróknak adja át (a kártyát aktivizáló kódot tartalmazó zárt borítékkal együtt). A kulcsgenerálást követően a magánkulcsot tartalmazó eszköz ún. transport módban van, ez biztosítja, hogy a kártyán lévő kulcsokkal nem történhet visszaélés.

A Szolgáltató (vagy a Szolgáltatóval szerződésben lévő külső regisztrációs szervezet) regisztrációs munkatársa csakis az Aláírónak adhatja át az intelligens kártyát és a hozzá tartozó (az aktiváló kódokat tartalmazó) borítékot, a regisztrációs munkatárs ilyenkor naplózza az átadás pontos idejét.

Amennyiben a végfelhasználó magánkulcsát az Aláíró generálja, akkor a magánkulcsot nem kell eljuttatni hozzá.

6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A szolgáltatói kulcsokat a Szolgáltató saját maga generálja, így nem kell őket hozzá eljuttatni. Amennyiben a Szolgáltató számára más hitelesítés szolgáltató – például a KGYHSZ – tanúsítványt bocsát ki, akkor a Szolgáltató biztonságos csatornán juttatja el saját nyilvános kulcsát.

Amennyiben a végfelhasználók kulcsait a hitelesítő szervezet generálja, a nyilvános kulcsot nem szükséges sehova sem továbbítani.

Amennyiben a végfelhasználó maga generálja a kulcspárját, akkor a 3.2.1. fejezetben leírt mechanizmusok (pl. PKCS#10), valamint SSL csatornán történő kommunikáció biztosítja,

hogy a hitelesítő szervezethez valóban a megfelelő nyilvános kulcs jut el.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

Lásd: 1.3.1. fejezet.

6.1.5. Kulcs méretek

Az egyes kulcsok hosszát a 6.1.1. fejezet tartalmazza.

6.1.6. A nyilvános kulcs paraméterek előállítása

A Szolgáltató tanúsítvány és időbélyegző aláírására minden esetben a Hatóság Eat. 18. § szerint kibocsátott határozata [17] 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-1 vagy SHA-256 lehet. Az SHA-256 alapú végfelhasználói tanúsítványokhoz kapcsolódó rendszerében a Szolgáltató az SHA-256 lenyomatképző függvényt használja. A Szolgáltató a későbbiekben további lenyomatképző függvényt is bevezethet.

6.1.7. 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.

A rendszerben használt valamennyi kriptográfiai hardver modul képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül. A modulokat az ezzel megbízott bizalmi munkakört betöltő munkatársak rendszeres időközönként tesztelik.

A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám generálásukat.

6.1.8. Hardver/szoftver kulcselőállítás

A Szolgáltató tanúsítványok és időbélyegzők kibocsátására használt kulcsainak generálása nCipher nShield F3 hardver eszközzel történik amely FIPS 140-1 szabvány szerint 3. szinten bevizsgált HSM.

A Szolgáltató a végfelhasználói kulcsokat, illetve a saját belső működéséhez szükséges kulcsokat biztonságos környezetben, kizárólag bizalmi munkakört betöltő személyek jelenlétében generálja.

6.1.9. A kulcs használat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)

A „kulcs használati" (Key Usage) mezők lehetséges (egyúttal kötelezően kitöltendő) értékei az alábbiak:

A hitelesítő szervezet kulcsai

- A Szolgáltató hitelesítő egységeinek kulcsai:
  "`keyCertSign`", "`CRLSign`" (kritikus)
- Az időbélyegző központ aláíró kulcsai:
  "`NonRepudiation`" és "`digitalSignature`" (kritikus),
  az „Extended Key Usage" mezőben: "`timeStamping`"
- A szolgáltató OCSP válaszadójának kulcsa:
  "`digitalSignature`", "`nonRepudiation`" (kritikus)
  az „Extended Key Usage" mezőben: "`OCSPSigning`"

Az Aláírók kulcsai

- A végfelhasználói aláíró kulcs:
  "`nonRepudiation`" és "`digitalSignature`" (kritikus)
  Kiterjesztett kulcshasználat: "`secureEmail`".
  A hozzá tartozó magánkulcs kizárólag aláírás létrehozására használható.

A kulcsokat kizárólag a fent leírt célokra szabad használni, amelyeket a Szolgáltató a kulcsokhoz tartozó tanúsítványokban feltüntet.

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 ugyanazt a magánkulcsot használja a kibocsátott tanúsítványok és a rájuk vonatkozó visszavonási listák aláírásra.

A Szolgáltató a hitelesítő szervezet a tanúsítványok és időbélyegzők kibocsátására használt magánkulcsait fizikailag biztonságos helyszínen, biztonságos hardvermodulban tárolja.

A Szolgáltató a végfelhasználók kulcsait a kulcsok átadása előtt fizikailag biztonságos helyszínen, intelligens kártyán tárolja.

6.2.1. Kriptográfiai modulra vonatkozó szabványok

A Szolgáltató kulcsainak generálása egy nCipher nShield F3 hardver eszközzel történik amely FIPS 140-1 szabvány szerint 3. szinten bevizsgált HSM. A Szolgáltató hitelesítő szervezetének kulcsait ezen modulokban tárolja.

6.2.2. A több-szereplős („n-ből m") magánkulcs visszaállítás ellenőrzése

A Szolgáltató a hitelesítő szervezetben alkalmazza az „n-ből m" ellenőrzést a magánkulcsokkal kapcsolatos kulcsgondozási funkciók aktivizálásánál.

6.2.3. Magánkulcs letétbe helyezésére és visszaállítására vonatkozó szabályzat

A Szolgáltató saját magánkulcsát nem helyezi letétbe.

A Szolgáltató az Aláírók magánkulcsait sem helyezi letétbe.

6.2.4. Magánkulcs mentése

A Szolgáltató hitelesítő szervezetének magánkulcsait a 6.2.1. fejezetben leírt biztonságos hardver modul segítségével menti. A mentés során a magánkulcs titkosított formában hagyja el a modult, e titkosított kulcsot később másik modulba be lehet tölteni. Mind a lementés, mind a visszatöltés csakis a 6.2.2. fejezetben leírt védelmi mechanizmus mellett alkalmazható.

6.2.5. Magánkulcs archiválása

A Szolgáltató a 6.2.4. fejezetben leírtakon kívül nem archiválja magánkulcsát.

6.2.6. Magánkulcs bejuttatása a kriptográfiai modulba

A Szolgáltató csakis a 6.2.2. fejezetben leírt módon juttat be magánkulcsot a biztonságos hardver modulba.

6.2.7. A magánkulcs aktivizálásának módja

A hitelesítő szervezet magánkulcsa biztonságos hardver modulban helyezkedik el, e hardvermodult a hozzá tartozó operátori kártyákkal lehet aktiválni. A hardvermodulban lévő magánkulcsokat a modul aktiválása előtt nem lehet használni. A hardvermodulhoz tartozó operátori kártyákat a Szolgáltató biztonságos környezetben tárolja és e kártyákat kizárólag a Szolgáltató erre jogosult munkatársai érhetik el.

