MICROSEC

Számítástechnikai Fejlesztő Kft.

Minősített e-Szignó Hitelesítés Szolgáltató

elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó

Szolgáltatási Szabályzat

Azonosító:	1.3.6.1.4.1.21528.2.1.1.1
Verzió:	3.2
Első verzió hatályba lépése:	2005. április 1.
Kezelési mód:	**Nyilvános**
Jóváhagyta:	Ellbogen András
Jóváhagyás dátuma:	
Belső auditor:	Tóth Elemér
Hatálybalépés dátuma:	2005. augusztus 8.

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

Változáskövetés

Verzió	Dátum	A változás leírása	Hatálybalépés	Készítette
1	2005-04-01	Első változat	2005-04-01	Berta István Zsolt, Endrődi Csilla
2	2005-04-15	Erdősi Péter külső auditor javaslataival kiegészített változat (azonos az 1.1-es verzióval)	2005-04-15	Berta István Zsolt
3	2005-05-15	A beérkezett módosítási javaslatok bevezetése	2005-05-15	Berta István Zsolt
3.1	2005-05-15	Apróbb javítások, kiegészítések	2005-05-15	Berta István Zsolt
3.2	2005-07-01	A hatósági szemlét követő módosítások	2005-08-08	Berta István Zsolt

Tartalomjegyzék

1. Bevezetés

Jelen szabályzat a MICROSEC Számítástechnikai Fejlesztő Kft. (továbbiakban: Szolgáltató) által üzemeltetett *e-Szignó Hitelesítés Szolgáltató* elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó Szolgáltatási Szabályzata (továbbiakban: Szabályzat).

A Szolgáltató a 2001. évi XXXV. törvényben [1] meghatározott *elektronikus aláírás hitelesítés szolgáltatást*, *időbélyegzést* és *aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezését* minősített szolgáltatóként nyújtja.

A Szolgáltató szolgáltatásait a vele szerződéses viszonyban álló ügyfelek részére biztosítja. Jelen Szabályzat vonatkozik a szolgáltatások segítségével létrehozott elektronikus aláírások és időbélyegzők ellenőrzésében érintett félre is.

Jelen Szabályzat a fenti szolgáltatások nyújtásának kereteit – a részletes eljárási és egyéb működési szabályokat – tartalmazza. A dokumentum pontos megértéséhez szükségesek a használt fogalmak értelmezésének pontos ismerete, amelyek az **A mellékletben** találhatóak.

Jelen Szabályzat nemzetközi [15] és hazai [4] ajánlások alapján készült, tartalmában és felépítésében követi azok 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 ügyfeleink és leendő ügyfeleink 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 azok megfelelnek-e, illetve az egyes szolgáltatások melyik típusa felel meg az igényeiknek, elvárásaiknak.

Jelen dokumentum feladata továbbá, hogy segítségével a Szolgáltató által kibocsátott *tanúsítványok*, *tanúsítvány visszavonási listák*, *online tanúsítvány-állapot válaszok* és *időbélyegzők*, valamint rendelkezésre bocsátott *aláírás-létrehozó eszközök igénylői, 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 a vonatkozó *Általános Szerződési Feltételek* [22,23], a szolgáltatóval kötött *Szolgáltatási Szerződés*, a *Hitelesítési Rend* [20], az *Időbélyegzési Rend* [21] illetve egyéb, a Szolgáltatótól független szabályzat illetve dokumentum is tartalmazhat.

1.1.2. A Szabályzat hatálya

A Szabályzat tárgyi hatálya

A Szabályzat az 1.1.4 pontban ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.

A Szabályzat 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.

A Szabályzat személyi hatálya

A Szabályzat az 1.3 alfejezetben azonosított közösség minden egyes tagjára – köztük természetes személyekre és jogi személyekre – egyaránt kiterjed.

A Szabályzat területi hatálya

A Szabályzat területi hatálya *Magyarország* területe.

1.1.3. A Szolgáltató

A Szolgáltató adatai

Név:	MICROSEC Számítástechnikai Fejlesztő Kft.
Cégjegyzék szám:	01-09-078353 a Fővárosi Bíróság mint Cégbíróság
Ügyvezető igazgató:	Vanczák József
Székhely:	1022 Budapest, Marcibányi tér 9.
Telephely:	1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Központi telefonszám:	(1) 438-6310
Központi telefax szám:	(1) 438-6320
Internet cím:	http://www.microsec.hu
Minősítések:	ISO 9001: 2000, BS 7799

Szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Szolgáltató egység vezetője:	Ellbogen András
Ügyfélszolgálati iroda:	1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	http://www.e-szigno.hu

A Szolgáltató bemutatása

A *MICROSEC Számítástechnikai Fejlesztő Kft.* jogelődje (Microsec Számítástechnikai Fejlesztő Kisszövetkezet) 1984-ben alakult, a mai cégformában 1991 óta működik.

Fő tevékenységi köre az *elektronikus aláírással kapcsolatos szolgáltatásokon* kívül a *szoftverfejlesztés* és *szoftver-rendszerek üzemeltetése*. A MICROSEC Kft. 2002 április 30. óta az *Igazságügyi Minisztérium* hitelesítés-szolgáltatója.

A MICROSEC Kft. fejlesztette ki az *e-Szignó aláírás-létrehozó alkalmazást*, amelynek 1.5.1-es verzióját jelenleg is használják például a pénzintézetekben és a cégbíróságokon; a 2.0-ás verzió megbízható aláírás-létrehozó modulja a normatív dokumentumoknak [1,2,3,14,15,16,17,18,19] megfelelő, tanúsítással rendelkező *minősített aláírás-létrehozó modul*.

A Hírközlési Felügyelet (HIF) – jelenleg Nemzeti Hírközlési Hatóság – 2002. május 30-án vette nyilvántartásba a Szolgáltatót *fokozott biztonságú szolgáltatóként*. Regisztrációs szám: **MH-6834-1/2002**.

A Nemzeti Hírközlési Hatóság 2005. május 15-én vette nyilvántartásba a Szolgáltatót minősített szolgáltatóként.

Minőség és információbiztonság

A MICROSEC Kft. kiemelten fontosnak tartja ügyfelei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a Szolgáltató *ISO 9001:2000 szabványnak megfelelő minőségbiztosítási rendszert* üzemeltet (2002. január 23., Lloyd's).

A MICROSEC Kft. nagy figyelmet szentel az által üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a *BS 7799-nek megfelelő információbiztonság-irányítási rendszert* üzemeltet (2003. május 19., Lloyd's).

A Szolgáltató önkéntes akkreditációs rendszer keretében nem lett tanúsítva, mert ilyen rendszer Magyarországon még nem működik.

1.1.4. Szolgáltatások

Az e-Szignó Hitelesítés Szolgáltató a 2001. évi XXXV. törvényben [1] meghatározott *elektronikus aláírás hitelesítés szolgáltatást*, *időbélyegzést* és *aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezését* minősített szolgáltatóként nyújtja, amelyeket ügyfelei számára a következő szolgáltatások keretében teszi elérhetővé:

- Hitelesítés szolgáltatás
- Időbélyegzés szolgáltatás
- Online tanúsítvány-állapot szolgáltatás

A *hitelesítés szolgáltatás* keretében a Szolgáltató a 2001. évi XXXV. törvényben [1] meghatározott *elektronikus aláírás hitelesítés szolgáltatást* és *aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezését* együttesen nyújtja.

Az *időbélyegzés szolgáltatás* keretében a Szolgáltató a 2001. évi XXXV. törvényben [1] meghatározott *időbélyegzés szolgáltatást* végzi.

Az *online tanúsítvány-állapot szolgáltatás* keretében a Szolgáltató az *elektronikus aláírás hitelesítés szolgáltatás* keretében kibocsátott minősített tanúsítványok adott időpontbeli állapotára vonatkozó hiteles igazolásokat bocsát ki online módon.

1.1.4.1. Hitelesítés szolgáltatás

A Szolgáltató a *hitelesítés szolgáltatás* keretében a szerződéses viszonyban álló Ügyfelei részére *minősített tanúsítványokat* bocsát ki, és azokkal kapcsolatban különböző tanúsítvány műveletek végzését teszi lehetővé a *szolgáltatás időtartama* alatt.

A szerződéses viszonyban álló felek:

a) a *Szolgáltató,*

b) az *Aláíró* (a kibocsátásra kerülő tanúsítvány által azonosított, az aláírás-létrehozó adatot és a BALE-t kizárólagosan használó természetes személy),

c) az *Aláíró Szervezete*, amennyiben a minősített tanúsítvány egy jogi személy képviseletében történő aláírásra vagy tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra az Aláíró részére,

d) a *Költségviselő*, amennyiben a szolgáltatással összefüggő díjakat és költségeket viselő személy az Aláírótól és az Aláíró Szervezetétől eltérő harmadik fél.

A *szolgáltatás időtartama* az az időszak, amelyre a Költségviselő megfizette a tanúsítvány fenntartásával kapcsolatos díjat. A szolgáltatás időtartama egybeesik az aktuális tanúsítvány érvényességi idejével.

A minősített tanúsítvány hitelesen összekapcsolja az azonosított Aláíró adatait és az általa birtokolt aláírás-létrehozó adathoz tartozó nyilvános aláírás-ellenőrző adatot. Az aláírás-létrehozó adatnak biztonságos aláírás-létrehozó eszközön kell lennie, amelyet Szolgáltató bocsát az Aláíró rendelkezésére.

A minősített tanúsítvány és a biztonságos aláírás-létrehozó eszköz segítségével *minősített elektronikus aláírás* hozható létre. A minősített elektronikus aláírás összekapcsolja az Aláíró személyét az aláírt dokumentummal. A minősített elektronikus aláírás egyenértékű a kézzel írott aláírással, a minősített elektronikus aláírással ellátott dokumentumhoz ugyanaz a joghatás fűződik, mintha az Aláíró azt kézzel írta volna alá.

A szolgáltatás időtartama alatt az Aláíró és az Aláíró Szervezete kérvényezheti a Szolgáltatótól a tanúsítvány *visszavonását, felfüggesztését*, *visszaállítását* és lecserélését (*tanúsítványcsere*). Szolgáltató a *kiadott tanúsítványokat* és a kiadott tanúsítványok visszavonási állapotát tartalmazó *visszavonási listákat* nyilvánosan elérhetővé teszi. A visszavont, a felfüggesztett és a lejárt tanúsítvány érvénytelen. Az érvénytelen tanúsítvány alapján létrehozott aláíráshoz nem fűződik semmilyen joghatás.

A *hitelesítés szolgáltatás* a következő elemekből áll:

a) *Regisztráció*, amely során az Aláíró személyazonosságának – illetve minden más, a tanúsítványba kerülő jellemzőjének – ellenőrzése történik meg. A folyamat eredményeit a tanúsítvány-előállítás folyamat használja fel.

b) *Tanúsítvány-előállítás*, amely során a Szolgáltató létrehozza és aláírja a regisztráció során ellenőrzött, az aláíró személyazonosságán és más tulajdonságain alapuló, az Aláíró nyilvános kulcsát is tartalmazó, a Szolgáltatási Szerződésben meghatározott típusú és fajtájú minősített tanúsítványt. A Szolgáltató a tanúsítványt és a hozzá kapcsolódó aláírás létrehozó adatot minősített aláírás létrehozására alkalmas módon generálja. A Szolgáltató biztonságos aláírás-létrehozó eszközön generálja az Aláíró magánkulcsát. E magánkulcs soha nem hagyja el a kártyát, így a Szolgáltató e kulcsot nem ismeri, és nem tárol belőle másolati példányt.

c) *Tanúsítvány-kibocsátás*, amely során a Szolgáltató feltölti az Aláíró tanúsítványát az Aláíró számára előkészített aláírás-létrehozó eszközre és átadja azt számára.

d) *Tanúsítványcsere*, amely során egy korábban kibocsátott tanúsítvány helyett új tanúsítvány kerül kibocsátásra.

e) *Tanúsítvány visszavonás/felfüggesztés kezelés*, amely során a Szolgáltató fogadja és feldolgozza a tanúsítvány *visszavonásával*, *felfüggesztésével* és *visszaállításával* kapcsolatos kérelmeket. A folyamat eredményei a visszavonási állapot közzététele révén kerülnek publikálásra. E szolgáltatás rendelkezésre állása 99,9%, az eseti szolgáltatás-kiesések nem haladhatják meg a három órát.

f) *Tanúsítvány közzététel*, amely során a Szolgáltató közzé teszi a kibocsátott tanúsítványokat. A tanúsítvány-közzététel szolgáltatás rendelkezésre állása 99,9%, az eseti szolgáltatás-kiesések nem haladhatják meg a három órát.

g) *Információ szolgáltatás,* amely során a Szolgáltató közzé teszi a hitelesítés szolgáltatással kapcsolatos dokumentációkat, elsősorban a Szolgáltatási Szabályzatot, a Hitelesítési Rendet, a vonatkozó Általános Szerződési Feltételeket, az aktuális árlistát és a szolgáltatás igénybe vételével kapcsolatos tájékoztatókat. A Szolgáltató a honlapján közzéteszi e dokumentumokat, valamint e dokumentumok nyomtatott változata a Szolgáltató ügyfélszolgálati irodájában is elérhető.

h) *Tanúsítvány visszavonási állapot közzététel*, amely során a Szolgáltató közzé teszi az általa kibocsátott tanúsítványok aktuális állapotát a rendszeres időközönként frissített tanúsítvány visszavonási listák (CRL) segítségével. Emellett a Szolgáltató online tanúsítvány-állapot szolgáltatást is biztosít. E szolgáltatások rendelkezésre állása is 99,9%, az eseti szolgáltatás-kiesések nem haladhatják meg a három órát.

i) *Biztonságos aláírás-létrehozó eszköz optikai megszemélyesítése*, amely során az aláírás-létrehozó eszközön elhelyezésre kerülnek a Szolgáltató arculati elemei valamint – kérés esetén – az Aláíró egyedi jellemzői.

j) *Biztonságos aláírás-létrehozó eszköz logikai megszemélyesítése*, amely során az aláírás-létrehozó eszközön létrehozásra kerül az aláírás-létrehozó és -ellenőrző adat.

1.1.4.2. Időbélyegzés szolgáltatás

A Szolgáltató az időbélyegzés *szolgáltatás* keretében a szerződéses viszonyban álló Ügyfelei – természetes és jogi személyek – részére *minősített időbélyegzőket* bocsát ki.

A minősített időbélyegző hitelesen összekapcsolja az Ügyfél által az időbélyegző kérésben eljuttatott dokumentum lenyomatot a kérés feldolgozásának pontos, hiteles időpontjával, amellyel így később harmadik fél előtt is bizonyítható, hogy a dokumentum az adott formában az adott időpontban létezett

Az *időbélyegzés szolgáltatás* a következő elemekből áll:

a) Időbélyegző kérés fogadása, amely során a Szolgáltató rendszere azonosítja az Ügyfelet és fogadja a kérését.

b) Időbélyegző előállítás, amely során a Szolgáltató rendszere előállítja az időbélyegzés kérésnek megfelelő, az aktuális, hiteles időpontot tartalmazó időbélyegzőt.

c) Időbélyegző kibocsátás, amely során a Szolgáltató eljuttatja az Ügyfélnek a kérése alapján számára előállított időbélyegzőt.

Az időbélyegzés szolgáltatás rendelkezésre állása 99,9%, az eseti szolgáltatás-kiesések nem haladhatják meg a három órát.

1.1.4.3. Online tanúsítvány-állapot szolgáltatás

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

Az online tanúsítvány-állapot válasz hiteles információt nyújt az Ügyfél 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 visszavonási állapota. Az online tanúsítvány-állapot válaszok kéréséhez az Ügyfélnek a Szolgáltatónál létrehozott egyedi azonosítóját kell használnia.

Az *online tanúsítvány-állapot szolgáltatás* a következő elemekből áll:

a) Online tanúsítvány-állapot kérés fogadása, amely során a Szolgáltató rendszere azonosítja az Ügyfelet és fogadja a kérését.

b) Online tanúsítvány-állapot válasz előállítás, amely során a Szolgáltató rendszere előállítja a kérésben hivatkozott tanúsítvány aktuális visszavonási állapotára vonatkozó információkat hitelesen tartalmazó választ.

c) Online tanúsítvány-állapot válasz kibocsátás, amely során a Szolgáltató eljuttatja az Ügyfélnek a kérése alapján számára előállított online tanúsítvány-állapot választ.

1.1.5. Szabványok és előírások

Jelen Szabályzat megfelel az „RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)” nemzetközi szabványnak [10].

A Szabályzat tartalmi vonatkozásokban eleget tesz a vonatkozó hazai jogszabályok előírásainak és ajánlásainak [1,2,3], továbbá a hitelesítés szolgáltatásra vonatkozóan felhasználja a „*Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények*” című nemzetközileg elfogadott (ETSI) műszaki specifikációt [7], valamint a „*Nyilvános kulcs és attribútum tanúsítvány keretrendszer*” című (ITU-T) ajánlást [12].

Jelen Szolgáltatási Szabályzathoz szervesen kapcsolódik – és ezzel összhangban került kialakításra – a Szolgáltató által kibocsátott tanúsítványok felhasználásának feltételeit előíró „*Minősített e-Szignó Hitelesítés Szolgáltató Biztonságos aláíró-eszközzel együttesen kiadott minősített tanúsítvány hitelesítési rend*” című dokumentum [20], valamint a „*Minősített e-Szignó Hitelesítés Szolgáltató Időbélyegzési rend*” című dokumentum [21].

A hitelesítés szolgáltatás keretében kibocsátott tanúsítványok illetve tanúsítvány visszavonási listák a következő ajánlásoknak felelnek meg:

- International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása – Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer” ajánlás [12] 3. verziója,
- RFC 3280: Certificate and Certificate Revocation List (CRL) Profile (az RFC 2459 újabb változata) [24]
- RFC 3739: Qualified Certificates Profile (az RFC 3039 újabb változata) [25],
- ETSI TS 101 862: Qualified Certificate Profile (v1.3.2; 2004-08) [26],
- ETSI TS 102 280: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons (v1.1.1; 2004-03) [27].

Az időbélyegzés szolgáltatás megfelel az RFC 3161: Time-Stamp Protocol (TSP) ajánlásban [28] megfogalmazottaknak.

Az online tanúsítvány-állapot szolgáltatás megfelel az RFC 2560: Online Certificate Status Protocol (OCSP) ajánlásban [29] megfogalmazottaknak.

1.1.6. Tanúsítványfajták, hitelesítési rend

Jelen szolgáltatási szabályzat csakis a Szolgáltató minősített e-Szignó Hitelesítés Szolgáltató önálló üzleti egysége által kibocsátott tanúsítványokról szól.

A minősített e-Szignó Hitelesítés Szolgáltató *minősített* végfelhasználói tanúsítványokat bocsát ki, amelyek megfelelnek a 2001. évi XXXV. Elektronikus aláírás törvényben a minősített tanúsítványokkal kapcsolatban megfogalmazott követelményeknek. Az ilyen tanúsítványok használata feltétele a *minősített elektronikus aláírás* létrehozásának.

Az e-Szignó Hitelesítés Szolgáltató által kibocsátott minősített végfelhasználói tanúsítványok által azonosított alany minden esetben *természetes személy*.

Az e-Szignó Hitelesítés Szolgáltató kizárólag biztonságos aláírás-létrehozó eszközön levő aláírás-létrehozó adathoz tartozó aláírás-ellenőrző adathoz bocsát ki tanúsítványt (MTT+BALE). A tanúsítvány kibocsátása, gondozása, kezelése és elfogadása során követendő hitelesítési rendeket a „*Minősített e-Szignó Hitelesítés Szolgáltató Biztonságos aláíró-eszközzel együttesen kiadott minősített tanúsítvány hitelesítési rendek"* [20] című dokumentum tartalmazza. A támogatott hitelesítési rendek közötti legfőbb különbségeket a 1.2.4. fejezet foglalja össze. Az alkalmazott hitelesítési rend azonosítója feltüntetésre kerül a tanúsítvány Certificate Policies mezejében.

Az e-Szignó Hitelesítés Szolgáltató több különböző tanúsítványfajtát ajánl ügyfelei részére, amelyek jellemzően az általuk hitelesen az Aláíróhoz kötött adatok és tulajdonságok körében térnek el. A tanúsítványfajták a következők:

Személyes tanúsítvány: egyértelműen összeköti az Aláíró személyét – valamely őt egyértelműen azonosító adat vagy adategyüttes alapján – az aláírás-ellenőrző adatával (nyilvános kulcsával).

Szervezeti tanúsítvány: az Aláíró Szervezete (például egy vállalat vagy egy közigazgatási intézmény) által igazolt szervezeten belüli beosztás vagy feladatkör, illetve a szervezet képviseletére való jogosultság kerül feltüntetésre. Ebben az esetben az Aláíró a tanúsítványt kizárólag a megnevezett szervezet képviseletében történő aláírásra vagy tevékenységének érdekében használhatja fel.

