MICROSEC

Számítástechnikai Fejlesztő Kft.

e-Szignó Hitelesítés Szolgáltató

Biztonságos aláíró-eszközzel együttesen kiadott minősített tanúsítvány hitelesítési rendek

Azonosító:	1.3.6.1.4.1.21528.2.1.1.2.3.1 és 1.3.6.1.4.1.21528.2.1.1.12.3.1
Verzió:	3.1
Első verzió hatályba lépése:	2005. április 1.
Kezelési mód:	**Nyilvános**
Jóváhagyta:	Ellbogen András
Jóváhagyás dátuma:	2006. december 4.
Hatálybalépés dátuma:	**2006. december 4.**

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

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat OID: 1.3.6.1.4.1.21528.2.1.1.2	2005-04-01	Berta István Zsolt Belső auditor: Tóth Elemér
2.0	A hatósági szemlét követő módosítások. Az álnevet kizáró és az álneves hitelesítési rend szétválasztása. OID: 1.3.6.1.4.1.21528.2.1.1.2 és 1.3.6.1.4.1.21528.2.1.1.12	2005-08-08	Berta István Zsolt Belső auditor: Tóth Elemér
3.0	Módosítás az Általános Szerződési Feltételek megváltozása miatt. OID: 1.3.6.1.4.1.21528.2.1.1.2 és 1.3.6.1.4.1.21528.2.1.1.12	2006-11-19	Dr. Berta István Zsolt
3.1	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően. OID: 1.3.6.1.4.1.21528.2.1.1.2.3.1 és 1.3.6.1.4.1.21528.2.1.1.12.3.1	2006-12-04	Dr. Berta István Zsolt

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a MICROSEC Számítástechnikai Fejlesztő Kft. (továbbiakban: Szolgáltató) által üzemeltetett minősített *e-Szignó Hitelesítés Szolgáltató* által támogatott hitelesítési rendeket tartalmazza. A dokumentum pontos megértéséhez szükségesek a használt fogalmak értelmezésének pontos ismerete, amelyek az A mellékletben találhatóak. E hitelesítési rendek a nemzetközi [7] és hazai [4] ajánlások alapján készültek, tartalmukban és felépítésükben követik azok előírásait.

1.1. Áttekintés

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

1.1.1. A definiált hitelesítési rendek

Jelen dokumentum az alábbi hitelesítési rendeket tartalmazza:

Azonosító	Hitelesítési rend neve
OID: 1.3.6.1.4.1.21528.2.1.1.2.3.1 NHH azonosító: HL-7789-2/2005	„Nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített hitelesítési rend”
OID: 1.3.6.1.4.1.21528.2.1.1.12.3.1	„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.

1.1.2. Többletvállalások az ETSI TS 101 456-hoz képest

Mindkét hitelesítési rend megfelel az ETSI TS 101 456-ban [7] megfogalmazott előírásoknak, a Szolgáltató ezen felül a következőket vállalja:

- Regisztráció során az aláíró által megadott adatokat a Szolgáltató közhiteles adatbázissal egyezteti.
- A tanúsítványok 24 órás telefonos ügyeleten keresztül függeszthetőek fel. A felfüggesztés a telefonos beszélgetés során megtörténik, és a megváltozott visszavonási állapotot a Szolgáltató azonnal közzé teszi visszavonási nyilvántartásában.
- Onnantól kezdve, hogy a telefonos felfüggesztési kérelem megérkezett a Szolgáltatóhoz, egészen addig a pillanatig, amíg a tanúsítvány érvénytelen állapota meg nem jelenik a Szolgáltató által közzétett visszavonási nyilvántartásban, a Szolgáltató vállalja a felelősséget a tanúsítvánnyal okozott károkért.
- A Szolgáltató OCSP szolgáltatás és visszavonási listák (CRL) segítségével teszi közzé a tanúsítványok visszavonási állapotát. A Szolgáltató 24 óránként bocsát ki CRL-t. Emellett a

Szolgáltató vállalja, hogy egy órán belül új CRL-t bocsát ki, ha bármely tanúsítvány állapota megváltozik.

- A Szolgáltató a végfelhasználói tanúsítványokban az aláíróra jellemző egyedi azonosítót (OID) szerepeltet. A Szolgáltató garantálja, hogy ha két tanúsítványban az egyedi azonosító értéke megegyezik, akkor a két tanúsítvány ugyanahhoz az aláíróhoz tartozik. (Ha az azonosító értéke különbözik, abból nem következik, hogy a két tanúsítvány nem ugyanahhoz az aláíróhoz tartozik.)

A fenti többletvállalások részleteit a Szolgáltatási Szabályzat tartalmazza.

1.1.3. Jogszabályi megfelelőség

A fenti hitelesítési rendek

- megfelelnek az [1] Törvény 2. számú mellékletében meghatározott követelményeknek;
- olyan hitelesítés szolgáltató adta ki őket, amely teljesíti az [1] Törvény 3. számú mellékletében meghatározott követelményeket;
- olyan biztonságos aláíró eszköz került felhasználásra, amely eleget tesz az [1] Törvény 1. számú mellékletében meghatározott követelményeknek;
- nyilvános körben kerültek kibocsátásra.

Ezen alapkövetelmények alapján kibocsátott minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon kielégítik, ahogy egy kézírásos aláírás kielégíti ugyanazt a követelményt a papír-alapú adatok vonatkozásában.

1.2. Azonosítás

A jelen dokumentumban meghatározott hitelesítési rendek azonosító adatai (nevük, OID-jük, illetve a Nemzeti Hírközlési Hatóság által hozzárendelt azonosítójuk) az előző fejezetben illetve a dokumentum fedőlapján találhatóak.

1.3. Közösség és alkalmazhatóság

1.3.1. Hitelesítő szervezet

A Szolgáltató szervezetén belül az *e-Szignó Hitelesítés Szolgáltató* egy önálló üzleti egység látja el a hitelesítés szolgáltatással kapcsolatos feladatokat. Ezen hitelesítő szervezet feladatát és hatáskörét a Szolgáltató által kibocsátott „e-Szignó Hitelesítés Szolgáltató – Szolgáltatási Szabályzat" (továbbiakban Szolgáltatási Szabályzat) című dokumentuma tartalmazza.

1.3.2. Regisztráló szervezet

A Szolgáltató a kezdeti regisztrációt és a tanúsítványok kibocsátásával kapcsolatos egyéb feladatokat, valamint a további tanúsítvány menedzsment feladatokat központilag, a saját szervezetén belül működő *ügyfélszolgálati iroda* keretén belül valósítja meg. Az iroda feladatait és hatáskörét a Szolgáltatási Szabályzat rögzíti. Az ügyfélszolgálati iroda feladatait – a Szolgáltatási Szabályzatban leírt feltételek mellett – mobil regisztrációs egységek is elláthatják. A Szolgáltató a saját maga által végzett regisztrációval egyenértékűnek fogadja el, ha a regisztráció során az Aláíró személyazonosságát közjegyző tanúsítja.

A Szolgáltató egyéb szervezetekkel is szerződést köthet külső regisztrációs irodák létrehozására, amelyek a központi iroda egyes feladatait külső helyszínen látják el. A külső regisztrációs irodák feladatait és hatáskörét a Szolgáltatási Szabályzat tartalmazza.

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 biztonságos aláíró eszközt kizárólagosan használó – természetes személy,

- az *Aláíró Szervezete (képviselt szervezet):* 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 az a szóban forgó szervezet, amely szintén megjelölésre kerül a tanúsítványban,
- az Előfizető: aki a tanúsítvány kibocsátásával kapcsolatos díjakat fizeti.
- az *Érintett fél:* a tanúsítvány felhasználásával létrehozott elektronikus aláírással ellátott elektronikus dokumentumot befogadó fél. Természetes vagy jogi személy, aki elfogadja a jelen hitelesítési rendben és a Szolgáltatási Szabályzatban leírt ajánlásokat.

Az *Aláíró* és az *Előfizető* szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Szolgáltatási Szerződésben, Általános Szerződési Feltételekben [22], jelen Hitelesítési Rendben [20] és a Szolgáltatási Szabályzatban foglaltak szerint. A Szolgáltató az Aláíróval és az Aláíró Szervezetével és az Előfizetővel 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) Az ezen hitelesítési rendek érvényességi körében kibocsátott minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon kielégítik, ahogy egy kézírásos aláírás kielégíti ugyanazt a követelményt a papír-alapú adatok vonatkozásában.
b) A kibocsátott minősített tanúsítványok kizárólag aláírási célra használhatók fel.

1.4. Kapcsolattartás

Szolgáltató

Név: MICROSEC Számítástechnikai Fejlesztő Kft.
Cégjegyzék szám: 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

Ügyfélszolgálati iroda

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

Hitelesítő szervezet

A hitelesítő szervezet elérése az ügyfélszolgálati irodán keresztül történik.

2. Általános rendelkezések

2.1. Kötelezettségek

A Szolgáltató általában:

a) A Szolgáltató – a hitelesítő szervezet és a regisztrációs szervezet(ek) – és a tanúsítványtár és a visszavonási nyilvántartás együttes tevékenységével) az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat biztosítja:
   - elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás, HSZ), ezen belül:
     - regisztráció,
     - tanúsítvány előállítás,
     - kibocsátás,
     - visszavonás kezelés,
     - visszavonási állapot közzététele
   - aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése (a továbbiakban eszközellátás, ESZ).

b) A Szolgáltató gondoskodik a Szolgáltatóra vonatkozó valamennyi, a 3.-8. fejezetekben részletezett állítás teljesüléséről.

c) A Szolgáltató szolgáltatásait hozzáférhetővé teszi minden érintett igénylő számára.

d) A Szolgáltató jogi személy.

e) A Szolgáltató megfelelően dokumentált megállapodásokkal és szerződéses kapcsolatokkal rendelkezik azon esetekre, amikor a szolgáltatások nyújtása alvállalkozókat, illetve más, harmadik felekkel kötött megegyezéseket érint.

f) A Szolgáltató olyan Szolgáltatási Szabályzattal rendelkezik, mely a hitelesítési rendekben azonosított valamennyi követelmény kielégítésére szolgáló gyakorlatra és eljárásra vonatkozik.

g) A Szolgáltató szolgáltatási szabályzata meghatározza a Szolgáltató szolgáltatásait támogató valamennyi külső szervezetre vonatkozó kötelezettségeket, beleértve az alkalmazandó szabályzatokat és gyakorlatokat is.

h) A Szolgáltató valamennyi szolgáltatását szolgáltatási szabályzatával összhangban nyújtja.

i) A Szolgáltatási Szabályzatot a Szolgáltató felső szintű irányító testülete hagyja jóvá.

j) A Szolgáltatási Szabályzat megfelelő megvalósításáért a Szolgáltató felső vezetősége felel.

k) A Szolgáltató szolgáltatási szabályzatát és egyéb kapcsolódó dokumentációját a hitelesítési rendnek való megfelelés felméréséhez szükséges mértékig az Aláíró, az Előfizető, az Aláíró Szervezete és az érintett felek rendelkezésére bocsátja.

l) A Szolgáltató rendszeresen felülvizsgálja hitelesítési rendjeit és szolgáltatási szabályzatát, az újra érvényesített dokumentumok tartalmazzák a szükséges módosításokat.

m) A Szolgáltató időben értesítést tesz közzé a hitelesítési rendjeiben és a Szolgáltatási Szabályzatban tervezett változtatásokról és a fenti (i. pont szerint történő) jóváhagyást követően az átdolgozott szolgáltatási szabályzatát a (k. pontban előírtak szerint) haladéktalanul hozzáférhetővé teszi.

2.1.1. A hitelesítő szervezet kötelezettségei

a) A hitelesítő szervezet biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatást:
   - tanúsítvány előállítás,

   egyúttal közreműködik (a visszavonási listák aláírásával) az alábbi elektronikus aláírással kapcsolatos szolgáltatás biztosításában:
   - visszavonási állapot közzététele.

A hitelesítő szervezet a tanúsítvány előállítás szolgáltatás biztosítása keretén belül:

b) ellenőrzi a regisztráló szervezettől érkező tanúsítvány kérelmet, benne az aláírandó tanúsítvány adatokat tartalmazó üzenet sértetlenségét és hitelességét;

c) feldolgozza a regisztráló szervezettől érkező hiteles és sértetlen tanúsítvány kérelmet, melynek keretén belül előállítja a tanúsítványt (aláírja az aláírandó tanúsítvány adatokat);

d) a minősített tanúsítvány aláírására használt magánkulcsát csak erre a célra (minősített tanúsítványok és visszavonási listák aláírására) használja fel;

e) csak olyan tanúsítványokat állít elő, amelyek megfelelnek a Szolgáltatási Szabályzatban meghatározott, támogatott hitelesítési rendeknek;

f) csak olyan minősített tanúsítványokat bocsát ki, amelyek megfelelnek az [1] 2. számú mellékletében, valamint a [2] 162. pontjában meghatározott követelményeknek;

g) gondoskodik arról, hogy a tanúsítványban foglalt „megkülönböztetett név” (distinguished name) egyedi legyen a Szolgáltató szolgáltatási körén belül;
h) gondoskodik arról, hogy a Szolgáltató teljes szolgáltatási körén belül kibocsátott tanúsítványokhoz tartozó kulcsok mindvégig egyediek maradjanak;
i) megválaszolja a regisztráló szervezetnek a tőle kapott tanúsítvány kérelmet, benne elküldve az előállított tanúsítványt, biztosítva a válaszüzenet sértetlenségét és hitelességét.

A hitelesítő szervezet a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:
j) ellenőrzi a regisztráló szervezettől érkező visszavonási kérelmet, és a kérelem sértetlenségét és hitelességét;
k) a visszavonási listák aláírására használt magánkulcsát a minősített tanúsítványok aláírása mellett más célra nem használja fel
l) rendszeresen új tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, naponta egyszer, a szolgáltatási szabályzatban meghatározott frissítési időponthoz igazodóan, mely tartalmazza a következő lista tervezett kibocsátási idejét is;
m) elküldi a visszavonási nyilvántartásnak az új tanúsítvány visszavonási listát, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét.
n) lehetőséget biztosít rá, hogy az Aláíró és az Érintett fél on-line módon lekérdezze az egyes tanúsítványok pillanatnyi érvényességét.