Az Aláírók magánkulcsát a Szolgáltató biztonságos aláírás-létrehozó eszközön generálja és tárolja. Mielőtt a Szolgáltató átadja ezen eszközt az Aláírónak, a biztonságos aláírás-létrehozó eszköz ún. transport módban van, az így védett eszköz segítségével nem lehet aláírást készíteni. Amikor az Aláíró átveszi a biztonságos aláírás-létrehozó eszközt, egy lezárt borítékban kapja meg az aktiválásához szükséges kódokat. Az Aláíró az eszköz átvételekor állítja be saját aláírói PIN kódját.

A kártya aktiváló kódja ezt követően csakis az Aláíró birtokában van, a következőkben az Aláíró felel e kód biztonságos tárolásáért és használatáért.

A nem intelligens kártyán tárolt kulcsok kezelése az Aláíró felelőssége.

6.2.8. A magánkulcs aktív állapotának megszüntetési módja

Az nCipher nShield HSM kriptográfiai hardver modul magánkulcsa akkor deaktiválódik, ha a modul (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

- a felhasználó deaktiválja a kulcsot,
- a modul áramellátása megszakad (kikapcsolás vagy tápellátási probléma),
- a modul hibaállapotba kerül.

Az így deaktivált magánkulcs mindaddig nem használható, amíg a modul ismét aktív állapotba nem kerül.

Az intelligens kártyák magánkulcsai akkor deaktiválódnak, ha az intelligens kártya (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

- az intelligens kártyát kiveszik az olvasó egységből,
- a felhasználó deaktiválás (pl. logout) parancsot ad ki az alkalmazáson keresztül,
- az intelligens kártya külső (az olvasó felöl kapott) áramellátása megszakad,
- az intelligens kártya hibaállapotba kerül.

Az így deaktivált magánkulcsok mindaddig nem használhatók, amíg az intelligens kártya ismét aktív állapotba nem kerül.

A nem intelligens kártyán tárolt kulcsok kezelése az Aláíró felelőssége.

6.2.9. A magánkulcs megsemmisítésének módja

A hitelesítő szervezet biztonságos hardvermoduljában tárolt magánkulcsok megsemmisítése a Szolgáltató két munkatársának (egy infrastruktúra adminisztrátor és egy biztonsági tisztviselő) együttes jelenlétében lehetséges.

A végfelhasználói tanúsítványokhoz kapcsolódó magánkulcsok megsemmisítése az Aláíró felelőssége.

Amennyiben az ügyfél a Szolgáltató ügyfélszolgálati irodájába személyesen elvisz egy intelligens kártyát, a Szolgáltató vállalja a kártya az ügyfél előtt történő megsemmisítését.

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, illetve a tanúsítvánnyal (vagy a tanúsítványra épülő elektronikus aláírással) kapcsolatban felmerült jogvita jogerős lezárásáig. A Szolgáltató ugyanezen időtartamig megőriz olyan eszközöket, amelyekkel a tanúsítvány tartalma megállapítható.

6.3.2. A nyilvános és magánkulcsok használatának periódusa

A hitelesítő szervezet kulcsai. A gyökér hitelesítő egységek kulcsainak és tanúsítványainak érvényességi ideje:

- A Microsec e-Szigno Root CA gyökér hitelesítő egység kulcsa 2017. április 6-áig érvényes.
- A e-Szigno OCSP CA gyökér hitelesítő egység kulcsa 2015. április 14-éig érvényes.
- A Microsec e-Szigno Root CA 2009 gyökér hitelesítő egység kulcsa 2029. december 30-áig érvényes.

A Szolgáltató köztes (nem gyökér) hitelesítő egységeinek kulcsai a hozzájuk tartozó tanúsítványok érvényességi idejének lejártáig érvényesek.

A Szolgáltató SHA-1 alapú időbélyegző egységeinek kulcsai a hozzájuk tartozó tanúsítványok érvényességi idejének lejártáig érvényesek.

A Szolgáltató az SHA-256 alapú időbélyegző egységei számára 12 évig érvényes időbélyegző tanúsítványokat bocsát ki. A Szolgáltató minden egyes időbélyegző kulcsot 1 évig használ, ezt követően a régi kulcsot megsemmisíti. A Szolgáltató évente új kulcsokkal és tanúsítványokkal látja el SHA-256 alapú időbélyegző egységeit.

A Szolgáltató OCSP válaszadójának kulcsának érvényességi ideje 12 év. A szolgáltató OCSP válaszadójának kulcsához tartozó tanúsítvány érvényességi ideje legfeljebb 1 nap.

Aláírók kulcsai. Az Aláírók kulcsainak érvényességi idejét jelen Szabályzat nem korlátozza, de a Szolgáltató egyazon kulcshoz legfeljebb 4 évre érvényes tanúsítványt bocsát ki.

Mind a szolgáltatói, mind a végfelhasználói kulcsok érvényességi idejét befolyásolhatja, ha a Hatóság Eat. 18. § szerinti határozata értelmében a tanúsítvány aláírására használt algoritmus már nem biztonságos, illetve nem alkalmas aláírások készítésére. Amennyiben ez bekövetkezik, a Szolgáltató visszavonja az érintett tanúsítványokat.

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

A Szolgáltató biztonságosan, véletlen szám generátor segítségével, fizikailag biztonságos körülmények között állítja elő az általa kibocsátott intelligens kártyák aktivizáló adatait.

6.4.2. Az aktivizáló adatok védelme

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

6.5. Számítógépes biztonsági óvintézkedések

6.5.1. Speciális számítógépes biztonsági műszaki követelmények

A Szolgáltató hitelesítő szervezete a következőkben leírt megbízható informatikai rendszereket és megoldásokat alkalmazza. Ennek megfelelően megbízható technológiákat alkalmaz, és rendszerét redundánsan alakította ki.

A Szolgáltató a pontos időt három referencia időforrásból nyeri. Egyrészt GPS-re, másrészt hosszúhullámú pontos idő szolgáltatásra (DCF77) támaszkodik. A Szolgáltató két független Stratum-1 időforrással rendelkezik, és ezekhez 0,1 másodperc pontossággal szinkronizálja saját belső óráját. E szinkronizációt a Szolgáltató naponta több, mint négy alkalommal végzi el. A Szolgáltató belső órájának helyességét a Szolgáltató biztonsági bizottsága évente ellenőrzi.

Ezen időforrásból származó időbélyeg szerepel a Szolgáltató elektronikus nyilvántartásain, naplófájljain is.