Hivatáshoz kapcsolódó tanúsítvány: az Aláíró valamely hivatását igazolja a tanúsítvány, amelyre való kijelöléséről a Szolgáltató győződik meg. Ilyen lehet például:

i) Közjegyzői tanúsítvány

ii) Ügyvédi tanúsítvány

iii) Bírói tanúsítvány

A szervezeti és a hivatáshoz kapcsolódó tanúsítványok együttes elnevezés „üzleti tanúsítvány".

1.1.7. A tanúsítvány felhasználásának korlátai

A Szolgáltató Magyarország területére korlátozza az általa kibocsátott minősített végfelhasználói tanúsítványok felhasználhatóságát. Emellett a Szolgáltató korlátozza tanúsítványok alkalmazhatóságát az egy alkalommal vállalható kötelezettség mértéke szerint is. Ezen pénzügyi tranzakciós korlát a tanúsítványban feltüntetésre kerül.

A Szolgáltató által kibocsátott minősített végfelhasználói tanúsítványok érvényessége egy vagy két év, minden tanúsítványban szerepel az érvényességi ideje.

1.1.8. Aláírás-létrehozó eszközök

Az e-Szignó Hitelesítés Szolgáltató kizárólag olyan aláírás-létrehozó eszközöket bocsát ügyfelei rendelkezésére, amelyek megfelelnek a 2001. évi XXXV. Elektronikus aláírás törvényben megfogalmazott biztonságos aláírás-létrehozó eszköz követelményeinek. Az ilyen eszközök használata feltétele a minősített aláírás létrehozásának.

1.2. Azonosítás

1.2.1. A Szabályzat azonosítása

Jelen dokumentum teljes neve „*Minősített e-Szignó Hitelesítés Szolgáltató elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó Szolgáltatási Szabályzat*", röviden: „*e-Szignó Szolgáltatási Szabályzat*". A *Szabályzat* egyértelmű azonosítására szolgáló adatok megtalálhatóak a dokumentum címlapján.

A Szabályzat hivatalos és aktuális verziója elérhető a következő címen: https://www.e-szigno.hu/SZSZ/, valamint nyomtatott változata megtekinthető a Szolgáltató ügyfélszolgálati irodájában.

1.2.2. A Szolgáltató azonosítása

A Szolgáltató azonosítására szolgáló adatok az 1.13. fejezetben találhatóak.

1.2.3. A szolgáltatások azonosítása

Jelen Szabályzat vonatkozik a minősített e-Szignó Hitelesítés Szolgáltató minden nyilvánosan nyújtott szolgáltatására. Ezek azonosítása megtalálható a 1.1.4. fejezetben.

1.2.4. A vonatkozó hitelesítési rendek és időbélyegzési rendek

Hitelesítési rendek

A jelen Szabályzat hatáskörébe a következő hitelesítési rendek tartoznak:

Azonosító	Hitelesítési rend neve
OID: 1.3.6.1.4.1.21528.2.1.1.2 NHH azonosító: HL-7789-2/2005	„Nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített hitelesítési rend”
OID: 1.3.6.1.4.1.21528.2.1.1.12	„Nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő álnevet tartalmazó tanúsítványok esetén alkalmazott minősített hitelesítési rend”

A fenti hitelesítési rendek alapvető követelményei megegyeznek, köztük mindössze egyetlen különbség van:

- A 1.3.6.1.4.1.21528.2.1.1.2 azonosítójú hitelesítési rend (a továbbiakban: álnevet kizáró hitelesítési rend) szerint kibocsátott tanúsítványokban a Szolgáltató a tanúsítványban nem tüntet fel álnevet.
- A 1.3.6.1.4.1.21528.2.1.1.12 azonosítójú hitelesítési rend (a továbbiakban: álneves hitelesítési rend) szerint kibocsátott tanúsítványokban a Szolgáltató a minden esetben álnevet tüntet fel.

A fenti két hitelesítési rendet a Szolgáltató külön hitelesítő egységhez (így külön szolgáltatói aláíró kulcspárhoz) rendeli.

Mindkét hitelesítési rend mindenkori aktuális változata elérhető a www.e-szigno.hu/HR/ címen.

Időbélyegzési rend

A jelen Szabályzat hatáskörébe a következő időbélyegzési rend tartozik:

- *„Minősített e-Szignó Hitelesítés Szolgáltató időbélyegzési rend”* [21], OID: 1.3.6.1.4.1.21528.2.1.1.3, NHH azonosító: HL-7789-2/2005a

Az időbélyegzési rend mindenkori aktuális változata elérhető a www.e-szigno.hu/IR/ címent.

1.3. Közösség és alkalmazhatóság

A jelen Szabályzat keretei között kibocsátott tanúsítványokat, tanúsítvány visszavonási listákat, időbélyegzőket és tanúsítvány-állapot válaszokat 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 hitelesítés szolgáltatás keretében végzett tanúsítvány előállítás és menedzsment 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 aláírás-létrehozó eszközök menedzselése és rendelkezésre bocsátása is, valamint az időbélyegzés szolgáltatást és az online tanúsítvány-állapot szolgáltatást is ez a szervezeti egység nyújtja. A szabályzatok menedzselésével kapcsolatos feladatokat is ez a szervezeti egység látja el.

A *minősített tanúsítványok* kibocsátásával kapcsolatban a következő *hitelesítő egységek* vesznek részt:

- *„Microsec e-Szigno Root CA”,* gyökér hitelesítő egység – önhitelesített

- *„Qualified e-Szigno CA”,* produktív hitelesítő egység, a gyökér hitelesítő egység hitelesíti.

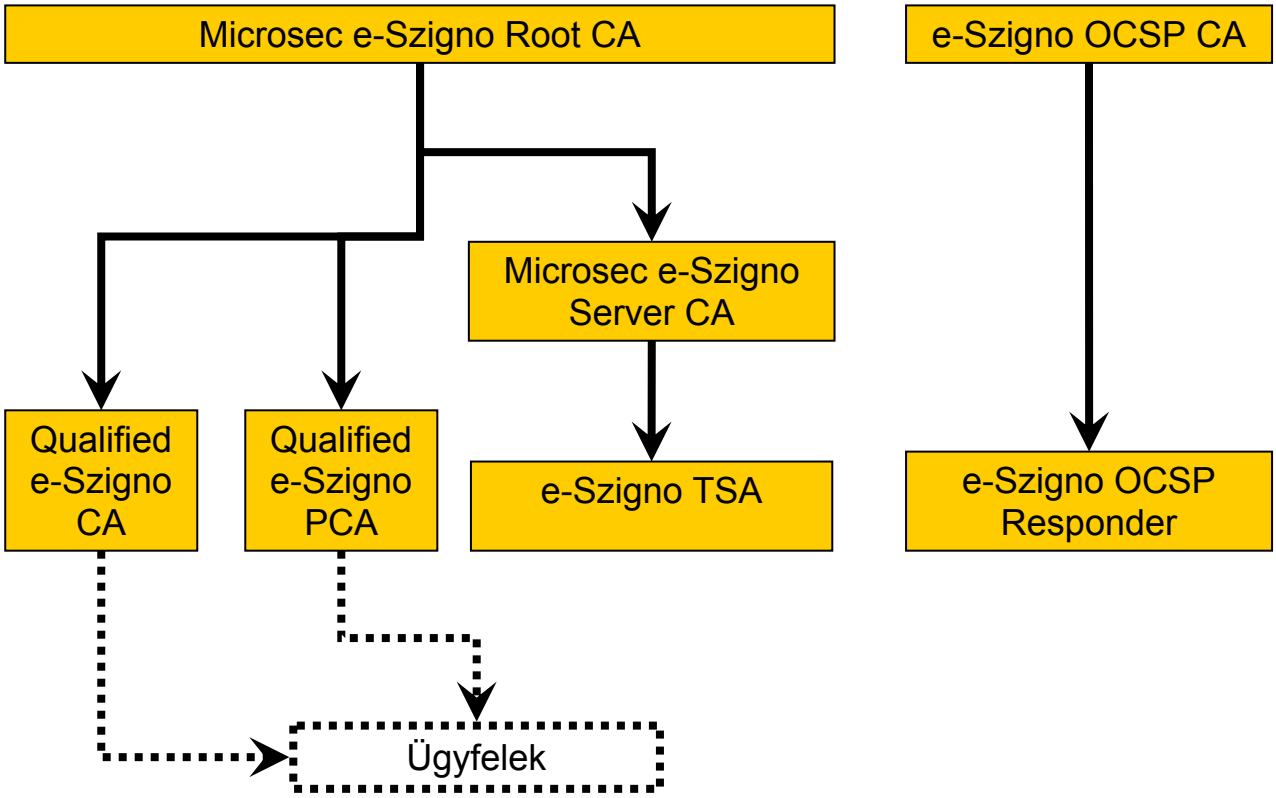
Az *időbélyegzők* előállítása során a következő *egységek* vesznek részt:

- *Microsec e-Szigno Server CA* (a Microsec e-Szigno Root CA hitelesíti)
- *e-Szigno TSA* (a Microsec e-Szigno Server CA hitelesíti).

Az *online tanúsítvány-állapot válaszok* előállítása során a következő *egységek* vesznek részt:

- *„e-Szigno OCSP CA”*, az OCSP válaszadó tanúsítványát kibocsátó hitelesítő egység
- *„e-Szigno OCSP Responder”,* OCSP válaszadó – az e-Szigno OCSP CA hitelesít.

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 többi hitelesítő egység tanúsítványát e két hitelesítő egység bocsátja ki az 1. ábra szerinti struktúrában.



1. ábra Az e-Szignó Hitelesítés Szolgáltató hitelesítő egységei

A Microsec e-Szigno Root CA tanúsítványában szereplő SHA-1 lenyomat értéke:	23 88 c9 d3 71 cc 9e 96 3d ff 7d 3c a7 ce fc d6 25 ec 19 0d
Az e-Szigno OCSP CA tanúsítványában szereplő SHA-1 lenyomat értéke:	56 2c 85 5 9c d9 be 0e 64 e6 f7 95 86 24 95 a1 09 3e f1 68

A fenti hitelesítő egységek közül a „Microsec e-Szigno Root CA” más hitelesítés szolgáltatók hitelesítő egységeit is felülhitelesítheti. E felülhitelesítéssel az e-Szignó Hitelesítés Szolgáltató kizárólag azt igazolja, hogy a felülhitelesített szolgáltató tanúsítványához tartozó magánkulcs valóban e szolgáltató birtokában van.

1.3.2. 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 belül valósítja meg.

Az iroda feladatai:

- a végfelhasználói minősített tanúsítványok alanyainak regisztrációja,
- a tanúsítványok kibocsátásához, az aláíró-eszköz rendelkezésre bocsátásához kapcsolódó adminisztrációs és regisztrációs tevékenység,
- az időbélyegzés és online tanúsítvány-állapot szolgáltatáshoz 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.

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

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.

1.3.3. Végfelhasználók

Hitelesítés szolgáltatás

A Szolgáltató által nyújtott hitelesítés szolgáltatás végfelhasználói (lásd: **A melléklet, Fogalomtár**):

- az Aláíró: a kibocsátásra kerülő tanúsítvány által azonosított, az aláírás-létrehozó adatot és a BALE-t kizárólagosan használó – természetes személy,
- az Aláíró Szervezete*:* amennyiben a minősített tanúsítvány egy jogi személy képviseletében történő aláírásra vagy tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra az Aláíró részére, akkor a szóban forgó szervezet, amely szintén megjelölésre kerül a tanúsítványban,
- az Érintett *fél:* a tanúsítvány felhasználásával létrehozott elektronikus aláírással ellátott elektronikus dokumentumot befogadó fél.

Az Aláíró és az Aláíró Szervezete szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Szolgáltatói Szerződésben, Általános Szerződési Feltételekben [22], Hitelesítési Rendben [20] és jelen Szolgáltatási Szabályzatban foglaltak szerint. A Szolgáltató az Aláíróval és az Aláíró Szervezetével elsősorban az ügyfélszolgálati irodán keresztül tart kapcsolatot.

Az Érintett fél a Szolgáltatóval szerződéses viszonyban nem álló harmadik személy. Tevékenységére vonatkozó ajánlásokat a Szabályzat és az abban megnevezett egyéb szabályzatok tartalmazzák. A Szolgáltató az Érintett féllel elsősorban az internetes honlapon keresztül tart kapcsolatot.

Időbélyegzés és online tanúsítvány-állapot szolgáltatás

A Szolgáltató által nyújtott időbélyegzés illetve online tanúsítvány-állapot szolgáltatás végfelhasználói (lásd: **A melléklet, Fogalomtár**):

- *az Ügyfél: a kibocsátásra kerülő időbélyegző illetve tanúsítvány-állapot válasz igénylője és felhasználója,*
- *az Érintett fél: az időbélyegzővel illetve az online tanúsítvány-állapot választ ellátott elektronikus dokumentumot befogadó fél.*

Az Ügyfél szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Szolgáltatói Szerződésben, Általános Szerződési Feltételekben [23], Időbélyegzési Rendben [21] és jelen Szolgáltatási Szabályzatban foglaltak szerint. A Szolgáltató az Aláíróval és az Aláíró Szervezetével elsősorban az Ügyfélszolgálati irodán keresztül tart kapcsolatot.

Az Érintett fél a Szolgáltatóval szerződéses viszonyban nem álló harmadik személy. Tevékenységére vonatkozó ajánlásokat a Szabályzat és az abban megnevezett egyéb szabályzatok tartalmazzák. A Szolgáltató az Érintett féllel elsősorban az internetes honlapon keresztül tart kapcsolatot.

1.3.4. Alkalmazhatóság

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

Engedélyezett alkalmazási lehetőségek

A kibocsátott minősített 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.

Korlátozások

A Szolgáltató a szabályzataiban szereplő feltételekkel korlátozza a kibocsátott tanúsítványok felhasználhatóságát a pénzügyi tranzakciós limit vagy egyéb vonatkozásokban. A kibocsátott végfelhasználói tanúsítványokra vonatkozó korlátozásokat az **1.1.7. A tanúsítvány felhasználásának korlátai**, illetve a **7. Tanúsítvány, tanúsítvány-visszavonási lista, időbélyeg és online tanúsítvány-állapot válasz profilok** fejezetek ismertetik ebben a dokumentumban. A Szolgáltató által alkalmazott „*Biztonságos aláíró-eszközzel együttesen kiadott minősített tanúsítvány”* tanúsítványtípus esetében a korlátozásokat a vonatkozó hitelesítési rend [20] tartalmazza.

Tiltott alkalmazási lehetőségek

A minősített végfelhasználói tanúsítványok csak az engedélyezett célra használhatóak; azokat – többek között – titkosításra, autentikációs célokra, más nyilvános kulcsú tanúsítványok aláírására – felhasználni nem szabad.

1.4. Kapcsolattartás

1.4.1. Szolgáltató

Név: MICROSEC Számítástechnikai Fejlesztő Kft.
Cégjegyzékszám: 01-09-078353 a Fővárosi Bíróság mint Cégbíróság
Székhely: 1022 Budapest, Marcibányi tér 9.
Postacím: 1031 Budapest, Záhony utca 7, Graphisoft Park
Központi telefonszám: (1) 505-4444
Központi telefax szám: (1) 505-4445
Internet cím: http://www.microsec.hu

1.4.2. Ügyfélszolgálati iroda

Név: e-Szignó Hitelesítés Szolgáltató Ügyfélszolgálati iroda
Cím: 1031 Budapest, Záhony u. 7. Graphisoft Park, D épület
Postacím: 1031 Budapest, Záhony u. 7, Graphisoft Park
Telefonszám: (+36-1) 505-4444
Telefax szám: (+36-1) 505-4445
E-mail cím: info@e-szigno.hu
Internet cím: http://www.e-szigno.hu

A szolgáltatásokkal kapcsolatos kérdésekkel, problémákkal a végfelhasználók az Ügyfélszolgálati irodához fordulhatnak szóban vagy írásban.

Az Ügyfélszolgálati iroda munkanapokon **9 és 12 óra között** tart nyitva, az ettől eltérő nyitva tartást a Szolgáltató a honlapján teszi közzé.

A visszavonással kapcsolatos regisztrációs és adminisztrációs szolgáltatás folyamatosan – napi 24 órában – elérhető a következő telefonszámokon:

(36-1) 505-4446
(36-30) 326-2187

1.4.3. Hitelesítő szervezet

A *hitelesítő szervezet* elérése az Ügyfélszolgálati irodán keresztül történik.

1.4.4. Illetékes fogyasztóvédelmi felügyelőség

Az illetékes fogyasztóvédelmi felügyelőség adatai a következők:

Név: *Budapest Főváros Közigazgatási Hivatal Fogyasztóvédelmi Felügyelőség*
Cím: 1088 Budapest, József krt. 6.
Postacím: 1364 Budapest, Pf. 234
Telefonszám: (+36-1) 4594-918
Telefax szám: (+36-1) 4594-870

2. Általános rendelkezések

A Szabályzat hatálya alá eső Közösség (lásd: **1.3. Közösség és alkalmazhatóság**) valamint a Költségviselő *kötelezettségeit* és *felelősségeit* a vonatkozó Szolgáltatói Szerződés, a vonatkozó Általános Szerződési Feltételek [22,23], a vonatkozó Hitelesítési Rend [20] illetve Időbélyegzési Rend [21] és a jelen Szolgáltatási Szabályzat tartalmazzák.

2.1. Kötelezettségek

Az e-Szignó Hitelesítés Szolgáltató elsődleges feladata a *hitelesítő* és *regisztráló szervezetek* üzemeltetése valamint a tanúsítványtár és a visszavonási információk közzététele is. A Szolgáltatónak szolgáltatásait a hatályos jogi szabályozással, szolgáltatási szabályzatával és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban kell nyújtania.

2.1.1. A Szolgáltató általános kötelezettségei

A Szolgáltató alapvető kötelezettsége, hogy vállalt szolgáltatásait a jelen 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 (lásd **1.1.4 Szolgáltatások**) nyújtása a vonatkozó szabályzatok szerint,
- a hitelesítés szolgáltatáshoz kapcsolódó szervezetek (hitelesítő szervezet, regisztráló szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése,
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés megszüntetése,
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket,
- a jogszabály szerinti publikus nyilvántartások és előírt saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az Interneten keresztül.

A Szolgáltató általános kötelezettségeit a vonatkozó ÁSZF-ek [22,23] valamint a vonatkozó Hitelesítési Rend [20] illetve Időbélyegzési Rend [21] részletesen tartalmazzák.

2.1.2. A hitelesítő szervezet kötelezettségei

Az e-Szignó Hitelesítés Szolgáltató feladata a hitelesítő egységek, valamint az időbélyegzés szolgáltatáshoz és az online tanúsítvány-állapot szolgáltatáshoz szükséges egységek (lásd: **1.3.1. Hitelesítő szervezet**) felállítása és működtetése, a tanúsítványtár és a visszavonási-állapot információ gondozása, a biztonságos aláírás-létrehozó eszközök menedzselése és rendelkezésre bocsátása, valamint a szabályzatok menedzselése.

A *hitelesítő egységek* 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 (lásd: **1.1.6 Tanúsítványfajták**) specifikálása, jóváhagyása és karbantartása,
- a hitelesítés szolgáltatási nyilvános szabályzatainak és a vonatkozó belső (nem nyilvános) előírásoknak előkészítése, egyeztetése jogszabályokkal és a belső (nem nyilvános) szabályzatokkal, továbbá az aktualizálások elvégzése,
- a hitelesítés szolgáltatási szabályzatokkal kapcsolatos észrevételek rögzítése és javaslatok elbírálása.

A hitelesítő szervezet kötelezettségeit a vonatkozó Hitelesítési Rend [20] illetve Időbélyegzési Rend [21] részletesen tartalmazza.

2.1.3. A regisztráló szervezet kötelezettségei

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

- a hitelesítés szolgáltatás, az időbélyegzés szolgáltatás és az online tanúsítvány-állapot szolgáltatás értékesítésében történő közreműködés,
- a regisztráció elvégzése (az Ügyfelek adatainak rögzítése és ellenőrzése),
- a különböző tanúsítvány műveletekre vonatkozó kérelmek fogadása (felfüggesztés, visszavonás, visszaállítás, tanúsítványcsere),
- az adatmódosítási bejelentések fogadása és kezelése,
- közreműködés a visszavonási állapot közzétételében,
- információs tevékenység nyújt Ügyfelek és az Érintett felek részére Szolgáltató által nyújtott elektronikus aláírással kapcsolatos tevékenységeivel kapcsolatban.
- tájékoztató anyagot ad át az Ügyfélnek, 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 Rend [20] illetve Időbélyegzési Rend [21] részletesen tartalmazza.

2.1.4. Az Ügyfél kötelezettségei

Az Ügyfelek kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatások felhasználása során, beleértve a tanúsítvány és magánkulcs igénylését és alkalmazását.

Az Ügyfelek kötelezettségeit a vonatkozó Hitelesítési Rend [20] illetve Időbélyegzési Rend [21] részletesen tartalmazza.

2.1.5. Az Érintett félre vonatkozó ajánlások a tanúsítványok ellenőrzésével kapcsolatban

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

Amennyiben az Érintett fél e kötelességét megszegi (vagyis nem az itt leírtaknak megfelelően jár el), az ebből következő károkért a Szolgáltató nem vállal felelősséget.