A hitelesítő szervezet tanúsítványtárat és visszavonási nyilvántartást üzemeltet, amelyre az alábbi kötelezettségek vonatkoznak:
a) A tanúsítványtár és a visszavonási nyilvántartás az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat biztosítják:
   - (tanúsítvány és szabályzat) kibocsátás,
   - visszavonási állapot közzététele

A tanúsítványtár:
b) közzé teszi a végfelhasználói tanúsítványokat;
c) nyilvánosságra hozza a szolgáltatási szabályzatot, általános szerződési feltételeket és egyéb ezekhez kapcsolódó információt;
d) biztosítja a b)-c) alatt szereplő információ folyamatos elérhetőségét, még rendkívüli üzemeltetési helyzet esetén is.

A visszavonási nyilvántartás:
e) közzé teszi a hiteles és sértetlen új tanúsítvány visszavonási listát;
f) biztosítja a legfrissebb tanúsítvány visszavonási lista folyamatos elérhetőségét, még rendkívüli üzemeltetési helyzet esetén is.

2.1.2. A regisztráló szervezet kötelezettségei

A regisztrációs szervezet feladata a Szolgáltató képviselete a szolgáltatások kapcsán a végfelhasználónál. Ennek keretében a következő feladatokat látja el:

a) A regisztráló szervezet biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:
   - elektronikus aláírás hitelesítés-szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás), ezen belül:
     - regisztráció,
     - visszavonás kezelés,
   - aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése,

   egyúttal közreműködik az alábbi elektronikus aláírással kapcsolatos szolgáltatások biztosításában:
   - tanúsítvány előállítás,
   - kibocsátás
   - visszavonási állapot közzététele

A regisztráló szervezet a regisztráció szolgáltatás keretén belül:
b) gondoskodik a tanúsítványt igénylő megfelelő azonosításáról, illetve arról, hogy a tanúsítványt igénylő formanyomtatványok teljesek, pontosak és kellőképpen hitelesek legyenek;

c) ellenőrzi a tanúsítványt igénylő személyazonosságát és a leendő Aláíró azon egyedi jellemzőit, melyet a minősített tanúsítvány igazol;
d) összegyűjti, illetve meghatározza a regisztráció során valamennyi, az [1] 2. számú mellékletében meghatározott, tanúsítványba kerülő adatot;
e) ellenőrzi a tanúsítványt igénylő által átadott személyazonosító és egyéb igazoló dokumentumok valódiságát, érvényességét, sértetlenségét és hitelességét. Összeveti egymással és a valósággal az egyes iratokon szereplő adatokat (így különösen a tanúsítványt személyesen igénylő ügyfél fotóját az arcával, aláírását a helyszíni aláírásával). Ellenőrzi a dokumentumok érvényességét, valódiságát valós idejű nyilvántartásokban is;
f) írásbeli indoklással visszautasítja a tanúsítvány kiadását, amennyiben a tanúsítvány igénylés nem teljes, nem helyes, nem az arra jogosult által történik, vagy egyéb módon nem felel meg az elvárt feltételeknek;
g) nyilvántartásba vesz minden, a tanúsítványok kiadásához kapcsolódó, a [2] 152. pontjában meghatározott valamennyi, információt;
h) megőrzi a g) pontbeli nyilvántartásokat a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig;
i) bizalmas információként kezeli az Aláíró, az Előfizető és az Aláíró Szervezete minden adatát, kivéve azokat, amelyeket a 2.8.2 alfejezet tárgyal. A Szolgáltató a birtokába jutott bizalmas információkat a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli, s csak a 2.8.3-2.8.7 alfejezetekben említett esetekben és személyek részére fedi fel őket;
j) korlátozás nélkül biztosítja az Aláíró számára a rá vonatkozó regisztrációs és egyéb információhoz történő hozzáférést (lásd 2.8.6).

A regisztráló szervezet a visszavonás kezelés szolgáltatás keretén belül:
k) ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét (lásd még 4.4.2 és 4.4.6), valamint szabályosságát (lásd még 4.4.3 és 4.4.7) ;
l) haladéktalanul végrehajtja a hiteles, érvényes és szabályos, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket (vagyis a kérelmezett változást átvezeti a tanúsítványtár alapját képező tanúsítvány állapot adatbázisába);
m) visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket;
n) haladéktalanul intézkedik egy tanúsítvány visszavonásáról, amennyiben olyan tényről szerez tudomást, ami a tanúsítvány felhasználhatóságának biztonságát fenyegeti;
o) tájékoztatja a visszavont, illetve felfüggesztett tanúsítvány tulajdonosát tanúsítványa állapotának változásáról;
p) folyamatosan és állandó rendelkezésre állással biztosítja a visszavonás kezelési szolgáltatást minden érdekelt fél számára, egyúttal szolgáltatási szabályzatában megadja az előre tervezett és rendkívüli leállások leghosszabb időtartamát.

A regisztráló szervezet az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:
q) gondoskodik valamennyi általa, az Aláíró számára végrehajtott kulcs előállítás biztonságosságáról, az Aláíró magánkulcsának titkosságáról;
r) az Aláíró részére előállított kulcspárt:
   - olyan kriptográfiai eszközzel állítja elő, mely tanúsítvánnyal igazoltan megfelel a [13] vagy [14] szabványok 3-as szintjének, vagy a [6] szabványos védelmi profilnak, egyben szerepel a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, tanúsított elektronikus aláírási termékek listáján is,
   - olyan algoritmus felhasználásával állítja elő, melyet a [2] 1. sz. melléklete illetve a [31] az elfogadott kriptográfiai algoritmusok között megfelelő kulcsgeneráló algoritmusként ismer el,
   - olyan aláíró algoritmushoz és olyan kulcshosszúságban állítja elő, melyet a [2] 1. sz. melléklete illetve a [31] az elfogadott kriptográfiai algoritmusok között megfelelő aláíró algoritmusként, illetve megfelelő paraméterként ismer el;
s) az Aláíró kulcspárját az Aláírónak később átadott biztonságos aláírás-létrehozó eszközön generálja
t) az Aláíró részére előállított magánkulcsot a biztonságos aláírás-létrehozó eszköz kibocsátása során nem ismeri meg, így adatbázisában nem tárol belőle másolatot
u) gondoskodik az általa biztosított biztonságos aláírás-létrehozó eszköz kibocsátása során az eljárás biztonságáról;
v) ellenőrzi a biztonságos aláírás-létrehozó eszköz kezelését;

w) ellenőrzi, hogy a szolgáltatás során felhasznált aláírás-létrehozó eszköz a Nemzeti Hírközlési Hatóság által nyilvántartásba vett biztonságos aláírás-létrehozó eszköz-e;
x) a biztonságos aláírás-létrehozó eszköz előkészítését megfelelően biztonságos környezetben (lásd 5.1 fejezet) hajtja végre;
y) biztonságos konfigurációt alakít ki a biztonságos aláírás-létrehozó eszközön az inicializálás, formázás és fájl-struktúra kialakítás során;
z) a biztonságos aláírás-létrehozó eszközt biztonságosan tárolja és juttatja el a szándék szerinti, azonosított Aláíróhoz;
aa) biztonságos módon előállítja a kezdeti aktivizáló adatokat, majd a biztonságos aláírás-létrehozó eszköztől elkülönítve eljuttatja az Aláíróhoz;
bb) biztosítja, hogy alkalmazottai nem élhetnek vissza a biztonságos aláírás-létrehozó eszközzel.

A regisztráló szervezet a tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:
cc) kezdeti tanúsítvány előállítás esetén a regisztráció szolgáltatás e) pontjában leírt módon összegyűjtött, tanúsítványba kerülő adatokat ellenőrzi az adott hitelesítési rendhez kapcsolódó hitelesítési/ellenőrzési eljárás szerint. A tanúsítvány kibocsátásához szükséges ellenőrzések és visszaigazolások sikeres befejeződése után a hitelesítő szervezet felé tanúsítvány kibocsátási kérelem üzenetet indít el;
dd) tanúsítvány kulcscsere és tanúsítványfrissítés kérelem esetén ellenőrzi a már korábban nyilvántartásba vett Aláírótól érkező tanúsítványcsere-kérelem teljességét, pontosságát, hitelességét és teljesíthetőségét. A hitelesség ellenőrzéséhez minden esetben megköveteli az Aláíró ismételt személyes megjelenését

A regisztráló szervezet a (tanúsítvány és szabályzat) kibocsátás szolgáltatásban való közreműködés keretén belül:
ee) fogadja a hitelesítő szervezettől kapott új tanúsítványokat, illetve új szabályzatokat, valamint ellenőrzi ezek hitelességét és sértetlenségét;

2.1.3. Az Aláíró és az Előfizető kötelezettségei

A Szolgáltató az Aláírót és az Előfizetőt megállapodáson (lásd a 2.6.1 és 4.1 alfejezeteket) keresztül az alábbiakra kötelezi:
a) szervezeti tanúsítvány esetén a regisztráló szervezetnél személyesen megjelenő Aláíró mutasson be az Aláíró szervezetétől származó olyan igazolást, amely szerint az Aláíró jogosult olyan tanúsítványra, amelyben az Aláíró Szervezete is megjelenik;
b) pontos és teljes információt adjon be a regisztráló szervezethez jelen hitelesítési rend követelményeinek megfelelően, különös tekintettel a regisztrációra;
c) a kulcspárt csak a vele közölt valamennyi korlátozásnak megfelelően használja;
d) ésszerű gonddal járjon el, hogy megelőzze az Aláíró magánkulcsának illetéktelen felhasználását;
e) Az Aláíró magánkulcsát aláírásra csak a biztonságos aláírás-létrehozó eszközzel használja,
f) késedelem nélkül értesítse a Szolgáltatót, amennyiben az alábbiak közül bármelyik bekövetkezik a tanúsítványban megadott érvényességi időszak vége előtt:
   - az Aláíró magánkulcsa elveszett, azt ellopták, esetlegesen kompromittálták,
   - az Aláíró elvesztette ellenőrzését magánkulcsa felett, aktivizálási adatai (például PIN kód) kompromittálódása, illetve más okokból kifolyólag,
   - tudomására jutott, hogy a tanúsítvány tartalmában vagy egyéb regisztrációs adatokban pontatlanság van, illetve változás következett be;
g) kompromittálódás esetén az Aláíró magánkulcsának használatát azonnal és véglegesen szakítsa meg.

2.1.4. Ajánlások az Érintett fél számára

Az érintett felek számára rendelkezésre bocsátott (lásd 2.6.1 alfejezetet) kikötések és feltételek tartalmaznak egy megjegyzést, miszerint, ha ésszerű módon egy tanúsítványra kívánnak hagyatkozni, az alábbiakat kell tenniük:
a) ellenőrizzék a tanúsítvány érvényességét az érvényes visszavonási állapot információ felhasználásával, a szabályzatoknak megfelelően;
b) vegyék figyelembe a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, melyek a tanúsítványban és a szabályzatokban szerepelnek;
c) tegyenek meg minden, megállapodásokban, illetve máshol előírt egyéb óvintézkedést.

A fenti lépéseket a Szolgáltatási Szabályzat részletesen tartalmazza.

2.2. Felelősség

A Szolgáltató általában:

a) A Szolgáltató felelősséget vállal az általa támogatott hitelesítési rendekben leírt eljárásoknak való megfelelőségért, még abban az esetben is, amikor a Szolgáltató egyes tevékenységeit alvállalkozók végzik.
b) A Szolgáltató a vele szerződéses jogviszonyban álló felekkel (ilyen az Aláíró és az Előfizető) szemben a Polgári Törvénykönyv szerződésszegésért való felelősség szabályai szerint felelős.
c) A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik féllel (ilyen az érintett fél) szemben a Polgári Törvénykönyv szerződésen kívüli károkozásról szóló szabályai (Ptk. 339. §) szerint felelős.
d) A Szolgáltató nem felelős az olyan kárért, mely abból adódott, hogy az érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és Szolgáltató szolgáltatói szabályzata szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.
e) A Szolgáltató nem vagyoni felelőssége tekintetében az Aláíró Szervezete és az érintett fél irányában a Polgári Törvénykönyv nem vagyoni felelősségről szóló szabályai alkalmazandóak.
f) A Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a hibájából, kötelezettségeinek megszegéséből, valamint a neki felróható okokból bekövetkező, bizonyítható károkért tartozik helyt állni.

2.2.1. A hitelesítő szervezet felelőssége

a) A hitelesítő szervezet felelős:
    - az általa kibocsátott tanúsítványok hitelességéért,
    - az általa kibocsátott szabályzatokért, azok jogszabályi megfelelőségéért és betartásáért,
    - általában kötelezettségei betartásáért.
    - a generált kulcspárok megfelelőségéért, a magánkulcs- nyilvános kulcs és tanúsítvány összetartozásáért,
b) A hitelesítő szervezet nem felelős:
    - az Aláírók magánkulccsal, illetve aláírás-létrehozó eszközzel kapcsolatos tevékenységeiért,
    - az érintett felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért.
    - az Aláíró, Aláíró Szervezete, érintett felek, és mások által kibocsátott szabályzatokért.

2.2.2. A regisztráló szervezet felelőssége

a) A regisztráló szervezet felelős:
    - az Aláíró személyes és az Aláíró Szervezetének szervezeti azonosságának megállapításáért, illetve az Előfizető szervezeti vagy személyes azonosságának megállapításáért,
    - a felvett regisztrációs adatok valódiságáért,
    - az aláírás-létrehozó eszköz - aktivizáló kód eszközre töltött kulcsok összetartozásáért,
    - általában kötelezettségei betartásáért.