A Szolgáltató hitelesítő szervezete a hitelesítő egységeit és a fenti rendszerelemeket háromfokozatú tűzfalrendszerrel védi. Minden tűzfalból két példány működik, bármelyik kiesése esetén egy cluster segítségével a másik ugyanolyan egység átveszi a funkcióját. VPN technológia garantálja, hogy kizárólag a regisztrációs szervezet számítógépeiről lehet a hitelesítő szervezet számítógépeihez kapcsolódni a szolgáltatásokhoz kapcsolódó adminisztrációs tevékenység ellátása végett.

6.5.2. Informatikai biztonsági minősítés

A Hitelesítő Szervezet informatikai rendszerében alkalmazott kriptográfiai hardver modulok minősítésére vonatkozóan lásd a 6.2.1. fejezetet. A Szolgáltató biztonsági minősítéseit a 1.1.3. fejezet tartalmazza.

6.6. Életciklusra vonatkozó műszaki óvintézkedések

6.6.1. Rendszerfejlesztési 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.

6.6.2. Biztonságkezelési óvintézkedések

A Szolgáltató a szolgáltatások nyújtásához olyan termékeket használ, amelyek biztosítják a hitelesítési rend biztonságra vonatkozó elvárásait a helyes konfigurációt megalapozó megfelelő útmutató dokumentációk használatával.

6.6.3. Az életciklusra vonatkozó biztonság osztályozása

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

6.7. Hálózatbiztonsági óvintézkedések

Hitelesítő szervezet

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

letagadhatatlanság elvesztése ellen. A magas szintű védelmet titkosítással és digitális aláírással biztosítják.

Regisztráló szervezet

Az ügyfélszolgálati iroda informatikai rendszer segítségével egyáltalán nem folytat kommunikációt a végfelhasználókkal.

6.8. A kriptográfiai modulok ellenőrzése

A Szolgáltató által alkalmazott valamennyi kriptográfiai hardver modul ellenőrzésre, bevizsgálásra és értékelésre került.

7. Tanúsítvány, CRL, OCSP és időbélyegző profilok

7.1. Tanúsítvány profil

7.1.1. Tanúsítvány alapmezők

A Szolgáltató által kibocsátott végfelhasználói tanúsítványok alap mezői a következők:

- Verzió (Version)
  Szolgáltató az ITU X.509 „Információ technológia – Nyílt rendszerek kapcsolódása – Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer” ajánlás [6] 3. verziójának felel meg. Ennek megfelelően a verzió értéke `"3"` („V3”). A mezőbe kerülő érték az RFC 3280 által meghatározott kódolásban a V3-nak megfelelő érték, „0x2”.

- Sorozatszám (Serial Number)
  A tanúsítványt kibocsátó hitelesítő egység által generált egyedi azonosító.

- Algoritmus azonosító (Algorithm Identifier)
  A tanúsítványokat hitelesítő elektronikus aláírásának algoritmusának azonosítója (OID). A Szolgáltató a tanúsítványok hitelesítésére `"sha1WithRSAEncryption"` (`"sha1RSA"`) algoritmust használ.

  A mezőbe kerülő érték az sha1RSA algoritmus OID-je `"1.2.840.113549.1.1.5"`.

- Aláírás (Signature)
  A Szolgáltató által készített, a tanúsítványt hitelesítő elektronikus aláírás, amelyet a Szolgáltató az Algoritmus azonosítóban megadott algoritmussal hozott létre.

- Kibocsátó (Issuer)
  A tanúsítványt kibocsátó hitelesítő egység egyedi azonosítója egyedi X.501 név formátum szerint (lásd: 3.1.1. fejezet).

- Érvényesség (Valid From & Valid To)
  A tanúsítvány érvényességének kezdete és vége.

  Az időpontok UTC szerint és az RFC 3280-nak megfelelő kódolásban kerülnek rögzítésre.

- Az Aláíró azonosítója (Subject)
  Az Aláíró egyedi azonosítója egyedi X.501 név formátum szerint (lásd: 3.1.1. fejezet). Mindig kitöltésre kerül.

- Az Aláíró nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)
  A Szolgáltató az "`rsaEncryption`" („RSA”) algoritmust támogatja a végrelhasználói tanúsítványokban. A nyilvános kulcs hossza legalább 1024 bit.

  A mezőbe kerülő érték az rsaEncryption OID-je, azaz "`1.2.840.113549.1.1.5`".

- Az Aláíró nyilvános kulcsa (Subject Public Key Value)
  Az Aláíró nyilvános kulcsa.

- Kibocsátó egyedi azonosító (Issuer Unique Identifier)
  Nem kitöltött.

- Az Aláíró egyedi azonosítója (Subject Unique Identifier)
  Nem kitöltött.

7.1.2. Tanúsítvány X509 kiterjesztések

A Szolgáltató által kibocsátott végfelhasználói tanúsítványok kiterjesztései a következők:

- Hitelesítési rendek (Certificate Policies) – nem kritikus
  OID: 2.5.29.32

  E mező tartalmazza a tanúsítvány kiadása és használata során érvényes hitelesítési rend (lásd 1.2.2.fejezet) megnevezését, valamint a tanúsítvány alkalmazhatóságára vonatkozó egyéb információkat.

  - III. hitelesítési osztály
    PolicyIdentifier= "`1.3.6.1.4.1.21528.2.1.1.11`"
    (PolicyQualifierId = id-qt 1,
    Qualifier = "`http://www.e-szigno.hu/ASZSZ/`")

(PolicyQualifierId = id-qt 2,
Intelligens kártyán kibocsátott tanúsítvány esetén:
Qualifier = "ALE, regisztrációkor a személyes megjelenés kötelező"
Nem intelligens kártyán kibocsátott tanúsítvány esetén:
Qualifier = "Regisztrációkor a személyes megjelenés kötelező."

– II. hitelesítési osztály
PolicyIdentifier= "1.3.6.1.4.1.21528.2.1.1.10"
(PolicyQualifierId = id-qt 1,
Qualifier = "http://www.e-szigno.hu/ASZSZ/")
(PolicyQualifierId = id-qt 2,
Természetes személy számára kibocsátott tanúsítvány esetén:
Qualifier = "Regisztrációkor személyes megjelenés NEM történt."
Nem természetes személy számára kibocsátott tanúsítvány esetén:
Qualifier = "Regiszrációkor személyes megjelenés NEM történt. A tanúsítvány alanya nem természetes személy."

– A közigazgatási hitelesítési rendeknek megfelelő tanúsítványok
PolicyIdentifier= {A hitelesítési rend OID-je, lásd: 1.2.2. fejezet.}
(PolicyQualifierId = id-qt 1,
Qualifier = "http://www.e-szigno.hu/ASZSZ/")
(PolicyQualifierId = id-qt 2,
Qualifier = "A KGYHSZ elhárít minden felelősséget, amely az általa kiadott tanúsítvány használatából, visszavonásából, a szabályzat megsértéséből, a KGYHSZ magatartásából, intézkedéséből, vagy annak hiányából ered."