A tanúsítványra vonatkozó ellenőrzéseket az Érintett félnek el kell végeznie a teljes tanúsítási láncra vonatkozóan. Ha az ellenőrzendő elektronikus aláírás, a hozzá kapcsolódó tanúsítvány vagy a tanúsítási lánc 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 el kell utasítania.

Az itt leírtakhoz képest a vonatkozó Hitelesítési Rend [20] illetve Időbélyegzési Rend [21] további ajánlásokat is tartalmazhat az érintett fél számára.

Az itt leírt lépések a hatályos jogszabályokból, a nemzetközi szabványokból és ajánlásokból, valamint a Szolgáltató által nyújtott szolgáltatások halmazából egyenesen levezethetőek, hozzájuk képest semmilyen további követelményt nem tartalmaznak. E lépések a jogszabályokban, szabványokban, ajánlásokban felsorolt követelményeket fejtik ki.

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

1. Ellenőriznie kell, hogy az aláírás valóban az aláíró tanúsítványához tartozik-e.
2. Ellenőriznie kell, hogy az aláíró tanúsítványa nem járt-e le, vagyis az aláírás időpontja (amely például az időbélyegekből állapítható meg) a tanúsítvány érvényességi idején belülre esik-e.
3. Ellenőriznie kell, hogy az aláírt dokumentum nem nagyobb pénzösszegről (vagy nagyobb pénzösszegnek megfelelő például eszmei vagy erkölcsi értékről) szól-e, mint amekkora pénzügyi tranzakciós korlát a hozzá tartozó tanúsítványban szerepel.
4. Ellenőriznie kell a tanúsítvány visszavonási állapotát. Erre a következő lehetőségei vannak:
    a. Online tanúsítvány állapot (OCSP) szolgáltatás: Az aláírás időpillanatában lekért OCSP válasz mindig pontos és helyes eredményt ad a tanúsítvány visszavonási állapotáról. Ez a leggyorsabb és legbiztonságosabb módja egy tanúsítvány visszavonási állapotának ellenőrzésének. (A később lekért OCSP válaszok már csak a tanúsítvány későbbi visszavonási állapotára vonatkoznak.)
    b. Az aláírás időpillanatában lekért delta CRL-en szintén mindig helyes eredmény szerepel, mert a Szolgáltató mindig új delta CRL-t bocsát ki, ha egy tanúsítvány állapota megváltozik. A később lekért delta CRL-ekből már nem biztos, hogy meg lehet állapítani az aláírás időpontjában érvényes visszavonási állapotot.
    c. A Szolgáltató nem bocsát ki minden eseménykor CRL-t, így az aláírás időpontját követő első CRL nem biztos, hogy a helyes visszavonási állapotot tartalmazza.
5. Ellenőrizni kell a „Qualified e-Szigno CA” hitelesítő egység tanúsítványának érvényességi idejét és visszavonási állapotát. Ez utóbbit csak CRL és OCSP alapján lehet ellenőrizni, amelyek közül a fent leírt okok miatt célszerű az OCSP-t választani.

A fentiek közül bármelyik ellenőrzés sikertelen, az aláírást nem szabad elfogadni.

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

Tanúsítvány-állapot válasz (OCSP válasz) ellenőrzésekor meg kell vizsgálni a válaszon lévő aláírás érvényességét, valamint azt, hogy a válasz valóban a 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 ellenőrizni kell azt is, hogy az OCSP válaszadó tanúsítványa az OCSP lekérdezés időpontjában érvényes volt-e.

OCSP választ kizárólag akkor szabad 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 nem szabad elfogadni.

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

Időbélyeg ellenőrzésekor meg kell vizsgálni, 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 minden, e tanúsítvány alapján kibocsátott, időbélyeget (visszamenőleg is) érvénytelennek kell tekinteni. (Lásd: RFC 3161, 4. fejezet, 1. és 2. pont) Vitás esetben az egyes időbélyegek érvényessége a Szolgáltató biztonságos naplófájljai segítségével bizonyítható.

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

Az időbélyegző egység tanúsítványát a végfelhasználói tanúsítványokéval megegyező módon kell ellenőrizni. A fentiek miatt, minden egyes alkalommal, amikor egy érintett fél időbélyegre kíván hagyatkozni, minden egyes alkalommal ellenőriznie kell az időbélyegző tanúsítványának aktuális visszavonási állapotát. Időbélyegekkel ellátott aláírás esetében ezt a legkülső időbélyegre kell elvégezni. (Lásd: CWA 14171, 5.4.7.3. fejezet illetve RFC 3161, 2.2. és 4. fejezet)

2.1.6. A közzétételhez kapcsolódó kötelezettségek

A hitelesítő szervezet feladata a tanúsítványok és tanúsítványok, a visszavonási listák, valamint a szolgáltatással kapcsolatos szabályzatok és dokumentációk minden végfelhasználó által elérhető módon történő közzététele (lásd: a **2.6.4** alfejezetet).

Az erre vonatkozó kötelezettségeket a megfelelő Hitelesítési Rend [20] illetve Időbélyegzési Rend [21] részletesen tartalmazza.

2.2. Felelősség

A Szolgáltató felelősségét jelen szolgáltatási szabályzat, a vonatkozó Általános Szerződési Feltételek [22,23], valamint az ügyféllel kötött szolgáltatási szerződés tartalmazzák.

2.2.1. A Szolgáltató általános felelőssége

A Szolgáltató felelősséget vállal az általa támogatott Hitelesítési Rendben [20] illetve Időbélyegzési Rendben [21] leírt eljárásoknak való megfelelésért, még abban az esetben is, amikor a Szolgáltató egyes tevékenységeit alvállalkozók végzik.

a) A Szolgáltató a vele szerződéses jogviszonyban álló felekkel (ilyen az Aláíró és az Aláíró Szervezete és az Ügyfél) szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésszegésért való felelősség szabályai szerint felelős.

b) 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.

c) A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az Aláíróval / Aláíró Szervezetével / Ügyféllel megkötött szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: **Pénzügyi felelősség korlátozása**).

Felelősség korlátozása

A Szolgáltató nem felelős az olyan károkért, amely abból adódott, hogy az Érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és a Szolgáltató szabályzatai szerint járt el, illetve nem úgy járt el, ahogyan az az adott helyzetben elvárható.

A Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helyt állni.

A Szolgáltató nem felelős az abból adódó károkért, amikor az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.

A Szolgáltató tevékenységét a 2/2002-es MeHVM irányelv által elfogadott kriptográfiai algoritmusok segítségével végzi, és a kibocsátott biztonságos aláírás-létrehozó eszközök is a 2/2002-es MeHVM irányelv által elfogadott kriptográfiai algoritmusokat használnak. A Szolgáltató nem felelős ezen kriptográfiai algoritmusok hibájából illetve gyengeségeiből eredő károkért.

A Szolgáltató a Belügyminisztérium közhiteles adatbázisaival végez adategyeztetést, mielőtt az Aláíró tanúsítványát kibocsátja. A Szolgáltató nem vállal felelősséget a Belügyminisztérium által szolgáltatott információk pontatlanságából eredő károkért.

Pénzügyi felelősség korlátozása

A Szolgáltató a kártérítés felső határát tanúsítványonként és összességében is (az összes tanúsítvánnyal és káreseménnyel kapcsolatban) korlátozza. A Szolgáltató pénzügyi felelősségével kapcsolatos további részleteket a vonatkozó Általános Szerződési Feltételek [22,23] tartalmazzák.

2.2.2. A hitelesítő szervezet felelőssége

Az e-Szignó Hitelesítés Szolgáltató felelős:

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

Az e-Szignó Hitelesítés Szolgáltató *nem felelős*:

- az Aláírók magánkulccsal, illetve aláírás-létrehozó eszközzel kapcsolatos tevékenységeiért,
- az Érintett felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért,
- az Érintett felek vagy mások által kibocsátott szabályzatokért.

2.2.3. A regisztráló szervezet felelőssége

Az ügyfélszolgálati iroda *felelős*:

- az Aláírók személyes, az Aláíró Szervezete szervezeti azonosságának megállapításáért; az Aláíró Szervezetét képviselő személy képviseleti jogosultságának megállapításáért,
- a felvett regisztrációs adatok valódiságáért,
- a szolgáltatások igénybevevőjének tájékoztatásáért a Szabályzat tartalmáról és elérhetőségéről, és a szolgáltatás igénybevételének feltételeiről a Szolgáltatói Szerződés megkötését megelőzően,
- általában kötelezettségei betartásáért.

2.2.4. Az Aláíró felelőssége

A hitelesítés szolgáltatással kapcsolatban az Aláíró *felelős*:

- a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért,
- az adataiban bekövetkezett változások haladéktalan bejelentéséért,
- a Szolgáltatási Szerződés betartásáért,
- magánkulcsának és a biztonságos aláírás-létrehozó eszközének a szabályzatoknak megfelelő felhasználásáért,
- magánkulcsának és aktivizáló kódjának biztonságáért,
- a biztonságos aláírás-létrehozó eszköz biztonságáért,
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben,

- általában a kötelezettségei betartásáért.

2.2.5. Az Aláíró Szervezete felelőssége

A hitelesítés szolgáltatással kapcsolatban az Aláíró Szervezete *felelős*:

- a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért,
- az adatokban bekövetkezett változások haladéktalan bejelentéséért,
- a Szolgáltatási Szerződés betartásáért,
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben,
- általában a kötelezettségei betartásáért.

2.2.6. A Költségviselő felelőssége

A hitelesítés szolgáltatással kapcsolatban a Költségviselő *felelős*:

- a hitelesítés szolgáltatás díja(i)nak szerződés szerinti kifizetéséért, azaz a számlákon szereplő összegek megjelölt időpontig történő kifizetéséért,
- általában a kötelezettségei betartásáért.

2.2.7. Az Ügyfél felelőssége

Az időbélyegzés és online tanúsítvány-állapot szolgáltatással kapcsolatban az Ügyfél *felelős*:

- a szolgáltatások díja(i)nak szerződés szerinti kifizetéséért, azaz a számlákon szereplő összegek megjelölt időpontig történő kifizetéséért,
- általában a kötelezettségei betartásáért.

2.2.8. Az Érintett fél felelőssége

Az Érintett fél felelős:

- a tanúsítványok elfogadása során tanúsított körültekintő eljárásért,
- általában a kötelezettségei betartásáért.
- Az Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a vonatkozó Hitelesítési Rend, Szolgáltatási Szabályzat, aláírási szabályzat illetve a hatályos jogszabályok szerint, a tőle elvárható gondossággal jár el.

2.3. Pénzügyi felelősség

A Szolgáltató pénzügyi felelőssége, valamint a 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.

2.3.1. A Szolgáltatóval szembeni kártérítés

Az Ügyfelek (hitelesítés szolgáltatás esetén az Aláíró, az Aláíró Szervezete és a Költségviselő, időbélyegzés és OCSP esetében pedig a szolgáltatásra előfizető illetve az azt igénybe vevő fél) és az Érintett fél kártérítési felelősséggel tartoznak a Szolgáltatóval szemben azokért a veszteségekért és károkért, amelyeket kötelezettségeik be nem tartásával okoznak számára.

2.3.2. 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.

2.4. Értelmezés és érvényesítés

2.4.1. 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 hatályos jogszabályokat lásd a vonatkozó Hitelesítési Rendben [20] illetve Időbélyegzési Rendben [21].

2.4.2. Érvénytelenség, fennmaradás, megszűnés és értesítések

Érvénytelenség

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

Fennmaradás

A Szabályzat 2. 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 Szabályzat a Közösség valamennyi kötelezettségét, felelősségét és jogát tartalmazza vagy meghivatkozza. A 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 Szabályzat csak írott és hitelesített formában módosítható, a Hatóság által vezetett szabályzat-nyilvántartásban való átvezetés mellett.

Értesítések

Az Ügyfelek (hitelesítés szolgáltatás esetén az Aláíró, az Aláíró Szervezete és a Költségviselő, időbélyegzés és OCSP esetében pedig a szolgáltatásra előfizető illetve az azt igénybe vevő fél) 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, illetve visszaállíthatók. 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.

2.4.3. Vitás kérdések megoldására vonatkozó eljárások

A szolgáltatásokkal kapcsolatos bármely vitás kérdés vagy panasz felmerülése esetén a vita jogi útra terelése előtt az Ügyfeleknek és az Érintett feleknek kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően. A felek vitáikat mindenkor megkísérlik tárgyalásos úton rendezni.

A Szolgáltató tevékenységével vagy a kiadott tanúsítványok, időbélyegzők és online tanúsítvány-állapot válaszok 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 beérkezett panaszokat a panasz bejelentésétől számított 30 napon belül mindenképpen kivizsgálja, és tájékoztatja a bejelentőt a vizsgálat eredményéről. 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 20 munkanapon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az érintett felek kölcsönösen alávetik magukat a Magyar Kereskedelmi és Iparkamara mellett szervezett Állandó Választottbíróság kizárólagos illetékességének. A Választottbírósági eljárás nyelve a magyar, az eljárásban irányadó jog a mindenkor hatályos magyar jog.

2.5. 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.

2.5.1. A hitelesítés szolgáltatásához kapcsolódó díjak és árak

A Szolgáltató a kibocsátott tanúsítványok fenntartásáért, valamint a tanúsítványcseréért és tanúsítvány-visszaállításáért a vonatkozó ÁSZF-ben [22] megjelölt díjelemekből és árakból megállapított összeget számláz ki a Költségviselő felé.

A Szolgáltató az átadott és megszemélyesített aláírás-létrehozó eszközökért az árlista szerinti árakat számláz ki a Költségviselő felé.

A Szolgáltató nem számol fel díjat

- a közzétett tanúsítványok eléréséért,
- a közzétett visszavonási listák eléréséért,
- a kibocsátott tanúsítványok visszavonásáért és felfüggesztéséért.

2.5.2. Időbélyegzés és online tanúsítvány-állapot szolgáltatási díjak

A Szolgáltató a szolgáltatásokért a vonatkozó ÁSZF-ben [23] megjelölt díjelemekből megállapított díjat számol fel az Ügyfél felé.

2.5.3. Visszatérítési elvek

2.5.3.1. Befizetett díjak visszaigénylése

Az adott időszakra már befizetett szolgáltatási díj nem igényelhető vissza.

Hitelesítés szolgáltatás esetében, amennyiben a tanúsítvány a szolgáltatási időszak lejárta előtt visszavonásra került, és az Ügyfél – a szolgáltatási időszak lejárta előtt – kérvényezi új tanúsítvány kibocsátását (tanúsítványcsere), akkor a korábban visszavont tanúsítvány szolgáltatási díjának az új tanúsítvány kibocsátási dátuma és a visszavont tanúsítvány eredeti lejárati dátuma közti időszakra eső arányos részét a Szolgáltató az új tanúsítvány szolgáltatási díjából jóváírja.

2.5.3.2. Tévesen kiállított számla

A Szolgáltató által kiállított számlát a Költségviselő a számlán feltüntetett fizetési határidőn belül köteles átutalással vagy pénztári befizetéssel kiegyenlíteni. A számla összege ellen a Költségviselő a számlán feltüntetett fizetési határnapig reklamációval élhet. Jogos reklamáció esetén a Szolgáltató a helyes összegről új számlát állít ki, amit a Költségviselőnek az azon feltüntetett új fizetési határidőn belül kell kiegyenlítenie.

Ha a még ki nem fizetett, tévesen kiállított számla összege ellen a Költségviselő csak a számlán feltüntetett fizetési határnapot követően él reklamációval, ebben az esetben a helyesen meghatározott összeg után az eredeti fizetési határidő szerint köteles késedelmi kamatot fizetni.

Ha a Költségviselő egy már megfizetett számla összege ellen szólal fel és reklamációja jogos, úgy a Szolgáltató a tévesen megállapított összeget a Költségviselő részére 8 napon belül jóváírja vagy visszatéríti.

Fizetési késedelem esetén mind a Szolgáltató, mind a Költségviselő a ki nem egyenlített összeg után a fizetési határidőt követő első naptól a mindenkori jegybanki alapkamat kétszeresének megfelelő, de minimum 10% késedelmi kamat megfizetésére kötelesek. A Költségviselőt alaptalan számlareklamáció esetén is – a ki nem egyenlített összeg erejéig – a fenti mértékű késedelmi kamatfizetési kötelezettség terheli.

A Szolgáltató a fel nem számított vagy tévedésből be nem szedett díjat az esedékesség napjától számított egy éven belül követelheti, a tévesen felszámított, illetve beszedett díjakra egy éven belül fogad reklamációkat.

2.6. Közzététel szolgáltatás

2.6.1. A szolgáltatói információ közzététele

2.6.1.1. Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában (MS-Word és / vagy Adobe Acrobat formátumokban) hozza nyilvánosságra a honlapján.

A honlapon az érvényben levő dokumentumokon kívül a korábbi verziók is elérhetőek.

2.6.1.2. Rendkívüli információk közzététele

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

- tevékenységének befejezése (lásd: **4.9 A szolgáltatások leállítása**),
- valamely, általa működtetett hitelesítő egység (lásd: **1.3.1 Hitelesítő szervezet**) magánkulcsának kompromittálódása.

2.6.1.3. Tanúsítványok nyilvánosságra hozatala

A Szolgáltató a *szolgáltatói tanúsítványokat* (az általa működtetett hitelesítő egységek, valamint az időbélyegzés szolgáltató és az online tanúsítvány-állapot szolgáltatásban részt vevő egységek tanúsítványát) a következő módszerekkel teszi közzé:

- A *Microsec e-Szignó Root CA* és az *e-Szignó Online Tanúsítvány-állapot CA* hitelesített tanúsítványait egy országos terjesztésű napilapban teszi közzé (lásd: **1.3.1 Hitelesítő szervezet**).
- Az *szolgáltatói tanúsítványok közül* a Microsec e-Szignó Root CA, Minősített e-Szignó CA és az e-Szignó Online Tanúsítvány-állapot CA tanúsítványait a Szolgáltató honlapján keresztül teszi közzé.
- Az Aláíró számára a végfelhasználói tanúsítvánnyal együtt a tanúsítási láncában szereplő tanúsítványokat átadja.

A Szolgáltató a *végfelhasználói tanúsítványokat* az Érintett felek részére közzéteszi a honlapján a http://www.e-szigno.hu/lookup.html címen.

2.6.1.4. A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala

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

- A *Microsec e-Szignó Root CA* és az *e-Szignó Online Tanúsítvány-állapot CA* önhitelesített tanúsítványainak állapotváltozásáról egy országos terjesztésű napilapban tesz közzé hirdetést. Az önhitelesített esetében ez az egyetlen módszer tekinthető hivatalos formának (lásd: **1.3.1 Hitelesítő szervezet**).
- A minősített végfelhasználói tanúsítványokat kibocsátó *Minősített e-Szignó CA*, valamint az időbélyegzőket kibocsátó *e-Szignó Időbélyegzés Szolgáltató* tanúsítványainak állapotváltozását a

visszavonási listákon, saját honlapján, valamint az online tanúsítvány-állapot válasz szolgáltatás keretében hozza nyilvánosságra.

- Az online tanúsítvány-állapot válaszokat aláíró *e-Szignó Online Tanúsítvány-állapot Szolgáltató* számára – a nemzetközi legjobb gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű (10 percig érvényes) tanúsítvány kerül kibocsátásra, ezzel kiküszöbölve azt, hogy a tanúsítvány visszavonási állapotát ellenőrizni kelljen. A 10 percig érvényes tanúsítvány visszavonási állapotát a Szolgáltató kizárólag olyan módon teszi közzé, hogy kulcs kompromittálódás vagy bármilyen egyéb probléma esetén egyszerűen nem kerül kibocsátásra újabb tanúsítvány. Az OCSP válaszok ellenőrzését bővebben a 2.1.5. 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.

A végfelhasználói tanúsítvány visszavonását és felfüggesztését a Szolgáltató akkor mindig nyilvánosságra hozza, ehhez nem szükséges az Aláíró hozzájárulása.

Az állapot-információk közlésének módszereit illetően lásd még a **4.4 Tanúsítvány-felfüggesztés és-visszavonás** alfejezetet.

2.6.2. A közzététel gyakorisága

Kikötések és feltételek közzétételi gyakorisága

A Szabályzattal kapcsolatos új verziók közzététele a **8. Leírás-adminisztráció** fejezetben ismertetett eljárásoknak megfelelően történik.

A Szolgáltató szükség szerint kibocsátja az egyéb szabályzatait és szerződéses feltételeit, illetve az újabb változatokat.