2.2.3. Az Aláíró felelőssége

a) Az Aláíró felelős:
    - regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért,
    - az adatokban bekövetkezett változások bejelentéséért,
    - az magánkulcsának és aláírás-létrehozó eszközének a szabályzatoknak megfelelő felhasználásáért,
    - magánkulcsának és aktivizáló kódjának biztonságáért,
    - a biztonságos aláírás-létrehozó eszköz biztonságáért,
    - általában kötelezettségei betartásáért.
    - Az Aláírónak büntetőjogi felelőssége áll fenn szolgáltatóval szemben az általa megadott adatok tekintetében.

2.2.4. A Szolgáltató felelőssége a tanúsítványok ellenőrzésével kapcsolatban

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

2.3. Pénzügyi felelősség

a) A Szolgáltató pénzügyi felelőssége, valamint a megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében a jogszabályi előírásoknak megfelelő bankgaranciával rendelkezik.
b) A Szolgáltató ezen felül, a megbízhatóság biztosítása érdekében a jogszabályi előírásoknak megfelelő felelősségbiztosítással is rendelkezik.

2.3.1. A Szolgáltatóval szembeni kártérítés

a) Az Aláíró, az Aláíró szervezete, az Előfizető és 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

b) 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 Szolgáltató tevékenységét a következő jogszabályok szabályozzák:

2001. évi XXXV. törvény az elektronikus aláírásról

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

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

9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

45/2005 (III. 11) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

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

1959. évi IV. törvény a Polgári Törvénykönyvről

2.4.2. Érvénytelenség, fennmaradás, megszűnés és értesítések

Érvénytelenség

a) Amennyiben jelen hitelesítési rend valamely pontja érvénytelen lenne, az a hitelesítési rend egészének és más pontjainak érvényességét nem érinti.

Fennmaradás

b) Jelen hitelesítési rend 2. fejezete érvényben marad a hitelesítési rend hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, amelyet a Szolgáltató jelen hitelesítési rend hatálya alatt bocsátott ki.

Megszűnés

c) Jelen hitelesítési rend a Közösség valamennyi kötelezettségét, felelősségét és jogát tartalmazza vagy meghivatkozza. A hitelesítési rend 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

d) Az Aláíró, az Előfizető és az Aláíró Szervezete jognyilatkozatot a Szolgáltató felé kizárólag írásban, aláírt módon tehetik meg. Szervezet képviseletében való aláírás csak a képviseleti jogosultság igazolásával együtt érvényes.

e) A Szolgáltató ügyfeleit a honlapján történő közzététel útján vagy elektronikus levélben tájékoztathatja.

2.4.3. Vitás kérdések megoldására vonatkozó eljárások

a) A Szolgáltató szabályzatokkal és eljárásokkal rendelkezik az ügyfeleitől, illetve más felektől származó, az elektronikus bizalmi szolgáltatásokkal és egyéb más ezzel kapcsolatos ügyekre vonatkozó reklamációk és viták megoldására.

2.5. Díjak és eszköz árak

A Szolgáltató szolgáltatásainak díjazására vonatkozó információt a szolgáltatási szabályzatok tartalmazzák.

2.5.1. A hitelesítés szolgáltatásához kapcsolódó díjak és árak

Lásd szolgáltatási szabályzatot illetve a Szolgáltató honlapján található árlistát.

2.5.2. Időbélyegzés és online tanúsítvány állapot szolgáltatási díjak

Lásd szolgáltatási szabályzatot illetve a Szolgáltató honlapján található árlistát.

2.5.3. Visszatérítési elvek

Lásd szolgáltatási szabályzat ot illetve a Szolgáltató honlapján található árlistát.

2.6. Tanúsítványtár és visszavonási nyilvántartás szolgáltatások

2.6.1. A szolgáltatói információ közzététele

Kikötések és feltételek közzététele

A Szolgáltató gondoskodik arról, hogy kikötései és egyéb feltételei az Aláíró, az Aláíró Szervezete, az Előfizető és az érintett felek rendelkezésére álljanak. Különösképpen:

a) A Szolgáltató az Aláíró, Aláíró Szervezete, az Előfizető és az érintett felek rendelkezésére bocsátja a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, köztük az alábbiakat:
   - az alkalmazott hitelesítési rend, beleértve egy egyértelmű nyilatkozat arra vonatkozóan, hogy a hitelesítési rend a nyilvánosság részére kibocsátott tanúsítványokra vonatkozik, és hogy megköveteli-e bármilyen speciális termék,

alkalmazás vagy eszköz használatát a kibocsátandó tanúsítvánnyal összekapcsolt kulcspár alkalmazására;
- a tanúsítványok használatára vonatkozó bárminemű korlátozás;
- a tanúsítvány ellenőrzésének mikéntjére vonatkozó információ, beleértve a tanúsítvány visszavonási állapot ellenőrzésére vonatkozó követelményeket, oly módon, hogy az érintett fél "ésszerű módon hagyatkozhasson" a tanúsítványra (lásd 2.1.4);
- a felelősség vállalásra vonatkozó bármilyen korlátozást, beleértve azokat az okokat/használatokat, melyek esetén a Szolgáltató elfogadja, illetve visszautasítja a felelősség vállalását (lásd 2.2);
- az az időtartam, amíg a regisztrációs információt (lásd 3.1) megőrzik;
- az az időtartam, amíg a Szolgáltató eseménynaplóját (lásd 4.5) megőrzik;
- reklamációkra és viták rendezésére vonatkozó eljárások (lásd 2.4.3);
- az alkalmazandó jogi rendszer (lásd 2.4.1); és
- az, hogy a Szolgáltatónak az adott hitelesítési rendnek való megfelelősége értékelésre került-e, s hogy ez milyen tanúsító rendszeren keresztül történt (lásd 2.7).

b) A Szolgáltató elérhetővé teszi a fenti a) pontban meghatározott információt web oldalain keresztül, közérthetően megfogalmazva, elektronikusan továbbítható formában.

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 magánkulcsának kompromittálódása.

Tanúsítványok nyilvánosságra hozatala

A Szolgáltató gondoskodik arról, hogy a tanúsítványok szükség esetén az Aláíró, Aláíró Szervezete, az Előfizető és érintett felek rendelkezésre álljanak. Részletesebben:

c) az előállítás után a teljes és pontos tanúsítvány rendelkezésre áll azon Aláíró számára, akinek a tanúsítvány kibocsátásra került;
d) a tanúsítványok csak azokban az esetekben érhetők el más számára, ha az Aláíró hozzájárult ehhez;
e) a Szolgáltató az érintett felek rendelkezésére bocsátja a tanúsítvány használatával kapcsolatos kikötéseket és feltételeket;
f) egy adott tanúsítvánnyal kapcsolatban a vonatkozó kikötések és feltételek könnyen azonosíthatók.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala

A Szolgáltató gondoskodik arról, hogy hiteles és érvényes tanúsítvány visszavonási kérelmek esetén a tanúsítványok időben visszavonásra, s ezen információ nyilvánosságra kerüljön. Részletesebben:

g) a Szolgáltató szolgáltatási szabályzatában dokumentálja a tanúsítványok visszavonásának eljárásait, beleértve az alábbiakat:
   - a visszavonási állapot információk nyilvánosságra hozatalánál használt mechanizmusok,
   - a legnagyobb késedelem a visszavonási kérelem fogadása, és az összes érintett fél rendelkezésére álló információk állapotának megváltozása között;
h) tájékoztatja a visszavont, illetve felfüggesztett tanúsítványhoz tartozó Aláírót (ahol ez alkalmazható, az Aláíró Szervezetét is) tanúsítványa állapotának megváltozásáról;
i) biztosítja, hogy a tanúsítvány visszavonási listákra teljesüljenek az alábbiak:
   - minden egyes visszavonási lista tartalmazza a következő visszavonási lista kibocsátási időpontját,
   - új visszavonási lista közzétehető a következő visszavonási lista kibocsátására megadott időpont előtt is,
   - a visszavonási listát a hitelesítő szervezet a Szolgáltató nevében elektronikusan aláírja;

2.6.2. A közzététel gyakorisága

Tanúsítványok nyilvánosságra hozatalának gyakorisága

A Szolgáltatási Szabályzat tartalmazza.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

A Szolgáltatási Szabályzat tartalmazza.

2.6.3. Hozzáférés-ellenőrzések

a) A Szolgáltató a nyilvánosságnak bocsát ki tanúsítványt, ezért a tanúsítványok használatára vonatkozó kikötések és feltételek nyilvánosak, szabványos felületen bárki által elérhetők. A tanúsítványok csak abban az esetben érhetőek el nyilvánosan, ha az Aláíró ehhez hozzájárult.
b) A visszavonásra vonatkozó kérelmeket hitelesíteni kell, a Szolgáltató feldolgozás előtt ellenőrzi, hogy hiteles forrásból származnak-e. Az ilyen jellegű kérelmeket meg kell erősíteni;
c) A Szolgáltató a nyilvánosságnak bocsát ki tanúsítványt, ezért a visszavonási állapotokat tartalmazó tanúsítvány visszavonási listák nyilvánosak, szabványos felületen bárki által elérhetők.

2.6.4. A tanúsítványtár és a visszavonási nyilvántartás

a) A Szolgáltató a tanúsítványokat, a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, valamint a tanúsítvány visszavonási listákat címtárán keresztül teszi hozzáférhetővé.
b) A tanúsítványtár és a visszavonási nyilvántartás elérhetőségét, valamint az általuk biztosított szabványos felületeket és támogatott lekérdezési műveleteket a Szolgáltatási Szabályzat határozza meg.

2.7. A megfelelőség vizsgálata

a) A Szolgáltatót fokozott biztonságú szolgáltatóként 2002. május 30-án a Hírközlési Felügyelet nyilvántartásba vette. A Szolgáltató 2005. május 15-től minősített szolgáltatóként is szerepel a Nemzeti Hírközlési Hatóság nyilvántartásában.
b) A Nemzeti Hírközlési Hatóság a jelen dokumentumban megnevezett álnevet kizáró és álneves hitelesítési rendeket nyilvántartásába vette.
c) A Szolgáltató olyan elektronikus aláírási termékeket használ „elektronikus aláírás hitelesítés-szolgáltatás” szolgáltatásához (kulcspárok előállításához, a kibocsátott tanúsítványok és tanúsítvány visszavonási listák aláírásához, valamint az ehhez szükséges magánkulcsok tárolásához), mely szerepel a Nemzeti Hírközlési Hatóság „tanúsított elektronikus aláírási termékek” listáján, vagy más EU tagállamban hasonló természetű tanúsításon estek át.
d) A Szolgáltató az „aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése” szolgáltatásához olyan biztonságos aláírás-létrehozó eszközt használ fel, mely szerepel a Nemzeti Hírközlési Hatóság „tanúsított elektronikus aláírási termékek” listáján.

2.7.1. A megfelelőség-vizsgálat gyakorisága

a) A minősített szolgáltatókra vonatkozó követelményeknek, valamint a hitelesítési rendnek való megfelelőség rendszeres felülvizsgálata érdekében a Nemzeti Hírközlési Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart Szolgáltatónál.
b) A Szolgáltató által felhasznált elektronikus aláírási termékek megfelelőség vizsgálatának gyakoriságát, illetve egyéb más megfelelőségi vizsgálatok gyakoriságát a Szolgáltatási Szabályzat határozza meg.

2.7.2. Az átvizsgáló szervezet megnevezése és jellemzői

a) A minősített szolgáltatókra vonatkozó követelményeknek, valamint a jelen hitelesítési rendnek való megfelelőség vizsgálatát a Nemzeti Hírközlési Hatóság végzi.
b) A Szolgáltató által felhasznált elektronikus aláírási termékek megfelelőség vizsgálatát, illetve tanúsítását végző szervezeteket, illetve az egyéb megfelelőségi vizsgálatokat végző szervezeteket a szolgáltatási szabályzat nevezi meg.

2.7.3. Az átvizsgáló szervezet és a vizsgált fél kapcsolata

a) A Nemzeti Hírközlési Hatóság felügyeleti eljárásában résztvevő szakértők a Szolgáltatótól függetlenek, tevékenységüket befolyástól mentesen végzik.

2.7.4. A vizsgálat által érintett területek

a) Az elektronikus aláírással kapcsolatos szolgáltatásokra vonatkozó hatósági eljárás az [1] törvény és a [3] rendelet előírásainak, valamint a Szolgáltató hitelesítési rendjének és saját szabályzatainak (köztük Szolgáltatási Szabályzatának) való megfelelőség vizsgálatára irányul.

2.7.5. Hiányosságok esetén végrehajtandó tevékenységek

a) A hatósági felügyeleti eljárás, vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató késlekedés nélkül megszünteti a vizsgálatot végző Nemzeti Hírközlési Hatóságtól kapott információk alapján.

2.7.6. Az eredményekről való tájékoztatás

A Szolgáltatási Szabályzat tartalmazza.

2.8. Bizalmasság

A Szolgáltató gondoskodik a jogszabályoknak való megfelelésről. Ennek keretén belül:

a) a fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól. A jogszabályoknak való megfelelés, valamint az alapvető üzleti tevékenységek támogatása érdekében szükség van bizonyos bejegyzések biztonságos megőrzésére is. (lásd 4.5 és 4.6);
b) gondoskodik az adatvédelmi törvényeknek való megfelelésről;
c) megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen kezelése ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen;
d) nyilvántartásba veszi az Aláíróval és az Előfizetővel aláírt megállapodást, beleértve az alábbiakat:
    - hozzájárulás az alábbi szolgáltatások során felhasznált információ Szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az Aláíró eszközzel való ellátása, esetleges későbbi visszavonás,
    - hozzájárulás a nyilvántartásba vett információ harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén, az erre az esetre vonatkozó szabályzat megkövetelt feltételei szerint,
    - hogy az Aláíró hozzájárul-e a tanúsítvány közzétételéhez és milyen feltételek mellett;
e) gondoskodik arról, hogy a regisztrációs eljárás során az adatvédelmi jogszabályok követelményeit figyelembe vegyék;
f) ellenőrzési politikája csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához;
g) gondoskodik az Aláíróra vonatkozó információ bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja;
h) védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az Aláíróval, az Előfizetővel illetve az Aláíró Szervezetével folytatott, illetve a hitelesítő szervezet – regisztráló szervezet – tanúsítványtár és visszavonási nyilvántartás rendszerkomponensek közötti adatcsere során is.