A Szolgáltató minden esetben kitölti ezen mezőt, és minden esetben megjelöl legalább egy olyan hitelesítési rendet, amely szerint a tanúsítványt kibocsátotta, és amely hitelesítési rend szerint később a tanúsítvánnyal kapcsolatban eljár. A Szolgáltató a kibocsátott tanúsítványokban feltünteti legalább egy ilyen hitelesítési rend azonosítóját (OID) és elérhetőségét (URL).

Amennyiben valamely tanúsítvány további hitelesítési rendeknek is megfelel – különösen a [11] dokumentumban leírt közigazgatási hitelesítési rendeknek, úgy a Szolgáltató ezen hitelesítési rendek azonosítóját és elérhetőségét (URL) is feltünteti a tanúsítványban.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
OID: 2.5.29.35

A tanúsítványt hitelesítő elektronikus aláírás létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.

A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.

- Aláíró kulcsazonosító (Subject Key Identifier) – nem kritikus
  OID: 2.5.29.14

  Az Aláíró nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
  A mező értéke: a nyilvános kulcs SHA-1 lenyomata.

- Aláíró alternatív nevei (Subject Alternative Names)
  OID: 2.5.29.17

  Lásd: 3.1.1. fejezet.

- Alapvető megkötések (Basic Constraints) – kritikus
  OID: 2.5.29.19

  Annak megadása, hogy a tanúsítvány CA számára lett-e kibocsátva. Végfelhasználói tanúsítványok esetében értéke „NEM”.

  A mező értéke: CA = `"FALSE"`.

- Kulcshasználat (Key Usage) – kritikus
  OID: 2.5.29.15

  A kulcs engedélyezett használati körének meghatározása. Lásd: 6.1.9. fejezet.

- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus

  A kulcs engedélyezett használati körének további meghatározása. Lásd: 6.1.9. fejezet.

- CRL szétosztási pont (CRL Distribution Points) – nem kritikus
  OID: 2.5.29.31

  Szolgáltató a tanúsítványok visszavonási állapotának ellenőrizhetősége érdekében folyamatosan közzéteszi a legfrissebb tanúsítvány visszavonási listát.

  A mező lehetséges értékeit a 4.10. fejezet tartalmazza.

- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.1

  A Szolgáltató által rendelkezésre bocsátott, a tanúsítvány használatához kapcsolódó egyéb szolgáltatásainak leírása.

  – Szolgáltató a tanúsítványok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást nyújt. A szolgáltatás elérhetőségét az egyes tanúsítványokkal kapcsolatban a 4.10. fejezet tartalmazza.

– A tanúsítványlánc felépítésének megkönnyítésére Szolgáltató megadja a tanúsítványt kibocsátó hitelesítési egység tanúsítványának elérési helyét.

A fenti mezők – az Aláíró alternatív nevei kivételével – mindig kitöltésre kerülnek. Más tanúsítvány kiterjesztés nem kerül kitöltésre.

A Szolgáltató által kibocsátott tanúsítványok a szabványoknak megfelelően tartalmazzák a Certificate Policies mezőt. Amennyiben egy tanúsítvány e mezőket nem tartalmazza, úgy teszt tanúsítványról van szó, amely kizárólag tesztelési célra használható, valós tranzakciók esetén el kell utasítani (1.2.3).

7.2. Tanúsítvány visszavonási lista (CRL) profil

7.2.1. Alap mezők

A Szolgáltató által kibocsátott visszavonási listák alap mezői a következők:

- Verzió (Version)
  A tanúsítvány visszavonási lista az RFC 3280 ajánlás 2. verziójának felel meg.
- Algoritmus azonosító (Signature Algorithm Identifier)
  Ez a szám a Szolgáltató visszavonási listát hitelesítő elektronikus aláírásának algoritmus azonosítója: SHA-1 (OID=1.2.840.113549.1.1.5).
- Aláírás (Signature)
  A Szolgáltató visszavonási listát hitelesítő elektronikus aláírása.
- Kibocsátó (Issuer)
  A visszavonási listát kibocsátó hitelesítő egység egyedi azonosítója (lásd: 1.3.1. fejezet). A visszavonási listát az adott hitelesítő egység a tanúsítványok aláírására használt kulcsával hitelesíti.
- Hatályba lépés (Effective Date)
  A visszavonási lista hatályba lépésének kezdete. A Szolgáltató által kibocsátott tanúsítványok esetében ez megegyezik a kibocsátás idejével. UTC szerinti érték az RFC 3280 szerinti kódolással.
- Következő kibocsátás (Next Update)
  A következő visszavonási lista kibocsátásának ideje (lásd: 4.10. fejezet). UTC szerinti érték az RFC 3280 szerinti kódolással.
- Visszavont tanúsítványok (Revoked Certificates)
  A visszavont tanúsítványok listája a tanúsítvány sorozatszámával és a visszavonás idejével.

7.2.2. Tanúsítvány visszavonási lista és Tanúsítvány visszavonási lista bejegyzés kiterjesztések

A Szolgáltató által használt visszavonás bejegyzési kiterjesztések a következők:

- Visszavonás oka (Reason Code) – nem kritikus
  Ebbe a mezőbe a visszavonás oka kerül.
- Érvénytelenség ideje (Invalidity Date) – nem kritikus
  Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerül.
- Útmutató a felfüggesztett tanúsítványokhoz (Hold Instruction) – nem kritikus
  Ebbe a mezőbe a felfüggesztett tanúsítvány kezelése kerül.

A Szolgáltató a kiterjesztéseket nem köteles kitölteni.

A Szolgáltató által kitöltött visszavonási lista kiterjesztések a következők:

- CRL sorozatszám (CRL number) – nem kritikus
  Ebbe a mezőbe a visszavonási listák egyesével növekvő sorozatszámai kerülnek.

7.3. Időbélyegző profil

Az alkalmazott időbélyegző profilt az RFC 3161: Time-Stamp Protocol (TSP) tartalmazza.

7.4. Online tanúsítvány-állapot válasz (OCSP) profil

Az alkalmazott online tanúsítvány-állapot válasz profilt az RFC 2560: Online Certificate Status Protocol tartalmazza.

Az Szolgáltató által kibocsátott OCSP válaszokkal kapcsolatban a 4.10. fejezet tartalmaz további információkat.

8. A megfelelőség vizsgálata

A Szolgáltató vizsgált és tanúsított elemeket (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz a szolgáltatásaihoz kapcsolódóan.

A Szolgáltató nShield F3 hardver kriptográfiai modult használ tanúsítványok és időbélyegzők aláírására, valamint szolgáltatói magánkulcsainak tárolására. E modul rendelkezik az Eat. 7 § (5) -(6) szerinti igazolással.