Rendkívüli információk közzétételi gyakorisága

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

Tanúsítványok nyilvánosságra hozatalának gyakorisága

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

- Az általa működtetett *Microsec e-Szignó Root CA* és *e-Szignó Online Tanúsítvány-állapot CA* tanúsítványát a szolgáltatás megkezdését követő vagy az új tanúsítvány kibocsátását követő 10 munkanapon belül teszi közzé
- Az általa működtetett *Minősített e-Szignó CA, Microsec e-Szignó Szerver CA*, *e-Szignó Időbélyegzés Szolgáltató* és az *e-Szignó Online Tanúsítvány-állapot Szolgáltató* tanúsítványait a kibocsátást követően haladéktalanul, honlapján 5 munkanapon belül hozza nyilvánosságra.
- A Szolgáltató a végfelhasználói tanúsítványokat a kibocsátást követően, a regisztrációs eljárás részeként, a biztonságos aláírás-létrehozó eszközön átadja az Aláíró részére.
- A Szolgáltató a végfelhasználói tanúsítványokat a tanúsítványtárban az előállítást követően haladéktalanul megjeleníti.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

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

A tanúsítványok állapotra vonatkozó információk a tanúsítványtárban a tanúsítvány-visszavonási listákon és a különbségi tanúsítvány-visszavonási listákon érhetőek el. A tanúsítvány-visszavonási listák kibocsátási gyakoriságát a **4.4.6 Visszavonási állapot közzététele** alfejezet tárgyalja.

2.6.3. 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 tanúsítványok és állapot-információk elérése a megfelelő Hitelesítési Rend [20] és jelen Szolgáltatási Szabályzat kikötéseinek és feltételeinek elfogadását jelenti.

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.

2.6.4. A tanúsítványtár

A Szolgáltató tanúsítványtára http lekérdezésekkel érhető el a Szolgáltató honlapjáról.

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

2.7. A megfelelőség vizsgálata

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

- a minősített tanúsítványok aláírására, az időbélyeg előállítására, valamint magánkulcsainak tárolására használt kriptográfiai hardver modult (nShield F3 SCSI hardver kriptográfiai modul), amely rendelkezik az Eat. 7 § (5) -(6) szerinti igazolással.
- a minősített tanúsítványok kibocsátásához, gondozásához használt CA szoftvert (RSA Keon Certificate Authority, v6.5.1),
- a saját informatikai rendszerén belül, az infrastrukturális és megbízható rendszervezérlési kulcsok generálására, tárolására és felhasználására alkalmazott intelligens kártyát (P8WE5032v0G mikrochipből, STARCOS SPK 2.3 v7.0 operációs rendszerből, valamint SafeSign 1.0.9.04 digitális aláírás alkalmazásból álló intelligens kártya), más infrastrukturális kulcsokat GemSafe intelligens kártyán illetve StarKey USB tokenen tárol.
- a saját informatikai rendszerén belül, az infrastrukturális kulcsok generálására, tárolására és felhasználására alkalmazott Gemsafe intelligens kártyát
- biztonságos aláírás-létrehozó eszközöket, amelyeket az Aláírók számára biztosít (P8WE5032v0G mikrochipből, STARCOS SPK 2.3 v7.0 operációs rendszerből, valamint a StarCert v2.2 digitális aláírás alkalmazásból álló intelligens kártya), e termék is rendelkezik az Eat. 7 § (5) -(6) szerinti igazolással.

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 tanúsításhoz a Szolgáltató külső szervezetet vesz igénybe (lásd: **2.7.2 Az átvizsgáló szervezet megnevezése és jellemzői**). A Szolgáltató e külső tanúsításokon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely rendszeresen vizsgálja a korábbi tanúsításoknak való megfelelőséget, és eltérés esetén megteszi a szükséges lépéseket.

A Szolgáltató 2002 óta rendelkezik az ISO 9001:2000 szabványnak megfelelő minőségirányítási, valamint 2003 óta a BS 7799-nek megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet auditál és vizsgál felül folyamatosan (**lásd: 1.1.3. A Szolgáltató**).

2.7.1. A megfelelőség-vizsgálat gyakorisága

A kriptográfiai hardver modulok, a saját informatikai rendszerén belül alkalmazott intelligens kártyák és a biztonságos aláírás-létrehozó eszközök tanúsítására a használatba vételt megelőzően kerül sor. A tanúsítás érvényessége 3 év, amelynek lejártával a megfelelőség-vizsgálatot meg kell ismételni.

A minősített tanúsítványok kezeléshez használt rendszerek és módszerek tanúsítására hatósági felülvizsgálati eljárás keretében kerül sor, s a jogszabályoknak megfelelően legalább évente átfogó helyszíni ellenőrzéssel jár együtt.

2.7.2. Az átvizsgáló szervezet megnevezése és jellemzői

A biztonságos aláírás-létrehozó eszköz tanúsítását egy erre feljogosított tanúsító szervezet (lásd: [1] törvény 24. §) végezte, amelynek kijelölésére a jogszabályi előírásoknak megfelelően került sor. A tanúsított elektronikus aláírási terméket a Hatóság nyilvántartásba vette.

A kriptográfiai hardver modul Szlovákiában szerepel a tanúsított elektronikus aláírás termékek listáján, amely az [1] törvény, értelmében Magyarországon is elfogadott.

2.7.3. Az átvizsgáló szervezet és a vizsgált fél kapcsolata

A Szolgáltatóval kapcsolatban tanúsítást végző szervezetek a Szolgáltatótól függetlenek, és befolyástól mentesen végzik tevékenységüket. A vizsgálatot végző szervezet és a Szolgáltató között nincs közvetlen vagy közvetett tulajdonosi kapcsolat. A tanúsító szervezet díjazása nem függött a tanúsítás során végzett tevékenységének megállapításaitól.

2.7.4. A vizsgálat által érintett területek

A biztonságos aláírás-létrehozó eszközök tanúsítása az [1] törvény 1. mellékletének való megfelelőség vizsgálatára irányult.

A minősített tanúsítványok kezeléshez használt rendszerek és módszerek tanúsítása az [1] törvény 3. mellékletének és a [32] rendelet előírásainak, valamint a Szolgáltató saját Hitelesítési Rend [20] illetve Időbélyegzési Rend [21] dokumentumának és egyéb szabályzatainak való megfelelőség vizsgálatára irányul.

2.7.5. Hiányosságok esetén végrehajtandó tevékenységek

A felölvizsgálati eljárás, vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató a Hatósággal megállapodott határidőn belül megszünteti a vizsgálatot végző Hatóságtól kapott információ és ajánlások alapján.

2.7.6. Az eredményekről való tájékoztatás

A Szolgáltató a tanúsítások eredményének tényét a honlapján közzéteszi. Ez nem vonatkozik a tanúsítási eljárás során feltárt, az eljárás végeredményét nem befolyásoló hiányosságokra és részeredményekre.

A felülvizsgálati eljárás eredményét a Hatóság a minősített hitelesítés-szolgáltatók adatait tartalmazó nyilvántartásban közli.

2.8. Bizalmasság

A Szolgáltató az Ügyfelek adatait a jogszabályoknak megfelelően kezeli. A Szolgáltató rendelkezik adatkezelési szabályzattal (lásd **4.10 Az Ügyfél adatainak kezelése**), 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 Aláírói adatlapon 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 Aláíró Szervezete tanúsítványban megjelenő adatai a tanúsítványba foglalva (lásd: **7. Tanúsítvány, tanúsítvány-visszavonási lista, időbélyeg és online tanúsítvány-állapot válasz profilok**), valamint a Szolgáltató tanúsítványtárán keresztül nyilvánosságra kerülnek a nyilvános kulcs tulajdonosának azonosítása céljából, a tanúsítványba nem kerülő adataikat a Szolgáltató védett módon tárolja az Aláíró személyes azonosságának, az Aláíró Szervezete 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.

2.8.1. Bizalmasan kezelendő információ-típusok

a) A Szolgáltató bizalmas információként kezeli az Ügyfelek minden adatát, kivéve azokat, amelyeket a **2.8.2 Nem bizalmasnak tekintett információ típusok** alfejezet tárgyal.

b) 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 **2.8.3**-**2.8.7** alfejezetekben említett esetekben és személyek/szervezetek részére fedi fel őket.

c) 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.

2.8.2. Nem bizalmasnak tekintett információ típusok

A Szolgáltató nem bizalmas információként kezeli mindazon adatokat, amelyet a tanúsítványba belefoglal. Ezek az adatok a Szolgáltatási Szerződéshez kapcsolódó Aláírói adatlapon egyértelmű jelöléssel szerepelnek.

2.8.3. Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése

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. Tanúsítvány visszavonási lista (CRL) profil** alfejezetben található.

2.8.4. Információszolgáltatás a hatóságok részére

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

b) A Szolgáltató rögzíti az a) pontbeli adatátadás tényét, de arról nem tájékoztatja az érintett Ügyfeleket.

2.8.5. Információszolgáltatás polgári eljárás keretében

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

b) A Szolgáltató rögzíti az a) pontbeli adatátadás tényét, és arról tájékoztatja az érintett Ügyfelet.

2.8.6. 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.

2.8.7. Egyéb információ-közzétételt eredményező körülmények

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

2.9. Szellemi tulajdonjogok

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

b) A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.

c) A visszavonási információ a Szolgáltató tulajdonát képezi.

d) A Szolgáltató által az Aláíró részére kibocsátott egyedi azonosító a Szolgáltató tulajdonát képezi.

e) A tanúsítványban szereplő Aláíró azonosító (Subject) használatára a megnevezett aláíró jogosult.

f) A Szolgáltató szabályzatai, szerződéses feltételei a Szolgáltató tulajdonát képezik.

3. Azonosítás és hitelesítés

3.1. Regisztráció

3.1.1. Név típusok

A tanúsítvány alapmezői között található *Kibocsátó azonosító* (Issuer) illetve *Aláíró azonosító* (Subject) mezők a [12] szerinti egyedi név formátum előírásainak felelnek meg. Ezen kívül a Szolgáltató támogatja az kiterjesztések között található Alternatív név mezők (Subject Alternative Names, Issuer Alternative Names) kitöltését is.

3.1.1.1. Kibocsátó azonosító

A *tanúsítvány kibocsátójának* azonosítója (az *Issuer* mező tartalma) a következő módon épül fel:

Mező	Értelmezés	Érték
Common Name (CN) OID: 2.5.4.3	A tanúsítványt kibocsátó hitelesítő egység neve ékezet nélkül	Qualified e-Szigno CA
Organization (O) OID: 2.5.4.10	A Szolgáltató szervezetének neve ékezet nélkül	Microsec Ltd.
Organizational unit (OU) OID: 2.5.4.11	A Szolgáltató szervezeti egységének neve ékezet nélkül	e-Szigno CA

Mező	Értelmezés	Érték
Country (C) OID: 2.5.4.6	A Szolgáltató székhelye szerinti ország kétbetűs rövidítése	HU
Locality (L) OID: 2.5.4.7	A Szolgáltató székhelye szerinti város neve ékezet nélkül	Budapest

A minősített végfelhasználói tanúsítvány kibocsátójának tanúsítványában, az alany azonosító mezőben (Subject) ugyanezen adatok szerepelnek.

3.1.1.2. Kibocsátó alternatív nevei

A minősített végfelhasználói tanúsítványokban a Kibocsátó alternatív nevei (Issuer Alternative Names) mező nem kerül kitöltésre.

A minősített végfelhasználói tanúsítvány kibocsátójának tanúsítványában, az Aláíró alternatív nevei mező kitöltésre kerül a következők szerint:

Mezőnév	Értelmezés és érték vagy szabály	Kritikus
Aláíró alternatív nevei *Subject Alternative Names* OID: 2.5.29.17	CN = Minősített e-Szignó CA O = Microsec Kft. OU = e-Szignó HSZ L = Budapest C = HU rfc822Name = info@e-szigno.hu	Nem

3.1.1.3. Aláíró azonosító

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

Mező	Értelmezés	Kitöltési szabály
Common Name (CN) OID: 2.5.4.3	Az Aláíró neve	A személyazonosító okmányban szereplő adat, magyar írásmód szerint (ékezetesen); kérésre ékezet nélkül.
Pseudonym (PSEUDO) OID: 2.5.4.65	Az Aláíró álneve	Álneves tanúsítvány esetén (kizárólag az álneves hitelesítési rend esetén) az aláíró által választott tetszőleges szöveg, amelyet a Szolgáltató nem ellenőriz. Nem álneves tanúsítvány esetén (álnevet kizáró hitelesítési rend esetén) e mező üresen marad.

Mező	Értelmezés	Kitöltési szabály
Serial Number (SN) OID: 2.5.4.5	Az Aláíró egyedi azonosítója az e-Szignó Hitelesítés Szolgáltató nyilvántartásában, vagy kérésre egyéb, a Szolgáltató által ellenőrzött egyedi azonosító az *Aláírói adatlap* szerint.	E mezőbe az e-Szignó Hitelesítés Szolgáltató nyilvántartásában szereplő egyedi azonosító (OID) kerül. Az azonosító értéke: 1.3.6.1.4.1.21528.2.2.x.y ahol x az aláírót regisztráló regisztrációs egység, y pedig az adott egység által regisztrált aláíró sorszáma. A Szolgáltató garantálja, hogy különböző személyekhez soha nem rendel azonos OID-et. Az Aláíró jogosult regisztrációkor friss, még senkihez hozzá nem rendelt OID-et kérni. Az Aláíró új tanúsítványában akkor kaphatja meg egy korábbi tanúsítványban szereplő OID-et, ha bizonyítja, hogy az a tanúsítvány is őhozzá tartozott. A tanúsítvány több SN mezőt is tartalmazhat, e további mezőkben 'típus' = 'értéke' formátumú párok is szerepelhetnek. pl2.: Szig.szám. = AAAAAA
Organization (O) OID: 2.5.4.10	Amennyiben az Aláíró egy szervezethez kapcsolódik, akkor annak a rövid neve. (Személyes és Hivatáshoz kapcsolódó tanúsítvány esetében nem; csak Szervezeti és közalkalmazotti/ köztisztviselői tanúsítvány esetében kerül kitöltésre.)	A cég/szervezet rövid neve az alapító okirat vagy a cégbejegyzés szerint ékezetesen vagy kérésre ékezet nélkül.
Organizational unit (OU) OID: 2.5.4.11	Amennyiben az Aláíró egy szervezeti egységhez kapcsolódik, akkor annak a neve. (Személyes és Hivatáshoz kapcsolódó tanúsítvány esetében nem; csak Szervezeti és közalkalmazotti/köztisztviselői tanúsítvány esetében kerül kitöltésre.)	A szervezeti egység vagy részleg rövid neve az *Aláírói adatlapnak* megfelelően (ékezetesen vagy ékezet nélkül).
Country (C) OID: 2.5.4.6	Az Aláíró állandó lakcíme szerinti ország (Személyes és Hivatáshoz kapcsolódó tanúsítvány esetében) vagy – amennyiben van ilyen – az Aláíróhoz kapcsolódó szervezet székhelye szerinti ország (Szervezeti és közalkalmazotti/köztisztviselői tanúsítvány esetében).	Az ország kétbetűs rövidítése kerül beírásra nagybetűkkel (pl. Magyarország esetében: HU).
Locality (L) OID: 2.5.4.7	Az Aláíró állandó lakcíme szerinti város (Személyes és Hivatáshoz kapcsolódó tanúsítvány esetében) vagy – amennyiben van ilyen – az Aláíróhoz kapcsolódó szervezet (cégbejegyzés vagy alapító okirat szerinti) székhelye szerinti város (Szervezeti és közalkalmazotti/ köztisztviselői tanúsítvány esetében).	A város neve a kért nyelven, ékezetesen vagy kérésre ékezet nélkül.

Mező	Értelmezés	Kitöltési szabály
Title (T) OID: 2.5.4.12	Amennyiben az Aláíró egy szervezethez kapcsolódik (Szervezeti és közalkalmazotti/ köztisztviselői tanúsítvány esetében), akkor az Aláíró szervezetben betöltött szerepe. Hivatás igazolása esetén (Hivatáshoz kapcsolódó tanúsítvány esetében) a hivatás megnevezése (közjegyző", „ügyvéd" vagy „bíró").	*Értéke:* • *Személyes tanúsítvány esetén nem szerepel Title mező a tanúsítványban.* • *Hivatáshoz kapcsolódó tanúsítvány esetében: „közjegyző", „ügyvéd" vagy „bíró".* • *Szervezeti és közalkalmazotti/ köztisztviselői tanúsítvány esetében a szervezet által igazolt, a szervezeten belüli szerep. Különleges szerepek a következők:* ○ *„A tanúsítványban szereplő szervezet képviseletére jogosult"* ○ *„Jogosult a tanúsítványban szereplő szervezethez tartozó tanúsítványok ügyében eljárni"*
E-mail address (EMAIL) OID: 1.2.840. 113549.1.9.1	Az Aláíró e-mail címe. Létező e-mail címnek kell lennie, valamint amennyiben az Aláíró szervezethez kapcsolódik, akkor a szervezeten belüli e-mail címnek kell lennie.	*Értéke:* E-mail cím az Aláírói adatlapnak megfelelően. *Kitöltése opcionális.* Meg kell egyeznie a tanúsítvány kiterjesztések között szereplő Aláíró alternatív névben megadott e-mail címmel.

3.1.1.4. Aláíró alternatív név

Az *Aláíró* alternatív nevei (Subject Alternative Names) a következő módon épül fel:

Mezőnév	Értelmezés és érték vagy szabály	Kritikus
Aláíró alternatív nevei *Subject Alternative Names* OID: 2.5.29.17	Ha a tanúsítvány tartalmazza az EMAIL mezőt, akkor a Subject Alternative Names RFC822name mezejébe ugyanezen e-mail cím kerül. Ha az Aláíró kéri, akkor a Subject Alternative Names Common Name (CN) mezejébe bekerülhet a Subject DN Common Name mezejében szereplő neve ékezetes illetve ékezet nélküli írásmóddal.	Nem

3.1.2. Igény a nevek értelmezhetőségére

Az Aláíró azonosítóra (Subject mezőre) a következő szabályok érvényesek:

- Az azonosítónak értelmezhetőnek kell lenni.
- Magyar állampolgárok nevének felvétele során a bemutatott személyazonosító okmányban szereplő írásmódot kell követni; alapértelmezés szerint ékezetesen, kérésre ékezet nélkül.

3.1.3. Különböző elnevezési formák értelmezési szabályai

A Kibocsátó azonosító (Issuer mező) a következő módon értelmezendő:

- A tanúsítványt a Microsec Kft. e-Szignó Hitelesítés Szolgáltató minősített tanúsítványokat kibocsátó hitelesítő szervezete adta ki.

Az Aláíró azonosító (Subject mező) a következő módon értelmezendő:

- A tanúsítvány által azonosított alany természetes személy, neve a Common Name mezőben, egyedi azonosítója a Serial Number mezőben szerepel.

- Amennyiben az Aláíró egy szervezethez kapcsolódik, akkor (és csak akkor) kitöltésre kerül az Organization mező, amely az Aláíró Szervezetének rövid nevét tartalmazza. Ha az Aláíró a szervezeten belül szervezeti egységhez is köthető, az az Organization Unit mezőben kerül feltüntetésre. Az Aláíró és az Aláíró Szervezete együttes megjelenítése a tanúsítványban azt jelenti, hogy az Aláíró Szervezete hozzájárult az Aláíró és az Aláíró Szervezete nevének együttes feltüntetéséhez.
- Amennyiben az Aláíró egy szervezethez kapcsolódik, akkor a Country (ország) és Locality (város) mezők az Aláíró Szervezetének székhelye szerinti országot vagy várost tartalmazzák. Egyébként az Aláíró tartózkodási helye szerinti országot illetve várost tartalmazzák.
- Az Aláíró e-mail címét az E-MAIL mező tartalmazza. Ennek értéke, amennyiben az Aláíró szervezethez kapcsolódik, az Aláíró Szervezetén belüli e-mail cím kell, hogy legyen.
- Az Aláíró igazolt szerepét a TITLE mező tartalmazza. Amennyiben az Aláíró egy szervezethez kapcsolódik, akkor a TITLE mezőben megjelölt szerep a szervezeten belül betöltött – az Aláíró Szervezete által igazolt – szerepet tartalmaz.

  Lényeges, hogy szervezeti tanúsítványok esetén a TITLE mezőben feltüntetett szerepet az Aláíró Szervezete igazolja. Ez esetben a Szolgáltató bármilyen az Aláíró Szervezete által meghatározott szerepet feltüntet a tanúsítványban, e szerep valódiságáért az Aláíró Szervezetét terheli a felelősség. Szervezeti tanúsítványok esetén a tanúsítvány Organization (O) mezeje minden esetben az Aláíró Szervezetének nevét tartalmazza.

Az azonosítók értelmezése érdekében az Érintett feleknek a jelen Szolgáltatási Szabályzatban leírtak alapján kell eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett félnek segítségre lenne szüksége, akkor a Szolgáltatóval közvetlen is felveheti a kapcsolatot. A Szolgáltató ilyen esetben az Aláíró és az Aláíró Szervezete egyéb adatairól többlettájékoztatást – feltéve, hogy jogszabály ezt nem írja elő – nem ad, csak a tanúsítványban feltüntetett adatok értelmezését segítő információt szolgáltatja.

3.1.4. A nevek egyedisége

Az Aláíró azonosító (Subject) a Szolgáltató tanúsítványtárában egyedi. Erről elsődlegesen az Aláíró azonosító Serial Number (SN) 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. Az Aláíró azonosító (Subject mező) ezáltal garantáltan egyedi lesz.