2.8.1. Bizalmasan kezelendő információ-típusok

a) A Szolgáltató bizalmas információként kezeli az Aláíró, az Előfizető és az Aláíró Szervezete 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) Amennyiben az Aláíró ehhez hozzájárul, a Szolgáltató nem bizalmas információként kezeli mindazon adatokat, melyet a tanúsítványba belefoglal. Ezek az adatok a tanúsítványigénylő űrlapon egyértelműen jelölve vannak.

2.8.3. Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése

a) A Szolgáltató az általa kibocsátott tanúsítványok visszavonását és felfüggesztését tanúsítvány-visszavonási listákban közzé teszi, a szolgáltatási szabályzatban meghatározott tartalommal, jellemzőkkel, illetve az ezekben általa támogatott keresési lehetőségekkel.

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 értesíti az érintett Aláírót, az Előfizetőt, Aláíró Szervezetét, illetve érintett feleket.

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) Az Aláíró és az Aláíró Szervezete hozzáférhet a rá vonatkozó regisztrációs és egyéb információhoz.

2.8.7. Egyéb információ-közzétételt eredményező körülmények

a) A Szolgáltató tevékenysége befejezésekor nyilvántartásait, a bizalmas felhasználói adatokkal együtt átadja más – szintén minősített – 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 és teljes jogú használója a Aláíró.
b) A Szolgáltató a tanúsítványt a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja, s egyéb módon 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 megkülönböztető név használatára a megnevezett Aláíró jogosult.
f) Az Aláíró, az Előfizető vagy az Aláíró Szervezete egyedi azonosítójában szereplő bármilyen védjegy, szervezeti- és személy név, egyéb adat az Aláíró, az Előfizető illetve az Aláíró Szervezete tulajdonát képezheti.
g) A Szolgáltató szabályzatai, szerződéses feltételei a Szolgáltató tulajdonát képezik.
h) A tanúsítványban szereplő hitelesítő azonosító a Szolgáltató tulajdonát képezi.

3. Azonosítás és hitelesítés

3.1. Regisztráció

A Szolgáltató a regisztráció során:
a) gondoskodik arról, hogy az Aláíró tanúsítvány kérelmei pontosak, hitelesek és teljesek legyenek;

b) megfelelő, hiteles források igazolásán alapulva megvizsgálja az Aláírók és az Aláíró Szervezete azonosságára vonatkozó bizonyítékokat, valamint nevük és a hozzá kapcsolódó adatok pontosságát.

3.1.1. Név típusok

A név típusok leírását a Szolgáltatási Szabályzat tartalmazza.

A jelen dokumentum által definiált két hitelesítési rend e ponton eltér egymástól:

- Az álnevet kizáró hitelesítési rend (OID: 1.3.6.1.4.1.21528.2.1.1.2) szerint kibocsátott tanúsítványokban a Szolgáltató mindig az aláíró igazi nevét tünteti fel. E hitelesítési rend szerint a Szolgáltató soha nem bocsát ki álneves tanúsítvány. E hitelesítési rendet a Szolgáltató külön hitelesítési egységhez rendeli, e hitelesítési egység sem bocsát ki soha álneves tanúsítványt.
- Az álneves hitelesítési rend (OID: 1.3.6.1.4.1.21528.2.1.1.12) szerint kibocsátott tanúsítványokban a Szolgáltató kizárólag álnevet tüntet fel. E hitelesítési rendet a Szolgáltató külön hitelesítési egységhez rendeli, e hitelesítési egység kizárólag álneves tanúsítványokat bocsát ki.

Az álnév feltüntetésének helyét és a fenti két hitelesítő egység megnevezését a Szolgáltatási Szabályzat 3.1.1. fejezete tartalmazza.

3.1.2. Igény a nevek értelmezhetőségére

A Szolgáltatási Szabályzat tartalmazza.

3.1.3. Különböző elnevezési formák értelmezési szabályai

A Szolgáltatási Szabályzat tartalmazza.

3.1.4. A nevek egyedisége

a) A Szolgáltató gondoskodik arról, hogy teljes élettartama alatt a tanúsítványban általa használt megkülönböztetett nevet sohasem fogja egy másik egyedhez rendelni.

3.1.5. Eljárások a nevekre vonatkozó vitás kérdések megoldására

A Szolgáltatási Szabályzat tartalmazza.

3.1.6. Márkanevek elismerése, hitelesítése és szerepe

A Szolgáltatási Szabályzat tartalmazza.

3.1.7. A magánkulcs birtoklása

a) Mivel ezen hitelesítési rend esetén a Szolgáltató maga generálja az Aláíró számára a nyilvános kulcsból és magánkulcsból álló kulcspárt, az Aláírónak nem kell bizonyítania a magánkulcs birtoklását.

3.1.8. A szervezeti azonosság hitelesítése

A Szolgáltatási Szabályzat tartalmazza.

3.1.9. A személyazonosság hitelesítése

A Szolgáltatási Szabályzat tartalmazza.

3.2. Tanúsítványcsere érvényes tanúsítvány esetén

A Szolgáltatási Szabályzat írja le ennek eljárásrendjét.

3.3. Tanúsítványcsere érvénytelen tanúsítvány esetén

A Szolgáltató a tanúsítványcsere elektronikus üzenetváltáson alapuló, személyes megjelenést nem igénylő megvalósítását nem teszi lehetővé.

3.4. Visszavonási kérelem

a) A Szolgáltató lehetővé teszi érvényes tanúsítvány visszavonásának és felfüggesztésének elektronikus üzenetváltáson alapuló, személyes megjelenést nem igénylő megvalósítását a szolgáltatási szabályzatban meghatározott módon és feltételekkel.
b) A Szolgáltató gondoskodik arról, hogy az a) pontban meghatározott, egy már korábban nála nyilvántartásba vett Aláírótól származó, tanúsítvány visszavonási vagy felfüggesztési kérelem teljes, pontos és kellőképpen hiteles legyen. Ennek érdekében a Szolgáltató szolgáltatási szabályzatának részeként (a 4.4 alfejezetben) dokumentálja a tanúsítványok visszavonásának, felfüggesztésének eljárásait, beleértve az alábbiakat:
    - ki adhat be visszavonási kérelmeket,
    - hogyan lehet ezeket beadni,
    - mik a visszavonási kérelmek megerősítésére vonatkozó esetleges követelmények,
    - mi a felfüggesztett állapot maximális időtartama.

4. Működésre vonatkozó követelmények

4.1. Tanúsítvány-kérelem

a) A Szolgáltató azt megelőzően, hogy egy Aláíróval szerződéses kapcsolatot létesít, tájékoztatja az Aláírót a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről a 2.6.1. alfejezetben megadottak szerint.
b) Az Aláírónak meg kell adnia egy fizikai címet vagy más jellemzőket, amelyek leírják, hogy az Aláíróval hogyan lehet felvenni a kapcsolatot.
c) A Szolgáltató nyilvántartásba vesz minden, az Aláíró azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat.
d) A Szolgáltató nyilvántartásba veszi az Aláíróval aláírt megállapodást, beleértve az alábbiakat:
    - az Aláíró kötelezettségeivel (lásd 2.1.3) történő egyetértést,
    - az Aláíró beleegyezését egy biztonságos aláírás-létrehozó eszköz használatára vonatkozóan,
    - hozzájárulás az alábbi szolgáltatások során felhasznált információ Szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az Aláíró eszközzel való ellátása (beleértve az Aláíróhoz történő továbbítást is), bármely ezt követő visszavonás, illetve ezen információ harmadik félhez történő továbbítása (a Szolgáltató szolgáltatásainak leállítása esetén használatos szabályzat megkövetelt feltételei szerint),
    - hogy az Aláíró hozzájárul-e a tanúsítvány közzétételéhez és milyen feltételek mellett,
    - annak megerősítését, hogy a tanúsítványban szereplő információ helyes.
    - az Aláíró Szervezete által kiállított igazolást, amelyben az Aláíró Szervezete igazolja, hogy az Aláíró jogosult az Aláíró Szervezetét tartalmazó tanúsítványban szerepelni
    - az Aláíró Szervezete vagy harmadik fél által kiállított igazolást, amely igazolja, hogy az Aláíró valóban rendelkezik a tanúsítványban megjelölt szereppel)
e) A Szolgáltató megőrzi a d)-e) pontokban megnevezett nyilvántartásokat 10 évig, illetőleg a velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig.

4.2. Tanúsítvány-kibocsátás

A Szolgáltató biztonságosan fenntartja az általa kibocsátott tanúsítványok hitelességét. Különösképpen:
a) Előállítása után a teljes és pontos tanúsítvány rendelkezésére áll azon Aláíró számára, akinek a tanúsítvány kibocsátásra került.
b) A tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a megfelelő regisztrációhoz, illetve a különböző tanúsítványcsere eljárásokhoz.
c) Az Aláíró számára a Szolgáltató által megvalósított kulcselőállításra:
    - a tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a Szolgáltató általi kulcspár előállításhoz;
    - az Aláíró magánkulcsát tartalmazó biztonságos aláírás-létrehozó eszközt biztonságosan továbbítják az Aláíróhoz.
d) A Szolgáltató csak akkor bocsát ki új tanúsítványt az Aláíró korábbiakban tanúsított nyilvános kulcsának felhasználásával (tanúsítvány frissítés), ha annak kriptográfiai biztonsága még megfelelő az új tanúsítvány tervezett élettartamára, és nincsenek arra utaló jelek, hogy az Aláíró

magánkulcsa kompromittálódott. A Szolgáltató legfeljebb egy alkalommal újít meg egy tanúsítványt ily módon.

4.3. Tanúsítvány-elfogadás

A Szolgáltatási Szabályzat tartalmazza.

4.4. Tanúsítvány-felfüggesztés és –visszavonás

a) A Szolgáltató gondoskodik arról, hogy hiteles és érvényes tanúsítvány visszavonási, illetve felfüggesztési kérelmek esetén a tanúsítványok haladéktalanul visszavonásra kerüljenek, s erről az Aláíró, az Előfizető, illetve az Aláíró Szervezete és az érintett felek hiteles és megbízható információt kapjanak.

4.4.1. A visszavonás körülményei

a) A Szolgáltató szolgáltatási szabályzata határozza meg, hogy milyen körülmények között lehet, illetve kell visszavonási kérelmet benyújtani.

4.4.2. Kik kérelmezhetik a visszavonást

a) A Szolgáltató szolgáltatási szabályzata határozza meg, hogy ki adhat be visszavonási kérelmet.

4.4.3. Visszavonási kérelemre vonatkozó eljárás

a) A Szolgáltató szolgáltatási szabályzata dokumentálja a tanúsítványok visszavonásának eljárásait, beleértve az alábbiakat:
   - hogyan lehet ezeket beadni,
   - a visszavonási kérelmek megerősítésére vonatkozó esetleges követelmények.

b) A Szolgáltató a tanúsítványok visszavonásra vonatkozó kérelmeket fogadásuk után haladéktalanul feldolgozza.

c) A visszavonásra vonatkozó kérelmeket hitelesíteni kell, a Szolgáltató ellenőrzi, hogy hiteles forrásból származnak-e. Az ilyen kérelmeket meg kell erősíteni azokban az esetekben, amelyekben ezt a Szolgáltató szolgáltatási szabályzata megköveteli.

d) A Szolgáltató tájékoztatja a visszavont tanúsítványhoz tartozó Aláírót, és ahol ez alkalmazható az Aláíró Szervezetét, a tanúsítvány állapotának megváltozásáról.

e) A Szolgáltató nem állítja vissza érvényesre a már egyszer véglegesen visszavonásra (azaz nem felfüggesztésre) került tanúsítványokat.

4.4.4. Visszavonási kérelemre vonatkozó türelmi idő

a) A legnagyobb késedelem a visszavonási kérelem fogadása, illetve az összes érintett fél rendelkezésére álló információ visszavonási állapotának megváltoztatása között: lásd a szolgáltatási szabályzatot.

4.4.5. A felfüggesztés körülményei

a) A Szolgáltató megerősítést igénylő visszavonási kérelem esetén a tanúsítvány visszavonási állapotát „felfüggesztett”-re állítja, amíg a visszavonás megerősítésre nem kerül.
b) A Szolgáltató szolgáltatási szabályzata határozza meg, hogy a tanúsítványok milyen okból kifolyólag függeszthetők fel.

4.4.6. Kik kérelmezhetik a felfüggesztést

a) A Szolgáltató szolgáltatási szabályzata határozza meg, hogy kik kérelmezhetik a tanúsítványok felfüggesztését.

4.4.7. Felfüggesztési kérelemre vonatkozó eljárás

a) A Szolgáltató szolgáltatási szabályzata határozza meg a felfüggesztési kérelemre vonatkozó pontos eljárást, beleértve azt is, hogyan lehet ezen kérelmeket beadni.
b) A Szolgáltató a tanúsítványok felfüggesztésére vonatkozó kérelmeket fogadásuk után haladéktalanul feldolgozza.
c) A Szolgáltató tájékoztatja a felfüggesztett tanúsítványhoz tartozó Aláírót, és ahol ez alkalmazható az Aláíró Szervezetét a tanúsítvány állapotának megváltozásáról.

4.4.8. A felfüggesztés időtartamára vonatkozó korlátozások

a) A Szolgáltató gondoskodik arról, hogy egy tanúsítvány ne legyen hosszabb ideig felfüggesztve, mint amennyi állapotának megerősítéséhez szükséges, de legfeljebb a szolgáltatási szabályzatban megjelölt időtartamig.