Az Aláírók részére a Szolgáltató a következő biztonságos aláírás-létrehozó eszközöket biztosíthatja:

- Intelligens kártyát, amely P8WE5032v0G mikrochipből, STARCOS SPK 2.3 v7.0 operációs rendszerből, valamint a StarCert v2.2 digitális aláírás alkalmazásból áll. (Gyártó: Giesecke & Devrient) E termék rendelkezik az Eat. 7 § (5) -(6) szerinti igazolással.
- Intelligens kártyát, amely ST19WR66I mikrochipből és Touch & Sign20048 V1.00 aláíró alkalmazásból áll. (Gyártó: ST Incard) E termék rendelkezik az Eat. 7 § (5) -(6) szerinti igazolással.
- Intelligens kártyát, amely SLE66CX322P mikrochipből és CardOS V4.3B aláíró alkalmazásból áll. (Gyártó: Siemens) E termék rendelkezik az Eat. 7 § (5) -(6) szerinti igazolással.

A Szolgáltató egyéb kártyákkal (illetve azokkal egyenértékű USB tokenekkel, valamint más kriptográfiai hardver eszközökkel) is jogosult a jelen Szabályzat szerint a Szolgáltatásokat nyújtani.

A Szolgáltató a szolgáltatások nyújtásához használt valamennyi rendszerelemet biztonsági osztályokba sorolta kockázat-menedzsment rendszere alapján. Ezen rendszerelemekről és a hozzájuk tartozó biztonsági besorolásról a Szolgáltató a kockázatmenedzsment rendszere keretében nyilvántartást vezet.

A Szolgáltató külső auditort vesz igénybe (lásd: 8.2. fejezet). A Szolgáltató e külső auditon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely rendszeresen vizsgálja a korábbi auditoknak való megfelelőséget, és eltérés esetén megteszi a szükséges lépéseket.

A Szolgáltató 2002 óta rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási, valamint 2003 óta a ISO 27001-nek (korábban BS 7799-nek) megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet auditál és vizsgál felül folyamatosan (lásd: 1.1.3. fejezet).

A Szolgáltató a közigazgatásban történő alkalmazásra is bocsát ki tanúsítványokat az 1.2.2. fejezetben meghivatkozott hitelesítési rendek szerint. A Nemzeti Hírközlési Hatóság vizsgálja, hogy a szolgáltató szabályzatai, valamint működése a közigazgatási felhasználásra tanúsítványt kibocsátók számára előírt követelményeket kielégíti-e.

8.1. Az ellenőrzések gyakorisága

A Szolgáltató évente külső megfelelőségi auditot hajt végre a Szolgáltatások nyújtását végző informatikai rendszerén.

8.2. Az auditor és szükséges képesítése

A rendszeres felülvizsgálatot a nyilvános kulcsú infrastruktúra területén többéves tapasztalattal rendelkező, a Nemzeti Hírközlési Hatóság által nyilvántartásba vett elektronikus

aláírás szakértő végzi.

8.3. Az auditor függetlensége

A Szolgáltató működését vizsgáló auditor a Szolgáltatótól függetlenül, és befolyástól mentesen végzi tevékenységét. Az auditor díjazása nem függ az audit során végzett tevékenységének megállapításaitól.

8.4. Az audit által érintett területek

Az audit az alábbi területeket fedi le:

- dokumentálás,
- folyamatok,
- fizikai biztonság,
- személyi állomány,
- műszaki biztonság,
- adatvédelem.

Az audit során megvizsgálásra kerül, hogy a Szolgáltató megfelel-e a hatályos jogszabályoknak – különösen az elektronikus aláírásról szóló [3] törvénynek és a [4] rendelet nem minősített szolgáltatókra vonatkozó részeinek – valamint hogy a Szolgáltatónál használt termékek (pl.: kriptográfiai modulok) megfelelő minősítéssel rendelkeznek-e. Az audit ezen kívül a Szolgáltató által támogatott hitelesítési rendeknek és időbélyegzési rendeknek (1.2.2. fejezet) való megfelelőség vizsgálatára irányul.

A közigazgatásban használható tanúsítványok kezeléséhez használt rendszerek és módszerek ellenőrzése az előző bekezdésben szereplő dokumentumokon túl a közigazgatás által közzétett [18], [8], [9], [10], [11] jogszabályoknak, illetve specifikációknak való megfelelőség vizsgálatára irányul.

8.5. Hiányosságok esetén végrehajtandó tevékenységek

A felügyeleti ellenőrzési eljárás vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató a Hatósággal megállapodott határidőn belül megszünteti a vizsgálatot végző Hatóságtól kapott információk alapján.

9. Üzleti és jogi tudnivalók

A Szabályzat hatálya alá eső Közösség (lásd: 1.3) kötelezettségeit és felelősségeit a vonatkozó szerződés és annak mellékletei (például jelen Szolgáltatási Szabályzat, illetve a vonatkozó hitelesítési rend) tartalmazzák. Az Előfizető jogait és kötelezettségeit az „e-Szignó Hitelesítés Szolgáltató – nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó – általános szerződési feltételek” [19] című dokumentumban szereplő általános szerződési feltételek is tartalmazzák.

9.1. Díjak és árak

A díjakat és árakat a Szolgáltató a honlapján közzéteszi és ügyfélszolgálati irodájában elérhetővé teszi. A Szolgáltató az árlistát módosíthatja. Az árlista módosítását a hatályba lépése előtt 15 nappal a Szolgáltató a honlapján közzéteszi. Az előre kifizetett szolgáltatások árát a módosítás nem érinti.

Az díjak kifizetésével és visszatérítésével kapcsolatos rendelkezéseket a szolgáltatási szerződés és mellékletei – különösen az általános szerződési feltételek – tartalmazzák.

9.2. Jogok, kötelezettségek és felelősség

9.2.1. A Szolgáltató kötelezettségei

A Szolgáltató alapvető kötelezettsége, hogy a Szolgáltatásokat a jelen Szolgáltatási Szabályzattal 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 szolgáltatások nyújtása a vonatkozó szabályzatok szerint,
- a Szolgáltatásokhoz 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 Szolgáltatások 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 Szolgáltató általános kötelezettségeit a vonatkozó hitelesítési és időbélyegzési rendek tartalmazzák.

A hitelesítő szervezet kötelezettségei

A hitelesítő szervezet feladata a hitelesítő egységek, valamint az online tanúsítvány-állapot és időbélyegzés szolgáltatáshoz szükséges egységek (lásd: 1.3.1) felállítása és működtetése, a tanúsítványtár és a visszavonási-állapot információ gondozása, az intelligens kártyák menedzselése és rendelkezésre bocsátása, valamint a szabályzatok menedzselése.

A hitelesítő szervezet belső működtetését a szolgáltató belső, operatív szabályzatai határozzák meg. A hitelesítő egységek által kibocsátott szolgáltatói tanúsítványok kezelése (regisztrációs munkatársak, ügyeletesek stb. számára) az operatív szabályzatok előírásainak megfelelően történik. Jelen szabályzat csak a végfelhasználói tanúsítványokkal kapcsolatban tartalmaz előírásokat.