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

3.1.6. Márkanevek elismerése, hitelesítése és szerepe

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

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

3.1.7. A magánkulcs birtoklása

A Szolgáltató saját szervezetén belül maga generáltatja a kulcsokat a biztonságos aláírás-létrehozó eszközökön, ezért nem kell ellenőriznie azt, hogy az Aláíró rendelkezik-e a hitelesítendő nyilvános kulcs magánkulcs-párjával.

3.1.8. A szervezeti azonosság hitelesítése

Bizonyos tanúsítványfajták esetén az Aláíró Szervezete is feltüntetésre kerül a végfelhasználói tanúsítványokban. Ezekben az esetekben az Aláíró Szervezetének is alá kell írnia a Szolgáltatói Szerződést. Ekkor kérésre a szervezeten belüli szervezeti egység is feltüntethető.

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

- az Aláíró Szervezetének teljes és rövid neve, székhelye
- a szervezeti egység neve, ha kérik ennek feltüntetését a tanúsítványban,
- az Aláírónak az Aláíró Szervezetében betöltött szerepe,
- az Aláíró Szervezetének hivatalos azonosító adatai,
- igazolás arra vonatkozóan, hogy a szervezet nevében a Szolgáltatási Szerződést aláíró személy jogosult-e az aláírás megtételére.

A tanúsítvány-igényléshez csatolni kell a 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. Cégbíróságon bejegyzett cégek esetében a cégkivonatot (új bejegyzésű szervezet esetében a hatósági tanúsítást), más szervezetek esetében a szervezet hivatalos bejegyzését tanúsító okiratot is mellékelni kell a kérelemhez.

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 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. A hiánypótlási határidő minden esetben 15 munkanap.

3.1.9. A személyazonosság hitelesítése

A Szolgáltató a tanúsítványban megnevezésre kerülő természetes személy azonosítását követeli meg a regisztráció és a tanúsítványcsere során.

A Szolgáltató az alábbi okmányokat fogadja el a személyazonosság hitelesítéséhez, de fenntartja a jogot, hogy további okmányokat is elfogadhasson, amennyiben azok hitelességéről meg tud győződni, és segítségével képes az Aláírót (igénylőt) hitelesíteni.

- Személyi igazolvány
- Útlevél,
- Jogosítvány

Az Aláírónak a személyazonosságát a fentiek közül legalább egy igazolvánnyal kell igazolnia.

A személyi igazolványban, útlevélben és jogosítványban szereplő fénykép alapján az Aláírónak egyértelműen felismerhetőnek kell lennie, és a benne szereplő aláírásnak meg kell egyezni az Aláírói nyilatkozaton tett aláírásával.

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 úti-okmány nyilvántartással és a gépjárművezetői nyilvántartással történő adategyeztetéssel ellenőrzik.

A Szolgáltató a bemutatott dokumentumokról az adatkezelési szabályzat szerint fénymásolatot készít és archiválja azokat, vagy jegyzőkönyvet vesz fel.

A Szolgáltató a tanúsítvány kibocsátását megtagadja az alábbi esetekben:

- az igénylő nem képes a szükséges adatokat hitelt érdemlően bizonyítani, vagy

- a bemutatott dokumentumok és az abban foglalt adatok nem valódiak, hiányosak vagy nem érvényesek,
- a Szolgáltató nem tud egyértelműen megbizonyosodni a bemutatott dokumentumok valódiságáról vagy érvényességéről, illetve az igénylő személyazonossága nem állapítható meg kétséget kizáróan.

3.2. Tanúsítványcsere érvényes tanúsítvány esetén

A Szolgáltató a tanúsítványok cseréjének elektronikus üzenetváltáson alapuló, személyes megjelenést nem igénylő megvalósítását nem teszi lehetővé, tanúsítványát az Aláíró az ügyfélszolgálati irodában újíthatja meg.

3.3. Tanúsítványcsere érvénytelen tanúsítvány esetén

A Szolgáltató a tanúsítványok cseréjének elektronikus üzenetváltáson alapuló, személyes megjelenést nem igénylő megvalósítását nem teszi lehetővé, tanúsítványát az Aláíró az ügyfélszolgálati irodában újíthatja meg.

3.4. Felfüggesztési és visszavonási kérelem

Szolgáltató tanúsítvány visszavonási és felfüggesztési szolgáltatásokat egyaránt nyújt. Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait a 4.4. fejezete tárgyalja.

3.5. Időbélyegzés és online tanúsítvány-állapot szolgáltatás

Időbélyegzés és online tanúsítvány-állapot szolgáltatás szerződés megkötéséhez a Szolgáltató a természetes személy előfizetőt személyi valamely személyazonosításra alkalmas igazolványa alapján azonosítja, a szervezeti előfizetőknek pedig igazolniuk kell a szervezet nyilvántartási számát (vállalatok esetén cégjegyzékszám), valamint igazolni kell az aláírási jogosultságukat is.
A szolgáltatás igénybevétele során a Szolgáltató HTTPS protokollon keresztül hitelesíti az előfizetőt. A szolgáltatás felhasználónév és jelszó párral vehető igénybe. A kezdeti jelszót szerződéskötéskor kell megadni.

4. Működésre vonatkozó követelmények

4.1. Tanúsítvány igénylés

Új végfelhasználói tanúsítvány kibocsátása a Szolgáltató ügyfélszolgálati irodában, vagy valamelyik külső regisztrációs szervezeténél igényelhető. A tanúsítványhoz tartozó aláírás létrehozó adat átvételéhez az Aláíró személyes megjelenése szükséges.

Az igénylési eljárás lépései a következők:

- Az Aláíró tájékozódik a Szolgáltató tanúsítványtípusairól és a szolgáltatás igénybevételének feltételeiről. Ezt a Szolgáltató honlapján vagy az ügyfélszolgálati irodájában teheti meg.
- Az Aláíró kitöltött aláíró adatlapot juttat el a Szolgáltató ügyfélszolgálati irodájába. Az Aláíró az aláírói adatlapot személyesen, postán, vagy elektronikusan juttathatja el az ügyfélszolgálati irodába. Elektronikus esetben a tanúsítvány igénylése minősített elektronikus aláírással is történhet.
- A Szolgáltató ellenőrzi az aláírói adatlapon szereplő és tanúsítványba is bekerülő információkat.
- A Szolgáltató adategyeztetést végez a Belügyminisztérium közhiteles adatbázisaival.
- olyan tanúsítvány esetén, amelyben az Aláíró Szervezet is szerepel, a Szolgáltató igazolást kér az Aláíró Szervezetétől arról, hogy az aláíró – az aláírói adatlapon megjelölt szerepkörben – jogosult a tanúsítványban szerepelni
- A Szolgáltató meghatározza az Aláíró egyedi nevét, ennek keretében globálisan egyedi azonosítót (OID) rendel az aláíróhoz.
- legkésőbb a tanúsítványhoz tartozó aláírás létrehozó adat átvételekor (és akkor mindenképpen) az Aláírónak személyesen meg kell jelennie a Szolgáltató vagy egy külső regisztrációs szervezete ügyfélszolgálati irodájában, ahol igazolnia kell magát valamely a 3.1.9. fejezetben megnevezett igazolvány segítségével

- A hitelesítés szolgáltatás szerződés megkötése.
- A Szolgáltató archiválja a hitelesítés szolgáltatás szerződést, az aláírói adatlapot és valamennyi igazolást, amelyet az Aláíró vagy az Aláró Szervezete 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.
A tanúsítványigénylő űrlap átvételét követően a Szolgáltató tájékoztatási kötelezettségét egy tájékoztató kiadvány az igénylő részére történő átadásával teljesíti. Az igénylőnek módja van a kiadvány helyszínen történő áttanulmányozására és helyszíni konzultációra. A kiadvány tartalma és a tanúsítványigénylő űrlap megtalálható a Szolgáltató honlapján is, így előzetesen is megtekinthető és kitölthető.

Amennyiben az Aláíró személyazonossága vagy az Aláíró Szervezetéhez való tartozása nem állapítható meg minden kétséget kizáróan, vagy valamely, az űrlapon feltüntetett adat nem helyes, akkor az igénylési eljárás félbeszakad. Ekkor a Szolgáltató az űrlapot visszaadja igénylő részére, akinek lehetősége van az adatok korrigálására, s újbóli igénylésre.
A Szolgáltató nyilvántartásba vesz minden, az Aláíró és az Aláíró Szervezete azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat is. A dokumentációkról a Szolgáltató másolatot készít.
Az Aláíró azonosítójának (egyedi nevének) megállapítása a 3.1.4 pontban tárgyaltaknak megfelelően történik.
A tanúsítványigénylő űrlap (aláírói adatlap) ezt követő aláírásával születik meg a hitelesítés szolgáltatás szerződés a szolgáltató és az igénylő között a Szolgáltató Általános Szerződési Feltételeinek megfelelően. Az igénylő aláírásával egyúttal nyilatkozik arról is, hogy szolgáltató feltételei és kikötései, saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Az aláírással az igénylő hozzájárul a szolgáltatások során felhasznált információ hitelesítés-szolgáltató által történő nyilvántartásba vételéhez, tanúsítványa és az azzal kapcsolatos állapot információ szolgáltatói tanúsítványtárba való felvételéhez, s ezen információ harmadik félhez történő továbbításához a hitelesítés-szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb jogszabályok által meghatározott esetekben a szolgáltató szabályzatai által meghatározott módon.

Az aláírás igazolja azt is, hogy az Aláíró (valamint az Aláíró Szervezete, ha van ilyen)
- vállalja a biztonságos aláírás-létrehozó eszköz használatát, védelmét,
- garantálja feltüntetett adatainak valódiságát,
- az adatok későbbi változásairól szolgáltatót értesíti.

4.2. Tanúsítvány-kibocsátás

Végfelhasználói tanúsítványok kibocsátására a tanúsítványigénylő eljárás lefolytatását követően kerül sor. A tanúsítvány elkészítésére az új tanúsítványigénylés során (az aláírói adatlapon) megadott, illetve a Szolgáltató rendelkezésére álló és a tanúsítványcsere igénylése során érvényesnek elismert adatok alapján kerül sor.
Az Aláíró titkos és nyilvános kulcsait a Szolgáltató biztonságos aláírás-létrehozó eszközön generálja, fizikailag védett környezetben, kizárólag bizalmi munkakört betöltő személyek jelenlétében. Az aláírás-létrehozó adat (titkos kulcs) soha nem hagyja el a biztonságos aláírás-létrehozó eszközt, a Szolgáltató ezen eszközt adja át az aláírónak.

A tanúsítványt a hitelesítő szervezet írja alá a saját magánkulcsával. Ezen aláírás (a tanúsítvány kibocsátása) két időpontban történhet:
- amennyiben az Aláíró közvetlenül a Szolgáltatótól igényelte a tanúsítványt, akkor a tanúsítvány kibocsátása közvetlenül azelőtt zajlik le, amikor az Aláíró személyesen átveszi aláírás-létrehozó adatot a Szolgáltató ügyfélszolgálati irodájában,
- amennyiben az Aláíró a Szolgáltatóval szerződésben lévő külső regisztrációs szervezettől igényelte a tanúsítványt, a tanúsítvány kibocsátása nem az Aláíró jelenlétében zajlik le.

Az aláírói adatlapon megadott adatok, illetve a tanúsítványcsere-kérelem, valamint az Aláíró nyilvános kulcsa a szolgáltató információs rendszerébe kerülnek.

A hitelesítő szervezet aláírja a tanúsítványt saját magánkulcsával, és visszaküldi azt a központi regisztráló szervezetnek. A hitelesítő szervezet a tanúsítványt nyilvános tanúsítványtárában 24 órán belül közzéteszi.

Az elkészült tanúsítványt a hitelesítés-szolgáltató a biztonságos aláírás-létrehozó eszközön juttatja el az Aláíróhoz. Amennyiben a hitelesítés-szolgáltató az igényelt tanúsítványkérelmet visszautasítja, akkor az Aláírónak a Szolgáltató (vagy a külső regisztrációs szervezet) értesítést küld a visszautasítás okának megjelölésével.

4.3. Tanúsítvány-elfogadás

A tanúsítványkérelem benyújtását követően egy későbbi időpontban az Aláíró személyesen veheti át a magánkulcsot a biztonságos aláírás-létrehozó eszközön.

Az átadás kétféleképpen történhet:

- amennyiben az Aláíró közvetlenül a Szolgáltatótól igényelte a tanúsítványt, akkor személyesen veheti át az aláírás-létrehozó adatot a Szolgáltató ügyfélszolgálati irodájában,
- amennyiben az Aláíró a Szolgáltatóval szerződésben lévő külső regisztrációs szervezettől igényelte a tanúsítványt, akkor ezen külső regisztrációs szervezet ügyfélszolgálati irodájában veheti azt át, szintén csak személyesen.

Az Aláíró csak akkor veheti át a biztonságos aláírás-létrehozó eszközt, ha a Szolgáltató (vagy a külső regisztrációs szervezet) ügyfélszolgálati munkatársa azonosította őt.

Az aláírás-létrehozó eszköz átvétele előtt az aláírónak ellenőriznie kell a tanúsítványban szereplő adatokat. Az aláírás-létrehozó adat átvételével egyidejűleg az Aláíró megkapja a biztonságos aláíró eszköz aktiválásához szükséges kódokat. E kódokat zárt borítékban kapja meg, amelyet átvételkor köteles felnyitni és ellenőrizni, hogy a kódok olvashatóak-e.
Az Aláíró a helyszínen meg kell, hogy változtassa az alapértelmezés szerinti ötjegyű kódot, egy hatjegyű aláírói kódra. Azzal, hogy az eredeti kód ötjegyű volt, az Aláíró megbizonyosodhat róla, hogy az eszközt korábban nem használták aláírásra.
Az eszköz átvételét követően az Aláíró a helyszínen kipróbálhatja az aláírás létrehozó eszközt.

Az eszköz átvételét követően az Aláírónak (kézzel) alá kell írnia az aláírói nyilatkozatot, amelyben – többek között – azt igazolja, hogy a tanúsítványban szereplő adatok helyesek, az aláírás-létrehozó eszközt és a hozzá tartozó aktiváló kódokat átvette, valamint azt, hogy ismeri az elektronikus aláírás használatának műszaki és jogszabályi feltételeit.

4.4. Tanúsítvány felfüggesztés és visszavonás

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatásokat 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/felfüggesztett tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. A visszavont tanúsítványhoz tartozó aláíró magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges.

Felelősségi szabályok a visszavont/visszavonandó tanúsítvány elfogadásából eredendő károkra:

- A visszavonási/felfüggesztési kérelem Szolgáltatóhoz történő megérkezéséig az Általános Szerződési Feltételeknek megfelelően az Aláíró felelős a felmerülő károkért,
- Miután a visszavonási/felfüggesztési kérelem a Szolgáltatóhoz megérkezett és a Szolgáltató a kérelmező visszavonási/felfüggesztési jogosultságáról meggyőződött, a tanúsítvány érvénytelen állapotának közzétételéig a Szolgáltató felelős a felmerülő károkért.
- Az érvénytelen állapot közzététele után az Érintett fél felelős a felmerülő károkért.

Az Aláírónak (vagy az Aláíró Szervezetének, ha van ilyen) lehetősége van telefonon, személyesen vagy elektronikusan aláírva felfüggeszteni a tanúsítványt. A telefonos felfüggesztés a hét minden napján, a nap 24 órájában működik. Személyesen felfüggeszteni kizárólag nyitvatartási időben lehet. Az Aláíró (vagy Szervezete) csak írásban (személyesen és papíron, postai levélben vagy elektronikusan aláírva) kérheti egy tanúsítvány visszavonását.

A Szolgáltató minden beérkező felfüggesztési és visszavonási kérelmet soron és azonnal kívül dolgoz fel, és az esetleg megváltozott visszavonási állapot a feldolgozást követően azonnal megjelenik a Szolgáltató visszavonási nyilvántartásában.
A Szolgáltató akkor tekinti úgy, hogy egy telefonos felfüggesztési kérelem megérkezett hozzá, amikor a kérelmező és a felfüggesztendő tanúsítvány azonosítása megtörtént, és a Szolgáltató megállapította a kérelmező felfüggesztési jogosultságát a 4.4.1. fejezetben leírtak szerint. A postán illetve elektronikus levélben érkező kérelmeket a Szolgáltató minden munkanapon ellenőrzi.

Ha az Aláíró (vagy Szervezete) vissza kívánja vonni a tanúsítványát, viszont nem képes személyesen bemenni a Szolgáltató ügyfélszolgálati irodájába, a Szolgáltató azt javasolja, hogy a visszavonásig az Aláíró (vagy Szervezete) a telefonos ügyelet segítségével függessze fel a tanúsítványt. A Szolgáltató úgy biztosítja az azonnali visszavonás szolgáltatást, hogy folyamatosan működő azonnali felfüggesztés szolgáltatást biztosít, és az Aláírónak a felfüggesztett tanúsítvány visszavonásáról elég később gondoskodnia.

Az Aláíró csak a saját tanúsítványát függesztheti fel, kivéve a szervezeti ügyintézők és az adott szervezet nevében aláírásra jogosultak, akik a saját szervezetükhöz 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 az Aláíró (vagy szervezeti ügyintéző) helyes felfüggesztő jelszavát (és az alábbi módon azt is meg tudja adni, hogy e jelszó melyik aláíróhoz tartozik).
A Szolgáltató minden felfüggesztési, visszaállítási és visszavonási kérelmet naplóz.

4.4.1. Felfüggesztés telefonon

A telefonos felfüggesztés a hét 7 napján, a nap 24 órájában működik. A telefonos felfüggesztés szolgáltatás rendelkezésre állása 99,9% (vagyis egy év perceinek 99,9%-ában folyamatosan működik), az eseti szolgáltatás-kiesések nem haladhatják meg a három órát. A telefonon beérkező kérelmeket a Szolgáltató soron kívül dolgozza fel és haladéktalanul teljesíti.

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

Nem szervezeti felfüggesztési kérelem esetén a Szolgáltató a következő adatok megadását kéri a kérelmezőtől, hogy egyértelműen meg tudja állapítani, hogy melyik Aláíró melyik tanúsítványát kell felfüggeszteni:

- az Aláíró kártyájának számát vagy
- az Aláíró regisztrációkor megadott valamely igazolványának a számát vagy
- az Aláíró tanúsítványában szereplő OID-jét vagy
- az Aláíró nevét (a regisztrációkor megadott igazolvány szerint), születéskori nevét, anyja nevét, születési helyét és idejét
- az Aláíró felfüggesztő jelszavát.
- a fentieken túl a Szolgáltató munkatársa a regisztrációkor megadott természetes azonosító adatokat (születési hely, születési idő, anyja neve) is kérdezhet az Aláírótól.

A Szolgáltató visszautasítja a kérelmet, ha a megadott adatok alapján nem tudja egyértelműen megállapítani, hogy melyik Aláíró melyik tanúsítványát kell felfüggeszteni, vagy ha a megadott jelszó vagy valamely természetes azonosító adat helytelen.

Szervezeti felfüggesztési kérelem esetén a kérelmezőnek (aki a szervezeti ügyintéző) a következő adatok mindegyikét meg kell adnia:

- A kérelmező szervezeti ügyintézői tanúsítványában szereplő OID-jét
- A kérelmező nevét (a regisztrációkor megadott igazolvány szerint)
- A kérelmező szervezetének nevét
- Az Aláíró kártyájának számát
- Az Aláíró nevét
- A szervezeti ügyintéző felfüggesztő jelszavát
- a fentieken túl a Szolgáltató munkatársa a regisztrációkor megadott természetes azonosító adatokat (születési hely, születési idő, anyja neve) is kérdezhet a kérelmezőtől.

A Szolgáltató elutasítja a kérelmet, ha a kérelmező nem ad meg valamely adatot, vagy a megadott jelszó illetve valamely természetes azonosító adat helytelen.

Amint a Szolgáltató munkatársa a telefonbeszélgetés során sikeresen megállapította, hogy a kérelmező mely tanúsítványt szeretné felfüggeszteni, valamint megállapította a kérelmező személyazonosságát illetve felfüggesztési jogosultságát, közli, hogy a kérelmet a Szolgáltató fogadta, és megkezdte annak feldolgozását. A Szolgáltató e pillanattól tekinti úgy, hogy a kérelem megérkezett hozzá, és e pillanattól a Szolgáltató felelősséget vállal a tanúsítvány elfogadásából eredő károkért amíg a tanúsítvány új visszavonási állapota meg nem jelenik a Szolgáltató visszavonási nyilvántartásában. A Szolgáltató OCSP szolgáltatása valamint delta CRL-jei segítségével azonnal közzéteszi a megváltozott visszavonási állapotot (lásd: 4.4.6. Visszavonási állapot közzététele).

A Szolgáltató emailben értesíti az Aláírót a felfüggesztés tényéről.