4.4.9. A tanúsítvány visszavonási lista kibocsátási gyakorisága

a) A Szolgáltató a visszavonási állapot információt tanúsítvány visszavonási listák egy adattáron keresztül történő nyilvánosságra hozatalán keresztül nyújtja.
b) A Szolgáltató a tanúsítvány visszavonási listákat a szolgáltatási szabályzatban meghatározott gyakorisággal közzé teszi.

4.4.10. Tanúsítvány visszavonási lista ellenőrzési követelményei

a) A Szolgáltató megvédi a tanúsítvány visszavonási lista sértetlenségét és hitelességét.

4.4.11. Valós idejű visszavonási állapot ellenőrzés elérhetősége

A Szolgáltató valós idejű visszavonási állapot szolgáltatásának elérhetőségét a szolgáltatási szabályzat határozza meg.

4.4.12. Valós idejű visszavonás ellenőrzési követelmények

A Szolgáltató valós idejű visszavonási állapot szolgáltatására vonatkozó követelményeket a szolgáltatási szabályzat tartalmazza.

4.4.13. A visszavonási hirdetmények egyéb elérhető formái

A visszavonási hirdetmények csak a Szolgáltató visszavonási nyilvántartásán (visszavonási listán és valós idejű visszavonási állapot szolgáltatáson) keresztül érhetők el. (Nincsenek egyéb elérhető formák.)

4.4.14. A visszavonási hirdetmények egyéb elérhető formáinak ellenőrzési követelményei

Mivel a visszavonási hirdetményeknek nincs egyéb elérhető formája, nincsenek erre vonatkozó követelmények.

4.4.15. Kulcs kompromittálódás esetére vonatkozó speciális követelmények

a) A tanúsítványhoz tartozó Aláíró kötelessége a kompromittálódott magánkulcs által esetlegesen érintett felek értesítése, és minden intézkedés megtétele az esetleges károk megelőzése és enyhítése érdekében.

4.5. A biztonsági naplózás folyamatai

a) A Szolgáltató szolgáltatási szabályzata határozza meg (a 4.5.1–4.5.8 pontok szempontrendszere alapján), hogy a biztonságos környezet fenntartása érdekében a Szolgáltató milyen eseménynaplózó és ellenőrző rendszereket valósít meg.

A jelen dokumentumban leírt hitelesítési rendek csak a tanúsítványokra vonatkozó adatok (regisztrációs információ, a Szolgáltató kulcsgondozási és tanúsítványgondozási eseményeire vonatkozó fontosabb információ) naplózási folyamatának alábbi általános jellegzetességeit adja meg:

b) A Szolgáltató a környezetére, kulcs- és tanúsítvány gondozására vonatkozó események pontos időpontját is rögzíti.
c) A Szolgáltató biztosítja személyzete felelősségre vonhatóságát tevékenységéért, többek között az eseménynapló megőrzésén és védelmén keresztül (lásd 4.5.1, 4.5.4, 4.5.5).

4.5.1. A tárolt események típusai

A Szolgáltató általános tevékenységével kapcsolatosan:

a) A naplózandó speciális eseményeket és adatokat a Szolgáltató szolgáltatási szabályzatában dokumentálja.

A regisztrációval kapcsolatosan:

b) A Szolgáltató gondoskodik arról, hogy naplózásra kerüljön valamennyi regisztrációval kapcsolatos esemény, beleértve a tanúsítványcserére (tanúsítványfrissítésre, tanúsítvány aktualizálására és kulcscserére) vonatkozó kérelmeket is.

A tanúsítvány előállítással kapcsolatosan:

c) A Szolgáltató naplózza a szolgáltatói kulcsok életciklusával kapcsolatos összes eseményt.
d) A Szolgáltató naplózza a tanúsítványok életciklusával kapcsolatos összes eseményt.

Az Aláíró eszközzel való ellátásával kapcsolatosan:

e) A Szolgáltató naplóz minden általa gondozott kulcs életciklusával kapcsolatos eseményt.
f) A Szolgáltató naplózza a biztonságos aláírás-létrehozó eszközök készítésével kapcsolatos valamennyi eseményt.

A visszavonás kezeléssel kapcsolatosan:

g) A Szolgáltató gondoskodik a visszavonással kapcsolatos összes kérés, valamint az ezek eredményét képező összes tevékenység naplózásáról.

4.5.2. A napló állomány feldolgozásának gyakorisága

a) A napló állományok feldolgozásának gyakoriságát a Szolgáltató szolgáltatási szabályzata határozza meg.

4.5.3. A napló-állomány megőrzési időtartama

a) A napló állományok megőrzési időtartamát a Szolgáltató szolgáltatási szabályzata határozza meg.

4.5.4. A napló állomány védelme

a) A Szolgáltató az eseményeket oly módon naplózza, ami nem törölhető, illetve nem tehető tönkre azon időtartam alatt, amíg azokat meg kell őrizni.
b) A Szolgáltató biztosítja a tanúsítványok és kulcsok gondozására vonatkozó napló rekordok bizalmasságát és sértetlenségét.

4.5.5. A napló állomány mentési folyamatai

a) A napló állomány mentési folyamatait a Szolgáltató szolgáltatási szabályzata határozza meg.

4.5.6. A napló gyűjtési rendszere

a) A napló gyűjtési rendszerét a Szolgáltató szolgáltatási szabályzata határozza meg.

4.5.7. Az eseményeket kiváltó aláírók értesítése

a) A Szolgáltató nem értesíti a naplóbejegyzéseket kiváltó Aláírót, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába.

4.5.8. Sebezhetőség felmérése

a) A sebezhetőség felmérésére végzett tevékenységeket a Szolgáltató szolgáltatási szabályzata határozza meg.

4.6. Adatok archiválása

a) A Szolgáltató gondoskodik arról, hogy a tanúsítványra vonatkozó minden lényeges információ megfelelő ideig rögzítésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

4.6.1. A tárolt események típusai

a) A Szolgáltató gondoskodik arról, hogy rögzítésre kerüljön az összes regisztrációs információ, beleértve az alábbiakat is:
    - az igénylő által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa,
    - az azonosító dokumentumok egyedi azonosító adatai (például az igénylő jogosítvány száma),

- az igénylő és azonosító dokumentumok (beleértve az Aláíróval kötött aláírt megállapodást (lásd 2.6.1) másolatainak tárolási helyszíne,
- az Aláíróval illetve Előfizetővel kötött megállapodás esetleges egyedi választásai (például a tanúsítvány közzétételéhez történő hozzájárulás),
- a kérelmet elfogadó regisztrációs ügyintéző[57] azonosítója,
- az azonosító dokumentumok ellenőrzéséhez használt módszer, ha ilyen létezik[58],
- a fogadó hitelesítő szervezet és/vagy a küldő regisztráló szervezet neve, amennyiben ez értelmezhető.

b) A tanúsítványokra vonatkozó valamennyi naplóbejegyzés archiválásra kerül (lásd 4.5.1 a.)-g.) pontokat).
c) Azon eseményeket, melyek a fent említett naplóbejegyzéseken túl kerülnek archiválásra (a biztonságos környezet fenntartásának és utólagos ellenőrizhetősége és bizonyíthatósága céljából), a Szolgáltató szolgáltatási szabályzata határozza meg.

4.6.2. Az archívum megőrzési időtartama

a) A Szolgáltató a 4.1. d) és e) pontjában megnevezett nyilvántartásokat megőrzi azon időtartamig, amelyet a Szolgáltató szerződéses feltételei (kikötések és feltételek, lásd 2.6.1 pontot) megjelöltek, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig.
b) A Szolgáltató a tanúsítványokra vonatkozó napló adatokat (lásd 4.5.1.a)-g) pontokat) megőrzi addig az időtartamig, amelyet a Szolgáltató szerződéses feltételei (kikötések és feltételek, lásd 2.6.1 pontot) megjelöltek.
c) A biztonságos környezet fenntartásának utólagos ellenőrizhetősége és bizonyíthatósága érdekében archivált egyéb naplóbejegyzések megőrzési időtartamát a Szolgáltató szolgáltatási szabályzata határozza meg.

4.6.3. Az archívum védelme

a) A Szolgáltató fenntartja a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét.
b) A Szolgáltató a tanúsítványokra vonatkozó naplóadatokat teljes körűen és a bizalmasságot garantáló módon archiválja a szolgáltatási szabályzatban leírt üzleti gyakorlatnak megfelelően.
c) A Szolgáltató a bejegyzéseket megvédi az elveszéstől, tönkretételtől és hamisítástól.
d) A Szolgáltató megfelelő műszaki és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen feldolgozása ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen.

4.6.4. Az archívum mentési folyamatai

a) Az archívum mentési folyamatait a Szolgáltató szolgáltatási szabályzata határozza meg.

4.6.5. A rekordok időbélyegzésére vonatkozó követelmények

a) Az archívum időbélyegzésére vonatkozó követelményeit és gyakorlatát a Szolgáltató szolgáltatási szabályzata határozza meg.

4.6.6. Az archívum gyűjtési rendszere

a) Az archívum gyűjtési rendszerét a Szolgáltató szolgáltatási szabályzata határozza meg.

4.6.7. Archív információ hozzáférését és ellenőrzését végző eljárások

a) A Szolgáltató a tanúsítványokra vonatkozó adatokat rendelkezésre bocsátja, ha arra jogi eljárásokban bizonyíték nyújtása céljából szükség van.
b) Az Aláíró hozzáférhet az Aláíróra vonatkozó regisztrációs és egyéb információhoz.

4.7. Tanúsítványcsere

a) A végfelhasználói tanúsítványok kulcscseréjét a Szolgáltató szolgáltatási szabályzata tárgyalja.

4.8. Helyreállítás rendkívüli üzemi helyzetek esetén

a) A Szolgáltató gondoskodik arról, hogy katasztrófa esetén, beleértve a saját magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, az üzemeltetés amint csak lehetséges helyreálljon.

4.8.1. Sérült számítási erőforrások, szoftverek és/vagy adatok

a) A Szolgáltató üzletmenet-folytonossági terve (illetve katasztrófa utáni helyreállítási terve) a kritikus szoftver/hardver komponensek sérülésével, mint katasztrófa helyzettel foglalkozik. Ilyen esetekben a tervezett eljárásokat életbe lépteti annak érdekében, hogy az üzemeltetés, amint csak lehetséges, helyreálljon.
b) A Szolgáltató minimalizálja a biztonsági események és hibás működések által okozott kárt, eseményjelentés és válaszadás eljárások használatán keresztül.
c) A Szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Ennek érdekében valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.

4.8.2. A szolgáltatói egység nyilvános kulcsának visszavonása

a) Egy szolgáltatói kulcs visszavonása esetén a Szolgáltató az alábbiakat vállalja:
   - a visszavonásról tájékoztatja az összes Aláírót és érintett felet,
   - jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes(ek).
b) A Szolgáltató a szolgáltatói kulcs visszavonását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint a végfelhasználók számára új nyilvános kulcsot biztosít új tanúsítvány kiadásával.

4.8.3. Egy szolgáltatói egység kulcsának kompromittálódása

a) Egy szolgáltatói kulcs kompromittálódása esetén a Szolgáltató az alábbiakat vállalja:
   - a kompromittálódásról tájékoztatja az összes Aláírót és érintett felet,
   - jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes(ek).
   - értesíti a Hatóságot a kulcs kompromittálódásának tényéről.
b) A Szolgáltató a szolgáltatói kulcs kompromittálódását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint a végfelhasználók számára új nyilvános kulcsot biztosít új tanúsítvány kiadásával.

4.8.4. Biztonsági képesség természeti vagy más katasztrófát követően

a) Természeti vagy más egyéb katasztrófát követően a Szolgáltató életbe lépteti az üzlet folytonossági terve (illetve katasztrófa utáni helyreállítási terve) által megtervezett eljárásokat annak érdekében, hogy az üzemeltetés helyreálljon a szolgáltatási szabályzatban megjelölt időn belül.
b) Egy katasztrófát követően a Szolgáltató (ha ez ésszerű) lépéseket tesz a katasztrófa ismételt bekövetkezésének megakadályozására.

4.9. A szolgáltatások leállítása

A Szolgáltató gondoskodik a szolgáltatásainak megszüntetéséből/szüneteltetéséből fakadó, az Aláírót, az Előfizetőt, Aláíró Szervezetét és az érintett feleket érintő esetleges zavarok minimalizálásáról. Különösképpen gondoskodik a jogi eljárásokhoz szükséges tanúsítvány nyilvántartások fenntartásáról. Ennek érdekében:

A Szolgáltató általános tevékenységével kapcsolatosan:

a) Mielőtt a Szolgáltató leállítja szolgáltatásait, végrehajtja az alábbi eljárásokat:
   - a leállítást megelőzően 60 nappal értesíti a Hatóságot a leállításról,
   - tájékoztatja az összes Aláírót és érintett felet,
   - megszünteti a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások összes felhatalmazását,
   - megteszi a szükséges lépéseket, hogy a regisztrációs információ (lásd 3.1) és az eseménynapló archívumok (lásd 4.6) fenntartására vonatkozó kötelezettségeket átruházza arra az időtartamra, amelyről az Aláírót, az Előfizetőt, az Aláíró Szervezetét és az érintett feleket tájékoztatta (lásd 2.6),
   - magánkulcsait megsemmisíti, illetve visszavonja a használatból a 6.2.9 alatt meghatározottak szerint.

b) A Szolgáltató szerződést köt a fenti követelmények teljesítésével kapcsolatos költségek fedezésére arra az esetre, ha csődbe menne, vagy más okból kifolyólag nem lenne képes a költségeket saját maga állni.
c) A Szolgáltató szolgáltatási szabályzata tartalmazza a szolgáltatás leállítása esetén alkalmazott konkrét eljárásokat, melyek magukban foglalják az alábbiakat:
- az érintettek értesítését,
- saját kötelezettségeinek más felekre történő átruházását,
- a már kibocsátott, de még le nem járt tanúsítványok visszavonási állapotának a kezelését.

5. Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A biztonsági óvintézkedésekről általában

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

a) A Szolgáltató kockázatelemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározása érdekében.
b) A Szolgáltató felelősséget vállal minden elektronikus aláírással kapcsolatos szolgáltatásért még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki. A Szolgáltató egyértelműen meghatározza a harmadik felek felelősségét, és megfelelő konstrukciók biztosítják azt, hogy a harmadik felek a Szolgáltató által megkövetelt összes ellenőrzés végrehajtására legyenek szorítva. A Szolgáltató felelősséget vállal valamennyi fél fentiekre vonatkozó gyakorlatának nyilvánosságra hozására.
c) A Szolgáltató vezetősége (amely felelős a Szolgáltató informatikai biztonság politikájának meghatározásáért, és e politika által érintett valamennyi alkalmazott részére történő közzétételért) az információ biztonságára vonatkozó útmutatót hagyott jóvá és adott ki.
d) A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetőségének kell jóváhagynia.
e) A Szolgáltató (rendszerbiztonsági szabályzatában) dokumentálta, majd megvalósította és folyamatosan fenntartja a hitelesítési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait.
f) A Szolgáltató gondoskodik az informatika biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez, illetve egységhez lettek kiadva.
g) A Szolgáltató biztonsági műveleteiért a végső felelősség a felső vezetőséget terheli. Ezen biztonsági műveletek közé az alábbiak tartoznak:
    - üzemeltetési eljárások és felelősségek
    - biztonsági rendszerek tervezése és elfogadása
    - káros szoftver elleni védelem
    - erőforrás gazdálkodás
    - hálózat menedzselés
    - a biztonsági napló aktív felügyelete, eseményelemzések és nyomkövetések
    - adathordozó eszköz kezelése és biztonsága
    - adat és szoftver csere

A fenti feladatokat felügyelet mellett végrehajthatja az üzemeltető személyzet is, a megfelelő biztonsági szabályzatban és a szerepkörökkel és felelősségekkel foglalkozó dokumentumokban meghatározottak szerint.

Az értékek osztályozása és kezelése

A Szolgáltató gondoskodik arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek. Különösképpen:

a) A Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit osztályokba sorolja és minősíti, az elvégzett kockázat elemzéssel (lásd 5. a. pontot) összhangban.

5.1. Fizikai óvintézkedések

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

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A Szolgáltató általános tevékenységével kapcsolatosan:

a) A Szolgáltató biztosítja az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.
b) A Szolgáltató óvintézkedéseket valósít meg az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

Tanúsítvány előállítással, Aláíró aláírás-létrehozó eszközzel való ellátásával, visszavonás kezeléssel kapcsolatosan:

c) A Szolgáltató egy egyértelműen meghatározott biztonsági körlet létrehozásával fizikai védelmet biztosít az alábbi szolgáltatások számára:
   - tanúsítvány előállítás,
   - az Aláíró aláírás-létrehozó eszközzel való ellátása,
   - visszavonás kezelés.

   Bármely más szervezettel megosztott rész e körleten kívül esik.
d) A Szolgáltató óvintézkedéseket valósít meg a fizikai és környezetbiztonsági rendszer erőforrások, illetve a működésük támogatására használt berendezések megvédése érdekében. A Szolgáltató
   - tanúsítvány előállítás,
   - az Aláíró aláírás-létrehozó eszközzel való ellátása,
   - visszavonás kezelés szolgáltatásainak fizikai- és környezetbiztonsági programjai foglalkoznak a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelem és tűzbiztonság tényezőivel, a támogató eszközök (ezen belül az áram és klíma berendezések) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, katasztrófa utáni helyreállítással, stb.
e) A Szolgáltató óvintézkedéseket valósít meg annak megakadályozása érdekében, hogy az elektronikus aláírással kapcsolatos szolgáltatáshoz szükséges berendezést, információt, adathordozót vagy szoftvert jogosulatlanul elvigyék a helyszínről.

5.1.2. Fizikai hozzáférés

a) A Szolgáltató
   - tanúsítvány előállítás,
   - az Aláíró aláírás-létrehozó eszközzel való ellátása,
   - visszavonás kezelés

   szolgáltatásokkal kapcsolatos eszközökhöz történő fizikai hozzáférést megfelelően felhatalmazott egyénekre korlátozza.
b) A Szolgáltató a
   - tanúsítvány előállítás,
   - az Aláíró aláírás-létrehozó eszközzel való ellátása,

   szolgáltatásokkal kapcsolatos eszközöket olyan környezetben működteti, amely fizikailag megvédi a szolgáltatásokat attól, hogy a rendszerekhez, illetve adatokhoz történő jogosulatlan hozzáférésen keresztül kompromittálódjanak.

5.1.3. Áramellátás, légkondicionálás

Lásd 5.1.1. d) pontot, illetve a Szolgáltatási Szabályzat 5.1.3 pontját.

5.1.4. Beázás és elárasztás veszélyeztetettsége

Lásd 5.1.1. d) pontot, illetve a Szolgáltatási Szabályzat 5.1.4 pontját.

5.1.5. Tűzmegelőzés és tűzvédelem

Lásd 5.1.1. d) pontot, illetve a Szolgáltatási Szabályzat 5.1.5 pontját.

5.1.6. Adathordozók tárolása

a) A Szolgáltató az adathordozó eszközöket biztonságosan kezeli a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.
b) A Szolgáltató az összes adathordozó eszközt biztonságosan kezeli az adatminősítési rendszer követelményeinek megfelelően (lásd 5. h.).

5.1.7. Selejt kezelése és megsemmisítése

a) A Szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztől biztonságosan válik meg, amennyiben azokra már nincs szükség.

5.1.8. Fizikailag elkülönítetten őrzött mentési példányok

A Szolgáltatási Szabályzat tartalmazza.

5.1.9. Villámvédelem

Lásd 5.1.1. d) pontot, illetve a Szolgáltatási Szabályzatot.

5.2. Eljárásbeli óvintézkedések

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

a) A Szolgáltató személyzete olyan adminisztratív és kezelési eljárásokat és folyamatokat végez, amely szinkronban van a Szolgáltató rendszerbiztonsági szabályzatának eljárásaival (lásd 5. e. pontot).

5.2.1. Bizalmi szerepkörök

a) A Szolgáltató az alábbiakban (lásd b. pont) egyértelműen azonosítja azokat a biztonsági munkaköröket, amelyektől a Szolgáltató működésének biztonsága függ. Ezeket a biztonsági munkaköröket és felelősségeket munka leírásokban dokumentálja.
b) A bizalmi munkakörök közé az alábbi munkakörök tartoznak:
   - A Szolgáltató informatikai rendszerért általánosan felelős vezető
   - Biztonsági tisztviselő: a Szolgáltatás biztonságáért általánosan felelős személy
   - Rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy,
   - Rendszerüzemeltető: a Szolgáltató informatikai rendszerének folyamatos üzemeltetését, mentését és helyreállítását végző személy,
   - Független rendszervizsgáló: a Szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy,
   - Regisztrációs felelős: a végfelhasználói tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy;
c) A bizalmi munkakörök közötti személyi átfedésekre vonatkozó korlátozásokat a Szolgáltató szabályzatai tartalmazzák.
d) A bizalmi munkakörökbe a Szolgáltató biztonságért felelős felső vezetése nevezi ki a munkatársakat.
e) Valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására, előzetesen kidolgozott eljárások kerülnek végrehajtásra.

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

a) A Szolgáltató (ideiglenes és állandó) munkatársainak munkaleírásai (lásd 5.2.1 a.) támogatják a feladatok szétválasztása és a legkisebb meghatalmazás szempontjait. A munkaleírások többek között meghatározzák az egyes feladatokhoz szükséges létszámot is (lásd 5.3 c.).
b) Csak bizalmi munkakört betöltő személyzet (lásd 5.2.1) végezheti legalább kettős ellenőrzés mellett az alábbi funkciókat:
   - a Szolgáltató saját (szolgáltatói) kulcsának előállítása,
   - a Szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktivizálása,
   - a Szolgáltató magán aláíró kulcsának másolása, letárolása, visszaállítása,
   - a Szolgáltató magán aláíró kulcsának megsemmisítése,
   - a hozzáférési jogok megadása, módosítása és visszavonása.

A fenti funkciók végrehajtására felhatalmazott személyzet köre a Szolgáltató szolgáltatási szabályzatának megfelelve, a lehető legkisebbre van korlátozva.

5.2.3. Az egyes munkakörökben elvárt azonosítás és hitelesítés

a) A Szolgáltató személyzete csak sikeres azonosítás és hitelesítés után használhatja a kulcs- és tanúsítvány gondozással kapcsolatos kritikus alkalmazásokat.

5.3. Személyzetre vonatkozó óvintézkedések

A Szolgáltató gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát. Különösképpen:

a) A Szolgáltató kellő számú, az elektronikus aláírással kapcsolatos szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet alkalmaz.
b) A Szolgáltató ügyvezetői, vezető beosztású munkatársainak és bizalmi munkaköröket betöltő munkatársainak (felelős munkatársak) függetlennek kell lenniük minden olyan kereskedelmi, pénzügyi és egyéb hatástól, ami hátrányosan befolyásolhatja a HSZ által nyújtott szolgáltatások iránti bizalmat.
c) A Szolgáltató (ideiglenes és állandó) munkatársai a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaleírásokkal rendelkeznek. A munkaleírások meghatározzák a beosztás érzékenységét a feladatok és a hozzáférési szintek, a háttér-ellenőrzés, az alkalmazott képzettség és tudatosság alapján. Ahol erre szükség van, megkülönböztetik az általános funkciókat és a Szolgáltató specifikus funkciókat. A munkaleírások meghatározzák az egyes feladatokhoz szükséges létszámot is, és tartalmazzák a szakismeretre és a tapasztalatra vonatkozó követelményeket is.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

a) A Szolgáltató olyan személyzetet alkalmaz, amely rendelkezik a kínált szolgáltatáshoz szükséges szakértői tudással, tapasztalattal és minősítésekkel.
b) A Szolgáltató kellő számú, a hitelesítési szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet alkalmaz.
c) A vezető személyzet tapasztalattal rendelkezik az elektronikus aláírási technológia terén, ismeri a biztonsági felelősséggel tartozó munkatársakra vonatkozó biztonsági eljárásokat, valamint gyakorlattal rendelkezik az informatika biztonság és a kockázat elemzés területein.

5.3.2. Biztonsági háttér ellenőrzésekre vonatkozó eljárások

a) A Szolgáltató nem nevez ki bizalmi munkakörbe, illetve a vezetőségbe olyan személyt, aki bűncselekményért, illetve más olyan vétségért el lett ítélve, amely beosztást illető alkalmasságát befolyásolja. A munkatársak nem férhetnek biztonsági funkciókhoz a szükséges, személyükre és alkalmasságukra vonatkozó ellenőrzések végrehajtása előtt.

5.3.3. Kiképzési követelmények

a) A Szolgáltató személyzete rendelkezik a kínált szolgáltatásokhoz szükséges szakértői tudással, tapasztalattal és minősítésekkel.

5.3.4. Továbbképzési gyakoriságok és követelmények

A Szolgáltatási Szabályzat előírásai szerint.

5.3.5. Munkabeosztás körforgásának gyakorisága és sorrendje

A Szolgáltatási Szabályzat előírásai szerint.

5.3.6. A felhatalmazás nélküli tevékenységek büntető következményei

A Szolgáltatási Szabályzat tartalmazza.

5.3.7. A szerződéses alkalmazottakra vonatkozó követelmények

A Szolgáltatási Szabályzat tartalmazza.

5.3.8. A személyzet számára biztosított dokumentációk

a) A személyzet számára biztosítandó dokumentáció tartalmazza az 5. e. pontban említett rendszerbiztonsági szabályzatot.

6. Műszaki biztonsági óvintézkedések

A Szolgáltató módosítás ellen védett, megbízható rendszereket és termékeket használ.

6.1. Kulcspár előállítás és telepítés

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

6.1.1. Kulcspár előállítás

A Szolgáltató saját kulcspár előállítása:

a) A Szolgáltatónál történő kulcselőállítást fizikailag védett környezetben (lásd 5.1), bizalmi munkakört betöltő személyzet (lásd 5.2.1) végzi, legalább kettős ellenőrzés mellett. A kulcselőállítás funkció végrehajtására felhatalmazott személyzet körét a Szolgáltató szolgáltatási szabályzatának még megfelelve, a lehető legkisebbre korlátozza.

b) A Szolgáltató a kulcselőállítást olyan biztonságos kriptográfiai modulban hajtja végre, amely tanúsítvánnyal igazoltan megfelel az alábbi követelményeknek:
   - a modulnak garantálnia kell a kulcsok bizalmasságát és sértetlenségét azok teljes életciklusa során,
   - A modulnak képesnek kell lennie felhasználói azonosítására és hitelesítésére,
   - A modulnak a felhasználó és annak szerepköre alapján azokra a szolgáltatásokra kell korlátoznia a hozzáférést, amelyek az adott felhasználó adott szerepköréhez vannak rendelve,
   - A modulnak képesnek kell lennie egy teszt sorozat lefuttatására, mely ellenőrzi működése helyességét, és hiba észlelése esetén egy biztonságos állapotba kell lépnie,
   - A modulnak észlelnie kell a fizikai módosítási kísérleteket, s ilyenkor egy biztonságos állapotba kell lépnie,
   - A modulnak naplóbejegyzéseket kell tudni készíteni minden biztonság-kritikus változtatásról,
   - A modul opcionálisan támogathatja a kulcsok mentését és visszaállítását, de a mentési adatok bizalmasságát és sértetlenségét meg kell védenie, s legalább kettős ellenőrzést kell megkövetelnie mind a mentés, mind a visszaállítás műveleténél.

   s amely szerepel a Nemzeti Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között, vagy más EU tagállamban hasonló szintű tanúsításon ment keresztül. A tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelmény-rendszer szerint, azzal egyenértékű értékeli szinten kell elvégezni.

c) A Szolgáltató a kulcs előállítását olyan algoritmussal valósítja meg, melyet jogszabály ismer el erre a célra alkalmasnak.