A szabályzatok menedzselése keretében ellátandó feladatok:

- az alkalmazott tanúsítványfajták specifikálása, jóváhagyása és karbantartása,
- a Szolgáltatások nyilvános szabályzatainak és a belső (nem nyilvános) előírásoknak előkészítése, egyeztetése a jogszabályokkal és a belső (nem nyilvános) szabályzatokkal, továbbá az aktualizálások elvégzése,
- a Szolgáltatásokra vonatkozó szabályzatokkal kapcsolatos észrevételek rögzítése és javaslatok elbírálása.

A vonatkozó hitelesítési és időbélyegzési rend további kötelezettségeket tartalmazhat a hitelesítő szervezettel kapcsolatban.

A regisztráló szervezet kötelezettségei

Az ügyfélszolgálati iroda feladata a Szolgáltató képviselete a szolgáltatások kapcsán a végfelhasználónál. Ennek keretében a következő feladatokat látja el:

- Közreműködik a Szolgáltatások értékesítésében.
- Elvégzi az Aláíró regisztrációját.
- A különböző tanúsítvány műveletekre vonatkozó kérelmeket fogadja (felfüggesztés, visszavonás, visszaállítás, tanúsítványcsere).

- Fogadja és kezeli az adatmódosítási bejelentéseket.
- Közreműködik a visszavonási állapot közzétételében.
- Információs tevékenységet nyújt Ügyfelek és az Érintett felek részére Szolgáltató által nyújtott Szolgáltatásokkal kapcsolatos tevékenységeivel kapcsolatban.
- Tájékoztató anyagot bocsát az ügyfél rendelkezésére, amely tartalmazza a 3/2005 IHM rendelet 35 §-ban és az Eat. 9 § (1)-ben szereplő információkat. A regisztrációs szervezet regisztrációs munkatársa lehetővé teszi, hogy az ügyfél ezen tájékoztató anyagot alaposan áttanulmányozza, majd az ügyfél esetleges kérdéseit megválaszolja.

Az ügyfélszolgálati iroda kötelezettségeit a vonatkozó hitelesítési és időbélyegzési rend részletesen tartalmazza.

9.2.2. Az Előfizető jogai

- Az Előfizető jogosult a Szolgáltatások igénybe vételére a jelen Szolgáltatási Szabályzatban leírtak szerint.
- Az online tanúsítvány-állapot és időbélyegzés szolgáltatást közvetlenül az Előfizető veheti igénybe.
- Az elektronikus aláírás hitelesítés szolgáltatás esetén az Előfizető jogosult írásban meghatározni, hogy mely Aláíró kaphasson tanúsítványt, illetve az Előfizető jogosult e tanúsítványok felfüggesztését és visszavonását kérni.
- Az Előfizető jogosult a hozzá tartozó Aláíró számára ún. szervezeti ügyintézői jogosultságot kérni. A szervezeti ügyintézőkön keresztül az Előfizető jogosult a 24 órás telefonos ügyeleten keresztül kérni a III. hitelesítési osztályba tartozó (és a közigazgatási területen felhasználható) tanúsítványok felfüggesztését.

9.2.3. Az Előfizető kötelezettségei

Az Előfizető kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a Szolgáltatások felhasználása során, beleértve a tanúsítványok és magánkulcsok igénylését és alkalmazását. Az Előfizető kötelezettségeit a szolgáltatási szerződés és annak mellékletei – különösen az általános szerződési feltételek – és a vonatkozó hitelesítési és időbélyegzési rendek tartalmazzák.

9.2.4. Az Aláíró jogai

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

9.2.5. Az Aláíró kötelezettségei

- Az Aláíró köteles a szolgáltatás igénybe vétele előtt megismerni 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, időbélyegzővel vagy 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 jelen Szolgáltatási Szabályzatban meghatározott módon, az itt 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 vonatkozó hitelesítési rendek további kötelezettségeket tartalmazhatnak az Aláíró számára.

9.2.6. 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.

9.2.7. A Szolgáltató általános felelőssége

A Szolgáltató felelősségét jelen szolgáltatási szabályzat, a vonatkozó hitelesítési és időbélyegzési rendek, valamint az Ügyféllel kötött szerződés és annak mellékletei tartalmazzák.

- A Szolgáltató felelősséget vállal az általa támogatott hitelesítési és időbélyegzési rendekben 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 helytállni.
- A Szolgáltató nem felelős az abból adódó károkért, amikor valamely külső, elháríthatatlan esemény miatt az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.
- A Szolgáltató közhiteles adatbázissal végez adategyeztetést, mielőtt az Aláíró tanúsítványát kibocsátja. A Szolgáltató nem vállal felelősséget ezen közhiteles adatbázis által szolgáltatott információk pontatlanságából eredő károkért.
- A Szolgáltató kizárólag azért vállal felelősséget, hogy a Szolgáltatásokat a jelen Szolgáltatási Szabályzatban, illetve az abban meghivatkozott dokumentumokban (hitelesítési és időbélyegzési, 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 korlátozást az Ügyféllel kötött (szolgáltatási, illetve aláírói) szerződés tartalmazza. A Szolgáltató díjcsomagokat határoz meg a Szolgáltatásokkal kapcsolatban, amelyek a Szolgáltató pénzügyi felelőssége

korlátozásának mértékében térnek el egymástól. Az Ügyféllel kötött (szolgáltatási, illetve aláírói) szerződésben ezen díjcsomag megnevezése szerepel.

A hitelesítő szervezet felelőssége

Az e-Szignó Hitelesítés Szolgáltató felelős:

- az általa kibocsátott tanúsítványok és időbélyegzők 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

A regisztráló szervezet 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.

9.2.8. A Szolgáltató felelőssége a tanúsítványok és időbélyegzők ellenőrzésével kapcsolatban

A Szolgáltató kizárja felelősségét, amennyiben az Érintett fél nem körültekintően jár el a tanúsítványok és időbélyegzők felhasználása vagy ellenőrzése során, azaz nem a vonatkozó hitelesítési és időbélyegzési rend, nem jelen Szolgáltatási Szabályzat, illetve nem a hatályos jogszabályok szerint jár el.

9.2.9. 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.

9.2.10. 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, illetve jogosult a Képviselt Szervezet tanúsítványában szerepelni. Amennyiben a Képviselt Szervezet által kiállított valamely igazolásban szereplő információ megváltozik, a Képviselt Szervezet felelőssége ezt haladéktalanul jelenteni a Szolgáltatónak.

9.2.11. Az Előfizető felelőssége

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

9.2.12. Pénzügyi felelősség

A Szolgáltató pénzügyi felelőssége, valamint az esetleges megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében a jogszabályi előírásoknak megfelelő bankgaranciával rendelkezik.

A Szolgáltató ezen felül, a megbízhatóság biztosítása érdekében a jogszabályi előírásoknak megfelelő felelősségbiztosítással is rendelkezik.