4.4.2. Felfüggesztés személyesen vagy elektronikusan aláírva

A Szolgáltató felfüggeszti az Aláíró tanúsítványát, ha az Aláíró kéri. Az Aláíró a kérelmét a Szolgáltató honlapjáról letölthető „felfüggesztési/visszaállítási kérelem” űrlap formájában nyújthatja be. 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 Aláíró Szervezetének (ha van ilyen).

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.

4.4.3. Felfüggesztés és visszavonás az Szolgáltató kezdeményezésére

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

- Ha az Ügyfél (a Költségviselő) 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.

A felfüggesztésről a Szolgáltató minden esetben értesíti az Aláírót (és az Aláíró Szervezetét, ha van ilyen).

4.4.4. Visszaállítás

A tanúsítvány visszaállítása azt a folyamatot jelenti, amelynek során a felfüggesztett tanúsítvány újra érvényes állapotba kerül. A visszaállítás pontosan ugyanúgy történik, mint a felfüggesztés. Végezheti az aláíró vagy szervezeti ügyintéző, és történhet telefonon, személyesen vagy elektronikusan aláírva.

A következő különbségek vannak:

- Telefonos visszaállításkor nem a felfüggesztő, hanem a visszaállító jelszót kell megadni
- Telefonos visszaállításkor minden esetben (nem szervezeti visszaállítási kérelem esetén is) ismerni kell a kérelmezőnek a kártyaszámot
- Ha ugyanarra a tanúsítványra több féltől is érkezik felfüggesztési kérelem, akkor az Szolgáltató csak akkor állítja vissza a tanúsítványt, ha mindegyik felfüggesztő fél kéri a visszaállítást is.

4.4.5. Visszavonás

Visszavonás kizárólag írásban (papíron vagy elektronikusan aláírva) történhet. Visszavonási kérelmeket a Szolgáltató egy munkanapon belül (de soron kívül) dolgoz fel. Kérelmeket személyesen leadni csakis nyitvatartási időben 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 az aláíró tanúsítványát. Az aláíró szervezete 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 aláíró szervezete nevében aláírni.

Ha a tanúsítványt a Szolgáltató harmadik féltől származó dokumentum alapján állította ki (pl. e dokumentumban harmadik fél igazolta az aláírónak 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 hitelesítés szolgáltatás szerződés megszűnik, vagy
- ha az Ügyfél (a Költségviselő) a fizetési határidőig nem fizet;
- 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 aláíró vagy az aláíró szervezete kéri, és a visszavonás okát nem adja meg, az Szolgáltató úgy tekinti, hogy a visszavonás oka az, hogy az aláíró illetve az aláíró szervezete a tanúsítványt a továbbiakban nem kívánja használni. A Szolgáltató a visszavonást ilyenkor is teljesíti.

4.4.6. Visszavonási állapot közzététele

Tanúsítványok állapotának lekérdezésére a Szolgáltató három lehetőséget biztosít:
- OCSP (online tanúsítvány visszavonási állapot lekérdezési szolgáltatás)
- CRL (visszavonási lista)
- Delta CRL (visszavonási lista változásai az utoljára kibocsátott visszavonási lista óta)

A visszavonási listában a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok visszaállítás hatására kikerülnek a listából. A tanúsítványok a tanúsítvány lejárta után törlődnek a listából.

Felfüggesztés, visszaállítás és visszavonás esetén a folyamat sikeres lezárását követően a tanúsítvány új állapota azonnal megjelenik a Szolgáltató visszavonási nyilvántartásában. Ettől a pillanattól kezdve a Szolgáltató által nyújtott OCSP válaszok már a tanúsítvány új visszavonási állapotát tartalmazza. A felfüggesztés, visszaállítás és visszavonás hatására a Szolgáltató új delta CRL-t hoz létre, ezen új delta CRL is a tanúsítvány új állapotát tartalmazza. Az aktuális CRL ekkor a tanúsítvány korábbi állapotát tartalmazza, a tanúsítvány új állapota a soron következő CRL-ben fog megjelenni, így a tanúsítvány ellenőrzéséhez a soron következő CRL ellenőrzése is szükséges.

A visszavonási állapot közzététele szolgáltatás rendelkezésre állása 99,9%, az eseti szolgáltatás-kiesések nem haladhatják meg a három órát.

Aláíróknak tanúsítványt a Szolgáltató *produktív hitelesítő egysége* ("Qualified e-Szigno CA") bocsát ki. A produktív hitelesítő egység 24 óránként bocsát ki CRL-t, emellett 30 percenként és minden eseménykor (visszavonás, felfüggesztés, visszaállítás) delta CRL-t is kibocsát.
A produktív hitelesítő egység CRL-je a http://www.e-szigno.hu/CA-Crl címen érhető el.
A produktív hitelesítő egység delta CRL-je a http://www.e-szigno.hu/CA-DeltaCrl címen érhető el.

A Szolgáltató produktív hitelesítő egységének tanúsítványát a Szolgáltató gyökér hitelesítő egysége („Microsec e-Szigno Root CA") bocsátja ki. A gyökér hitelesítő egység root CA havonta bocsát ki CRL-t, de delta CRL-t nem bocsát ki.
A gyökér hitelesítő egység CRL-je a http://www.e-szigno.hu/rootCA.crl címen érhető el.

Az időbélyegzés szolgáltatásra („*e-Szigno TSA*") vonatkozó visszavonási lista a http://www.e-szigno.hu/SCA-Crl címen érhető el. A Microsec e-Szignó Szerver CA-ra vonatkozó visszavonási lista a http://www.e-szigno.hu/rootCA.crl címen érhető el.
A visszavonási listák hatályba lépésének időpontja azt az időpontot 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) 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 egy-két perccel hosszabb időintervallumok is megjelenhetnek, ez nem befolyásolja azt, hogy a visszavonási listák megjelenése között pontosan 24 óra, 30 perc illetve egy hónap telik el.

Az OCSP válaszadó CA („*e-Szigno OCSP CA*") csak az *OCSP válaszadó* („*e-Szigno OCSP Responder*") tanúsítványát bocsátja ki, ezek a tanúsítványok csak nagyon rövid ideig érvényesek. Az OCSP válaszadó CA CRL-je a http://www.e-szigno.hu/OCSPCA-Crl címen érhető el.

Az OCSP válaszadó az aláírók, a produktív CA, az időbélyegzés szolgáltató és az OCSP válaszadó CA tanúsítványai visszavonási állapotára vonatkozóan ad OCSP válaszokat.
A gyökér hitelesítő egységgel kapcsolatos OCSP szolgáltatás a https://rca.e-szigno.hu/ocsp címen érhető el. A Microsec e-Szigno Server CA tanúsítványát kibocsátó hitelesítési egységgel kapcsolatos OCSP szolgáltatás a https://rca.e-szigno.hu/ocsp címen érhető el. Az időbélyegzés szolgáltató tanúsítványával kapcsolatos OCSP szolgáltatás a https://sca.e-szigno.hu/ocsp címen érhető el. Az OCSP válaszadó tanúsítványát kibocsátó hitelesítési egységgel kapcsolatos OCSP szolgáltatás a https://ocspca.e-szigno.hu/ocsp címen érhető el. A produktív hitelesítő egységgel kapcsolatos OCSP szolgáltatás a https://ca.e-szigno.hu/ocsp címen érhető 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.

4.4.7. Időbélyeg kibocsátás

Az időbélyegzés szolgáltatás igénybevétele során az Ügyfél egy dokumentum lenyomatát adja meg, amelyre a Szolgáltató aláírt időbélyeget ad vissza. Az időbélyegzés szolgáltatás igénybevétele felhasználónév és jelszó alapján történik. Az időbélyegzés szolgáltatás rendelkezésre állása 99,9%, az eseti szolgáltatás-kiesések nem haladhatják meg a három órát.

4.5. A biztonsági naplózás folyamatai

Szolgáltató hitelesítési 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 pontos időt szolgáltató pontos idő egysége biztosítja, ami legfeljebb 1 másodperces eltérést engedélyez a valódi időhöz képest. Az esetleges ennél nagyobb eltérések szintén naplózásra kerülnek. Szolgáltató egyéb rendszerei szintén naplóznak. E naplózások tulajdonságai az adott alkalmazások függvényei. A naplózások elemei elkülönülten keletkeznek a különböző modulokban.
Operatív szinten az egyes rendszerek üzemeltetési leírásai, valamint a Szolgáltató biztonsági szabályzata szabályozzák a napló adatok kezelését.

4.5.1. 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,
- a biztonságos aláírás-létrehozó eszközök készítésével kapcsolatos valamennyi esemény,
- az esetleges hibaesemények.

4.5.2. A napló állomány feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása minden munkanapon megtörténik. Szolgáltató hálózati védelmi riasztás funkciókkal is rendelkeznek 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.

4.5.3. A napló-állomány megőrzési időtartama

A napló-állományokat 90 napig tárolják a keletkezésük helyén. Ezek után 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.

4.5.4. 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 (ásd. 4.5.5 A napló állomány mentési folyamatai). 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. Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a Szolgáltató biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

4.5.5. 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 (lásd 5.1.6 és 5.18).
A mentés operatív folyamatait Szolgáltató mentési szabályzatai írják le részletesen.

4.5.6. 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.

4.5.7. Az eseményeket kiváltó aláírók értesítése

A naplóbejegyzéseket kiváltó személyeket, szervezeteket és alkalmazásokat a Szolgáltató nem értesíti, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az eseményt kiváltásában közreműködőknek ilyen esetben kötelessége a Szolgáltatóval való együttműködés.

4.5.8. 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.

4.6. Adatok archiválása

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

4.6.1. 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.),
- az igénylő személyes és szervezeti identitásának igazolására bemutatott valamennyi dokumentum fénymásolatát,
- a Szolgáltató, az Aláíró, Aláíró Szervezete és a Költségviselő között megkötött valamennyi megállapodást.

Szolgáltató központi ügyfélszolgálata és regisztrációs szervezete jogosult hangfelvételt készíteni az ügyelethez beérkező felfüggesztések és visszaállítások során elhangzott párbeszédekről.

4.6.2. 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.

4.6.3. Az archívum védelme

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

4.6.4. Az archívum mentési folyamatai

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

4.6.5. A rekordok időbélyegzésére vonatkozó követelmények

Lásd a 4.6.3 Az archívum védelme alfejezetet.

4.6.6. Az archívum gyűjtési rendszere

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

4.6.7. Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés Aláírónak és az Aláíró Szervezetének a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.8.4, 2.8.5 és 2.8.6 alfejezetek szerint.

4.7. Tanúsítványcsere

A Szolgáltató által kibocsátott végfelhasználói tanúsítványok érvényességi ideje *1 vagy 2 év*. Az érvényesség kezdete a tanúsítvány „érvényesség” (Validity) mezőjében megadott kezdeti érték (Not before) által mutatott dátum.

Tanúsítványcsere alatt azt a folyamatot értjük, amikor egy már regisztrált (a regisztráció 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 vissza kell vonni. A tanúsítványcserére a következő szabályok vonatkoznak:

- Egyazon magánkulcshoz a Szolgáltató legfeljebb kétszer bocsát ki minősített tanúsítványt.
- A Szolgáltató által biztosított biztonságos aláíró eszköz legfeljebb 6 évig használható, vagyis a rajta lévő első tanúsítvány érvényességi idejének kezdete és az utolsó tanúsítvány érvényességi idejének vége között nem telhet el több, mint 6 év. Amennyiben ez nem biztosítható, a tanúsítványt a Szolgáltató csak új kártyán adhatja ki.
- Ha az aláíró korábbi tanúsítványa a tanúsítványcsere előtt lejárt vagy visszavonásra került, az új tanúsítványt a Szolgáltató csak új kulcshoz bocsátja ki új regisztráció keretén belül.
- Ha az aláírónak valamely olyan adata változik meg, amely a tanúsítványában szerepel, akkor a Szolgáltató visszavonja a tanúsítványát. Ha az Aláíró, az Aláíró Szervezete vagy a költségviselő kéri, a Szolgáltató nem azonnal, hanem az Aláíróval, az Aláíró Szervezetével vagy a Költségviselővel egyeztetett ütemben vonja vissza a régi tanúsítványt (például csak akkor, amikor az aláíró már hozzájutott az új tanúsítványhoz). A Szolgáltató ehhez csak akkor járul hozzá, ha úgy ítéli meg, hogy a tanúsítványt felhasználó Érintett felek nem értelmezhetik különbözőképpen a régi és az új tanúsítványt.
- Ha az aláíró egyedi kártyával rendelkezik, és olyan adata változik, amely a kártyáján optikailag megszemélyesítve szerepel, a Szolgáltató dönthet úgy, hogy az új tanúsítványt nem ugyanazon a kártyán bocsátja ki.
- Ha a tanúsítványcserére azért kerül sor, mert az aláíró korábbi tanúsítványa le fog járni, a korábbi tanúsítványt az új tanúsítvány kibocsátását követően vissza kell vonni.

4.8. 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.

4.8.1. 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.
A Szolgáltató bármely egy eszköz kiesése esetén képes zavartalanul folytatni a működését. Amennyiben a Szolgáltatónak egyszerre több egysége esik ki, a Szolgáltató 3 órán belül képes hidegtartalék-rendszerének beindítására, amely képes biztosítani a Szolgáltató folyamatosan működő – tanúsítványtár közzététele, felfüggesztés és visszavonás kezelés és visszavonási állapot közzététele – szolgáltatásait a Szolgáltató ügyfelei számára.

4.8.2. A szolgáltatói egység nyilvános kulcsának visszavonása

A szolgáltatói nyilvános kulcsok visszavonásáról *Szolgáltató* a **2.6.1** alfejezetnek megfelelően értesítést tesz közzé.

4.8.3. Egy szolgáltatói egység kulcsának kompromittálódása

Szolgáltató katasztrófa elhárítási terve a szolgáltatói magánkulcsok kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik az ez által érintett valamennyi fél értesítéséről (a 2.6.1 alfejezettől függetlenül, de arra tekintettel), megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet és a kompromittálódás által érintett végelhasználókat.

4.8.4. Biztonsági képesség 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 a 4.8.1 alfejezet szerint nem kezelhető, Szolgáltató a másodlagos helyszínen is képes szolgáltatásainak beindítására.
Ilyen esetekben Szolgáltató a következő szolgáltatások legfeljebb 3 órán belüli elindítását vállalja:

- tanúsítványtár közzététele szolgáltatás
- felfüggesztés és visszavonás kezelés szolgáltatás,
- visszavonási állapot közzététele szolgáltatás.

4.9. A szolgáltatások leállítása

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

4.9.1. A hitelesítés szolgáltatás és online tanúsítvány-állapot szolgáltatás leállítása

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

- regisztráció
- tanúsítvány-előállítás,
- tanúsítvány-kibocsátás,
- biztonságos aláírás-létrehozó eszköz optikai megszemélyesítése,
- biztonságos aláírás-létrehozó eszköz logikai 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,
- online tanúsítvány-állapot szolgáltatás.

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

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

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait, a bizalmas felhasználói adatokkal együtt a **2.8.7** alfejezet 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* és az *e-Szigno OCSP CA* tanúsítványának visszavonását 5 nappal megelőzően a **2.6.1.** alfejezetnek megfelelően hirdetményt tesz közzé.

A *Microsec e-Szigno Root CA* illetve a *Microsec e-Szigno Server CA* tanúsítványa visszavonása esetén vagy gondoskodni kell az *e-Szigno TSA* számára más CA által kiadott tanúsítványról, vagy az időbélyegzés szolgáltatást is meg kell szüntetni.

A Szolgáltató a hitelesítés szolgáltatási tevékenysége 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.

4.9.2. 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 „e-Szigno TSA” tanúsítványt vissza kell vonni. A Szolgáltató a tanúsítvány visszavonását 5 nappal megelőzően a 2.6.1. alfejezetnek megfelelően hirdetményt tesz közzé.

4.10. Az Ügyfél adatainak kezelése

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

A Szolgáltató – a szolgáltatási szerződésnek megfelelően – nyilvánosságra hozza az aláírók tanúsítványban szereplő adatait és a tanúsítványra vonatkozó visszavonási információt. A tanúsítványban a Szolgáltató feltünteti az Aláíró személyéhez rendelt egyedi azonosítót (OID-et).

A Szolgáltató az időbélyegzés és online tanúsítvány-állapot szolgáltatások előfizetőiről kizárólag a szolgáltatás igénybevételéhez 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 hitelesítés szolgáltatás, időbélyegzés szolgáltatás és online tanúsítvány-állapot szolgáltatás 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.

5. Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A Szolgáltató gondoskodik arról, hogy kellő, az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

5.1. Fizikai óvintézkedések

A hitelesítés-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 körleteire irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.
A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a Szolgáltató rendszerében. A biztosított védelem arányban áll a Szolgáltató által végzett kockázat elemzésben megállapított kockázatokkal.

- A hitelesítő szervezet védett számítógép termében valósítják meg a leginkább veszélyeztetett szolgáltatásokat. Ez a számítógép terem 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 lettek kiválasztva, hogy reális költségek mellett képesek legyenek kielégíteni a regisztrációs szolgáltatásokkal szemben támasztott követelményeket.
- 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 körletben valósítja meg, és az ehhez szükséges valamennyi eszközt egy a biztonsági körlet részét képező védett számítógép teremben helyezte el.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A hitelesítő szervezet egy elkülönített biztonsági körletben lévő ablaktalan helyiségekben helyezkedik el. A körletet vastag és elektromágneses sugárzást át nem engedő falak veszik körül. A hitelesítő szervezet másodlagos telephelye az elsődleges telephelytől távol helyezkedik el egy védett szervertermemben.

5.1.2. Fizikai hozzáférés

A hitelesítő szervezet védett számítógép terme úgy lett kialakítva, hogy illetéktelen személyek nehezen juthassanak be. A biztonsági körletnek nincs ablaka, a bejárati ajtókon kívül csak falbontással lehet behatolni ide. A biztonsági körlet integráltan megvalósított behatolás jelző (riasztó) és beléptető rendszerrel van ellátva. A biztonsági körletet 24 órás videó kamerás megfigyelő rendszer is védi. A védett számítógép terembe 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 számítógép termének 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 energia ellátás,
- dízelmotoros generátoregység,

- villamos zavar-, villám- és túlfeszültség védelem,

A hidegtartalékon működő szerverterem folyamatos áramellátását
- akkumulátoros szünetmentes energia ellátás,
- villamos zavar-, villám- és túlfeszültség védelem,

biztosítják.

Légkondicionálás

A hitelesítő szervezet védett számítógép terme 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 körletének kialakítása során fontos szempont volt a beázás és elárasztódás veszélyének minimalizálása. A biztonsági körlet teljes területe mentes a vizesblokkoktól, illetve a közelben nincs se csatorna se vízvezeték. A védett számítógép teremben a fenti biztonságot tovább növeli az álpadló alkalmazása.

5.1.5. Tűzmegelőzés és tűzvédelem

A hitelesítő szervezet géptermében tűzvédelmi rendszer működik, melyet a 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 egy rekeszenként külön-külön zárható lemezszekrény szolgál az adathordozók biztonságos tárolására

5.1.7. Selejt kezelése és megsemmisítése

A hitelesítő szervezet biztonsági körletében a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat még tartalmuk törlése után sem használják fel nem minősített 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 merev lemezeket (a befogadó épületben központilag biztosított célberendezés felhasználásával) demagnetizálás után összetörik.
- az optikai lemezeket összetörik

5.1.8. Fizikailag elkülönítetten őrzött mentési példányok

A *hitelesítő szervezet* biztonság-kritikus szolgáltatásaira vonatkozó adatok mentési példányait a *hidegtartalék* biztonsági körletében tárolják.

5.2. Eljárásbeli óvintézkedések

A hitelesítés-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 Szolgáltató jogszabályoknak és belső szabályzatainak megfelelő és naprakész működést. Rendszerében minden rendszerelemhez és minden folyamathoz egyértelműen hozzárendelhető az adott rendszerelemért illetve 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:

- az önálló üzleti egység vezetője: Az Szolgáltató informatikai rendszeréért átfogóan felelős vezető.
- 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.
- biztonságtechnikai főmunkatárs: Feladata és felelőssége a Szolgáltató biztonsági szabályzatának betartatása a Szolgáltató alkalmazottaival.
- biztonsági tisztviselő: Feladata és felelőssége az infrastruktúra adminisztrátorok tevékenységének felülvizsgálata, ellenőrzése.
- regisztrációs tisztviselő: Feladata az ügyfelek azonosítása, regisztrációja, valamint tanúsítványok kiadása, felfüggesztése és visszavonása. Felelős a regisztráció pontos és helyes elvégzéséért.
- a perszonalizáció területén tevékenykedő regisztrációs tisztviselő: Feladata a biztonságos aláírás-létrehozó eszközök gondozása, megszemélyesítése, valamint a tanúsítványkérelmek összeállítása.
- rendszervizsgáló: Feladata a biztonságos és funkcionálisan helyes működés ellenőrzése a naplófájlok és az archivált adatok alapján. Azért felelős, hogy a tőle elvárható legnagyobb mértékben felderítse a Szolgáltató rendszerében lévő működési rendellenességeket, valamint a biztonsági eseményeket, és jelentse őket az önálló üzleti egység vezetője illetve a Szolgáltató felső vezetése felé.
- rendszeroperátor: Feladata a napi archiválási feladatok elvégzése, azért felelős, hogy az archiválás valóban megtörténjen.
- ügyeletes tisztviselő: Feladata a 24 órás ügyelet biztosítása. Felelős az ügyelet elérhetőségéért, valamint azért, hogy a beérkező 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.