A Szolgáltató által más felek számára előállított kulcspár előállítás:

d) A Szolgáltató által saját szervezeti egységei /pl. tanúsítványtár, regisztrációs szervezetek/ számára előállított kulcsokat biztonságos módon, olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak

e) A Szolgáltató által saját szervezeti egységei /pl. tanúsítványtár, regisztrációs szervezetek/ számára előállított kulcsokat biztonságos módon, olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak.

f) A biztonságos aláírás-létrehozó eszköz elkészítését (logikai és fizikai megszemélyesítését) a Szolgáltató ellenőrzi.

6.1.2. Magánkulcs eljuttatása a tulajdonoshoz

Amikor a Szolgáltató kulcsokat generál más felek számára:

a) az általa más felek számára előállított kulcsokat a címzett félhez történő továbbításig biztonságos módon tárolja;

b) az általa más felek számára előállított magánkulcsot a címzett félhez olyan módon továbbítja, hogy a magánkulcs titkossága ne sérüljön;

c) a szállítást követően csak a címzett férhet hozzá saját magánkulcsához;

d) a Szolgáltató biztonságosan ellenőrzi a biztonságos aláírás-létrehozó eszköz elkészítését;

e) a Szolgáltató a biztonságos aláírás-létrehozó eszközt biztonságosan tárolja és osztja szét;

f) A Szolgáltató biztonságosan ellenőrzi a biztonságos aláírás-létrehozó eszköz kiiktatását és újraaktivizálását;

g) A Szolgáltató a biztonságos aláírás-létrehozó eszköz aktivizálási adatait (PIN kód) biztonságosan készíti el és az aláírás-létrehozó modultól elkülönítve osztja szét.

6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

a) A Szolgáltató biztosítja a nyilvános kulcs sértetlenségét a kulcspár előállításának helyszínéről (a regisztráló szervezettől) a tanúsítvány kibocsátásának helyszínére (a hitelesítő szervezethez) történő továbbítás során.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

a) A Szolgáltató saját aláírás-ellenőrző (szolgáltatói) nyilvános kulcsait elérhetővé teszi az érintett felek részére olyan módon, mely biztosítja a Szolgáltató nyilvános kulcsának, valamint az összes ezzel kapcsolatos paraméter sértetlenségét és hitelességét.

6.1.5. Kulcs méretek

A Szolgáltató saját kulcsának mérete:

a) A Szolgáltató aláíró kulcsára olyan kulcshosszúságot és algoritmust választ, melyet jogszabály ismer el erre a célra alkalmasnak.

A Szolgáltató által más felek számára előállított kulcsok mérete:

b) A Szolgáltató által más felek (regisztráló szervezetek illetve az Aláíró) számára generált kulcsok olyan hosszúságúak és olyan algoritmushoz tartozók, melyet jogszabály ismer el erre a célra alkalmasnak.

6.1.6. A nyilvános kulcs paraméterek előállítása

a) A Szolgáltató a nyilvános kulcs paramétereinek előállítása során /beleértve az ehhez szükséges véletlen szám generálást is/ olyan szabványos megoldást használ, melyet jogszabály ismer el erre a célra alkalmasnak.

6.1.7. A paraméterek megfelelőségének ellenőrzése

a) A Szolgáltató ellenőrzi valamennyi kulcspár előállítása során a paraméterek minőségét.

6.1.8. Hardver/szoftver kulcselőállítás

a) A Szolgáltató valamennyi kulcspár előállítását olyan biztonságos kriptográfiai modulban hajtja végre, amely tanúsítvánnyal igazoltan megfelel a 6.1.1 alatt felsorolt követelményeknek, s amely szerepel a Nemzeti Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában a tanúsított elektronikus aláírási termékek között, vagy más EU tagállamban hasonló szintű tanúsításon ment keresztül. A tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelmény-rendszer szerint, azzal egyenértékű értékeli szinten kell elvégezni.

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

a) A Szolgáltató saját kulcsainak használati célja az alábbiak egyike lehet:
   - tanúsítvány aláírás,
   - visszavonási lista aláírás,
   - titkosítás.

b) A Szolgáltató által az Aláíró számára előállított kulcsok használati célja kizárólag aláírás lehet.

6.2. A magánkulcsok védelme

a) A Szolgáltató gondoskodik valamennyi általa (saját maga, regisztráló szervezetek, illetve az Aláíró számára) előállított magánkulcs titkosságáról és sértetlenségéről.

b) A Szolgáltató külön aláíró magánkulcsot használ tanúsítvány aláírásra, és tanúsítvány visszavonási lista aláírásra, egyúttal ezen kulcsokat semmilyen más célra nem használja.

c) A Szolgáltató a tanúsítványokat, illetve a tanúsítvány visszavonási listákat aláíró magánkulcsait fizikailag biztonságos helyszínen használja.

6.2.1. Kriptográfiai modulra vonatkozó szabványok

Hitelesítő szervezet

a) A Szolgáltató a tanúsítványokat és tanúsítvány visszavonási listákat aláíró magánkulcsait olyan biztonságos kriptográfiai modulban állítja elő, amely tanúsítvánnyal igazoltan megfelel a 6.1.1 alatt felsorolt követelményeknek, s amely szerepel a Nemzeti Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között, vagy más EU tagállamban hasonló szintű tanúsításon ment keresztül. A tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelmény-rendszer szerint, azzal egyenértékű értékeli szinten kell elvégezni.

b) A hitelesítő szervezet tanúsítványokat és tanúsítvány visszavonási listákat aláíró magánkulcsait olyan biztonságos kriptográfiai modulban tárolja és használja, amely tanúsítvánnyal igazoltan megfelel a 6.1.1 alatt felsorolt követelményeknek , s amely szerepel a Nemzeti Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között, vagy más EU tagállamban hasonló szintű tanúsításon ment keresztül. A tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelmény-rendszer szerint, azzal egyenértékű értékeli szinten kell elvégezni.

Végfelhasználók

a) Az Aláíró magán aláíró kulcsát olyan biztonságos aláíráslétrehozó eszközben generálja, tárolja, illetve használja, amely nem kompromittálja a magánkulcs biztonságát, megfelel a [4] szabvány szerint kidolgozott SSCD-PP védelmi profil [15] követelményeinek, s amely szerepel a Nemzeti Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között.

6.2.2. A több-szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése

Hitelesítő szervezet

a) A hitelesítő szervezet magán aláíró kulcsait csak bizalmi munkakört betöltő személyzet állíthatja vissza, legalább kettős ellenőrzés mellett, fizikailag biztonságos környezetben (lásd 5.2.2).

Végfelhasználók

a) Az Aláíró magán aláíró kulcsa nem kerül mentésre, így visszaállítása nem lehetséges.

6.2.3. Magánkulcs letétbe helyezése

a) A Szolgáltató az Aláíró magán aláíró kulcsait nem tárolja, és nem tartja olyan módon sem, mely lehetővé tenné a (kulcs)adatok későbbi dekódolását.

6.2.4. Magánkulcs mentése

Hitelesítő szervezet

a) A hitelesítő szervezet magán aláíró kulcsát csak bizalmi munkakört betöltő személyzet másolhatja le, illetve tárolhatja le, legalább kettős ellenőrzés mellett, fizikailag biztonságos környezetben (lásd az 5.2.2 pontot).

b) A hitelesítő szervezet magán aláíró kulcsainak mentett másolataira ugyanolyan szintű biztonsági előírások vonatkoznak, mint a használatban levő kulcsokra.

Végfelhasználók

c) A Szolgáltató által az Aláírónak előállított magánkulcsok mentése nem lehetséges.

6.2.5. Magánkulcs archiválása

a) A Szolgáltató magánkulcsot nem archivál.

6.2.6. Magánkulcs bejuttatása a kriptográfiai modulba

Hitelesítő szervezet

a) A hitelesítő szervezet magánkulcsait az ezeket felhasználó kriptográfiai hardver modul állítja elő, így ezeket nem kell külön a modulba juttatni.
b) Arra az időre, amíg a fenti kulcsok a kriptográfiai hardver modult elhagyják (átmenetileg, mentési célból, a mentés célját szolgáló tartalék kriptográfiai hardver modulra való áttöltés során, lásd 6.2.4) a hitelesítő szervezet kódolja magánkulcsait, olyan algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs vagy kulcsrészlet teljes hátralévő életciklusában.
c) A hitelesítő szervezet kriptográfiai hardver modulja kikapcsolt állapotban a magánkulcsokat kódolva tárolja, olyan algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs teljes hátralévő életciklusában.

Végfelhasználók

d) A Szolgáltató az általa előállított magánkulcsoknak a biztonságos aláírás-létrehozó eszközbe való bejuttatása (áttöltése) során a magánkulcsokat kódolja, olyan protokollt, algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt magánkulcs teljes hátralévő életciklusában.
e) Az Aláíró magán aláíró kulcsa a feltöltést követően a biztonságos aláírás-létrehozó eszközben marad, azt semmilyen célból nem hagyja el.
f) Az Aláíró biztonságos aláírás-létrehozó eszköze kikapcsolt állapotban a magánkulcsokat kódolva tárolja, olyan algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs teljes hátralévő életciklusában.

6.2.7. A magánkulcs aktivizálásának módja

Hitelesítő szervezet

a) A hitelesítő szervezet (tanúsítványokat és tanúsítvány visszavonási listákat aláíró) magánkulcsai aktivizálását az erre felhatalmazott felhasználó birtokláson és tudáson alapuló kombinált hitelesítési eljárással aktivizálhatja.
b) A hitelesítő szervezet egyéb (a Szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsai aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.

Regisztráló szervezet

c) A regisztráló szervezet (az archiválandó regisztrációs adatokat és tranzakciókat aláíró) magánkulcsa aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.
d) A regisztráló szervezet egyéb (a Szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsai aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.

Végfelhasználók

e) Az Aláíró magánkulcsa illetéktelen felhasználásának megakadályozása érdekében (lásd 2.1.3 d. pont követelményét) a biztonságos aláírás-létrehozó eszközben tárolt magánkulcs használatát az Aláíró csak tudáson alapuló hitelesítési eljárással aktivizálhatja.

6.2.8. A magánkulcs aktív állapotának megszűnésének módja

Hitelesítő és regisztráló szervezet

a) A magánkulcsok aktív állapotának megszüntetése (deaktiválása) akkor lehetséges, ha a magánkulcsot tároló kriptográfiai hardver modulok szabályos vagy szabálytalan módon kikerülnek az aktivizálást és felhasználást lehetővé tevő állapotból. (Az erre vonatkozó részleteket a Szolgáltatási Szabályzat tartalmazza.)

Végfelhasználók

b) A magánkulcsok deaktiválása akkor lehetséges, ha a magánkulcsot tároló biztonságos aláírás-létrehozó eszköz szabályos vagy szabálytalan módon kikerül az aktivizálást és felhasználást lehetővé tevő állapotból. (Az erre vonatkozó részleteket a Szolgáltatási Szabályzat tartalmazza.)

6.2.9. A magánkulcs megsemmisítésének módja

Hitelesítő és regisztráló szervezet magánkulcsainak megsemmisítése

A Szolgáltató gondoskodik arról, hogy magán aláíró kulcsai ne legyenek felhasználhatók életciklusuk vége után. Különösképpen:

a) A Szolgáltató magán aláíró kulcsainak használatát korlátozza oly módon, hogy az összhangban legyen a tanúsítvány előállításához használt lenyomatoló függvényre, aláíró algoritmusra és kulcshosszra vonatkozó (6.1.5. pontban kifejtett) gyakorlatnak.
b) A Szolgáltató kriptográfiai hardver moduljában tárolt szolgáltatói magán aláíró kulcsokat a hardver modul visszavonásakor megsemmisíti oly módon, hogy a magánkulcsok ne legyenek helyreállíthatók.
c) A Szolgáltató magán aláíró kulcsainak megsemmisítésekor azok összes másolatát is megsemmisíti oly módon, hogy a magánkulcsok ne legyenek helyreállíthatók.

6.2.10. A Szolgáltató által az Aláíró számára generált magánkulcsok megsemmisítése

a) A Szolgáltató az Aláíró magánkulcsát azon a biztonságos aláírás-létrehozó eszközön generálja, amelyet a Szolgáltató az Aláírónak átad. A Szolgáltató ezen eszközről az Aláíró magánkulcsát nem képes kinyerni, így e kulcsot a Szolgáltató adatbázisában nem tárolja.
b) Az Aláíró magánkulcsának életciklus végén történő megsemmisítése kívül esik a Szolgáltató felelősségi körén.

6.3. A kulcspár gondozásának egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

a) A Szolgáltató - tanúsítvány archiválási szolgáltatása keretén belül – archiválja a végfelhasználók nyilvános kulcsait.

6.3.2. A nyilvános és magánkulcsok használatának periódusa

Hitelesítő és regisztráló szervezet

a) A Szolgáltató saját magánkulcsai használati periódusa nem haladja meg azok érvényességi idejét, ahogyan azt a 6.2.9 alfejezet is állítja (a Szolgáltató gondoskodik arról, hogy magán aláíró kulcsai ne legyenek felhasználva életciklusuk vége után), összhangban a 6.2.5 alfejezet állításával (a Szolgáltató magán aláíró kulcsot nem archivál).

Végfelhasználók

b) Az Aláíró magánkulcsának használati periódusa nem haladhatja meg a tanúsítvány érvényességi idejét, ennek betartása viszont kívül esik a Szolgáltató felelősségi körén. Ennek betartása az Aláíró kötelessége (lásd 2.1.3 c. pontja), ellenőrzése pedig az érintett felek kötelessége (lásd 2.1.4 b. pontja).