A Szolgáltató iránti kártérítés

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.

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. Bizalmasság

A Szolgáltató az ügyfelek adatait a jogszabályoknak megfelelően kezeli. A Szolgáltató rendelkezik adatkezelési szabályzattal (lásd 9.4 fejezet), amely a személyes adatok kezelésével kiemelten foglalkozik.

Az ügyfél a tanúsítvány igénylésével, illetve a Szolgáltatói Szerződés aláírásával hozzájárul ahhoz, hogy a személyes adatait a Szolgáltató (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A hozzájárulás vonatkozik a törvény által meghatározott és nyilvántartásba vett információk harmadik félhez történő továbbítására a Szolgáltató szolgáltatásainak leállítása esetén, valamint – kizárólag a szolgáltatással összefüggő feladatok elvégzése céljából – a Szolgáltató alvállalkozóinak való továbbításra. A Szolgáltatási Szerződéshez tartozó tanúsítványkérelem űrlapon az Aláírónak nyilatkoznia kell arról, hogy hozzájárul a tanúsítvány nyilvánosságra hozatalához. A Szolgáltató az ügyfelek adatait kizárólag a szolgáltatásaival összefüggésben használja fel. Az Aláíró és a Képviselt Szervezet tanúsítványban szereplő adatait a Szolgáltató a tanúsítvánnyal együtt nyilvánosságra hozza, amennyiben az Aláíró ehhez hozzájárul. A tanúsítványba nem kerülő adataikat a Szolgáltató védett módon tárolja az Aláíró személyazonosságának, a Képviselt Szervezet szervezeti azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

A Szolgáltató a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi. A Szolgáltató az adatok megőrzése során gondoskodik az információk sértetlenségéről, bizalmasságáról és biztonságos tárolásáról. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja. A Szolgáltató gondoskodik a nem nyilvános információk bizalmasságáról és sértetlenségéről az ügyfelek adatainak továbbítása során, továbbá – megbízható rendszerek alkalmazásával és az adatok rendszeres archiválásával – a megfelelő rendelkezésre állásról.

9.3.1. Bizalmasan kezelendő információ-típusok

A Szolgáltató bizalmas információként kezeli az Ügyfelek minden adatát, kivéve azokat, amelyeket a 9.3.2. fejezetben nem bizalmasnak tekintett információnak minősít.

- A Szolgáltató a birtokába jutott bizalmas információt a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény rendelkezéseinek megfelelően kezeli, s csak a 9.3.2. fejezetben említett esetekben és személyek/szervezetek részére fedi fel őket.
- A Szolgáltató bizalmas információként kezeli a következő adatokat és dokumentumokat az előbbieken kívül:
  - magánkulcsok és aktivizáló kódok,
  - tanúsítványigénylések és Szolgáltatási Szerződések,
  - tranzakciós és napló adatok,
  - nem nyilvános szabályzatok,
  - minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

9.3.2. Nem bizalmasnak tekintett információ típusok

Amennyiben az Aláíró ehhez hozzájárul, a Szolgáltató nem bizalmas információként kezeli mindazon adatokat, amelyet a tanúsítványba belefoglal. Ezek az adatok a Szolgáltatási Szerződéshez kapcsolódó tanúsítványkérelem űrlapon egyértelmű jelöléssel szerepelnek.

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 7.2. fejezetben alfejezetben található.

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 [3] törvény 11.§ (2) bekezdése szerinti körben.

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

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 [3] törvény 11.§ (3) bekezdése szerinti körben.

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

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.

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 [3] törvény 16. § 2. bekezdése szerint.

9.4. Az ügyfelek adatainak kezelésére vonatkozó szabályzat

A Szolgáltató nyilvántartásában azonosító adatokat, tanúsítványban szereplő adatokat, 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 hitelesítés-szolgáltatás

esetében az adatok megőrzését az Eat. 9. § (7) bekezdése írja elő, az ott írt határidő eltelte előtt az adatokat az ügyfél kérésére sem lehet a Szolgáltató nyilvántartásából törölni.

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 és időbélyegzésszolgáltatások 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.

9.5. 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. Értelmezés és érvényesítés

9.6.1. 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.

A vonatkozó jogszabályok:

- 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.
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.
- 1959. évi IV. törvény a Polgári Törvénykönyvről.
- A közigazgatási hatósági eljárásról szóló 2004. évi CXL. törvény.
- 194/2005. (IX.22.) Korm. rendelet a közigazgatási hatósági eljárásokban használt elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés szolgáltatókra vonatkozó követelményekről.
- 195/2005. (IX.22.) Korm. rendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról.

9.6.2. Érvénytelenség, fennmaradás, megszűnés és értesítések

Érvénytelenség

Amennyiben a Szolgáltatási Szabályzat valamely pontja érvénytelen lenne, az a Szolgáltatási Szabályzat egészének és más pontjainak érvényességét nem érinti.

Fennmaradás

A Szolgáltatási Szabályzat 9. fejezete érvényben marad a Szabályzat hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, amelyet a Szolgáltató a Szabályzat hatálya alatt bocsátott ki.

Megszűnés

A Szolgáltatási Szabályzat az 1.3.4. fejezetben szereplő közösség valamennyi kötelezettségét, felelősségét és jogát tartalmazza vagy meghivatkozza. A Szolgáltatási Szabályzat egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében, beleértve a Szolgáltató és más szervezet jövőbeli esetleges összeolvadásának esetét is. A Szolgáltatási Szabályzat csak írott és hitelesített formában módosítható, a Hatóság által vezetett szabályzat-nyilvántartásban való átvezetés jelen Szolgáltatási Szabályzatban leírt módon történő kezdeményezése mellett.

Értesítések

Az ügyfelek jognyilatkozataikat a Szolgáltató felé kizárólag írásban, aláírt módon tehetik meg. Szervezet képviseletében való aláírás csak a képviseleti jogosultság igazolásával együtt érvényes.

A kibocsátott tanúsítványok telefonon is felfüggeszthetők. Egyéb jellegű értesítés írásban, elektronikus levél vagy fax formájában is megtehető.

A e-Szignó Hitelesítés Szolgáltató ügyfeleit a honlapján történő közzététel útján vagy elektronikus levélben tájékoztatja.

9.6.3. Vitás kérdések megoldására vonatkozó eljárások

A Szolgáltató és az Ügyfél kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalan értesítsen és teljes körűen tájékoztasson az ügy minden vonatkozását illetően. A Szolgáltató tevékenységével vagy a kiadott tanúsítványok felhasználásával kapcsolatos kérdéseket, kifogásokat és panaszokat az Ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 3 munkanapon belül a Szolgáltató értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a Szolgáltató köteles írásban válaszolni a bejelentőnek. A Szolgáltató a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől. A Szolgáltató a panaszt 30 napon belül kivizsgálja, és az eredményekről

értesíti a bejelentőt. Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a Szolgáltató bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a Szolgáltatóval és az érintett felekkel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 10 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a Szolgáltató válaszát és egyéb szükséges információkat tartalmazó dokumentumokat. Amennyiben az egyeztetés a panasz benyújtásától számított 30 napon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az érintett felek kölcsönösen alávetik magukat a Budai Központi Kerületi bíróság, illetve a Fővárosi Bíróság kizárólagos illetékességének.