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.
A Szolgáltató szolgáltatói magánkulcsának generálása a Szolgáltató öt ügyvezetőjének jelenlétében kell, hogy történjen.
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 hitelesítés-szolgáltató működésének megbízhatóságát.

A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a lehetőségekkel való visszaélés 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 ismereteket 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 felsőfokú 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- illetve 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 az 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 kinevezési eljárás, illetve az alapkiképzés során:
- A Szolgáltató szervezeti biztonsági szabályzata
- aláírt titoktartási nyilatkozat,
- egyéni munkaköri leírás,

a tervezett és rendkívüli továbbképzések alkalmával:
- az adott oktatási formához tartozó oktatási segédanyagok

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

6. Műszaki biztonsági óvintézkedések

A hitelesítés-szolgáltató módosítás ellen védett, megbízható rendszereket és termékeket használ.

A Szolgáltató 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 hitelesítés-szolgáltató gondoskodik valamennyi általa (saját maga, egyes szervezeti egységei /pl. tanúsítványtár, regisztrációs szervezetek/, illetve az alanyok számára) generált magánkulcs biztonságos és az ipari szabványoknak megfelelő generálásáról.

6.1.1. Kulcspár előállítás

A Szolgáltató az alábbi kulcspárokat használja:
1. a Szolgáltató gyökér hitelesítő egységének (*„Microsec e-Szigno Root CA”*) kulcsa, 2048 bit
2. a Szolgáltató végfelhasználói minősített tanúsítványokat aláíró kulcsa (a Szolgáltató produktív hitelesítő egységének, a *„Qualified e-Szigno CA”*-nak a kulcsa), 2048 bit
3. a Microsec e-Szigno Server CA kulcsa, 2048 bit
4. a szolgáltató időbélyegző szerverének (*„e-Szigno TSA”*) kulcsa, 2048 bit
5. a szolgáltató OCSP válaszadójának tanúsítványát aláíró hitelesítő egység (*„e-Szigno OCSP CA”*) kulcsa, 2048 bit
6. a szolgáltató OCSP válaszadójának (*„e-Szigno OCSP Responder”*) kulcsa, 1024 bit
7. az SSL protokollhoz felhasznált kulcspárok, 1024 bit
8. VPN protokollhoz felhasznált kulcspárok, 1024 bit
9. az Aláírók minősített aláírás létrehozására alkalmas kulcspárjai, 1024 bit

A Szolgáltató valamennyi kulcspárt saját maga generálja. A fenti kulcsok közül az első hatot a Szolgáltató biztonságos hardvermodulban generálja, e magánkulcsok a (6.2.4 alatt részletezett) mentést leszámítva, teljes életciklusukat a kriptográfiai hardver modulokban töltik, megsemmisítésükig soha sehová nem kell őket továbbítani.
Az SSL protokollokban a kliensek kulcspárjait a Szolgáltató intelligens kártyán generálja, e kulcsok teljes életciklusukat a kártyán töltik, sehova sem kerülnek továbbításra. Az SSL protokollokban a szerverek kulcspárjait a Szolgáltató biztonságos hardvermodulban generálja, e magánkulcsok sem hagyják el a modult, és sehova sem kerülnek továbbításra. A VPN protokollokhoz felhasznált kulcsok szoftveresen léteznek a VPN technológiát megvalósító célhardverekben, illetve olyan számítógépeken amelyek biztonságáról a Szolgáltató fokozottan gondoskodik. E magánkulcsok sem kerülnek továbbításra.

A végfelhasználók által használt kulcspárokat a Szolgáltató biztonságos aláírás-létrehozó eszközön, fizikailag biztonságos környezetben generálja. A minősített aláíró kulcs a teljes életciklusa alatt csak a biztonságos aláírás-létrehozó eszközön (intelligens kártya) marad, a végfelhasználókhoz való továbbítása magának az intelligens kártyának a végfelhasználóhoz történő továbbítását jelenti.

6.1.2. Magánkulcs eljuttatása a tulajdonoshoz

Mivel a Szolgáltató valamennyi kulcspárja helyben generálódik (lásd 6.1.1), így azokat nem kell sehová továbbítani.

A végfelhasználók (alanyok) aláíró magánkulcsát a magánkulcs védett tárolását és felhasználását biztosító biztonságos aláírás-létrehozó eszközzel együtt a regisztrációs ponton személyesen megjelenő alanyoknak adják át (a biztonságos aláírás-létrehozó eszközt aktivizáló kódot tartalmazó zárt borítékkal együtt). A kulcsgenerálást követően az aláírás-létrehozó adatot külön ún. transport PIN védi, a biztonságos aláírás-létrehozó eszközzel együtt ez biztosítja, hogy az aláírás-létrehozó adathoz időközben más ne férhessen hozzá.

A Szolgáltató (vagy a Szolgáltatóval szerződésben lévő külső regisztrációs szervezet) ügyfélszolgálati irodájának regisztrációs munkatársa csakis az aláírónak adhatja át a biztonságos aláírás-létrehozó eszközt és a hozzá tartozó (az aktiváló kódokat tartalmazó) borítékot, a regisztrációs munkatárs ilyenkor naplózza az átadás pontos idejét.

6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Mind a hitelesítő szervezet, mind a végfelhasználók kulcsait a hitelesítő szervezet generálja, a nyilvános kulcsot így nem szükséges sehova sem továbbítani.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

A Hitelesítő Szervezet mindenki számára elérhetővé teszi a Gyökér Hitelesítő Egység által aláírt nyilvános kulcsot tartalmazó tanúsítványokat a tanúsítványtárban.

6.1.5. Kulcs méretek

Az egyes kulcsok hosszát a **6.1.1. Kulcspár előállítás** tartalmazza.

6.1.6. A nyilvános kulcs paraméterek előállítása

A Szolgáltató digitális aláírásra minden esetben a Hatóság Eat. 18. § szerint kibocsátott határozata értelmében biztonságosan felhasználható algoritmust használ.
Az RSA algoritmussal van aláírva a rendszer által kibocsátott minden tanúsítvány, és ezt az algoritmust használják a rendszeren belül is a letagadhatatlanság (tranzakciók aláírása, 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. 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 feltételek, összefüggések 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 kulcsainak generálása egy nCipher nShield F3 SCSI hardver eszközzel történik amely FIPS 140-1 szabvány szerint 3. szinten bevizsgált HSM.
Az aláírók aláíró kulcspárjainak generálása a biztonságos aláírás létrehozó eszközön on-board hardver generálással történik (tehát az intelligens kártyán).

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:

Hitelesítő szervezet

Kulcs megnevezése	A “kulcs használati” mező értéke	Kritikus / Nem kritikus
a szolgáltató gyökér hitelesítő egységének kulcsa, a Szolgáltató e kulcsot használja a gyökér hitelesítő egység visszavonási listáinak aláírására is	***keyCertSign és CRLSign***	**K**
a Szolgáltató végfelhasználói minősített tanúsítványokat aláíró kulcsa, a Szolgáltató e kulcsot használja a visszavonási listák aláírására is	***keyCertSign és CRLSign***	**K**
a Microsec e-Szigno Server CA kulcsa	***keyCertSign és CRLSign***	**K**
az időbélyegző központ aláíró kulcsai	***NonRepudiation és digitalSignature***	**K**
	az „Extended Key Usage” mezőbe: ***timeStamping***	**K**
a szolgáltató OCSP válaszadójának tanúsítványát aláíró hitelesítő egység kulcsa	***keyCertSign és CRLSign***	**K**
a szolgáltató OCSP válaszadójának kulcsa	***digitalSignature, nonRepudiation***	**K**

Aláírók

Kulcs megnevezése	“kulcs használati” mező értéke	Kritikus / Nem kritikus
végfelhasználói minősített aláíró kulcs	***nonRepudiation***	**K**

6.2. A magánkulcsok védelme

A Szolgáltató gondoskodik saját magánkulcsainak titkosságáról és sértetlenségéről, valamint az Aláírók magánkulcsainak titkosságáról és sértetlenségéről az Aláíróknak való átadás előtt.
A Szolgáltató ugyanazt az aláíró magánkulcsot használja a végfelhasználói minősített tanúsítványok és a tanúsítvány visszavonási listák aláírásra.
A Szolgáltató a hitelesítő szervezet magánkulcsait fizikailag biztonságos helyszínen, biztonságos hardvermodulban tárolja. Az Aláírók kulcsait az Aláíróknak való átadás előtt fizikailag biztonságos helyszínen, intelligens kártyán tárolja.

6.2.1. Kriptográfiai modulra vonatkozó szabványok

A Szolgáltató kulcsainak generálása egy nCipher nShield F3 SCSI 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 helyezése

A Szolgáltatónál magánkulcsot nem lehet letétbe helyeztetni.

6.2.4. Magánkulcs mentése

A Szolgáltató hitelesítő szervezetének magánkulcsait a **6.2.1 Kriptográfiai modulra vonatkozó szabványok** alatt 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 A több-szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése** fejezetben leírt védelmi mechanizmus mellett alkalmazható.

6.2.5. Magánkulcs archiválása

A Szolgáltató a 6.2.4 Magánkulcs mentése fejezetben leírtakon kívül más magánkulcsokat nem archivál.

6.2.6. Magánkulcs bejuttatása a kriptográfiai modulba

A Szolgáltató csakis a **6.2.2 A több-szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése** fejezetben leírt módon juttat be magánkulcsot a biztonságos hardver modulba.
Az Aláírók magánkulcsait a Szolgáltató biztonságos aláírás-létrehozó eszközön generálja, e magánkulcsok soha nem hagyják el ezen eszközt.

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 csakis 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 eszközt ötjegyű ún. transport PIN kód védi. Az így védett eszköz segítségével nem lehet dokumentumokat aláírni. Amikor az Aláíró átveszi a biztonságos aláírás-létrehozó eszközt, köteles az ötjegyű transport PIN kódot megváltoztatni a saját aláírói PIN kódjára. Az aláírói PIN csak hatjegyű lehet.
Abból, hogy a korábbi PIN ötjegyű volt, az Aláíró megbizonyosodhat róla, hogy a magánkulcsával sem a Szolgáltató sem a Szolgáltató munkatársai nem végeztek elektronikus aláírás műveletet.
A biztonságos aláírás-létrehozó eszköz aktiváló kódja ezt követően csakis az Aláíró birtokában van, a következőkben az Aláíró felel e kód biztonságos tárolásáért és használatáért.

6.2.8. A magánkulcs aktív állapotának megszüntetési módja

Hitelesítő szervezet

A 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.

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.
Az Aláíró magánkulcsának megsemmisítése az Aláíró felelőssége, ugyanis a Szolgáltató olyan biztonságos aláírás-létrehozó eszközön generálja az Aláíró magánkulcsát, amelyet átad az Aláírónak, így a Szolgáltató nem rendelkezik az Aláíró magánkulcsával.

6.3. A kulcspár gondozásának egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

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

6.3.2. A nyilvános és magánkulcsok használatának periódusa

Hitelesítő szervezet

Kulcs megnevezése	Érvényesség
a szolgáltató gyökér hitelesítő egységének kulcsának és a hozzá tartozó tanúsítványnak az érvényességi ideje	**12 év**
a Szolgáltató végfelhasználói minősített tanúsítványokat aláíró kulcsának és a hozzá tartozó tanúsítványnak érvényességi ideje	**10 év**
az időbélyegző központ tanúsítványát kibocsátó Microsec e-Szigno Server CA tanúsítványának érvényességi ideje	**10 év**
az időbélyegző központ aláíró kulcsának és a hozzá tartozó tanúsítványnak az érvényességi ideje	**10 év**
a szolgáltató OCSP válaszadójának tanúsítványát aláíró hitelesítő egység	**10 év**

kulcsának és a hozzá tartozó tanúsítványnak az érvényességi ideje	
a szolgáltató OCSP válaszadójának kulcsa	**10 év**
a szolgáltató OCSP válaszadójának kulcsához tartozó tanúsítvány	**10 perc**

SSL protokollhoz szükséges kulcspárok

Kulcs megnevezése	Érvényesség
SSL protokollhoz szükséges kulcspárok és a hozzá tartozó tanúsítványok	**3 év**

Aláírók

Kulcs megnevezése	Érvényesség
végfelhasználói minősített aláíró kulcs	**legfeljebb 2+2 év**
végfelhasználói minősített aláíró kulcshoz tartozó tanúsítvány	**1 vagy 2 év**

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

A Szolgáltató biztonságosan, véletlenszám generátor segítségével, fizikailag biztonságos körülmények között állítja elő az általa kibocsátott biztonságos aláírás-létrehozó eszközök aktivizáló adatait.

6.4.2. Az aktivizáló adatok védelme

A Szolgáltató az általa kibocsátott biztonságos aláírás-létrehozó eszközök aktivizáló adatait műszaki és szervezési intézkedések segítségével védi és a biztonságos aláírás-létrehozó eszköztől elkülönítve osztja szét.

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 a hitelesítő egység Sun Solaris technológiát alkalmaz, ahol a Sun számítógépek clusterben működnek. A Szolgáltató kulcsait nCipher nShield F3 SCSI biztonságos hardver modulokban tárolja, a modulokat RSA Keon Certificate Authority szoftverek kezelik. Minden rendszerelemből két példány fut, bármelyik kiesése esetén egy cluster segítségével a másik ugyanolyan elem átveszi a funkcióját.

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 és a kibocsátott időbélyegein is. A

A Szolgáltató hitelesítő szervezete 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 az ügyfélszolgálati iroda számítógépeiről csakis a hitlesítő szervezet számítógépeihez lehet hozzákapcsolódni.

6.5.2. Informatikai biztonsági minősítés

A Hitelesítő Szervezet informatikai rendszerében alkalmazott kriptográfiai hardver modulok minősítésére vonatkozóan lásd a (**6.2.1 Kriptográfiai modulra vonatkozó szabványok**) és (**6.7 A kriptográfiai modul ellenőrzése**) alfejezeteket.
Az ügyfélszolgálati iroda informatikai rendszerében alkalmazott intelligens kártyákra vonatkozóan lásd a (**6.2.1 Kriptográfiai modulra vonatkozó szabványok**) és (**6.7 A kriptográfiai modul ellenőrzése**) alfejezeteket.

6.6. Életciklusra vonatkozó műszaki óvintézkedések

6.6.1. Rendszerfejlesztési óvintézkedések

Annak érdekében, hogy az e-Szignó Hitelesítés Szolgáltató valamennyi rendszerfejlesztési projektjében a biztonság 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 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, tanúsítvány-visszavonási lista, időbélyeg és online tanúsítvány-állapot válasz profilok

7.1. Tanúsítvány profil

7.1.1. Tanúsítvány alapmezők

A Szolgáltató által kibocsátott végfelhasználói tanúsítványok alap mezői a következők:

Mezőnév	Értelmezés és érték vagy szabály
Verzió *Version*	Szolgáltató az ITU X.509 "Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer" ajánlás [30] 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 32 karakter hosszúságú egyedi azonosító.
Algoritmus azonosító *Algorithm Identifier*	A tanúsítványokat hitelesítő elektronikus aláírásának algoritmusának azonosítója (OID). Szolgáltató a tanúsítványok hitelesítésére „**sha1WithRSAEncryption"** („sha1RSA") algoritmust használ. A mezőbe kerülő érték az sha1RSA algoritmus OID-je a [9] szerint, „**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 (Qualified e-Szigno CA) egyedi azonosítója egyedi X.501 név formátum szerint, UTF8String formátumban (lásd: **3.1.1.**).
Érvényesség *Valid From & Valid To*	A tanúsítvány érvényességének kezdete és vége (lásd: **4.7.**). Az időpontok UTC szerint [9] és az RFC 3280-nak megfelelő kódolásban kerülnek rögzítésre. Szolgáltató az Aláírók számára – a választott díjcsomagtól függően – egy vagy két évig érvényes tanúsítványokat bocsát ki.
Aláíró azonosítója *Subject*	Az Aláíró egyedi azonosítója egyedi X.501 név formátum szerint, UTF8String formátumban (lásd: **3.1.1**). Mindig kitöltésre kerül.
Aláíró nyilvános kulcsának algoritmus-azonosítója *Subject Public Key Algorithm Identifier*	Az Aláíró nyilvános kulcsának algoritmus azonosítója Szolgáltató az Aláírók számára „**rsaEncryption"** („RSA") algoritmusnak megfelelő kulcspárt szolgáltat, amelyben az Aláíró nyilvános kulcsának hossza 1024 bit. A mezőbe kerülő érték az rsaEncryption OID-je a [9] szerint, „**1.2.840.113549.1.1.5**".
Aláíró nyilvános kulcsa *Subject Public Key Value*	Az Aláíró nyilvános kulcsa.
Kibocsátó egyedi azonosító *Issuer Unique Identifier*	Nem kitöltött.
Aláíró egyedi azonosító *Subject Unique Identifier*	Nem kitöltött.

7.1.2. Tanúsítvány X509 kiterjesztések

A Szolgáltató által kibocsátott végfelhasználói tanúsítványok kiterjesztései a következők:

Mezőnév	Értelmezés és érték vagy szabály	Kritikus
Hitelesítési rendek *Certificate Policies* OID: 2.5.29.32	A tanúsítvány kiadása és használata során érvényes hitelesítési rend (lásd 1.2.4.fejezet) megnevezése, valamint a tanúsítvány alkalmazhatóságára vonatkozó egyéb információk. *Nyilatkozatok:* **1.** A tanúsítvány – a 2001. évi XXXV. törvény és végrehajtási rendeletei alapján – **minősített tanúsítvány**, **amely biztonságos aláírás-létrehozó eszközön** levő aláírás-létrehozó adathoz lett kibocsátva. **2.** A tanúsítvány értelmezéséhez és elfogadásához szükséges ismereteket a tanúsítványhoz kapcsolódó **Hitelesítési Rend** tartalmazza, amely elérhető a következő címen: http://www.e-szigno.hu/HR/. A PolicyIdentifier mező határozza meg, hogy az itt elérhető hitelesítési rendek közül a tanúsítványt mely rend szerint bocsátották ki. **3.** A Szolgáltató tevékenységeire vonatkozó **Szolgáltatási Szabályzat** a következő címen érhető el: http://www.e-szigno.hu/SZSZ/. **4.** A tanúsítvány kizárólag a(z) <**Szolgáltatási Szerződésben meghatározott értéket>** meg nem haladó ügyletekben használható fel. (A tanúsítványban mindig a konkrét érték szerepel.) **5.** A Szolgáltató a jelen tanúsítványhoz kapcsolódó dokumentációt – a 2001 évi XXXV. törvény alapján – a tanúsítvány lejártát követő **10 évig**, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi. *A mező értéke:* PolicyIdentifier= {1.3.6.1.4.1.21528.2.1.1.2 vagy 1.3.6.1.4.1.21528.2.1.1.12} (PolicyQualifierId = id-qt 1, Qualifier = „http://www.e-szigno.hu/HR/”) (PolicyQualifierId = id-qt 2, Qualifier = „Minősített,BALE, Tranzakcióslimit:{limit értéke} MFt, adatmegőrzési idő:10év, Hitelesítési Rend: http://www.e-szigno.hu/HR/, Szolg.Szab.:http://www.e-szigno.hu/SZSZ/”	Nem
Kibocsátó kulcsazonosító *Authority Key Identifier* OID: 2.5.29.35	A tanúsítványt hitelesítő elektronikus aláírás létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója. *A mező értéke*: a nyilvános kulcs SHA1 lenyomata.	Nem
Aláíró kulcsazonosító *Subject Key Identifier* OID: 2.5.29.14	Az Aláíró nyilvános kulcsának 40 karakter hosszú egyedi azonosítója. *A mező értéke*: a nyilvános kulcs SHA1 lenyomata.	Nem

Mezőnév	Értelmezés és érték vagy szabály	Kritikus
Aláíró alternatív nevei *Subject Alternative Names* OID: 2.5.29.17	Az Aláíró neve eltérő írásmóddal (ékezettel/ékezet nélkül), e-mail címe, vagy megegyezés szerinti egyéb, a CA által ellenőrzött adata az Aláírói adatlap szerint. Kizárólag kérésre kerül kitöltésre.	Nem
Alapvető megkötések *Basic Constraints* OID: 2.5.29.19	Annak megadása, hogy a tanúsítvány CA számára lett-e kibocsátva. Végfelhasználói tanúsítványok esetében értéke „**NEM**” („**FALSE**”). *A mező értéke:* cA = „FALSE”	Igen
Kulcshasználat *Key Usage* OID: 2.5.29.15	Az kulcs engedélyezett használati körének meghatározása. A Szolgáltató által az Aláírók számára kibocsátott tanúsítványokhoz kapcsolódó magánkulcsokat kizárólag elektronikus aláírás létrehozására szabad használni. Ennek megfelelően a beállított értékek a ’nonRepudiaton’ (1) és ’digitalSignature’ (0). *A mező értéke: 1*	Igen
CRL szétosztási pont *CRL Distribution Points* OID: 2.5.29.31	Szolgáltató a tanúsítványok visszavonási állapotának ellenőrizhetősége érdekében folyamatosan közzéteszi a legfrissebb tanúsítvány visszavonási listát. *A mező értéke:* DistributionPointName= http://www.e-szigno.hu/CA-Crl	Nem
Legfrissebb CRL *Freshest CRL* OID: 2.5.29.46	A legutóbb kibocsátott tanúsítvány visszavonási lista kibocsátása óta visszavont tanúsítványokat tartalmazó lista elérési helyét adja meg. *A mező értéke:* DistributionPointName= http://www.e-szigno.hu/CA-DeltaCrl	Nem
Szolgáltatói információ elérése *Authority Information Access* OID: 1.3.6.1.5.5.7.1.1	A Szolgáltató által rendelkezésre bocsátott, a tanúsítvány használatához kapcsolódó egyéb szolgáltatásainak leírása. **1.** Szolgáltató a tanúsítványok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást nyújt. Ez a következő címen érhető el: https://ca.e-szigno.hu/ocsp **2.** A tanúsítvány lánc felépítésének megkönnyítésére Szolgáltató megadja a tanúsítványt kibocsátó Hitelesítési Egység tanúsítványának elérési helyét. Ez a következő címeken érhető el: http://www.e-szigno.hu/CA.crt **3.** Szolgáltató időbélyegzés szolgáltatást is végez. Ez a szolgáltatás a következő címen érhető el: https://tsa.e-szigno.hu/tsa *A mező értéke:* (accessMethod= 1.3.6.1.5.5.7.48.1 accessLocation= https://ca.e-szigno.hu/ocsp) (accessMethod= 1.3.6.1.5.5.7.48.2 accessLocation= http://www.e-szigno.hu/CA.crt) (accessMethod= 1.3.6.1.5.5.7.48.3 accessLocation= https://tsa.e-szigno.hu/tsa)	Nem
Minősített tanúsítvánnyal kapcsolatos állítások *Qualified Certificate Statements* OID: 1.3.6.1.5.5.7.1.3	Minősítettség: Annak kijelentése, hogy a kiadott tanúsítvány minősített tanúsítvány. *A mező értéke:* (statementId = 0.4.0.1862.1.1)	Nem

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

A Szolgáltató által kibocsátott tanúsítványok a szabványoknak megfelelően tartalmazzák a Qualified Certificate Statements (1.3.6.1.5.5.7.1.3) és a Certificate Policies (2.5.29.32) mezőket. Amennyiben egy tanúsítvány e mezőket nem tartalmazza, úgy teszt tanúsítványról van szó, amely kizárólag tesztelési célra használható, valós tranzakciók esetén el kell utasítani.