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

a) A Szolgáltató biztonságosan állítja elő az általa kibocsátott biztonságos aláírás-létrehozó eszközök aktivizáló adatait.

6.4.2. Az aktivizáló adatok védelme

a) A hitelesítés- szolgáltató az általa kibocsátott biztonságos aláírás-létrehozó eszközök aktivizáló adatait a biztonságos aláírás-létrehozó eszköztől elkülönítve osztja szét.

6.5. Számítógépes biztonsági óvintézkedések

6.5.1. Speciális számítógépes biztonsági műszaki követelmények

A Szolgáltató gondoskodik arról, hogy az informatikai rendszeréhez való hozzáférés kellően felhatalmazott egyénekre legyen korlátozva. Különösképpen:

a) A Szolgáltató védi rendszerei és információi sértetlenségét vírusok, káros és engedély nélküli szoftverek ellen.
b) A Szolgáltató biztonságosan kezeli adathordozó eszközeit a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.
c) A Szolgáltató gondoskodik a felhasználói hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.
d) A Szolgáltató gondoskodik arról, hogy az információhoz és az alkalmazói rendszer funkciókhoz történő hozzáférés, a hozzáférés ellenőrzési szabályzatnak megfelelően korlátozott legyen, és hogy a Szolgáltató rendszere megfelelő informatikai biztonsági ellenőrzéseket nyújtson a Szolgáltató szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében, beleértve a biztonsági, adminisztrátori és üzemeltetési funkció elkülönítését. Különösképpen a rendszer szolgáltatási programok használatát korlátozza és ellenőrzi szigorúan.
e) A Szolgáltató gondoskodik arról, hogy személyzetét sikeresen azonosítsák és hitelesítsék, mielőtt a tanúsítvány gondozásával kapcsolatos kritikus alkalmazásokat használhatnák.
f) A Szolgáltató eljárásokat dolgoztat ki és hajtat végre valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására.
g) A Szolgáltató műszaki óvintézkedéseket juttat érvényre (például tűzfalak segítségével), hogy a Szolgáltató belső hálózati tartományai védettek legyenek a harmadik felek számára elérhető külső hálózati tartományoktól.
h) A Szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.
i) A Szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni és regisztrálni az erőforrásaihoz való jogosulatlan és/vagy szabálytalan hozzáférési kísérleteket, valamint képes legyen ezekre időben reagálni.
j) A Szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.
k) A Szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ (hálózatról történő) módosítására vonatkozóan.
l) A Szolgáltató gondoskodik arról, hogy az érzékeny adatokat megvédjék az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.
m) A Szolgáltató biztosítja, hogy személyzetének minden tagja felelősségre vonható legyen tevékenységéért.

6.5.2. Informatikai biztonsági minősítés

a) A Szolgáltató szolgáltatásaira vonatkozóan végrehajtott kockázat elemzés (lásd 5. a.) azonosította azokat a kritikus szolgáltatásokat, amelyekhez megbízható informatikai rendszerek kellenek, egyben meghatározta a szükséges értékelési garanciaszinteket.
b) A Szolgáltató olyan megbízható informatikai rendszereket alkalmaz, melyek megfelelő biztonsági értékeléseken alapuló minősítésekkel (tanúsításokkal) rendelkeznek.

6.6. Életciklusra vonatkozó műszaki óvintézkedések

6.6.1. Rendszerfejlesztési óvintézkedések

a) A Szolgáltató gondoskodik arról, hogy az általa, illetve a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény-meghatározási fázisban figyelembe vegyék, annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.
b) A Szolgáltató konfiguráció kezelési eljárásokat alkalmaz valamennyi működő szoftvere esetében a kibocsátásokra, a módosításokra és a sürgős szoftver javításokra vonatkozóan.

6.6.2. Biztonságkezelési óvintézkedések

a) A Szolgáltató olyan eszközöket és eljárásokat alkalmaz, melyek garantálják a kritikus szolgáltatásait (lásd 6.5.2. a. pontja) megvalósító megbízható informatikai rendszereire az operációs rendszer beállítások, valamint a hálózati konfiguráció biztonságát, egyúttal az alkalmazott biztonsági mechanizmusok sértetlenségének, helyes működésének ellenőrzését.

6.6.3. Az életciklusra vonatkozó biztonság osztályozása

a) A Szolgáltató által alkalmazott megbízható informatikai rendszerek [4] (Common Criteria) szabványnak megfelelő biztonsági értékelései (lásd 6.5.2.b. pont) magukban foglalnak életciklusra vonatkozó független biztonsági értékelést is.

6.7. Hálózatbiztonsági óvintézkedések

A Szolgáltató gondoskodik arról, hogy informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerüljön sor. Különösképpen:

A Szolgáltató általános tevékenységével kapcsolatosan:
a) Az érzékeny adatokat megvédi, amikor azok átvitele (cseréje) nem biztonságos hálózatokon keresztül történik.
b) A Szolgáltató biztosítja általános informatikai biztonságát még akkor is, ha a Szolgáltató egyes funkciót más szervezet (pl. a regisztráló szervezet) valósítja meg.

A regisztrálással kapcsolatosan:
c) A regisztrációs adatok bizalmasságát és sértetlenségét megvédik, különösen az Aláíróval és az Aláíró Szervezetével folytatott külső, illetve a Szolgáltató egyes komponensei közötti belső adatcsere során.
d) A Szolgáltató (a hitelesítő szervezeten keresztül) ellenőrzéssel biztosítja, hogy regisztrációs adatokat csak általa elismert, azonosságában hitelesített regisztrációs szolgáltatókkal cserél.

A tanúsítvány előállítással és visszavonás kezeléssel kapcsolatosan:
e) A Szolgáltató gondoskodik arról, hogy a helyi hálózati komponensek (például routerek) fizikailag biztonságos környezetben legyenek és konfigurációikat időszakonként auditálják.
f) A Szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni, regisztrálni az erőforrásaihoz (hálózatról) történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre.

A tanúsítvány kibocsátásával kapcsolatosan:
h) A Szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.

A tanúsítvány visszavonás kezeléssel kapcsolatosan:
b) A Szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ (hálózatról történő) módosítására vonatkozóan.

6.8. A kriptográfiai modulok ellenőrzése

A Szolgáltató gondoskodik a kriptográfiai hardver biztonságáról annak teljes élettartama alatt. Különösképpen gondoskodik arról, hogy:

a) a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják szállítás közben;
b) a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják tárolás közben;
c) a Szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktivizálása, mentése és visszaállítása legalább két bizalmi munkakört betöltő alkalmazott együttes jelenlétét kívánja meg (lásd 5.2.2);
d) a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardver helyesen működik;
e) a Szolgáltató kriptográfiai hardverén tárolt Szolgáltatói magán aláíró kulcsokat az eszköz visszavonásakor megsemmisítik.

7. Tanúsítvány, tanúsítvány-visszavonási lista, időbélyeg és on-line tanúsítvány állapot válasz profilok

7.1. Tanúsítvány profil

a) A Szolgáltató által kibocsátott tanúsítványok megfelelnek a [9] szabványban leírt X.509 3-as verziójú tanúsítványoknak.
b) A Szolgáltató által a végfelhasználóknak kibocsátott tanúsítványok megfelelnek a [11] szabványban leírt minősített tanúsítványoknak.
c) A Szolgáltató által a végfelhasználóknak kibocsátott tanúsítványok megfelelnek a [8] szabványban leírt minősített tanúsítványoknak.

7.1.1. Tanúsítvány alapmezők

Lásd a 7.1 a. b. és c. állításokat, valamint a Szolgáltatási Szabályzatot.

7.1.2. Tanúsítvány X509 kiterjesztések

A Szolgáltatási Szabályzat tartalmazza.

7.2. Tanúsítvány visszavonási lista (CRL) profil

a) A hitelesítő-szolgáltató által kibocsátott tanúsítvány visszavonási listák megfelelnek a [12] ajánlásának.
d) A hitelesítő-szolgáltató által kibocsátott tanúsítvány visszavonási listák megfelelnek a [9] szabványban leírt X.509 2-as verziójú tanúsítvány visszavonási listáknak.

7.2.1. Alap mezők

Lásd a 7.2 a. és b. állításokat, valamint a Szolgáltatási Szabályzatot.

7.2.2. „Tanúsítvány visszavonási lista" és „Tanúsítvány visszavonási lista bejegyzés" kiterjesztések

Lásd a 7.2 a. és b. állításokat, valamint a Szolgáltatási Szabályzatot.

7.3. Időbélyegző profil

Az alkalmazott időbélyegző profil megfelel a [28] ajánlásban leírt időbélyegző profilnak.

7.4. On-line tanúsítvány állapot válasz (OCSP) profil

Az alkalmazott on-line tanúsítvány állapot válasz profil megfelel a [29] ajánlásban leírt profilnak.

8. Leírás-adminisztráció

a) A Szolgáltató rendelkezik egy olyan (szolgáltatási) szabályzattal, mely vonatkozik az általa támogatott hitelesítési rendben azonosított, valamennyi állítást megvalósító gyakorlatra és eljárásra.
b) A Szolgáltató szolgáltatási szabályzata meghatározza a Szolgáltató szolgáltatásait támogató valamennyi külső szervezetre vonatkozó kötelezettségeket, beleértve az alkalmazandó szabályzatokat is.

8.1. Leírás-változtatási eljárások

a) A Szolgáltató felülvizsgálati folyamatot határoz meg, mely kiterjed a hitelesítési rend és szolgáltatási szabályzat gondozására is.
b) A Szolgáltató időben értesítést tesz közzé az általa támogatott hitelesítési rendben, illetve szolgáltatási szabályzatában tervezett változtatásokról, majd a (8.3 a) pont szerint történő) jóváhagyást követően az átdolgozott hitelesítési rendet illetve szolgáltatási szabályzatot (a 8.2 a) pontban előírtak szerint) haladéktalanul hozzáférhetővé teszi.

8.2. Közzétételi és tájékoztatási elvek

a) A Szolgáltató az általa támogatott hitelesítési rendet, valamint szolgáltatási szabályzatát és egyéb más fontos dokumentációját az Aláíró, az Előfizető, az Aláíró Szervezete és az érintett felek rendelkezésére bocsátja, a hitelesítési rendnek való megfelelés felméréséhez szükséges mértékig.
b) A Szolgáltató a tanúsítvány használatával kapcsolatos kikötéseit és feltételeit az Aláíró, az Előfizető, Aláíró Szervezete és az összes potenciális érintett fél számára megismerhetővé teszi, a 2.6.1-ben meghatározottak szerint.

8.3. Szolgáltatás szabályzat jóváhagyási eljárások

A hitelesítési rend vonatkozóan:

a) A hitelesítési rend tartalmilag megfelel az MTT+BALE [7] tanúsítványtípusokkal szemben támasztott minimális követelményeknek.
b) A Szolgáltató jóváhagyás előtt megvizsgálja a hitelesítési rend (fenti a.-b. pontokban meghatározott) követelményeknek való megfelelőségét.
c) A hitelesítési rend jóváhagyására a Szolgáltató felsőszintű irányító testülete rendelkezik végső hatáskörrel és felelősséggel.
d) A Nemzeti Hírközlési Hatóság nyilvántartásba veszi a Szolgáltató által jóváhagyott és bejelentett hitelesítési rendet.

A szolgáltatási szabályzatra vonatkozóan:

a) A Szolgáltatási Szabályzat tartalmilag és formailag megfelel a hitelesítési rendnek.
b) A Szolgáltató jóváhagyás előtt megvizsgálja a Szolgáltatási Szabályzatot a hitelesítési rendeknek való megfelelőség szempontjából.
c) A Szolgáltatási Szabályzat jóváhagyására a Szolgáltató felsőszintű irányító testülete rendelkezik végső hatáskörrel és felelősséggel.
d) A Szolgáltatási Szabályzat jogszabályi megfelelőségét a Nemzeti Hírközlési Hatóság is megvizsgálja a nyilvántartásba vételt megelőzően.

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.

Aláíró (Signatory)
Az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra 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.

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 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.

Előfizető
Az a fél, aki a tanúsítvány kibocsátásával és fenntartásával kapcsolatos díjakat fizeti.

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

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.

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.

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

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 aláíráslétrehozó adatot) biztonságos aláíráslétrehozó 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: aláíráslétrehozó adat).

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.

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

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

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

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

Minősített Szolgáltató (Qualified Certification Service Provider)
Az elektronikus aláírási törvényben és a hozzá kapcsolódó rendeletekben foglalt követelményeknek megfelelő, valamint ennek alapján nyilvántartásba vett 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 aláíráslétrehozó eszközzel együtt bocsát ki tanúsítványt, ily módon garantálja, hogy a tanúsítványhoz tartozó aláíráslétrehozó adat a biztonságos aláíráslétrehozó 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. 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.

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

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

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 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 az elektronikus aláírásról szóló törvény szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.

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

Tanúsítvány kibocsátás (Certificate dissemination)
A tanúsítvány átadása az Aláírónak, valamint a 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 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 Szolgáltató bocsát ki.

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: On-line Certificate Status Response, On-line 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

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

[4] Minősített tanúsítványtípus minták minősített 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 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 3647 (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: e-Szignó Hitelesítés Szolgáltató Biztonságos aláíró-eszközzel együttesen kiadott minősített tanúsítvány hitelesítési rendjei

[21] IR-MS-05/001: 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 – Általános Szerződési Feltételek, OID: 1.3.6.1.4.1.21528.2.1.1.13

[23] e-Szignó Hitelesítés Szolgáltató - Szolgáltatási Szabályzat , OID: 1.3.6.1.4.1.21528.2.1.1.1

[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

[31] A Nemzeti Hírközlési Hatóság HL-20336-9/2005 ügyiratszámú határozata az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok és paramétereik meghatározása.