9.7. Leírás-adminisztráció

A Szolgáltató rendelkezik szolgáltatási szabályzattal, amely mind honlapján, mind az ügyfélszolgálati irodájában elérhető.

9.7.1. Szabályzat-változtatási eljárások

Szolgáltató hitelesítő szervezetén belül olyan csoport működik, amely a szabályzatok és dokumentációk karbantartásáért felelős. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz. A szabályzatot az e-Szignó Hitelesítés Szolgáltató igazgatója hagyja jóvá.

A változtatásokat gyűjtve a csoport belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A Szolgáltató törekedik arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A szolgáltatási szabályzat módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

9.7.2. Értesítés nélkül változtatható elemek

A Szolgáltató jelen szabályzatban bekövetkező minden változást – a jogszabályi előírásoknak megfelelően – a változás életbe lépése előtt 30 nappal bejelent a Hatóságnak, és a megváltozott szabályzatot közzéteszi weboldalán.

9.7.3. Értesítéssel változtatható elemek

Minden, a tanúsítványok biztonsági szintjét, felhasználhatóságát módosító változtatás értesítésköteles.

9.7.4. Észrevételek kezelése

A 9.7.5. fejezet szerint közzétett új szabályzattal kapcsolatos észrevételeket szolgáltató a hatályba lépést megelőző 14 napig fogadja az `info@e-szigno.hu` címen. A szabályzat észrevételekkel módosított változatát szolgáltató a hatályba lépést megelőző 7. nap zárja le és teszi közzé.

9.7.5. Szabályzati objektum-azonosítót vagy -mutatót változtató módosítások

A Szolgáltató minden módosítás esetén új objektum azonosítót ad a kibocsátott szabályzatainak és rendjeinek. Az egyes szabályzatok az előző verziótól eltérő web címen kerülnek közzétételre, így csak az újonnan kibocsátott tanúsítványok mutatói fognak rá hivatkozni. A Szolgáltató honlapján a Szolgáltató nyilvános dokumentumainak korábban hatályos változatai is megtalálhatóak.

9.8. Közzétételi és tájékoztatási elvek

A szabályzatban nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen szolgáltatási szabályzat több ilyet is megemlít). A 8.4. fejezetben leírt eljárások ezeket a dokumentumokat is vizsgálják.

A szabályzat közzététele

A Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal közzéteszi web oldalain. A Szolgáltató alkalmanként ezt megelőzően is tájékoztatja a közösséget a tervezett változtatásairól.

Szolgáltatási szabályzat jóváhagyási eljárások

Jelen szolgáltatási szabályzat [1], [20] szabványoknak, valamint az 1.2.2. fejezetben leírt hitelesítési rendeknek való megfelelőségét közzététel előtt a Szolgáltató megvizsgálta.

A Nemzeti Hírközlési Hatóság vizsgálja, hogy a szolgáltató szabályzatai, valamint működése a közigazgatási felhasználásra tanúsítványt kibocsátók számára előírt követelményeket kielégíti-e.

A. Hivatkozások

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

[1] RFC 3647 (Internet X.509 Nyilvános kulcsú infrastruktúra - tanúsítványtípus és szolgáltatási szabályzat keretrendszer).

[2] e-Szignó Hitelesítés Szolgáltató – nem minősített időbélyegzési rend.

[3] 2001. évi XXXV. törvény az elektronikus aláírásról (a 2004. évi módosításokkal).

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

[5] ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

[6] ITU X.509 "Információ technológia - Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer" ajánlás 3. verzió.

[7] e-Szignó Hitelesítés Szolgáltató – nem minősített tanúsítvány hitelesítési rendek.

[8] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban a hitelesítés-szolgáltatók által végzett viszontazonosítás protokolljának műszaki specifikációjára, 2006.

[9] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára, 2006.

[10] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható időbélyegzés formátum műszaki specifikációjára, 2006.

[11] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható hitelesítési rendekre, 2006.

[12] RFC 3161: Time-Stamp Protocol (TSP).

[13] RFC 2560: Online Certificate Status Protocol (OCSP).

[14] A Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) hitelesítési rendje, http://www.kgyhsz.gov.hu/KGYHSZ_HR_v1.0.pdf, 1.0.

[15] RFC 3280 (Internet X.509 Nyilvános kulcsú infrastruktúra - tanúsítvány és tanúsítvány visszavonási lista profil).

[16] A Nemzeti Hírközlési Hatóság Hivatalának tájékoztatója az elektronikus aláírással kapcsolatos szolgáltatások nyújtásához kapcsolódó bizalmi munkakörök vonatkozásában, 2008. május 15.

[17] A Nemzeti Hírközlési Hatóság HL2191713/2008 ügyiratszámú határozata az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok és paramétereik meghatározása.

[18] 194/2005. (IX.22.) Korm. rendelet a közigazgatási hatósági eljárásokban használt elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés szolgáltatókra vonatkozó követelményekről.

[19] e-Szignó Hitelesítés Szolgáltató – nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó – általános szerződési feltételek.

[20] ETSI TS 102 280: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons (v1.1.1; 2004-03).

B. A tanúsítványokban szereplő vezetéknév

A tanúsítványokban feltüntethető mezőket az RFC 3280 és további, ezen alapuló, ezt meghivatkozó szabványok ajánlások tartalmazzák. Az RFC 3280 szerinti mezők – az angolszász szokásoknak megfelelően – a teljes név (Common Name) vezetéknévre (Surname) és keresztnévre (Given Name) történő felbontását támogatják. A magyar jogszabályok szerint a magyar nevek ennél jelentősen komplexebbek és nem minden esetben egyszerű őket az RFC 3280 szerinti módon kettéválasztani. Tekintetbe véve, hogy egyes támogatott hitelesítési rendek megkövetelik a Surname mező kitöltését, a Szolgáltató a hatályos jogszabályokkal és a [9] ajánlással összhangban, és a fent leírtak figyelembevételével a következő szabály szerint tölti ki a Surname mezőt:

> „Az Surname mezőbe a Common Name mező minden olyan része kerül, amely nem az Aláíró titulusa (ilyen például a Dr. jelzés) és nem az Aláíró utóneve."

Példák:

- Kovács József – Kovács
- Dr. Kovács József – Kovács

- B. Kovács József – Kovács
- Kovács József Béláné – Kovács
- Kovácsné Nagy Izabella – Nagy
- Kovács Józsefné Nagy Izabella – Nagy