7.2. Tanúsítvány visszavonási lista (CRL) profil

7.2.1. Alap mezők

A Szolgáltató által kibocsátott visszavonási listák alap mezői a következők:

Mezőnév	Értelmezés és érték vagy szabály
Verzió *Version*	A tanúsítvány visszavonási lista a [12] ajánlás 2. verziójának felel meg.
Algoritmus azonosító *Signature Algorithm Identifier*	Ez a szám a Szolgáltató **visszavonási listát hitelesítő elektronikus aláírásá**nak algoritmus azonosítója: **SHA-1** (OID=1.2.840.113549.1.1.5).
Aláírás *Signature*	A Szolgáltató visszavonási listát hitelesítő elektronikus aláírása a [9] szerint generálva és kódolva.
Kibocsátó *Issuer*	A visszavonási listát kibocsátó hitelesítő egység egyedi azonosítója (lásd: **3.1.1.**). 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. UCT szerinti érték a [9] szerinti kódolással.
Következő kibocsátás *Next Update*	A következő visszavonási lista kibocsátásának ideje (lásd: **4.4.9**). UCT szerinti érték a [9] 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:

Mezőnév	Érték vagy szabály	Kritikus
Visszavonás oka *Reason Code*	Ebbe a mezőbe a visszavonás oka kerül.	Nem
Érvénytelenség ideje *Invalidity Date*	Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerül.	Nem
Útmutató *Hold Instruction*	Ebbe a mezőbe a felfüggesztett tanúsítvány kezelése kerül.	Nem

A Szolgáltató a kiterjesztéseket nem köteles kitölteni.

A Szolgáltató által kitöltött visszavonási lista kiterjesztések a következők:

Mezőnév	Érték vagy szabály	Kritikus
CRL sorozatszám *CRL number*	Ebbe a mezőbe a visszavonási listák egyesével növekvő sorozatszámai kerülnek.	Nem

7.3. Időbélyegző profil

Az alkalmazott időbélyegző profilt az RFC 3161: Time-Stamp Protocol (TSP) [28] tartalmazza.

7.4. Online tanúsítvány-állapot válasz (OCSP) profil

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

8. Leírás-adminisztráció

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

8.1. Leírás-változtatási eljárások

8.1.1. 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. Szolgáltató törekedik arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.
A szolgáltatási szabályzat módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

8.1.2. 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.

8.1.3. Értesítéssel változtatható elemek

Minden, a tanúsítványok biztonsági szintjét, felhasználhatóságát módosító változtatás értesítésköteles a **8.2. Közzétételi és tájékoztatási elvek** fejezet szerint.

8.1.4. Észrevételek kezelése

A **8.1.5 Szabályzati objektum-azonosítót vagy -mutatót változtató módosítások** 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.

8.1.5. Szabályzati objektum-azonosítót vagy -mutatót változtató módosítások

Minden olyan jelentősebb módosítás, melyet szolgáltató csak az újonnan kibocsátásra kerülő tanúsítványok esetében alkalmaz (s a már kibocsátottak esetében nem) a szolgáltatási szabályzat verziószámának fő jegyét, és a szabályzat objektumazonosítóját is módosítja. E szabályzatok az előző főbb verziótól eltérő web címen kerülnek közzétételre, így csak az újonnan kibocsátott tanúsítványok mutatói fognak rá hivatkozni.

8.2. Közzétételi és tájékoztatási elvek

8.2.1. A szabályzatban nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen szolgáltatási szabályzat több ilyet is megemlít). A **2.7 A megfelelőség vizsgálata** fejezetben leírt tanúsítási eljárások ezeket a dokumentumokat is vizsgálják.

8.2.2. A szabályzat közzététele

A Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal közzéteszi web oldalain, a https://www.e-szigno.hu/SZSZ/ címen. A Szolgáltató alkalmanként ezt megelőzően is tájékoztatja a közösséget a tervezett változtatásairól.

8.2.3. Szolgáltatás szabályzat jóváhagyási eljárások

Jelen szolgáltatási szabályzat [10] szabványnak, valamint az **MTT+BALE** hitelesítési rendnek való megfelelőségét közzététel előtt a Szolgáltató megvizsgálta. A vizsgálatot a tanúsítást végző szervezet is elvégzi évente rendszeresen végzett felülvizsgálata során.

A szabályzat jogszabályoknak való megfelelőségét a Nemzeti Hírközlési Hatóság is vizsgálja a szabályzat hatályba lépését megelőzően. Szolgáltató szolgáltatási szabályzatának a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal átadja a Hírközlési Felügyelet részére. Szolgáltató alkalmanként ezt megelőzően is konzultál a Nemzeti Hírközlési Hatósággal a tervezett változtatásairól.

A. FOGALMAK

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

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

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

Aláírás-létrehozó eszköz optikai megszemélyesítése
Az aláírás-létrehozó eszköz külső felületén az Aláíróra jellemző adatok vagy kép feltüntetése.

Aláírás-létrehozó eszköz logikai megszemélyesítése
Az aláírás-létrehozó eszközön a kriptográfiai kulcsok generáltatása.

Aláíró (Signatory)
Az a természetes személy, aki az aláírás-létrehozó adat kizárólagos használatára jogosult.

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

Aláíró eszköz szolgáltatás
Az Eat.-ban [1] meghatározott „aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése” szolgáltatás.

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

Bizalmi munkakör
Lásd: **5.2.1 Bizalmi szerepkörök**.

Biztonságos aláírás-létrehozó eszköz (BALE)
Az elektronikus aláírás törvény [1] 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.

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

Elektronikus aláírás ellenőrzése (Electronic Signature Validation)
Az elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, valamint a tanúsítvány felhasználásával.

Elektronikus aláírás felhasználása
Elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése.

Elektronikusan történő aláírás
Elektronikus aláírás hozzárendelése, illetve logikailag való hozzárendelése az elektronikus adathoz.

Elektronikus aláírási termék
Olyan szoftver vagy hardver, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, így különösen elektronikus aláírások, illetőleg időbélyegző készítéséhez, vagy ellenőrzéséhez használható.

Elektronikus dokumentum
Elektronikus eszköz útján értelmezhető adat, mely elektronikus aláírással van ellátva.

Fokozott biztonságú elektronikus aláírás (Advanced Electronic Signature)
Elektronikus aláírás, amely megfelel a következő követelményeknek
• alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,
• olyan eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll,
• a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően az iraton, illetve dokumentumon tett - módosítás érzékelhető.

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

Szolgáltatási Szerződés
Olyan szerződés, melynek keretében az Ügyfél hitelesítés szolgáltatást (Hitelesítés Szolgáltatási Szerződés) vagy egyéb szolgáltatást rendel meg a Szolgáltatótól.

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

Hatóság
Az elektronikus aláírással kapcsolatos szolgáltatásokat nyújtó szolgáltatókat felügyelő hatóság, a Nemzeti 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.

Igénylő
A minősített tanúsítvány iránti igényt benyújtó személy.

Informatikai rendszer
A szolgáltató által a szolgáltatói kulcspár kezeléséhez, az aláírás létrehozó adat előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezelési szolgáltatáshoz, valamint e tevékenységek informatikai

védelméhez használt, az Eat. 3. számú mellékletének f) pontja szerinti megbízható rendszerek és termékek.

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

Körlet
Fizikai védelemmel ellátott helyiségek, területek, melyekre valamilyen biztonsági szabályrendszer vonatkozik.

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

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

Kriptográfiai magánkulcs
Egy kriptográfiai kulcspár egyik kulcsa. A titkos kulcsot titokban kell tartani, mert például aláírásra szolgáló kulcspár esetén a magánkulcs birtokában bárki aláírhat a kulcs tulajdonosa nevében. Ezért a magánkulcsokat (más néven aláírás-létrehozó adatot) biztonságos aláírás-létrehozó eszközön szokás tárolni.

Kriptográfiai nyilvános kulcs
Egy kriptográfiai kulcspár egyik kulcsa. A nyilvános kulcsot nem szükséges titokban tartani, aláírásra szolgáló kulcspár esetén a nyilvános kulcs szolgál az aláírás ellenőrzésére (lásd: aláírás-létrehozó adat).

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

Minősített tanúsítványtípus (Qualified Certificate Policy)
Olyan tanúsítványtípus, amely megfelel az elektronikus aláírási törvény 2. és 3. mellékletében foglalt követelményeknek.

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

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

MTT+BALE
Olyan tanúsítványtípus, melynek keretében a Szolgáltató csakis biztonságos aláírás-létrehozó eszközzel együtt bocsát ki tanúsítványt, ily módon garantálja, hogy a tanúsítványhoz tartozó aláírás-létrehozó adat a biztonságos aláírás-létrehozó eszközön generálódott, és nem léteznek róla másolati példányok.

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;

Root hitelesítő szervezet
Root CA A hierarchikusan elhelyezkedő hitelesítő szervezetek tanúsítványait a hierarchiában eggyel magasabb szinten elhelyezkedő hitelesítő szervezet hitelesíti saját elektronikus aláírásával. A hierarchia csúcsán álló root hitelesítő szervezet tanúsítványát ő saját maga írja alá.

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

Szervezeti felfüggesztési/visszaállítási kérelem
Olyan felfüggesztési vagy visszaállítási kérelem, amelyet szervezeti ügyintéző küldött el, és nem a saját tanúsítványát, hanem egy másik, ugyanahhoz a szervezethez tartozó tanúsítványt szeretné felfüggeszteni vagy visszaállítani.

Szolgáltatás időtartama
Az az időszak, amelyre a Költségviselő megfizette a tanúsítvány fenntartásával kapcsolatos díjat. Pontosan egybeesik az aktuális tanúsítvány érvényességi idejével.

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

Szolgáltató
Jelen dokumentumban a MICROSEC Kft., amely az Elektronikus aláírás törvényben [1] foglaltaknak megfelelő a hitelesítés-szolgáltatást, az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást és időbélyegzés szolgáltatást minősített szolgáltatóként nyújtja.

Szolgáltatói kulcspár (CA key pair)
A szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs.

Szolgáltatói magánkulcs (CA private key)
Olyan kriptográfiai magánkulcs, amelyet a hitelesítés-szolgáltató vagy az időbélyegzést nyújtó szolgáltató saját elektronikus aláírási szolgáltatásának igazolására, így különösen a tanúsítvány kibocsátására, a visszavonási nyilvántartásokra, az időbélyegzésre, a naplózáshoz, az archiváláshoz használ.

Szolgáltatói nyilvános kulcs (CA public key)
Olyan kriptográfiai nyilvános kulcs, amelyet a szolgáltatói magánkulcs használatával létrehozott elektronikus aláírás ellenőrzésére használnak.

Tanúsítvány (Certificate)
A hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot egy meghatározott személyhez kapcsolja, akinek személyazonosságáról meggyőződött.

Tanúsítvány aktualizálás
A tanúsítványcsere egyik változata. Új tanúsítvány biztosítása, amelyben a tanúsítványtulajdonos régi nyilvános kulcsát és megváltozott új adatait a hitelesítés-szolgáltató (új érvényességi időtartamra) érvényes magánkulcsával aláírja.

Tanúsítvány előállítás (Certificate generation)
A regisztráció szolgáltatásra alapozva tanúsítványok létrehozása és aláírása. Magában foglalja a kezdeti tanúsítvány előállítást és a tanúsítványcserének különböző formáit is.

Tanúsítvány felfüggesztés (Certificate suspension)
A tanúsítvány érvényességének felfüggesztése az elektronikus aláírási törvény 14. § (1) alatt meghatározott esetekben.

Tanúsítvány frissítés
A tanúsítványcsere egyik változata. Új tanúsítvány biztosítása, amelyben a tanúsítványtulajdonos változatlan (régi) nyilvános kulcsát és egyéb adatait a hitelesítés-szolgáltató (új érvényességi időtartamra) érvényes magánkulcsával aláírja.

Tanúsítvány kibocsátás (Certificate dissemination)
A tanúsítvány átadása az Alárónak, az Aláíró Szervezetének valamint a hitelesítés-szolgáltató nyilvántartásában a tanúsítvány elérhetővé tétele az aláíró által meghatározott kör részére.

Tanúsítvány kulcscsere (Re-key)
A tanúsítványcsere egyik változata. Új tanúsítvány biztosítása, melyben a tanúsítványtulajdonos megváltozott új nyilvános kulcsát és régi adatait a hitelesítés-szolgáltató (új érvényességi időtartamra) érvényes magánkulcsával aláírja.

Tanúsítványcsere (Certificate renewal)
Az alábbi három fogalom együttese:
- tanúsítvány frissítés,
- tanúsítvány aktualizálás,
- tanúsítvány kulcscsere

Tanúsítvány típus
Lásd: hitelesítési rend.

Tanúsítvány visszavonás (certificate revocation)

A tanúsítvány érvényességének végleges visszavonása az elektronikus aláírási törvény által meghatározott esetekben.

Tanúsítvány visszavonás kezelés (revocation management)
Az Eat.-ban meghatározott esetekben a kibocsátott tanúsítványok visszavonására és felfüggesztésére vonatkozó eljárások lefolytatása.

Tanúsítvány visszavonási lista (Certificate Revocation List)
Valamely okból visszavont, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, amelyet a hitelesítés-szolgáltató bocsát ki.

Tanúsítványfajta
A Szolgáltató az Aláírók számára különböző tanúsítványfajtákat kínál fel. Más fajtájú tanúsítványt kap az aláíró, ha magánszemélyként igényel tanúsítványt, mintha szervezeti személyként igényelné. A Szolgáltató által megkülönböztetett tanúsítványfajtákat az 1.1.6 fejezet írja le.

Tanúsítványtípus (Certificate Policy, CP)
Szabályok összessége, amely megmutatja adott tanúsítványok alkalmazhatóságát egy bizonyos közösségre, illetve alkalmazások olyan csoportjára, ahol azonosak a biztonsági követelmények.

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

Ügyfél
Hitelesítés szolgáltatás esetében az Aláíró, az Aláíró Szervezete és a Költségviselő együttesen; időbélyegzés és online tanúsítvány-állapot szolgáltatás esetében a szolgáltatást igénybe vevő fél.

Végfelhasználó
Az Aláíró, Aláíró Szervezete és az Érintett fél együttesen.

Visszavonási nyilvántartások
Nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.

Visszavonási állapot közzététele (Revocation status service)

Információ nyújtása az érintett (fogadó) fél számára a tanúsítványok visszavonásáról. A szolgáltatás lehet valós idejű, vagy az információk előre meghatározott időközönkénti aktualizálásán kell alapulnia.

B. RÖVIDÍTÉSEK

CA: Certification Authority, Hitelesítés Szolgáltató
CRL: Certificate Revocation List, Tanúsítvány visszavonási lista
OCSP: Online Certificate Status Response, Online tanúsítvány-állapot válasz
NHH: Nemzeti Hírközlési Hatóság
RA: Registration Authority, Regisztráló szervezet
TSA: Time Stamping Authority, Időbélyegzés Szolgáltató
CP: Certificate Policy, Tanúsítványtípus, Hítelesítési Rend
CPS: Certificate Practice Statement, Hitelesítés Szolgáltatási Szabályzat
GPS: Global Positioning System, Globális Helymeghatározó Rendszer

C. HIVATKOZÁSOK

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

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

[2] 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

[3] 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

[4] Minősített tanúsítványtípus minták minősített hitelesítés-szolgáltatók számára, 1.2. verzió

[5] ISO 3166

[6] FIPS PUB 140-1 (1994. január 11): "Kriptográfiai modulok biztonsági követelményei"

[7] ETSI TS 101 456 Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények

[8] ETSI TS 101 862 Minősített tanúsítvány profil

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

[10] RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)

[11] RFC 3039 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)

[12] International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer”

[13] CEN 14167-1 munkacsoport egyezmény: „Biztonsági követelmények elektronikus aláírásokkal kapcsolatos tanúsítványokat kezelő rendszerek megbízható rendszereire”

[14] MSZ ISO/IEC 15408:2002 Az információbiztonság értékelésének közös szempontrendszere (Common Criteria for Information Technology Security Evaluation version 2.1):

MSZ ISO/IEC 15408-1: 1. rész: Bevezetés és általános modell (Introduction and general model)

MSZ ISO/IEC 15408-2: 2. rész: A biztonság funkcionális követelményei (Security functional requirements)

MSZ ISO/IEC 15408-3: 3. rész: A biztonság garanciális követelményei (Security assurance requirements)

[15] EU Directive 1999/93/EC of the European Parliament and the council of 13 December 1999 on a Community framework for electronic signatures;

[16] CEN CWA 14170: Security Requirements for Signature Creation Applications

[17] CEN CWA 14171: Procedures for Electronic Signature Verification

[18] PP-MS-03/001: Biztonsági specifikáció Minősített elektronikus aláírás létrehozó és kezelő alkalmazáshoz

[19] ST-MS-03/001: Biztonsági előirányzat Minősített elektronikus aláírás létrehozó és kezelő alkalmazáshoz

[20] HR-MS-05/001: Minősített e-Szignó Hitelesítés Szolgáltató Biztonságos aláíró-eszközzel együttesen kiadott minősített tanúsítvány hitelesítési rendek, OID: 1.3.6.1.4.1.21528.2.1.1.2

[21] IR-MS-05/001: Minősített e-Szignó Hitelesítés Szolgáltató időbélyegzési rend, OID: 1.3.6.1.4.1.21528.2.1.1.3

[22] ASZF_HSZ-MS-05/001: e-Szignó Hitelesítés Szolgáltató által nyújtott hitelesítés szolgáltatásra vonatkozó Általános Szerződési Feltételek, OID: 1.3.6.1.4.1.21528.2.1.1.4

[23] ASZF-ISZ-MS-05/001: e-Szignó Hitelesítés Szolgáltató által nyújtott időbélyegzés és online tanúsítvány-állapot szolgáltatásokra vonatkozó Általános Szerződési Feltételek, OID: 1.3.6.1.4.1.21528.2.1.1.5

[24] RFC 3280: Certificate and Certificate Revocation List (CRL) Profile (az RFC 2459 újabb változata),

[25] RFC 3739: Qualified Certificates Profile (az RFC 3039 újabb változata)

[26] ETSI TS 101 862: Qualified Certificate Profile (v1.3.2; 2004-08)

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

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

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

[30] ITU X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer” ajánlás 3. verziójának

[32] 3/2005 IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről