Informatikai és Hírközlési Minisztérium

A közigazgatásban alkalmazható hitelesítési rendek

2. számú melléklet

Kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rendek 1.0 verzió

[EHR+_Ü], OID: 0.2.216.1.100.42.101.3.2.1
[EHR+_K], OID: 0.2.216.1.100.42.101.4.2.1

Tartalom

1. Bevezetés

1.1 Áttekintés

A hitelesítési rend olyan szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.

Jelen dokumentum célja az alábbi Hitelesítési rendek meghatározása:

- Közigazgatási, ügyfélhez kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend.
- Közigazgatási, köztisztviselőhöz kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend.

Mindkét Hitelesítési rend megfelel az európai szabványosítás keretében kidolgozott, [6]-ban definiált "NCP+" egységesített hitelesítési rendnek. Ugyanakkor számos helyen tovább pontosítják, illetve konkretizálják az "NCP+" követelményeit, a magyar közigazgatáson belüli egységes és biztonságos felhasználhatóság, valamint a hazai jogszabály előírásoknak való megfelelőség érdekében (egyúttal a magánkulcsokat tároló és aktivizáló kriptográfiai hardver eszköztől nem várja el a BALE minősítést).

A két (kriptográfiai hardver eszköz használatát megkövetelő) egységesített Hitelesítési rend nagyon hasonló, az alábbi területeken van köztük csak eltérés:

- előfizetők és alanyok (1.3.3),
- megfelelő tanúsítvány használat (1.4.1),
- szervezet azonosságának hitelesítése (3.2.2),
- egyén azonosságának hitelesítése (3.2.3),
- kulcsletét és visszaállítás rendje és szabályai (4.12.1),
- tanúsítványprofil (7.1).

A fenti különbségek ellenére a jelen dokumentumban megfogalmazott szabályok (elvárások) többsége mindkét Hitelesítési rendre vonatkoznak. Ezért a tömörebb megfogalmazás, egyben az áttekinthetőség megtartása érdekében az alábbi jelöléseket használjuk:

- Azon szabályok (elvárások) előtt, melyek csak az egyik Hitelesítési rendben szerepelnek, külön feltüntetjük az érintett Hitelesítési rend azonosítóját.
- Azokon a helyeken ahol a több lehetséges alternatíva közül jelen dokumentum a Hitelesítési rend szintjén nem akar egyet rögzíteni, ott az alábbi kifejezést használjuk: „*A Szolgáltatási Szabályzatban meghatározott.*"
- Azokon a helyeken ahol a több lehetséges alternatíva közül (köztük az a lehetőség is, hogy az adott tárgyban egyáltalán nincs elvárás) jelen dokumentum a Hitelesítési rend szintjén nem akar egyet sem rögzíteni, ott az alábbi kifejezés szerepel: „*Nincs megkötés.*"

1.2 A dokumentum neve és azonosítója

A jelen dokumentumban meghatározott Hitelesítési rend neve és azonosítói az alábbiak:

[EHR+_Ü] esetén:

Név: Közigazgatási, ügyfélhez kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend

Azonosító: [EHR+_Ü]

OID: ……. 0.2.216.1.100.42.101.3.2.1

[EHR+_K] esetén:

Név: Közigazgatási, köztisztviselőhöz kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend

Azonosító: [EHR+_K]

OID: ……. 0.2.216.1.100.42.101.4.2.1

Azzal, hogy egy hitelesítés-szolgáltató egy tanúsítványban a fenti objektum azonosítók valamelyikét szerepelteti, azt állítja, hogy megfelel az adott Hitelesítési rendnek.

A hitelesítés-szolgáltatónak az előfizetők és érintett felek rendelkezésére bocsátott szabályzataiban[1] a támogatott Hitelesítési rendek azonosítóit szerepeltetnie kell, utalva a megfelelőség állítására.

1.3 PKI szereplők

1.3.1 Hitelesítés-szolgáltatók

A jelen dokumentumban meghatározott Hitelesítési rendek azokra a hitelesítés-szolgáltatókra vonatkoznak, melyek felvállalják az adott Hitelesítési rendnek való megfelelést.

1.3.2 Regisztráló szervezetek

A Szolgáltatási Szabályzatban meghatározott.

1.3.3 Előfizetők és alanyok

[EHR+_Ü] esetén:

Jelen Hitelesítési rendben az alanyok a magyar elektronikus közigazgatás szolgáltatásait igénybe vevő ügyfelek, akik a magyar elektronikus közigazgatási rendszerben elektronikus ügyintézést kívánnak lebonyolítani.

[1] A szabályzatokba beleértendők a szerződéses feltételek is.

Jelen Hitelesítési rendben az előfizetők vagy az ügyfelek, vagy az ügyfelek által képviselt szervezetek.

[EHR+ K] esetén:

Jelen Hitelesítési rendben az alanyok a magyar közigazgatás köztisztviselői, akik a magyar elektronikus közigazgatási rendszerben egymással, illetve az ügyfelekkel kommunikálnak a rendszer keretén belül.

Jelen Hitelesítési rendben az előfizetők a közigazgatási szervek.

1.3.4 Érintett felek

Az érintett fél az az entitás, aki egy adott tanúsítványon alapuló nyilvános kulcsú technikára hagyatkozva jár el.

Jelen Hitelesítési rend vonatkozásában érintett fél minden olyan felhasználó a közigazgatási bizalmi tartományon belül és kívül, aki a magyar közigazgatási nyilvános kulcsú infrastruktúrában kibocsátott tanúsítványokat ellenőrzi, alkalmazza.

1.3.5 Egyéb szereplők: Közigazgatási Gyökér Hitelesítés-Szolgáltató

A magyar közigazgatásban használható tanúsítványokat kibocsátó hitelesítés-szolgáltatók szolgáltatói tanúsítványát felülhitelesítő szervezet.

A Közigazgatási Gyökér Hitelesítés-Szolgáltató (KGyHSz) a tanúsítvány kiadásával igazolja, hogy a hitelesítés-szolgáltató és a tanúsítvány adatainak egyezését, valamint a megfelelő Hitelesítési rend és Szolgáltatási Szabályzat előírásainak megfelelőségét ellenőrizte, illetve a felültanúsított hitelesítés-szolgáltató a tanúsítvány elfogadásával magára nézve kötelezőnek ismeri el a KGyHSz által kiadott szabályzatokat és a KGyHSz felügyeleti, ellenőrzési jogát.

1.4 Tanúsítvány használat

1.4.1 Megfelelő tanúsítvány használat

a) A jelen dokumentumban meghatározott Hitelesítési rend megfelel a közigazgatási felhasználásra vonatkozó követelményeknek.

[EHR+ Ü] esetén:

b) A jelen dokumentumban meghatározott Hitelesítési rend szerepel az NHH Hivatala hatósági nyilvántartásában, az ügyfél által használt aláíráshoz kapcsolódó Hitelesítési rendek között.

[EHR+ K] esetén:

b) A jelen dokumentumban meghatározott Hitelesítési rend szerepel az NHH Hivatala hatósági nyilvántartásában, a hivatali aláíráshoz kapcsolódó Hitelesítési rendek között.

c) A tanúsítványt az arra jogosítottak, a tanúsítványhoz tartozó Hitelesítési rendben (jelen dokumentum 4.5.1 és 6.1.7 pontjaiban) meghatározott célokra használhatják.

1.4.2 Tiltott tanúsítvány használat

a) A tanúsítványt csak az arra jogosítottak, és csak a tanúsítványhoz tartozó Hitelesítési rendben meghatározott célra használhatják (lásd jelen dokumentum 4.5.1 és 6.1.7 pontját). A tanúsítvány minden más célú használata tiltott.

1.5 A Hitelesítési rend adminisztrálása

1.5.1 A Hitelesítési rend adminisztrációs szervezete

a) A közigazgatási nyilvános kulcsú infrastruktúra irányítását az informatikai és hírközlési miniszter látja el.

b) Jelen Hitelesítési rend adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatók meg.

A szervezet adatai	
Szervezet neve	Informatikai és Hírközlési Minisztérium
Szervezet címe	1077 Budapest, Dob utca 75-81.
Telefonszám	+36 1 461 3423
Faxszám	+36 1 322 2264
Email cím	**Később meghatározott**

1.5.2 Kapcsolattartó személy

A hitelesítés-szolgáltatónak saját kapcsolattartási lehetőséget kell megjelölnie az előfizetői számára kiadott dokumentumaiban.

1.5.3 A Szolgáltatási Szabályzatok jelen Hitelesítési rendnek való megfelelőségéért felelős személy/szervezet

a) A Szolgáltatási Szabályzatot kibocsátó szolgáltató a felelős a Szolgáltatási Szabályzat jelen dokumentumban meghatározott Hitelesítési rendnek való megfelelőségéért és az ebben foglaltak szerinti szolgáltatás nyújtásáért. A szolgáltatás nyújtása feletti felügyeletet az NHH Hivatala látja el. Az NHH Hivatala hatósági nyilvántartást vezet a közigazgatási felhasználásra vonatkozó követelményeknek megfelelő Hitelesítési rendekről, valamint az ezt alkalmazó (ennek megfelelő Szolgáltatási Szabályzattal rendelkező) hitelesítés-szolgáltatókról.

1.5.4 A Szolgáltatási Szabályzat elfogadási eljárása

a) A Szolgáltatási Szabályzatot a hitelesítés-szolgáltató vezetésének kell jóváhagynia.

1.6 Meghatározások

Alany	A hitelesítés-szolgáltató által kiadott tanúsítványban azonosított természetes személy, aki a tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja, vagy szervezet, amely a szerver tanúsítványában szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.
Elektronikus aláírás	Elektronikus dokumentumhoz azonosítás céljából hozzárendelt vagy azzal logikailag összekapcsolt elektronikus adat.
Előfizető	A hitelesítés-szolgáltatónál egy vagy több alany nevében előfizető természetes, vagy jogi személy, vagy jogi személyiség nélküli szervezet, aki közvetlenül vagy közvetve elfogadja a hitelesítés-szolgáltató kikötéseit és feltételeit.
Érintett fél	Az érintett fél az az entitás, aki egy adott tanúsítványon alapuló nyilvános kulcsú technikára (elektronikus aláírásra, titkosításra vagy hitelesítésre) hagyatkozva jár el
Hitelesítési rend	Olyan szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.
Hitelesítés-szolgáltató (HSz)	A tanúsítványba foglalt nyilvános kulcs és a tulajdonos azonosító adatainak hiteles összekapcsolásáért felelős, a kommunikációban résztvevő felek mindegyike által hitelesnek tartott szervezet.
Időbélyegzés	Az a folyamat, melynek során az elektronikus dokumentumhoz olyan igazolás rendelődik, amely tartalmazza a bélyegzés hiteles időpontját, és amely a dokumentumhoz oly módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető.
Közigazgatási Gyökér Hitelesítés-Szolgáltató (KGyHSz)	A magyar közigazgatásban használható tanúsítványokat kibocsátó hitelesítés-szolgáltatók szolgáltatói tanúsítványát felülhitelesítő szervezet.
Nyilvános kulcsú infrastruktúra (PKI)	A tanúsítványok és kulcsok kezelését biztosító jogszabályok, irányelvek, eljárások, szervezetek, hardver- és szoftvereszközök összessége.
Szolgáltatási Szabályzat	A hitelesítés-szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.
Szolgáltatói kulcspár	A szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs.
Szolgáltatói magánkulcs	Olyan kriptográfiai magánkulcs, amelyet a hitelesítés-szolgáltató saját szolgáltatása keretében így különösen a tanúsítvány kibocsátásához, a visszavonási nyilvántartások aláírásához, az időbélyegzéshez, a naplózáshoz, az archiváláshoz használ.
Szolgáltatói nyilvános kulcs	Olyan kriptográfiai nyilvános kulcs, amelyet a szolgáltatói magánkulcs használatával létrehozott elektronikus aláírás ellenőrzésére használnak.

Tanúsítvány	Hitelesítés-szolgáltató által kibocsátott digitális igazolás, amely a belefoglalt nyilvános kulcsot egy meghatározott entitáshoz kapcsolja.
Tanúsítvány visszavonási lista (CRL)	Valamely okból visszavont, vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a hitelesítés-szolgáltató bocsát ki, s aláírásával hitelesít.

1.7 Rövidítések és jelölések

CRL	tanúsítvány visszavonási lista	Certificate Revocation List
DN	megkülönböztetett név	Distinguished Name
KHE	kriptográfiai hardver eszköz	---
EHR	Egységesített Hitelesítési rend	Normalized Certification Policy
EHR+	(kriptográfiai hardver eszköz használatát megkövetelő) Egységesített Hitelesítési rend	(extended) Normalized Certification Policy
OCSP	valós idejű tanúsítvány állapot protokoll	On-line Certificate Status Protocol
OID	objektum azonosító	Object Identifier
URI	egységes forrás azonosító	Uniform Resource Identifier
URL	egységes forrás meghatározó	Uniform Resource Locator
UTF	egységes átalakítás formátum	Unicode Transformation Format

1.8 Hivatkozások

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

[2] FIPS PUB 140: "Kriptográfiai modulok biztonsági követelményei".

[3] MSZ/ISO/IEC 15408 1999: Informatika - Biztonságtechnika - Az informatikai biztonságértékelés közös szempontjai (1-3 részek).

[4] CEN CWA 14167-2: Védelmi profil hitelesítés-szolgáltató aláírási műveletét végző, mentési funkcióval rendelkező kriptográfiai moduljára

[5] ETSI TS 102 042 Szabályozási követelmények a nyilvános kulcsú tanúsítványokat kibocsátó hitelesítés-szolgáltatók számára (Műszaki specifikáció) v1.2.1 (2005-05)

[6] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[7] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára

2. Közzétételre és tárolásra vonatkozó felelősségek

2.1 Adatbázisok

A Szolgáltatási Szabályzatban meghatározott.

2.2 A tanúsítványokra vonatkozó információk közzététele

A Szolgáltatási Szabályzatban meghatározott.

2.3 A közzététel gyakorisága

Tanúsítványok, kikötések és feltételek nyilvánosságra hozatala:

a) A hitelesítés-szolgáltatónak biztosítania kell saját szolgáltatói tanúsítványai, valamint az általa kibocsátott tanúsítványok használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét (a 4.10.2 pontban meghatározott rendelkezésre állás mellett). Az általa kibocsátott végfelhasználói tanúsítványok nyilvánosságra hozatala csak az érintett alany, illetve előfizető hozzájárulása esetén megengedett.

Visszavonási állapot információ nyilvánosságra hozatala:

b) A hitelesítés-szolgáltatónak a visszavonási és felfüggesztési kérelem fogadásától számított 3 órán belül meg kell állapítania a kérelem érvényességét (a kérelmező jogosultságát), és nyilvántartásában át kell vezetnie az érvényes kérelem szerinti visszavonási állapot megváltozását.

c) A b) pontban foglaltak teljesítését követő 1 órán belül a hitelesítés-szolgáltatónak a kérelem szerint módosított visszavonási állapotot közzé kell tennie.

d) A hitelesítés-szolgáltatónak a tanúsítvány visszavonási listákat (beleértve ezek bármely változatát is) legalább 24 óránként közzé kell tennie.

2.4 Az adatbázisok elérésének szabályozása

Tanúsítványok, kikötések és feltételek elérhetősége:

a) A tanúsítványtárnak, valamint a tanúsítványok használatára vonatkozó kikötéseknek és feltételeknek nyilvánosnak és nemzetközileg elérhetőnek kell lenniük.

Visszavonási állapot információ elérhetősége:

b) A hitelesítés-szolgáltató köteles a visszavonási állapot információt tanúsítvány visszavonási lista (CRL) formájában közzé tenni.

c) A tanúsítvány visszavonási listának (beleértve ennek bármely változatát is), nyilvánosnak és korlátozás nélkül (nemzetközileg is) elérhetőnek kell lennie.

d) Amennyiben a hitelesítés-szolgáltató valós idejű tanúsítvány állapot protokoll (OCSP) szolgáltatást (is) biztosít, ennek elérhetőségét a Szolgáltatási Szabályzatban kell meghatároznia.

3. Azonosítás és hitelesítés

3.1 Megnevezési konvenciók

3.1.1 Név típusok

a) A hitelesítés-szolgáltató által kiállított tanúsítványokra a következő névkonvenció érvényes:

- X.500 formátum (ITU-T X.501 /ISO/IEC 9594-2:1997, RFC 2459),
- Az alany személyazonosságának igazolására elfogadott hatósági igazolványban (lásd 3.2.3 c) pont) foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve CN és SN mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév), az UTF-8 kódolást használva.
- A tanúsítvány „SubjectAltname" mezőjében szereplő elektronikus levelezési cím struktúrája feleljen meg az RFC 822 előírásainak.

3.1.2 Igény a nevek értelmezhetőségére

a) A hitelesítés-szolgáltatónak be kell tartania a [7] 8. táblázata (a különböző tanúsítványok Subject elemének elvárt adattartalma) által a nevek értelmezhetőségére vonatkozó szabályokat.

3.1.3 Álnevek használata

a) A tanúsítványok DN mezőiben valós neveknek kell szerepelniük, a jelen dokumentumban meghatározott Hitelesítési rend kizárja az álnév használatát.

3.1.4 A különböző elnevezési formák értelmezési szabályai

Nincs megkötés.

3.1.5 A nevek egyedisége

a) A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy az általa kiadott tanúsítványokban használt megkülönböztetett nevet (DN) sohasem fogja egy másik entitáshoz rendelni.

b) A nevek kiadására vonatkozó igények teljesítését érkezési sorrendben kell végezni.

3.1.6 Márkanevek elismerése, azonosításuk és szerepük

Nincs megkötés.

3.2 Kezdeti regisztrálás / személyazonosság megállapítása

3.2.1 A magánkulcs birtoklásának igazolása

a) A tanúsítvány generálása előtt a hitelesítés-szolgáltató megbízható rendszerének biztosítani kell annak ellenőrzését és igazolását, hogy az igénylő valóban birtokolja a tanúsítványba foglalandó nyilvános kulcsnak megfelelő magánkulcsot. Ennek módszere a Szolgáltatási Szabályzatban meghatározott.

3.2.2 Szervezet azonosságának hitelesítése

[EHR+ Ü] esetén:

a) Ha az ügyfél tanúsítványával kifejezetten jelezni kívánja, hogy ő egy adott szervezethez tartozik, akkor a regisztrációhoz magával kell vinnie az adott szervezet nevében aláírásra jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében a tanúsítványt használja, az aláírásra jogosító aláírási címpéldányt, valamint a szervezet azonosságát is hitelesítő dokumentumot.

[EHR+ K] esetén:

a) Egy közigazgatási szervet képviselő természetes személynek a regisztrációhoz magával kell vinnie egy, az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a hivatal képviseletében a hitelesítés-szolgáltatónál előforduló ügyekben eljárjon, mely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti. A természetes személynek külön is azonosítani kell magát a 3.2.3 pont szerint.

3.2.3 Egyén azonosságának hitelesítése

a) A regisztrációt megelőzően az igénylő alanynak személyesen meg kell jelennie a regisztrációt végző szervezet előtt. A hitelesítés-szolgáltató által a Szolgáltatási Szabályzatban meghatározott esetben a személyes megjelenéssel egyenértékű a regisztrációt végző szervezet külső helyszínen lefolytatott eljárása is, ha azonos feltételekkel biztosítható az ügyfél személyazonosságának előzetes ellenőrzése.

b) A regisztráció során az igénylő személyazonosságát személyazonosság igazolására alkalmas hatósági igazolvány alapján ellenőrizni kell.

c) A regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét az igénylőnek nyilatkozatban, saját kezű aláírásával ellátva kell igazolnia.

d) A b) pont szerinti hatósági igazolvány azonosító adatait, a megadott adatok egyezését és a hatósági igazolvány érvényességét a regisztrációs szervezetnek közhiteles nyilvántartásban kell ellenőriznie. Amennyiben az adott hatósági igazolvány vonatkozásában ez megvalósítható, a hatósági igazolványt folyamatosan elérhető elektronikus nyilvántartásban kell ellenőrizni.

e) A regisztrációt végző szervezet regisztrációban részt vevő ügyintézőjének aláírásával kell igazolnia, hogy a hatósági igazolványon szereplő arckép megfeleltethető az igénylő arcának és az igazolványban szereplő aláírás azonos a c) pont szerinti nyilatkozatot igazoló aláírással.

f) Ha a regisztrációt végző szervezet a kriptográfiai hardver eszközt nem a c)- e) pontokban foglaltakat követően azonnal, ugyanazon a helyszínen adja át az igénylőnek, – ideértve ha az átadást más elektronikus aláírással kapcsolatos szolgáltató végzi – akkor a kriptográfiai hardver eszköz átadását megelőzően az átvételre jogosultságot a b), c) és e) pontban foglaltak szerinti eljárásnak megfelelően kell igazolni.

[EHR+ Ü] esetén:

g) **Elektronikus aláírás** közigazgatási felhasználása esetén a hitelesítés-szolgáltató az ügyintéző hatóság megkeresésére viszontazonosítást végez, melynek keretében:

- a hatóság a hitelesítés-szolgáltatónak megküldi:

  a) a megadott természetes személyazonosító adatokat (vagy azok egy részét),

b) a viszontazonosítás alapjául szolgáló ellenőrző adatot (tanúsítványt vagy más, a viszontazonosítást végző szervezetnél az ügyfél azonosítására alkalmas adatot), és

c) a viszontazonosítási kérést azonosító adatot.

- a a hitelesítés-szolgáltató összeveti a megadott természetes személyazonosító adatokat az általa kezelt, beazonosított természetes személyazonosító adatokkal, és válaszként megküldi a viszontazonosítást kérő hatóságnak

  a) az adatok egyezőségének vagy annak hiányának tényét, valamint

  b) a viszontazonosítási kérést azonosító adatot.

h) A hitelesítés-szolgáltató a g) pont szerinti viszontazonosítást elektronikus úton végzi, s ennek keretében:

- az elektronikus úton küldött viszontazonosítási kérés hitelességének ellenőrzése céljából az ügyintéző hatóság elektronikus aláírását ellenőrzi,
- hiteles viszontazonosítási kérés esetén a választ haladéktalanul megküldi.

[EHR+ K] esetén:

g) A köztisztviselők számára történő tanúsítvány kibocsátást megelőző regisztrációt az alábbiak kezdeményezhetik:

- a hatóságot képviselő természetes személy a hitelesítés-szolgáltató előtt, ha a regisztrációhoz magával viszi a hatóság által kiállított és közokiratba foglalt, a közigazgatási szerv nevét tartalmazó, a hivatal képviseletére feljogosító meghatalmazást;
- a hatóság, ha a regisztrációs szervezet a természetes személy azonosítását külső helyszíni regisztráció útján – szükség szerint a hatóság által kijelölt közigazgatási szerv közreműködésével – végzi el.

h) A g) pont első bekezdése szerinti (a hitelesítés-szolgáltató előtti) regisztráció esetén a hitelesítés-szolgáltató köteles a meghatalmazást kiállító hatóságot – a regisztrációban érintett köztisztviselő adatainak megadása nélkül – a tanúsítvány kibocsátásának tényéről és a hatóság által kiadott meghatalmazásban foglalt iktatószámról értesíteni.

3.2.4 Nem ellenőrzött előfizetői információk

Nincs megkötés.

3.2.5 Jogok, felhatalmazások ellenőrzése

Lásd 3.2.2 a).

3.2.6 Az együttműködési képességre vonatkozó követelmények

Nincs megkötés.

3.3 Azonosítás és hitelesítés kulcs megújítás kérelem esetén

3.3.1 Azonosítás és hitelesítés szokásos kulcs megújítás esetén

a) A szokásos kulcs megújítás előtt az igénylő írásban nyilatkozhat arról, hogy adatai változatlanok. Ebben az esetben a hitelesítés-szolgáltató képviselője az adatokat ellenőrzés nélkül elfogadhatja.

b) Amennyiben az igénylő adatai változtak, az igénylőnek az új tanúsítvány igénylése esetén szükséges azonosító adatokat kell benyújtania, s ezeket a hitelesítés-szolgáltató képviselőjének le kell ellenőriznie.

3.3.2 Azonosítás és hitelesítés visszavonást követő kulcs megújítás esetén

a) Visszavonást követő kulcs megújításra jelen Hitelesítési rend szerint nincs lehetőség.

3.4 Azonosítás és hitelesítés tanúsítvány visszavonási kérelem esetén

A Szolgáltatási Szabályzatban meghatározott.

4. A tanúsítvány életciklusra vonatkozó követelmények

4.1 Tanúsítványkérelem

4.1.1 Ki nyújthat be tanúsítványkérelmet

a) Tanúsítványkérelmet azok az előfizetők nyújthatnak be, akik előzetesen a hitelesítés-szolgáltatóval szerződéses kapcsolatot létesítettek.

b) A hitelesítés-szolgáltatónak azt megelőzően, hogy az előfizetővel szerződéses kapcsolatot létesít, tájékoztatnia kell az előfizetőt a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről.

c) Amennyiben az alany nem azonos az előfizetővel, őt is tájékoztatni kell kötelességeiről.

d) A hitelesítés-szolgáltatónak a b) pontban említett kikötéseket és feltételeket tartalmazó, közérthető nyelven megfogalmazott dokumentumot elektronikusan letölthető formában és tartós eszközön (pl. papírra vagy CD-re írva) egyaránt hozzáférhetővé kell tennie.

4.1.2 A tanúsítványigénylés folyamata és a résztvevők felelőssége

a) Az előfizetőnek a tanúsítványigénylés folyamatában meg kell adnia azon cím- és egyéb adatait, melyek alapján a későbbiekben az előfizetővel fel lehet venni a kapcsolatot.

b) A hitelesítés-szolgáltatónak nyilvántartásba kell vennie minden, az alany azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat.

c) A hitelesítés-szolgáltatónak nyilvántartásba kell vennie az előfizetővel aláírt megállapodást[2], beleértve az alábbiakat:

- annak megerősítését, hogy a regisztráció során megadott információ pontos[3].
- az előfizető nyilatkozatát arra vonatkozóan, hogy kötelezettségeit megismerte és azok betartását vállalja,
- az előfizető nyilatkozatát arra vonatkozóan, hogy a részére biztosított kriptográfiai hardver eszköz használatával kapcsolatos kötelezettségeit megismerte és azok betartását vállalja,
- az érintett hozzájárulását az egyes szolgáltatások során felhasznált információk hitelesítés-szolgáltató által történő nyilvántartásba vételéhez,
- azt, hogy az előfizető megköveteli-e, az alany pedig hozzájárul-e a tanúsítvány közzétételéhez és milyen feltételek mellett,
- [EHR+_Ü] esetén: azt, hogy az előfizető és az alany hozzájárul-e a titkosító magánkulcsokra opcionálisan biztosított letétbe helyezési és visszaállítási szolgáltatás igénybevételéhez, és milyen feltételek mellett.

[2] Az előfizető ezen megállapodás különböző pontjaihoz a regisztráció különböző fázisai során is hozzájárulhat. Például a tanúsítványban szereplő információk korrektségére vonatkozó megállapodás a megállapodás egyéb szempontjait követően is megkötheti.
[3] A fenti megállapodás elektronikus formát is ölthet.

- [EHR+_K] esetén: azt, hogy az előfizető és az alany hozzájárul-e a titkosító magánkulcsokra biztosított letétbe helyezési és visszaállítási szolgáltatás igénybevételéhez, és milyen feltételek mellett.

d) A fent megnevezett nyilvántartásokat meg kell őrizni a Szolgáltatási Szabályzatban vállalt időtartamig (de legalább a hatályos jogszabályokban előírt időtartamig), illetve jogi eljárásokban a tanúsítványon keresztüli bizonyításához szükséges ideig.

4.2 A tanúsítványkérelem feldolgozása

4.2.1 Az azonosítási és hitelesítési funkciók megvalósítása

a) A hitelesítés-szolgáltató a Szolgáltatási Szabályzatában meghatározott azonosítási és hitelesítési funkciókkal ellenőrzi a tanúsítványkérelem érvényességét.

4.2.2 A tanúsítványkérelem jóváhagyása vagy visszautasítása

a) A hitelesítés-szolgáltató a Szolgáltatási Szabályzatában meghatározott feltételek alapján elfogadja vagy visszautasítja a tanúsítványkérelmet.

4.2.3 A tanúsítványkérelem feldolgozásának időtartama

A Szolgáltatási Szabályzatban meghatározott.

4.3 Tanúsítvány kibocsátás

4.3.1 A hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

Nincs megkötés.

4.3.2 Az előfizető értesítése a tanúsítvány kibocsátásról

A Szolgáltatási Szabályzatban meghatározott.

4.4 Tanúsítvány elfogadás

4.4.1 A tanúsítvány elfogadás esetei

a) A tanúsítványt igénylő a tanúsítvány aktiválása (használatba vétele) előtt köteles visszaigazolni a tanúsítvány átvételét, és a tanúsítvány adatainak helyességét. A visszaigazolás egyben a Hitelesítési rend, a Szolgáltatási Szabályzat és az Általános szerződési feltételek, valamint az esetleges egyedi szerződéses kikötések elfogadását is jelenti.

4.4.2 A tanúsítvány közzététele a hitelesítés-szolgáltató által

A Szolgáltatási Szabályzatban meghatározott. A tanúsítvány nyilvánosságra hozatala csak az érintett előfizető, illetve alany hozzájárulása esetén megengedett.

4.4.3 A további szereplők értesítése a tanúsítvány kibocsátásról

Nincs megkötés.

4.5 Kulcspár- és tanúsítvány használat

4.5.1 Az alany magánkulcs- és tanúsítvány használata

a) Az alany magánkulcsát és tanúsítványát csak a hitelesítés-szolgáltatóval szerződésben rögzített korlátozásnak megfelelően használhatja.

b) Az alany csak a megfelelő tanúsítvány elfogadása után (lásd 4.4.) használhatja magánkulcsát.

c) Az alany a megfelelő tanúsítvány lejárta után nem használhatja tovább magánkulcsát.

d) Az alanynak az adott helyzetben általában elvárható gondosságot kell tanúsítania annak érdekében, hogy megelőzze magánkulcsának illetéktelen felhasználását.

e) Az alany különböző magánkulcsait csak olyan célokra és olyan alkalmazásokkal használhatja, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat" és „kiterjesztett kulcshasználat" mezőinek tartalmával (lásd még 6.1.7 és 7.1.2).

4.5.2 Az érintett felek nyilvános kulcs- és tanúsítvány használata

Annak érdekében, hogy az érintett fél megalapozottan hagyatkozhasson a tanúsítvánnyal igazolt kriptográfiai kulcspár használatával működő alkalmazásra, a kulcspár megfelelő használatát és a hozzá tartozó tanúsítványt az adott helyzetben tőle általában elvárható gondossággal ellenőriznie kell. Ennek során többek között az alábbiakra kell figyelemmel lennie:

a) Az érintett fél csak olyan célokra és olyan alkalmazásokkal fogadhat el nyilvános kulcsokat, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat" és „kiterjesztett kulcshasználat" mezőinek tartalmával.

b) Mielőtt egy tanúsítványba foglalt nyilvános kulcsot felhasználna, az érintett félnek ellenőriznie kell a tanúsítvány érvényességét, valamint azt, hogy a tanúsítvány nincs felfüggesztve, illetve visszavonva az érvényes visszavonási állapot információ alapján, a tanúsítványt kibocsátó szolgáltató szabályzatainak megfelelően.

c) Amennyiben ésszerű módon egy tanúsítványra kíván hagyatkozni, az érintett félnek figyelembe kell vennie a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban és a tanúsítványt kibocsátó szolgáltató szabályzatokban szerepel.

4.6 Tanúsítvány megújítás

A tanúsítvány megújítás az a folyamat, amelynek során a hitelesítés-szolgáltató úgy bocsát ki egy megújított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai (köztük a nyilvános kulcs is) változatlanok.

4.6.1 A tanúsítvány megújítás körülményei

a) A tanúsítvány megújítása akkor lehetséges, ha valamennyi alábbi feltétel teljesül:

- a tanúsítvány érvényes,
- a tanúsítvány nem szerepel a tanúsítvány visszavonási listán,
- a kezdeti regisztráció alkalmával rögzített, tanúsítványba foglalt összes adat még érvényes,
- a tanúsítványhoz tartozó magánkulcs nem kompromittálódott,

- a tanúsítvány még nem volt korábban megújítva.

4.6.2 Ki kérelmezheti a megújítást

a) A tanúsítvány megújítást olyan személy kezdeményezheti, aki a kezdeti tanúsítvány kérelem benyújtására is jogosult volt, vagy jelenlegi felhatalmazása alapján jogosult lett volna.

4.6.3 A tanúsítvány megújítási kérelmek feldolgozása

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy egy már korábban nála nyilvántartásba vett alany tanúsítványára vonatkozó megújítási kérelem teljes, pontos és kellőképpen hiteles legyen. Különösképpen:

a) A hitelesítés-szolgáltatónak ellenőriznie kell a tanúsítvány létezését és érvényességét, valamint azt, hogy az alany azonosságának és jellemzőinek igazolására használt információ még mindig érvényes-e.

b) Amennyiben a hitelesítés-szolgáltató bármely feltétele, illetve kikötése megváltozott, azokat közölnie kell az előfizetővel, és azok előfizető általi elfogadását a 4.1.2 c) pontjának megfelelően rögzíteni kell.

c) Amennyiben bármilyen az alanyra vagy az előfizetőre vonatkozó információ megváltozott, azt a 3.2.3 a pontnak, illetve szervezet képviselete esetén kiegészítésképpen a 3.2.2 pontnak megfelelően a hitelesítés-szolgáltatónak ellenőriznie kell, nyilvántartásba kell vennie, és ehhez az előfizetőhozzájárulását be kell szereznie.

d) A hitelesítés-szolgáltató csak akkor bocsáthat ki egy új tanúsítványt az alany korábbiakban tanúsított nyilvános kulcsának felhasználásával, ha annak kriptográfiai biztonsága még megfelelő az új tanúsítvány tervezett élettartamára, és nincsenek arra utaló jelek, hogy az alany magánkulcsa kompromittálódott.

A fent leírt eljárásnak az a célja, hogy a hitelesítés-szolgáltató meggyőződjön arról, hogy a tanúsítvány megújításra vonatkozó kérelmet az arra jogosult kérelmezi, az előfizető a megváltozott szolgáltatói feltételekről, kikötésekről tudomást szerezzen, azokat elfogadja, illetve a megújítás során a szolgáltató megbízható tanúsítványt állítson elő.

4.6.4 Az előfizető értesítése az új tanúsítvány kibocsátásáról

A Szolgáltatási Szabályzatban meghatározott.

4.6.5 A megújított tanúsítvány elfogadása

Lásd. a 4.4.1 pontban.

4.6.6 A megújított tanúsítvány közzététele

A Szolgáltatási Szabályzatban meghatározott.

4.6.7 A további szereplők értesítése a tanúsítvány kibocsátásról

Nincs megkötés.

4.7 Kulcscsere

A kulcscsere az a folyamat, amelynek során a hitelesítés-szolgáltató úgy bocsát ki egy megújított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai közül csak a nyilvános kulcs kerül lecserélésre.

4.7.1 A kulcscsere körülményei

a) Kulcscserére a következő esetekben lehet szükség:

- a tanúsítvány valamilyen okból visszavonásra került,
- a tanúsítvány lejárt,
- a magánkulcsot tartalmazó kriptográfiai hardver eszköz megsérült és nem használható.

4.7.2 Ki kérelmezheti a kulcscserét

a) A kulcscserét olyan személy kezdeményezheti, aki a kezdeti tanúsítvány kérelem benyújtására is jogosult volt, vagy jelenlegi felhatalmazása alapján jogosult lett volna.

4.7.3 A kulcscserére vonatkozó kérelmek feldolgozása

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy egy már korábban nála nyilvántartásba vett alany tanúsítványára vonatkozó kulcscsere kérelem teljes, pontos és kellőképpen hiteles legyen. Különösképpen:

a) A hitelesítés-szolgáltatónak ellenőriznie kell a tanúsítvány létezését és érvényességét, valamint azt, hogy az alany azonosságának és jellemzőinek igazolására használt információ még mindig érvényes-e.

b) Amennyiben a hitelesítés-szolgáltató bármely feltétele, illetve kikötése megváltozott, azokat közölnie kell az előfizetővel, és azok előfizető általi elfogadását a 4.1.2 c) pontjának megfelelően rögzítenie kell.

c) Amennyiben bármilyen, az alanyra vagy az előfizetőre vonatkozó információ megváltozott, azt a 3.2.3 a pontnak, illetve szervezet képviselete esetén kiegészítésképpen a 3.2.2 pontnak megfelelően a hitelesítés-szolgáltatónak ellenőriznie kell, nyilvántartásba kell vennie, és ehhez az előfizetőhozzájárulását be kell szereznie.

d) A hitelesítés-szolgáltatónak a megújítandó tanúsítványt (amennyiben annak érvényessége még nem járt le) a megújított tanúsítvány kibocsátása előtt vissza kell vonnia.

A fent leírt eljárásnak az a célja, hogy a hitelesítés-szolgáltató meggyőződjön arról, hogy a kulcscserére vonatkozó kérelmet az arra jogosult kérelmezi, az előfizető a megváltozott szolgáltatói feltételekről és kikötésekről tudomást szerezzen, valamint azokat elfogadja.

4.7.4 Az előfizető értesítése az új tanúsítvány kibocsátásáról

A Szolgáltatási Szabályzatban meghatározott.

4.7.5 A kulcscserével megújított tanúsítvány elfogadása

Lásd. a 4.4.1 pontban.

4.7.6 A kulcscserével megújított tanúsítvány közzététele

A Szolgáltatási Szabályzatban meghatározott.

4.7.7 A további szereplők értesítése a tanúsítvány kibocsátásról

Nincs megkötés.

4.8 Tanúsítvány módosítás

A tanúsítvány módosítás az a folyamat, amelynek során a hitelesítés-szolgáltató úgy bocsát ki egy módosított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai – a nyilvános kulcs kivételével – változnak, és a tanúsítvány az új adatokkal, valamint a régi nyilvános kulccsal kerül kiadásra.

4.8.1 A tanúsítvány módosítás körülményei

a) Tanúsítvány módosításra a következő esetekben lehet szükség:

- a tanúsítvány alanyra vonatkozó adatai – a nyilvános kulcs kivételével – megváltoztak.

4.8.2 Ki kérelmezheti a tanúsítvány módosítást

a) A tanúsítvány módosítást olyan személy kezdeményezheti, aki a kezdeti tanúsítvány kérelem benyújtására is jogosult volt, vagy jelenlegi felhatalmazása alapján jogosult lett volna.

4.8.3 A tanúsítvány módosításra vonatkozó kérelmek feldolgozása

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy egy már korábban nála nyilvántartásba vett alany tanúsítványára vonatkozó módosítási kérelem teljes, pontos és kellőképpen hiteles legyen. Különösképpen:

a) A hitelesítés-szolgáltatónak ellenőriznie kell a tanúsítvány létezését és érvényességét, valamint azt, hogy az alany azonosságának és jellemzőinek igazolására használt információ még mindig érvényes-e.

b) Amennyiben a hitelesítés-szolgáltató bármely feltétele, illetve kikötése megváltozott, azokat közölnie kell az előfizetővel, és azok előfizető általi elfogadását a 4.1.2 c) pontjának megfelelően rögzítenie kell.

c) Amennyiben bármilyen az alanyra vagy az előfizetőre vonatkozó információ megváltozott, azt a 3.2.3 a pontnak, illetve szervezet képviselete esetén kiegészítésképpen a 3.2.2 pontnak megfelelően a hitelesítés-szolgáltatónak ellenőriznie kell, nyilvántartásba kell vennie, és ehhez az előfizetőhozzájárulását be kell szereznie.

d) A hitelesítés-szolgáltató csak akkor bocsáthat ki egy új tanúsítványt az alany korábbiakban tanúsított nyilvános kulcsának felhasználásával, ha annak kriptográfiai biztonsága még megfelelő az új tanúsítvány tervezett élettartamára, és nincsenek arra utaló jelek, hogy az alany magánkulcsa kompromittálódott.

e) A hitelesítés-szolgáltatónak a módosítandó tanúsítványt a módosított tanúsítvány kibocsátása előtt vissza kell vonnia.

A fent leírt eljárásnak az a célja, hogy a hitelesítés-szolgáltató meggyőződjön arról, hogy a tanúsítvány módosítására vonatkozó kérelmet az arra jogosult kérelmezi, az előfizető a megváltozott szolgáltatói feltételekről, kikötésekről tudomást szerezzen és azokat elfogadja, illetve a módosítás során a szolgáltató megbízható tanúsítványt állítson elő.

4.8.4 Az előfizető értesítése az új tanúsítvány kibocsátásáról

A Szolgáltatási Szabályzatban meghatározott.

4.8.5 A módosított tanúsítvány elfogadása

Lásd. a 4.4.1 pontban.

4.8.6 A módosított tanúsítvány közzététele

A Szolgáltatási Szabályzatban meghatározott.

4.8.7 A további szereplők értesítése a tanúsítvány kibocsátásról

Nincs megkötés.

4.9 Tanúsítvány visszavonás és felfüggesztés

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy hiteles és érvényes tanúsítvány visszavonási (felfüggesztési) kérelmek esetén a tanúsítványok haladéktalanul visszavonásra (felfüggesztésre) kerüljenek, s erről az alanyok, előfizetők, illetve érintett felek hiteles és megbízható információt kapjanak.

4.9.1 A visszavonás körülményei

a) A hitelesítés-szolgáltató köteles intézkedni a tanúsítvány visszavonásáról az alábbi esetekben:

- a tanúsítvány megújítása (kulcscsere),
- a tanúsítvány módosítása (alanyra vonatkozó adatok változása),
- a szolgáltatással kapcsolatos – jogszabályban, a szolgáltatási szabályzatban vagy az általános szerződési feltételekben meghatározott – rendellenességről szerez tudomást, s ez a rendellenesség nem orvosolható,
- a hitelesítés-szolgáltató tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy a magánkulcs nem az aláíró kizárólagos birtokában van,
- a hitelesítés-szolgáltató tevékenységét befejezte,
- a visszavonást jogszabály kötelezővé teszi,
- a Szolgáltatási Szabályzatban meghatározott egyéb esetek.

4.9.2 Ki kérelmezheti a visszavonást

a) Tanúsítvány visszavonási kérelmet az alábbiak kezdeményezhetik:

- olyan személy, aki a kezdeti tanúsítvány kérelem benyújtására is jogosult volt, vagy jelenlegi felhatalmazása alapján jogosult lett volna,
- a hitelesítés-szolgáltató.

4.9.3 Visszavonási kérelemre vonatkozó eljárás

a) A hitelesítés-szolgáltató Szolgáltatási Szabályzatának dokumentálnia kell a tanúsítványok visszavonásának eljárásait, beleértve az alábbiakat:

- a kérelem beadásának módja,
- a visszavonási jelentések és kérelmek megerősítésére vonatkozó esetleges követelmények[4].
- eljárás abban az esetben, ha a bejelentő nem tudja jogosultságát igazolni.

b) A visszavonásra vonatkozó kérelmeket és jelentéseket hitelesíteni kell, és ellenőrizni kell, hogy hiteles forrásból származnak-e[5]. Az ilyen jellegű jelentéseket és kérelmeket meg kell erősíteni, amennyiben ezt a hitelesítés-szolgáltató szabályzatában megköveteli.

c) Egy visszavont tanúsítvány alanyát, és ahol ez alkalmazható az előfizetőt, tájékoztatni kell a tanúsítvány állapotának megváltozásáról.

d) Ha egy tanúsítvány véglegesen visszavonásra került (azaz nem felfüggesztésre), azt nem szabad érvényesre visszaállítani.

4.9.4 A visszavonási kérelemre vonatkozó kivárási idő

a) A hitelesítés-szolgáltatónak a visszavonási, illetve felfüggesztési kérelem fogadásától számított 3 órán belül meg kell állapítania a kérelem érvényességét (a kérelmező jogosultságát), és érvényes kérelem esetén a visszavonási állapot megváltozását a nyilvántartásában át kell vezetnie.

b) A visszavonási kérelemre vonatkozó kivárási idő betartása úgy is teljesíthető, hogy a kivárási időn belül a tanúsítványt a szolgáltató nem visszavonja, hanem felfüggeszti, és a visszavonást később – esetleg összetettebb felhasználó-azonosítást követően végzi el.

c) Az a) pontban foglaltak teljesítését követő 1 órán belül a hitelesítés-szolgáltatónak a visszavonási (illetve felfüggesztési) kérelem szerint módosított visszavonási állapotot közzé kell tennie.

4.9.5 A visszavonási eljárás maximális hossza

a) A hitelesítés-szolgáltató köteles a benyújtott visszavonási (felfüggesztési) kérelmeket haladéktalanul, minden más típusú tevékenysége (pl. tanúsítvány előállítás, kibocsátás) elé helyezve feldolgozni, és az arra jogosult által benyújtott kérelmeket teljesíteni.

b) A visszavonási eljárás maximális hossza 4 óra lehet (lásd 4.9.4).

[4] Például amennyiben a kompromittálódást egy harmadik fél jelentette, megkövetelhető az előfizető megerősítése.

[5] Amennyiben harmadik fél kérelmezi a visszavonást, a kérelem hitelessége nem biztos hogy ellenőrizhető, ezért a Szolgáltatási szabályzatban meghatározott kiegészítő ellenőrzések végrehajtásával lehet csak elfogadni.

4.9.6 Az érintett felek kötelezettsége a visszavonási információ ellenőrzésére

a) Amennyiben az érintett felek kellő gondossággal kívánnak eljárni a tanúsítvány visszavonási állapotának ellenőrzésekor, a tanúsítvány visszavonási információ hitelességéről és sértetlenségéről is meg kell győződniük.

4.9.7 A visszavonási lista kibocsátás gyakorisága

a) A hitelesítés-szolgáltató által kibocsátott tanúsítvány visszavonási listák érvényességi ideje legfeljebb 25 óra.

b) A hitelesítés-szolgáltatónak új visszavonási listát kell kibocsátania minden tanúsítványállapot változást követő 1 órán belül (lásd 4.9.8), de legkésőbb az utoljára kiadott visszavonási lista lejárata előtt.

4.9.8 A visszavonási lista előállítása és közzététele közötti idő maximális hossza

a) A visszavonási lista előállítása és közzététele között legfeljebb 1 óra telhet el (lásd 4.9.4 c).

4.9.9 Valósidejű tanúsítvány állapot ellenőrzés elérhetősége

a) Amennyiben a hitelesítés-szolgáltató valósidejű tanúsítvány állapot szolgáltatást is biztosít, a Szolgáltatási Szabályzatnak kell meghatároznia annak elérhetőségét.

4.9.10 A valósidejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények

a) Amennyiben a hitelesítés-szolgáltató valósidejű tanúsítvány állapot szolgáltatást is biztosít, a Szolgáltatási Szabályzatnak kell meghatároznia az ellenőrzésre vonatkozó követelményeket.

4.9.11 A visszavonási hirdetmények egyéb elérhető formái

Nincs megkötés.

4.9.12 A kulcs kompromittálódásra vonatkozó speciális követelmények

Nincs megkötés.

4.9.13 A felfüggesztés körülményei

A Szolgáltatási Szabályzatban meghatározott[6].

4.9.14 Ki kérelmezheti a felfüggesztést

A Szolgáltatási Szabályzatban meghatározott.

4.9.15 A felfüggesztési kérelemre vonatkozó eljárás

A Szolgáltatási Szabályzatban meghatározott.

6 A Szolgáltatási Szabályzatban kell meghatározni, hogy a tanúsítványok felfüggeszthetők-e, és ha igen, milyen körülmények között.

4.9.16 A felfüggesztés maximális hossza

A Szolgáltatási Szabályzatban meghatározott.

4.10 Tanúsítvány állapot szolgáltatások

A hitelesítés-szolgáltatónak a visszavont tanúsítványok listáját az általa kibocsátott tanúsítványokban meghatározott URL-en kell elérhetővé tennie[7].

4.10.1 Működési jellemzők

Nincs megkötés.

4.10.2 A szolgáltatás rendelkezésre állása

a) A hitelesítés-szolgáltatónak biztosítania kell a tanúsítványtár, valamint a szolgáltató által kibocsátott tanúsítványok használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét, 99%-os rendelkezésre állás mellett, ahol az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

b A hitelesítés-szolgáltatónak biztosítania kell a visszavonási nyilvántartások és a visszavonás kezelési szolgáltatás legalább 99%-os rendelkezésre állását, az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

4.10.3 Nem kötelező tulajdonságok

Nincs megkötés.

4.11 A tanúsítványelőfizetés vége

Nincs megkötés.

4.12 Kulcs letétbe helyezése és visszaállítása

4.12.1 Kulcsletét és visszaállítás rendje és szabályai

a) A hitelesítés-szolgáltatónak tilos az alany aláíró magánkulcsát letétbe helyeznie.

b) A hitelesítés-szolgáltatónak tilos az alany hitelesítő magánkulcsát letétbe helyeznie.

[EHR+ Ü] esetén:

c) A hitelesítés-szolgáltatónak (az alannyal kötött szerződés alapján, lásd 4.1.2) az alany titkosító magánkulcsát letétbe helyezheti, illetve visszaállíthatja

d) A hitelesítés-szolgáltató által a titkosító magánkulcsokra biztosított opcionális letétbe helyezési és visszaállítási szolgáltatására vonatkozó előírásokat külön dokumentumokban (a Kulcsvisszaállítási rendben és a Kulcsvisszaállítási szabályzatban) kell meghatározni.

7 Amennyiben a hitelesítés-szolgáltató valósidejű tanúsítvány állapot szolgáltatást is biztosít, akkor Szolgáltatási Szabályzatában vállalnia kell ennek a szolgáltatásnak az elérhetővé tételét is, az általa kibocsátott tanúsítványokban meghatározott URL-en.

[EHR+ K] esetén:

c) A hitelesítés-szolgáltató (az alannyal kötött szerződés alapján, lásd 4.1.2) az alany titkosító magánkulcsát letétbe kell helyeznie, illetve hiteles kérés esetén vissza kell állítania.

d) A hitelesítés-szolgáltató által a titkosító magánkulcsokra biztosított letétbe helyezési és visszaállítási szolgáltatására vonatkozó előírásokat külön dokumentumokban (a Kulcsvisszaállítási rendben és a Kulcsvisszaállítási szabályzatban) kell meghatározni.

4.12.2 Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nincs megkötés.

5. Elhelyezési, irányítási és működtetési előírások

A biztonsági előírásokról általában:

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy kellő, az elismert szabványoknak megfelelő adminisztratív és irányítási eljárások kerüljenek alkalmazásra. Különösképpen:

a) A hitelesítés-szolgáltatónak kockázat elemzést kell végrehajtania üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és védelmi intézkedések meghatározása érdekében.

b) A hitelesítés-szolgáltatónak felelősséget kell vállalnia minden hitelesítési szolgáltatásáért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki. A harmadik felek felelősségét a hitelesítés-szolgáltatónak egyértelműen meg kell határoznia, és megfelelő konstrukcióknak kell biztosítania azt, hogy a harmadik felek a hitelesítés-szolgáltató által megkövetelt összes ellenőrzés végrehajtására legyenek szorítva. A hitelesítés-szolgáltatónak felelősséget kell vállalnia valamennyi fél fentiekre vonatkozó gyakorlatának nyilvánosságra hozására.

c) A hitelesítés-szolgáltató vezetőségének az információ biztonságra vonatkozóan útmutatást kell adnia egy megfelelően magas szintű irányító fórumon keresztül, amely felelős a hitelesítés-szolgáltató informatikai biztonsági szabályzatának meghatározásáért, és e szabályzat által érintett valamennyi alkalmazott részére történő közzétételért.

d) A hitelesítés-szolgáltatón belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenn kell tartani. A biztonság szintjére hatást gyakorló bárminemű változtatást a hitelesítés-szolgáltató felső vezetésének kell jóváhagynia.

e) Rendszerbiztonsági szabályzatban dokumentálni kell, egyúttal meg kell valósítani és fenn kell tartani a hitelesítési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonság kezelési (ellenőrzési és üzemeltetési) eljárásait[8].

f) A hitelesítés-szolgáltatónak gondoskodnia kell az informatikai biztonság fenntartásáról akkor is, ha a hitelesítés-szolgáltató funkciókra vonatkozó felelősség más szervezethez, illetve egységhez lett kiadva.

g) A hitelesítés-szolgáltató felső vezetősége felelős gyakorlatai megfelelő megvalósításáért.
A hitelesítés-szolgáltató biztonsági műveleteit el kell különíteni az egyéb műveletektől.
A hitelesítés-szolgáltató biztonsági műveleteivel kapcsolatos felelősségek közé tartoznak az alábbiak:
- 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 (változásmenedzsment)
- folyamatos működés biztosítása,
- kockázatkezelés
- fizikai biztonság

[8] Ajánlott, hogy a rendszerbiztonsági szabályzat azonosítsa a nyújtott szolgáltatásokkal kapcsolatos valamennyi fontos célt és potenciális veszélyt, valamint az ezen veszélyek hatásainak elkerülése, illetve korlátozása érdekében szükséges védelmi intézkedéseket. Ajánlott leírnia az arra vonatkozó szabályokat, irányelveket és eljárásokat is, hogy a meghatározott szolgáltatásokat és az ezekkel kapcsolatos biztonsági garanciákat hogyan biztosítják.

E felelősségeket a hitelesítés-szolgáltató biztonsági műveletei kezelik, azokat nem szakértő üzemeltető személyzet csak megfelelő felügyelet és a felelősségrevonhatóságot biztosító ellenőrzési rend mellett hajthatja végre.

Az értékek osztályozása, minősítése és kezelése

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek. Különösképpen:

h) A hitelesítés-szolgáltatónak valamennyi informatikai értékéről leltárt kell vezetnie, ezek védelmi követelményeit osztályokba kell sorolnia, minősítenie kell a kockázat elemzés (lásd 5. a. pontot) eredményével összhangban.

5.1 Fizikai előírások

A hitelesítés-szolgáltatónak gondoskodnia kell 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 hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

a) Biztosítani kell az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.

b) Előírásokat kell érvényre juttatni az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

Tanúsítvány előállítással, alanyok kriptográfiai hardver eszközzel való ellátásával, visszavonás kezeléssel kapcsolatosan:

c) Fizikai védelmet kell biztosítani a tanúsítvány előállítás, az alanyok kriptográfiai hardver eszközzel való ellátása, illetve a visszavonás-kezelés szolgáltatások köré, egyértelműen meghatározott biztonsági körlet létrehozásával. Bármely más szervezettel megosztott résznek e körleten kívül kell esnie.

d) Fizikai és környezeti biztonsági előírásokat kell érvényre juttatni a rendszer erőforrásokat tartalmazó berendezéseknek, maguknak a rendszer erőforrásoknak, illetve a működésük támogatására használt berendezések megvédése érdekében. A hitelesítés-szolgáltató tanúsítvány előállítás, kriptográfiai hardver eszköz ellátás és visszavonás kezelés szolgáltatásainak fizikai- és környezeti biztonsága érdekében foglalkozni kell az alábbiakkal: a fizikai hozzáférés szabályozása, természeti katasztrófa elleni védelem, villámvédelem és tűzbiztonság, a támogató infrastruktúra (például áram, telekommunikáció, klíma berendezés) meghibásodása, az építmény összeomlása, vízvezeték szivárgás, talajvíz elleni védelem, lopás, betörés és behatolás elleni védelem, katasztrófa utáni helyreállítás[9].

e) Előírásokat kell érvényre juttatni annak megakadályozása érdekében, hogy a hitelesítés-szolgáltató szolgáltatásokkal kapcsolatos berendezéseit, információkat, adathordozót és szoftvereket jogosulatlanul elvigyék a helyszínről.

[9] A fizikai és környezeti biztonsággal kapcsolatban útmutatóként lásd az MSZ/ISO/IEC 17799 dokumentumot.

5.1.2 Fizikai hozzáférés

a) A szolgáltatás nyújtásával összefüggésben használt elektronikus aláírási termékeket, illetve azokat a helyiségeket, amelyekben a szolgáltató ilyen termékeket helyez el, a jogosulatlan hozzáféréstől fizikailag is védeni kell, a jogosulatlan személyek bejutását kizárva.

b) A hitelesítés-szolgáltatónak meg kell akadályoznia, hogy az a) pontban említett helyiségekbe olyan személyek jussanak be, akik erre nem jogosultak.

c) A belépésre jogosultak belépésének időpontját, tartozkodásának célját, kilépésének időpontját naplóban kell rögzíteni.

5.1.3 Áramellátás és légkondicionálás

Lásd 5.1.1 d) pontot.

5.1.4 Beázás és elárasztódás veszély kezelése

Lásd 5.1.1 d) pontot.

5.1.5 Tűzmegelőzés és tűzvédelem

Lásd 5.1.1 d) pontot.

5.1.6 Adathordozók tárolása

a) Az adathordozó eszközöket biztonságosan kell kezelni azok sérülése, ellopása és jogosulatlan hozzáférés elleni védelme érdekében.

b) Az összes adathordozó eszközt biztonságosan kell kezelni az adat-minősítési rendszer követelményeinek megfelelően (lásd 5. h.).

5.1.7 Hulladék megsemmisítése

a) Az érzékeny adatokat tartalmazó adathordozó eszközt - amennyiben azokra már nincs szükség - biztonságosan kell megsemmisíteni.

5.1.8 A mentési példányok fizikai elkülönítése

Nincs megkötés.

5.2 Eljárásbeli előírások

A hitelesítés-szolgáltató eljárásbeli előírásainak meg kell felelniük a személyes adatok védelmére és a minősített adatok, valamint a jogszabályban nevesített, vagy az előfizetővel kötött szerződésben meghatározott titokfajták kezelésére vonatkozó jogszabályi és mértékadó dokumentumokban meghatározott, a legjobb gyakorlatot tükröző műszaki-szervezési előírásoknak. (lásd 9.15 a)

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse.

a) A személyzetnek olyan adminisztratív és kezelési eljárásokat és folyamatokat kell végeznie, amely szinkronban van a hitelesítés-szolgáltató informatika biztonság kezelési (ellenőrzési és üzemeltetési) eljárásaival (lásd 5. e. pontot).

5.2.1 Bizalmi munkakörök

a) A hitelesítés-szolgáltató szolgáltatási és informatikai biztonsági szabályzatában meghatározott bizalmi munkaköröket és felelősségeket munkaköri leírásokban kell dokumentálni. Egyértelműen azonosítani kell azokat a bizalmi munkaköröket, amelyektől a hitelesítés-szolgáltató működésének biztonsága függ.

b) Az alábbi munkakörök tartoznak a bizalmi munkakörök közé:

- Biztonsági tisztviselő: a szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért általánosan felelős személy.
- Rendszeradminisztrátor és üzemeltető: az informatikai rendszer telepítését, konfigurálását, karbantartását, valamint az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.
- Független rendszervizsgáló: a hitelesítés-szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a hitelesítés-szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.
- Regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

c) Bizalmi munkakörökbe a biztonságért felelős felső vezetésnek kell formálisan kineveznie a hitelesítés-szolgáltató munkatársait.

d) Üzemeltetési eljárásokat kell kidolgozni valamennyi olyan bizalmi és adminisztratív feladatra, amely hatást gyakorol a hitelesítési szolgáltatásokra, s ezeket az eljárásokat be kell tartani.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

a) A hitelesítés-szolgáltató (ideiglenes és állandó) munkatársai munkaleírásainak (lásd 5.2.1 a.) támogatniuk kell a feladatok szétválasztásának és a legkisebb meghatalmazás elvének szempontjait. A munkaleírásoknak (lásd 5.3 c.) többek között meg kell határozniuk az egyes feladatokhoz szükséges létszámot is.

b) Csak védett környezetben (5.1), legalább két, bizalmi munkakört (5.2.1) betöltő, erre feljogosított személy együttes részvételével, más személyek jelenlétét kizárva kerülhet sor az alábbi funkciók végrehajtására:

- a hitelesítés-szolgáltató saját szolgáltatói kulcsának előállítása (6.1.1),
- a hitelesítés-szolgáltató szolgáltatói magánkulcsának mentése (6.2.4),
- a hitelesítés-szolgáltató szolgáltatói magánkulcsának visszaállítása (6.2.2),
- a hitelesítés-szolgáltató szolgáltatói magánkulcsának megsemmisítése (6.2.10).

5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

a) A hitelesítés-szolgáltató személyzetét megfelelően azonosítani és hitelesíteni kell, mielőtt a tanúsítvány kezeléssel kapcsolatos kritikus alkalmazásokat használnák.

5.2.4 Egymást kizáró munkakörök

a) A bizalmi munkakörök közötti személyi átfedésekre az alábbi korlátozások vonatkoznak:

- a biztonsági tisztviselő nem töltheti be a független rendszervizsgáló munkakört.

5.3 Személyzetre vonatkozó előírások

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy személyzeti gyakorlata fokozza és támogassa a hitelesítés-szolgáltató működésének megbízhatóságát. Különösképpen:

a) A hitelesítés-szolgáltatónak kellő számú, a hitelesítési szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet kell alkalmaznia.

b) A hitelesítés-szolgáltató valamennyi bizalmi munkakört betöltő munkatársának függetlennek kell lennie minden olyan ütköző érdektől, ami hátrányosan érinthetné a hitelesítés-szolgáltató tevékenységeinek semlegességét, a szolgáltatás megbízhatóságát és biztonságát.

c) A hitelesítés-szolgáltató (ideiglenes és állandó) munkatársainak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaleírásokkal kell rendelkezniük. A munkaleírásoknak meg kell határozniuk a beosztás érzékenységét, a feladatok elvégzéséhez szükséges hozzáférési jogosultságok alapján. Ahol erre szükség van, meg kell különböztetni az általános funkciókat és a hitelesítés-szolgáltató specifikus funkciókat. A munkaleírásoknak meg kell határozniuk az egyes feladatokhoz szükséges létszámot is. Ajánlott, hogy a munkaleírások tartalmazzák a szakismeretre és a tapasztalatra vonatkozó követelményeket is.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

a) A hitelesítés-szolgáltatónak olyan személyzetet kell alkalmaznia, amely rendelkezik a kínált szolgáltatáshoz szükséges és megfelelően naprakész tudással és tapasztalattal.

b) Olyan vezető személyzetet kell alkalmazni, mely tapasztalattal rendelkezik az elektronikus aláírási technológia terén, ismeri a bizalmi munkakörökre vonatkozó biztonsági elvárásokat, valamint gyakorlattal rendelkezik az informatika biztonság és a kockázat elemzés területein.

5.3.2 Előélet vizsgálatára vonatkozó eljárások

a) A hitelesítés-szolgáltatónak nem szabad bizalmi munkakörbe, illetve a vezetőségbe kineveznie olyan személyt, aki bűncselekményért, illetve más olyan vétségért el lett ítélve, amely beosztást illető alkalmasságát befolyásolja. A munkatársaknak nem szabad hozzáférniük biztonsági funkciókhoz mindaddig, amíg a szükséges, személyükre és alkalmasságukra vonatkozó ellenőrzések végrehajtása meg nem történik.

5.3.3 Kiképzési követelmények

a) Az üzemeltető személyzetet a rendszer használatba vétele előtt ki kell képezni

- a nyilvános kulcsú infrastruktúra elméletéből,
- a rendszer használatáról,
- a regisztrációs, tanúsítási és visszavonási eljárásrendekről,
- az egyes tevékenységek jogi következményeiről,

- az informatikai biztonsági követelményekről,
- a Hitelesítési rend és a Szolgáltatási Szabályzat alkalmazásának jelentőségéről.

b) A képzést meg kell ismételni minden, a rendszerben történő változás után (a változás által érintett területen).

5.3.4 Továbbképzési gyakoriságok és követelmények

A Szolgáltatási Szabályzatban meghatározott.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs megkötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

Nincs megkötés.

5.3.7 Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

Nincs megkötés.

5.3.8 A személyzet számára biztosított dokumentációk

a) A személyzet számára biztosítandó dokumentációknak tartalmazniuk kell az 5. e. pontban említett rendszerbiztonsági szabályzatot.

5.4 Naplózási eljárások

A hitelesítés-szolgáltató Szolgáltatási Szabályzatának kell meghatároznia (az 5.4.1–5.4.8 pontok szempontrendszere alapján), hogy a biztonságos környezet fenntartása érdekében a hitelesítés-szolgáltató milyen eseménynaplózó és ellenőrző rendszereket valósít meg.

A jelen dokumentumban tárgyalt Hitelesítési rendek csak a tanúsítványokra vonatkozó adatok (regisztrációs információk, a hitelesítés-szolgáltató kulcsgondozási és tanúsítványgondozási eseményeire vonatkozó fontosabb információk) naplózási követelményeit határozzák meg.

Ezen belül viszont fontos, általános követelmények az alábbiak:

a) A hitelesítés-szolgáltató környezetére, kulcs- és tanúsítványgondozására használt óra szinkronizálására vonatkozó fontosabb események pontos időpontját is rögzíteni kell[10].

b) Biztosítani kell a hitelesítés-szolgáltató személyzet felelősségre vonhatóságát tevékenységéért, például az eseménynapló megőrzésén keresztül.

5.4.1 A tárolt események típusai

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

[10] Ajánlott, hogy a hitelesítés-szolgáltató Szolgáltatási szabályzatában ismertetve legyen az események időzítéséhez használt óra pontossága, és az, hogy ez a pontosság hogyan van biztosítva.

a) A naplózandó speciális események és adatok körét a hitelesítés-szolgáltatónak (a Szolgáltatási Szabályzatában) dokumentálnia kell.

b) A következő események naplózása feltétlenül szükséges:

- a működtető rendszerek környezetében bekövetkező, illetve a kulcsok és tanúsítványok kezelésével kapcsolatos események,
- a naplózási funkció elindítása és leállítása,
- a naplózási paraméterek megváltoztatása,
- a naplózás tárolási hibája miatt végzett tevékenységek.

A regisztrációval kapcsolatosan:

c) A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy naplózásra kerüljön valamennyi regisztrációval kapcsolatos esemény, köztük a tanúsítvány megújításra, módosítására, illetve kulcscserére vonatkozó kérelmek, és e kérelmek jóváhagyásával kapcsolatos események is.

A tanúsítvány előállítással kapcsolatosan:

d) A hitelesítés-szolgáltatónak naplóznia kell a saját szolgáltatói kulcsai életciklusával kapcsolatos összes eseményt.

e) A hitelesítés-szolgáltatónak naplóznia kell a saját tanúsítványai életciklusával kapcsolatos összes eseményt.

f) A hitelesítés-szolgáltatónak naplóznia kell az általa kibocsátott tanúsítványok életciklusával kapcsolatos összes eseményt.

Az alanyok kriptográfiai hardver eszközzel való ellátásával kapcsolatosan:

g) A hitelesítés-szolgáltatónak naplóznia kell minden általa gondozott kulcs életciklusával kapcsolatos eseményt.

h) A hitelesítés-szolgáltatónak naplóznia kell a kriptográfiai hardver eszközök készítésével és átadásával kapcsolatos valamennyi eseményt.

A visszavonás és felfüggesztés kezeléssel kapcsolatosan:

i) A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy a visszavonás és a felfüggesztés kezeléssel kapcsolatos összes kérés és jelentés naplózva legyen.

5.4.2 A napló fájl feldolgozásának gyakorisága

Az alábbi követelmények kielégítésével folyamatos ellenőrzés biztosítható a hitelesítés-szolgáltató/regisztrációs szervezet erőforrásaihoz történő illetéktelen, vagy szokatlan hozzáférési kísérletek vonatkozásában:

a) Folyamatos felügyelő és riasztó eszközöket kell biztosítani, hogy a hitelesítés-szolgáltató képes legyen felismerni, regisztrálni az erőforrásaihoz történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre[11].

b) A visszavonás állapotokat kezelő alkalmazásnak hozzáférés ellenőrzést kell érvényesítenie a visszavonás állapot információ módosítására irányuló próbálkozások esetében.

[11] A hitelesítés-szolgáltató erre használhat például egy behatolás észlelő rendszert, vagy hozzáférés ellenőrzést felügyelő és riasztási eszközöket.

c) A hitelesítés-szolgáltatónak biztosítania kell a rendszeres napló fájl kiértékeléseket.

5.4.3 A napló fájl megőrzési időtartama

A naplóadatokat archiválni szükséges. Az archívum megőrzési idejét lásd az 5.5.2 pontban.

5.4.4 A napló fájl védelme

a) A naplózott adatállománynak tartalmaznia kell a naplózott esemény bekövetkezésének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az események kiváltásában közreműködő felhasználó vagy más érintett személy nevét.

b) A naplózott adatállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személy, elsősorban a független rendszervizsgáló férhessen hozzá.

c) A napló kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása.

5.4.5 A napló fájl mentési eljárásai

A napló fájlról rendszeresen mentést kell készíteni.

5.4.6 A naplózás adatgyűjtési rendszere (belső vagy külső)

Nincs megkötés.

5.4.7 Az eseményeket kiváltó alanyok értesítése

Nincs megkötés.

5.4.8 Sebezhetőség felmérése

Nincs megkötés.

5.5 Adatok archiválása

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy a tanúsítványokra vonatkozó minden lényeges információ rögzítésre és megfelelő ideig tárolásra kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében[12].

5.5.1 Az archivált adatok típusai

a) A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy archiválásra kerüljön az összes regisztrációs információ, beleértve az alábbiakat is:

- a kérelmező által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa;

[12] A tanúsítványokra vonatkozó adatok regisztrációs információkat és a hitelesítés-szolgáltató környezeti, kulcsgondozási és tanúsítványgondozási eseményeire vonatkozó fontosabb információkat tartalmaznak.

- az azonosító dokumentumok egyedi azonosító adatai (például a kérelmező személyi igazolvány száma);
- a kérelmező és azonosító dokumentumok (beleértve az aláírt, előfizetővel kötött megállapodást (lásd 4.1.2 c) pontja) másolatainak tárolási helyszíne;
- az előfizetővel kötött megállapodás esetleges egyedi választásai (például a tanúsítvány közzétételéhez történő hozzájárulás);
- a kérelmet elfogadó regisztrációs ügyintéző azonosítója;
- az azonosító dokumentumok ellenőrzéséhez használt módszer és adatbázis;
- a fogadó hitelesítés-szolgáltató és/vagy a küldő regisztrációs szervezet neve, amennyiben ezek értelmezhetők.

b) A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy archiválásra kerüljön a tanúsítvány előállítására, az alanyok kriptográfiai hardver eszközzel való ellátására, valamint a visszavonás kezelésére vonatkozó valamennyi naplóbejegyzés (lásd 5.4.1.d)-i) pontokat).

c) A hitelesítés-szolgáltató Szolgáltatási Szabályzatának kell meghatároznia azon eseményeket, mely a fent említett naplóbejegyzéseken túl kerülnek archiválásra, a biztonságos környezet fenntartásának, valamint a szolgáltatás megbízhatóságának utólagos ellenőrizhetősége és bizonyíthatósága céljából.

5.5.2 Az archívum megőrzési időtartama

a) A tanúsítványokkal kapcsolatos elektronikus információkat – beleértve az azok előállításával összefüggőket is – és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejártától számított 10 évig, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikusan aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig meg kell őrizni.

b) Az a) pontban meghatározott adatokon kívüli naplózott adatokat a keletkezésüktől, a Szolgáltatási Szabályzatot és annak módosításait pedig hatályon kívül helyezésétől számított 10 évig meg kell őrizni, illetve megőrzéséről gondoskodni kell.

c) A biztonságos környezet fenntartásának utólagos ellenőrizhetősége és bizonyíthatósága érdekében archivált egyéb naplóbejegyzések megőrzési időtartamát a hitelesítés-szolgáltató Szolgáltatási Szabályzatának kell meghatároznia.

5.5.3 Az archívum védelme

a) Az archivált adatállomány minden bejegyzését védeni kell a jogosulatlan módosítástól, törléstől, megsemmisítéstől, illetve biztosítani kell azt, hogy az adatállomány tartalmához jogosulatlanul ne férhessenek hozzá.

b) Az elektronikus formában tárolt archivált adatállományt legalább fokozott biztonságú aláírással és időbélyegzővel kell ellátni.

c) A hitelesítés-szolgáltatónak biztosítania kell, hogy mindaddig, amíg az archivált adatokat őrzi, azok hitelesek maradjanak.

5.5.4 Az archívum mentési folyamatai

Nincs megkötés.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Lásd 5.5.3 b) pontját.

5.5.6 Az archívum gyűjtési rendszere (belső vagy külső)

Nincs megkötés.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

a) A hitelesítés-szolgáltatónak biztosítania kell, hogy mindaddig, amíg az archivált adatokat őrzi, az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

b) A tanúsítványokra vonatkozó adatokat rendelkezésre kell bocsátani, ha azokra jogi eljárásokban bizonyíték nyújtása céljából szükség van.

c) Az alanynak, illetve az adatvédelmi követelmények korlátozásain belül az előfizetőnek hozzá kell tudniuk férni az alanyra vonatkozó regisztrációs és egyéb információkhoz.

5.6 Kulcscsere

Nincs megkötés.

5.7 Kompromittálódást és katasztrófát követő helyreállítás

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy katasztrófa esetén, beleértve a saját szolgáltatói magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, az üzemeltetés a lehető legrövidebb időn belül helyreálljon.

5.7.1 Váratlan esemény és kompromittálódás kezelési eljárások

a) A hitelesítés-szolgáltatónak a rendkívüli üzemeltetési helyzetek esetére (különösen a kompromittálódás és a katasztrófa bekövetkezésére) olyan eljárást kell kidolgoznia, amely lehetővé teszi a megbízható szolgáltatás mielőbbi helyreállítását.

b) A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását meg kell, hogy előzze.

5.7.2 Meghibásodott számítási erőforrások, szoftverek és/vagy adatok

a) A hitelesítés-szolgáltató üzlet folytonossági terve (illetve katasztrófa utáni helyreállítási terve) a kritikus szoftver/hardver komponensek meghibásodásával, mint katasztrófa helyzettel kell, hogy foglalkozzon. Ilyen esetekben a tervezett eljárásokat érvénybe kell léptetni annak érdekében, hogy az üzemeltetés, amint csak lehetséges, helyreálljon.

b) A biztonsági események és hibás működések által okozott kárt eseményjelentés és válaszadás eljárások használatán keresztül minimalizálni kell.

c) A hitelesítés-szolgáltatónak időben és összehangoltan fel kell lépnie 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.

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárások

a) Saját magánkulcsának kompromittálódása esetén a hitelesítés-szolgáltatónak legalább az alábbiakat kell vállalnia:

- A kompromittálódásról tájékoztatnia kell az összes előfizetőt, érintett felet és egyéb olyan más hitelesítés-szolgáltatót, amellyel megállapodása, illetve másféle kialakult kapcsolata van.
- Jeleznie kell, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok és visszavonási állapot információk már nem érvényesek.

b) Előfizetőnek kibocsátott tanúsítványhoz tartozó magánkulcs kompromittálódása esetén a hitelesítés-szolgáltatónak legalább az alábbiakat kell vállalnia:

- A kompromittálódásról (a visszavonás kezelés, illetve visszavonás állapot szolgáltatásokon keresztül) tájékoztatnia kell az összes érintett felet.

5.7.4 Működés folyamatosságának biztosítása katasztrófát követően

a) Természeti vagy más egyéb katasztrófát követően a hitelesítés-szolgáltató üzlet folytonossági terve (illetve katasztrófa utáni helyreállítási terve) által megtervezett eljárásokat érvénybe kell léptetni annak érdekében, hogy az üzemeltetés mielőbb helyreálljon.

b) Egy katasztrófát követően (ahol ez ésszerű), a hitelesítés-szolgáltatónak lépéseket kell tennie a katasztrófa ismételt bekövetkezésének megakadályozására.

5.8 Hitelesítésszolgáltató vagy regisztrációs szervezet leállítása

A hitelesítés-szolgáltatónak a jogszabályokban előírtaknak megfelelően gondoskodnia kell a szolgáltatásainak megszüntetéséből származó, az előfizetőket és az érintett feleket érintő potenciális zavar minimalizálásáról. Különösképpen gondoskodnia kell arról, hogy a jogi eljárásokhoz szükséges tanúsítvány nyilvántartások fenn legyenek tartva.

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

a) Mielőtt a hitelesítés-szolgáltató leállítja szolgáltatásait, legalább az alábbi eljárásokat végre kell hajtania:

- A hitelesítés-szolgáltatónak legalább 60 nappal a leállítás előtt értesítenie kell az általa kibocsátott és még vissza nem vont tanúsítványok tulajdonosait, valamint az NHH-t,
- A hitelesítés-szolgáltatónak legalább 20 nappal a leállítás előtt vissza kell vonnia az általa kibocsátott és még vissza nem vont tanúsítványokat, de nyilvánosságra hozatali kötelezettségének egészen a leállításig továbbra is eleget kell tennie,
- A hitelesítés-szolgáltatónak intézkednie kell az iránt, hogy legkésőbb a leállításig, más – vele azonos besorolású – szolgáltató átvegye nyilvántartásait és ellássai feladatait
- A hitelesítés-szolgáltatónak tájékoztatnia kell az összes előfizetőt, érintett felet és azokat a más hitelesítés-szolgáltatókat, melyekkel megállapodásai, illetve másféle kialakult kapcsolatai vannak.
- A hitelesítés-szolgáltatónak meg kell szűntetnie a tanúsítványok kibocsátását és megújítását.
- A hitelesítés-szolgáltatónak meg kell szűntetnie a tanúsítványok kibocsátási folyamatában a hitelesítés-szolgáltató nevében eljáró alvállalkozások összes felhatalmazását.
- A hitelesítés-szolgáltatónak meg kell tennie a szükséges lépéseket, hogy a regisztrációs információ (lásd 3.2.3.d)) és az eseménynapló archívumok (lásd 5.5.1 b)) fenntartására

vonatkozó kötelezettségeket átruházza arra az időtartamra, amelyről az előfizetőket és az érintett feleket tájékoztatta, de legalább a hatályos jogszabályokban előírt időtartamra (lásd 4.1.2 d)).

- A hitelesítés-szolgáltatónak fenn kell tartania, vagy egy megbízható félre kell átruháznia azon kötelezettségét, hogy szolgáltatásaihoz kapcsolódó nyilvános kulcsát vagy tanúsítványait elérhetővé tegye az érintett felek számára, a jelen Hitelesítési rendben, illetve a Szolgáltatási Szabályzatában meghatározott időtartamig.
- A hitelesítés-szolgáltatónak magánkulcsait meg kell semmisítenie, illetve vissza kell vonni a használatból a (6.2.10) alatt meghatározottak szerint.

b) A hitelesítés-szolgáltatónak tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést kell készítenie. A mentett adatállományokat védeni kell a jogosulatlan módosítástól, illetve biztosítani kell azt, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá. Biztosítani kell továbbá, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

c) A hitelesítés-szolgáltató Szolgáltatási Szabályzatának tartalmaznia kell a szolgáltatás leállítására vonatkozó előírásokat. Ennek magában kell foglalnia az alábbiakat:

- az érintettek értesítését,
- saját kötelezettségeinek más felekre történő átruházását,
- a már kibocsátott, de még le nem járt tanúsítványok visszavonási állapotának a kezelését.

6. Műszaki biztonsági intézkedések

A hitelesítés-szolgáltatónak módosítás ellen védett megbízható rendszereket és termékeket[13] kell használnia[14] a biztonsági osztályba sorolás szintjével arányosan. ([1] 3. melléklet (f).)

6.1 Kulcspár előállítása és telepítése

A hitelesítés-szolgáltatónak gondoskodnia kell valamennyi általa (saját maga, címtárak, regisztrációs szervezetek, illetve alanyok számára) előállított magánkulcs biztonságos és az ipari szabványoknak, valamint a hatályos jogszabályi előírásoknak megfelelő előállításáról.

6.1.1 Kulcspár előállítás

A hitelesítés-szolgáltató saját kulcspár előállítása:

a) A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), legalább két, bizalmi munkakört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, más személyek jelenlétét kizárva kell végezni.

b) A hitelesítés-szolgáltató kulcs előállítását olyan eszközön belül kell végrehajtani, amely:

- megfelel a FIPS 140 [2] 3-as, illetve annál magasabb szintű követelményeinek, vagy
- megfelel a CEN 14167-2 [4] munkacsoport egyezmény követelményeinek, vagy
- olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [3] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten van értékelve. Ezt a rendszert a jelen dokumentum követelményeinek megfelelő olyan biztonsági rendszertervnek, vagy védelmi profilnak kell megalapoznia, mely kockázat elemzésen alapul és figyelembe veszi a fizikai és egyéb nem műszaki biztonsági intézkedéseket is.

c) A hitelesítés-szolgáltató által történő RSA kulcspár előállítást az [1] 18.§ szerint kiadott NHH határozatban szereplő, RSA kulcspár előállításra alkalmasnak elismert algoritmussal kell megvalósítani.

A hitelesítés-szolgáltató által más felek számára előállított kulcspár előállítása:

d) A hitelesítés-szolgáltató által más felek (pl. bizalmi munkakört betöltő saját munkatársai és az alanyok) számára előállított kulcsok előállítását fizikailag védett környezetben kell végezni, kizárólag bizalmi munkakört betöltő személyek részvételével.

e) a hitelesítés-szolgáltató által más felek (pl. bizalmi munkakört betöltő saját munkatársai és az alanyok) számára előállított kulcsokat olyan algoritmussal kell előállítani, melyet az [1] 18.§-a szerint kiadott NHH határozat erre a felhasználásra alkalmasnak ismer el.

[13] A megbízható rendszerek követelményei biztosíthatóak például olyan rendszerek használatával, amelyek kielégítik egy megfelelő, az MSZ/ISO/IEC 15408 [3], illetve azzal egyenértékű dokumentum alapján meghatározott védelmi profilt (vagy védelmi profilokat).

[14] Ajánlott, hogy a hitelesítés-szolgáltató szolgáltatásaira vonatkozóan végrehajtott kockázat elemzés (lásd 5. a.) azonosítsa azokat a kritikus szolgáltatásokat, amelyekhez megbízható rendszerek kellenek, illetve a szükséges garanciális szinteket.

f) A hitelesítés-szolgáltató a más felek számára előállított aláíró magánkulcsot csak a szolgáltatást igénybe vevő személy kriptográfiai hardver eszközében tárolhatja. Amennyiben a magánkulcsot a kriptográfiai hardver eszközön kívül hozzák létre, az aláíró magánkulcs kriptográfiai hardver eszközön kívüli minden másolatát azonnal törölni kell, amint a magánkulcs a kriptográfiai hardver eszközbe kerül. Az aláíró magánkulcs másolatát olyan módon kell törölni, hogy annak további használata lehetetlenné váljon.

6.1.2 Magánkulcs eljuttatása az előfizetőhöz

a) A hitelesítés-szolgáltató által más felek számára előállított magánkulcsokat a címzett félhez történő továbbításig biztonságos módon kell tárolni.

b) A más felekhez olyan módon kell a magánkulcsot továbbítani, hogy a kulcs titkossága ne sérüljön.

c) A kriptográfiai hardver eszköz elkészítését a hitelesítés-szolgáltatónak biztonságosan ellenőriznie kell.

d) A kriptográfiai hardver eszközt biztonságosan kell tárolni és szétosztani.

e) A hitelesítés-szolgáltatónak biztosítania kell, hogy a kriptográfiai hardver eszközt csak a valódi, hitelesített címzett vehesse át.

6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

a) A regisztrációs szervezettől az ott (kriptográfiai hardver eszközön) előállított kulcspár nyilvános kulcs részét olyan módon kell a tanúsítvány létrehozását végző hitelesítés-szolgáltatóhoz eljuttatni, ami biztosítja a továbbított adat sértetlenségét, valamint a feladó hitelességét.

6.1.4 A hitelesítésszolgáltató nyilvános kulcsának közzététele az érintett felek számára

a) A hitelesítés-szolgáltatónak a saját szolgáltatói nyilvános kulcsát tartalmazó, a Közigazgatási Gyökér Hitelesítés-Szolgáltató által kibocsátott tanúsítványt elérhetővé kell tennie az érintett felek számára.

6.1.5 Kulcsméretek

A hitelesítés-szolgáltató saját kulcsának mérete:

a) A hitelesítés-szolgáltató RSA szolgáltatói kulcsa legalább 2048 bites legyen.

A hitelesítés-szolgáltató által más felek számára előállított kulcsok mérete:

b) a hitelesítés-szolgáltató által más felek (címtárak, regisztrációs szervezetek és alanyok) számára előállított RSA kulcsok hossza legalább 1024 bites legyen.

6.1.6 Nyilvános kulcs paraméterek előállítása, a paraméterek ellenőrzése

Nincs előírás.

6.1.7 A kulcs használat célja (az X.509 v3 kulcshasználati mező tartalmának megfelelően)

a) A hitelesítés-szolgáltató (ezen Hitelesítési rend keretében) természetes személyek számára, fokozott biztonságú aláírásra használható aláíró, valamint hitelesítő és titkosító tanúsítványt bocsáthat ki, melyekre teljesülnek az alábbiak:

- az aláíró tanúsítvány kulcshasználati mezője kritikus, és a mezőben a "NonRepudiation" bit van „true” értékre beállítva, s ezen kívül legfeljebb a "DigitalSignature” bit lehet még "true” értékre beállítva,
- a hitelesítő tanúsítvány kulcshasználati mezője kritikus, és a "DigitalSignature", valamint a "KeyAgreement" bitek vannak "true” értékre beállítva,
- a titkosító tanúsítvány kulcshasználati mezője kritikus, és a "KeyEncipherment", valamint a "DataEncipherment" bitek vannak "true” értékre beállítva.

6.2 A szolgáltatói magánkulcsok védelme és a kriptográfiai modulokkal kapcsolatos műszaki előírások

a) A szolgáltatói magánkulcsokat biztonságos módon kell tárolni, és meg kell akadályozni, hogy a szolgáltatói magánkulcshoz jogosulatlan személyek hozzáférhessenek, vagy a kulcsot arra jogosulatlan személyek használhassák.

b) Amennyiben a hitelesítés-szolgáltató a szolgáltatói magánkulcsot többé nem kívánja használni, az lejárt vagy kompromittálódott, azt olyan módon kell megsemmisítenie, hogy a kulcs további használata lehetetlenné váljon.

c) A hitelesítés-szolgáltatónak a tanúsítványok aláírásához használt magánkulcsát, ezeken kívül, csak a tanúsítvány visszavonási lista (CRL) aláírására szabad felhasználnia.

6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások

A hitelesítés-szolgáltató magánkulcsának tárolása, felhasználása:

a) A hitelesítés-szolgáltató szolgáltatói magánkulcsait olyan biztonságos kriptográfiai eszközben (kriptográfiai modulban) kell tartani, illetve használni, amely:

- megfelel a FIPS 140 [2] 3-as, illetve annál magasabb szintű követelményeinek, vagy
- megfelel a CEN 14167-2 [4] munkacsoport egyezmény követelményeinek, vagy
- olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [3], illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb szintű értékelési garancia szinten van értékelve. Ezt a rendszert a jelen dokumentum követelményeinek megfelelő olyan biztonsági rendszertervnek vagy védelmi profilnak kell megalapoznia, mely kockázat elemzésen alapul és figyelembe veszi a fizikai és egyéb nem műszaki biztonsági intézkedéseket is.

b) A hitelesítés-szolgáltató szolgáltatói magánkulcsait a kriptográfiai modulon (lásd a fenti a) pontot) kívül kódolni kell, olyan algoritmust és kulcs hosszat használva, melyek szerepelnek [1] 18.§-a szerint kiadott NHH határozatban, a biztonságos titkosító algoritmusok és kulcs méretek között, valamint képesek ellenállni a kriptográfiai támadásoknak a kulcs teljes hátralevő élettartamának ideje alatt.

A regisztrációs szervezet magánkulcsának tárolása, felhasználása:

c) A regisztrációs szervezet magán aláíró kulcsát olyan termékben, alkalmazásban vagy eszközben kell tartani, illetve használni, amely nem kompromittálja a magánkulcs biztonságát, s amely:

- megfelel a FIPS 140 [2] 2-es, illetve annál magasabb szintű követelményeinek, vagy
- egy olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [3], illetve azzal egyenértékű biztonsági kritériumok szerint 3-as vagy magasabb szintű értékelési garancia szinten van értékelve.

6.2.2 Magánkulcs többszereplős ("n-ből m") használata

a) A hitelesítés-szolgáltató szolgáltatói magánkulcsait csak bizalmi munkakört betöltő személyzet állíthatja vissza, legalább 3 erre feljogosított munkatárs közül legalább 2 jelenléte mellett, védett környezetben (lásd 5.1 pont), más személyek jelenlétét kizárva.

6.2.3 Magánkulcs letétbe helyezése

a) A hitelesítés-szolgáltatónak tilos szolgáltatói magánkulcsát letétbe helyeznie.

6.2.4 Magánkulcs mentése

a) A hitelesítés-szolgáltató szolgáltatói magánkulcsait csak védett környezetben (5.1), legalább két, bizalmi munkakört (5.2.1) betöltő, erre feljogosított személy együttes részvételével, más személyek jelenlétét kizárva lehet mentési célból másolni

b) A hitelesítés-szolgáltató szolgáltatói magánkulcsainak mentett másolataira ugyanolyan, vagy még magasabb szintű biztonsági előírásoknak kell vonatkozni, mint a használatban levő magánkulcsokra.

6.2.5 Magánkulcs archiválása

a) A hitelesítés-szolgáltató magán aláíró kulcsát nem szabad archiválni.

6.2.6 Magánkulcs bejuttatása kriptográfiai modulba, vagy onnan történő exportja

a) A hitelesítés-szolgáltató szolgáltatói magánkulcsait a kriptográfiai modulban kell előállítani, így ilyenkor azt kívülről nem szükséges bejuttatni.

b) A szolgáltatói magánkulcsok kriptográfiai modulba kívülről történő bejuttatására egyedül a magánkulcs véletlen megsérülése, megsemmisülése esetén lehet szükség. Az ilyen esetekre a 6.2.2 pont elvárása vonatkozik.

c) A szolgáltatói magánkulcsok kriptográfiai modulból történő exportálására kizárólag mentési célból kerülhet sor. Az ilyen esetekre a 6.2.4 pont elvárásai vonatkoznak.

6.2.7 Magánkulcs tárolása kriptográfiai modulban

a) A hitelesítés-szolgáltató szolgáltatói magánkulcsait egy külön hardver kriptográfiai modulban kell tárolni. Hozzáférés-ellenőrzéseket kell alkalmazni annak biztosítása érdekében, hogy a magánkulcsok a kriptográfiai modulon kívül ne legyenek hozzáférhetők.

6.2.8 A magánkulcs aktiválásának módja

A Szolgáltatási Szabályzatban meghatározott.

6.2.9 A magánkulcs deaktiválásának módja

A Szolgáltatási Szabályzatban meghatározott.

6.2.10 A magánkulcs megsemmisítésének módja

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy szolgáltatói magánkulcsai ne legyenek felhasználhatók életciklusuk vége után. Különösképpen:

a) A hitelesítés-szolgáltató kriptográfiai moduljában tárolt szolgáltatói magánkulcsait a modul visszavonásakor meg kell semmisíteni, védett környezetben (5.1), legalább két, bizalmi munkakört (5.2.1) betöltő, erre feljogosított személy együttes részvételével.

b) A hitelesítés-szolgáltató szolgáltatói magánkulcsainak összes másolatát meg kell semmisíteni oly módon, hogy a magánkulcsok ne legyenek helyreállíthatók.

6.2.11 A kriptográfiai modulok értékelése

a) Összhangban a 6.2.1 elvárásaival, a szolgáltatói magánkulcsokat tartalmazó és aktivizáló kriptográfiai moduloknak az alábbi értékelési eredmények valamelyikével kell rendelkezniük:

- FIPS 140 [2] szerint, legalább 3-as szinten,
- MSZ/ISO/IEC 15408 [3] szerint, legalább 4-es szintű értékelési garancia szinten.

b) A tanúsítványok előállításához csak olyan kriptográfiai modul használható, mely rendelkezik az NHH által által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiállított (az a) pontban szereplő értékelési eredményeken alapuló), vagy azzal egyenértékű igazolással is.

6.3 A kulcspár kezelésének egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

Nincs megkötés.

6.3.2 A tanúsítványok és kulcspárok használatának periódusa

a) A hitelesítés-szolgáltató szolgáltatói magánkulcsainak használati periódusa nem haladhatja meg azok érvényességi idejét.

a) A hitelesítés-szolgáltató által kibocsájtott tanúsítványok használati periódusa (érvényességi időtartama) nem haladhatja meg a 2 évet.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

A Szolgáltatási Szabályzatban meghatározott.

6.4.2 Az aktivizáló adatok védelme

a) A hitelesítés-szolgáltató a kriptográfiai hardver eszközhöz tartozó aktivizáló adatokat (PIN kód) csak abból a célból rögzítheti, hogy azt a szolgáltatást igénybe vevő személy számára – másolat megőrzése nélkül – átadhassa.

b) A kriptográfiai hardver eszközhöz tartozó aktivizáló adatot (PIN kód) a kriptográfiai hardver eszköztől elkülönítve[15] kell szétosztani.

c) A hitelesítés-szolgáltatónak a kriptográfiai hardver eszközt, valamint az ehhez tartozó aktivizáló adatokat (PIN kód) biztonságosan kell szétosztania.

6.4.3 Az aktivizáló adatok egyéb szempontjai

Nincs megkötés.

6.5 Informatikai biztonsági előírások

6.5.1 Speciális informatikai biztonsági műszaki követelmények

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy az informatikai rendszeréhez való hozzáférés kellően felhatalmazott egyénekre legyen korlátozva. Különösképpen:

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

a) A hitelesítés-szolgáltató rendszereinek és információinak a sértetlenségét védeni kell vírusok, káros és engedély nélküli szoftverek ellen.

b) Az adathordozó eszközöket biztonságosan kell kezelni azok sérülése, ellopása és jogosulatlan hozzáférése elleni védelem érdekében.

c) A hitelesítés-szolgáltatónak gondoskodnia kell a felhasználói[16] hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.

d) A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy az információkhoz és az alkalmazói rendszer funkciókhoz történő hozzáférés, a hozzáférés ellenőrzési szabályzatnak megfelelően korlátozott legyen, és hogy a hitelesítés-szolgáltató rendszere megfelelő számítógép biztonsági ellenőrzéseket nyújtson a hitelesítés-szolgáltató szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében, beleértve a biztonsági adminisztrátori és üzemeltetési funkció elkülönítését. Különösképpen a rendszer szolgáltatási és segédprogramok használatát kell korlátozni és szigorúan ellenőrizni.

e) A hitelesítés-szolgáltató személyzetét sikeresen azonosítani és hitelesíteni kell, mielőtt a tanúsítvány kezeléssel kapcsolatos kritikus alkalmazásokat használnák.

f) Eljárásokat kell kidolgozni és végrehajtani valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítés-szolgáltatások nyújtására.

[15] Az elkülönítés megoldható annak biztosításával, hogy a szétosztás és szállítás más időpontokban, vagy más úton történik.

[16] A felhasználó fogalma itt felöleli a rendszerüzemeltetőket, rendszeradminisztrátorokat és bármely olyan felhasználót, akinek közvetlen hozzáférése van a rendszerhez.

g) Műszaki előírásokat kell érvényre juttatni (például tűzfalak[17] segítségével) annak érdekében, hogy a hitelesítés-szolgáltató belső hálózati tartományai védettek legyenek a jogosulatlan hozzáféréstől, beleértve az alanyok, előfizetők és harmadik felek részéről történő hozzáférést is.

h) A hitelesítés-szolgáltató időben és összehangoltan lépjen fel 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) Folyamatos felügyelő és riasztó eszközöket kell biztosítani, hogy a hitelesítés-szolgáltató képes legyen felismerni és regisztrálni az erőforrásaihoz való jogosulatlan és/vagy szabálytalan hozzáférési kísérleteket, valamint képes legyen ezekre időben reagálni[18].

j) A nyilvánosságra hozatal (közzététel) alkalmazásnak hozzáférés ellenőrzést kell érvényesítenie a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információk módosítására irányuló kísérletekre vonatkozóan.

k) A visszavonás állapot alkalmazásnak hozzáférés ellenőrzést kell érvényesítenie a visszavonás állapot információ módosítására irányuló próbálkozások esetében.

l) Az érzékeny adatokat[19] védeni kell az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.

m) Biztosítani kell a hitelesítés-szolgáltató személyzet felelősségre vonhatóságát tevékenységéért, például a napló fájlok megőrzésén keresztül.

6.5.2 Az informatikai biztonság értékelése

A hitelesítés-szolgáltató csak megbízható rendszereket és termékeket használhat szolgáltatásainak biztosításához:

Az informatika biztonság értékelését nemzetközileg elfogadott módszertanok szerint kell tervezni és végrehajtani.

6.6 Életciklusra vonatkozó műszaki előírások

6.6.1 Rendszerfejlesztési előírások

a) Elemezni kell a biztonsági követelményeket a hitelesítés-szolgáltató, illetve a hitelesítés-szolgáltató nevében végzett minden egyes rendszer fejlesztési projekt tervezési és követelmény meghatározási fázisában, annak biztosítása érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

b) Változtatás kezelési eljárásokat kell alkalmazni valamennyi működő szoftver esetében a kibocsátásokra, a módosításokra és a sürgős szoftver javításokra vonatkozóan.

6.6.2 Biztonságkezelési előírások

A hitelesítés-szolgáltatóval kapcsolatban általában:

[17] Ajánlott, hogy a tűzfalakat úgy konfigurálják, hogy azok a hitelesítés-szolgáltató működéséhez nem szükséges protokollokat és hozzáféréseket kiiktassák.

[18] A hitelesítés-szolgáltató erre használhat például egy behatolás észlelő rendszert, vagy hozzáférés ellenőrzést felügyelő és riasztási eszközöket.

[19] Az érzékeny adatok közé tartoznak a regisztrációs információk is.

a) A hitelesítés-szolgáltatónak kockázat elemzést kell végrehajtania üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározása érdekében.

A rendszer tervezésével kapcsolatban:

b) Nincs különös követelmény.

A tanúsítványok aláírására használt hardver biztonsági modul kezelésével kapcsolatban:

A hitelesítés-szolgáltatónak gondoskodnia kell a kriptográfiai hardver biztonságáról annak teljes élettartama alatt. Különösképpen:

c) a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják szállítás közben;

d) a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják tárolás közben;

e) a hitelesítés-szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktiválása, mentése és visszaállítása legalább két bizalmi munkakört betöltő alkalmazott együttes jelenlétét kívánja meg;

f) a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardver helyesen működik;

g) a hitelesítés-szolgáltató kriptográfiai hardverén tárolt hitelesítés-szolgáltatói magán aláíró kulcsokat az eszköz visszavonásakor megsemmisítik.

6.6.3 Életciklusra vonatkozó biztonsági előírások

Nincs megkötés.

6.7 Hálózatbiztonsági előírások

A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy informatikai rendszerében megfelelő hálózat biztonsági ellenőrzésekre kerüljön sor. Különösképpen:

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

a) Az érzékeny adatokat[20] védeni kell, amikor azok átvitele nem biztonságos hálózatokon keresztül történik.

b) A hitelesítés-szolgáltatónak gondoskodnia kell informatika biztonsága fenntartásáról akkor is, ha a hitelesítés-szolgáltató funkciókra vonatkozó felelősség más szervezethez, illetve egységhez lett kiadva.

A regisztrálással kapcsolatosan:

c) A regisztrációs adatok bizalmasságát és sértetlenségét védeni kell, különösen az előfizetővel/alannyal folytatott, illetve osztott hitelesítés-szolgáltató rendszer esetén az egyes komponensek közötti adatcsere során.

[20] Az érzékeny adatok közé tartoznak a regisztrációs információk is.

d) Amennyiben külső regisztrációs szolgáltatókat vesz igénybe, a hitelesítés-szolgáltatónak ellenőrzéssel biztosítania kell, hogy regisztrációs adatokat csak elismert, azonosságában hitelesített regisztrációs szolgáltatókkal cserél.

A tanúsítvány előállítással és visszavonás kezeléssel kapcsolatosan:

e) A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy a helyi hálózati komponensek (például útirányítók, tűzfalak) fizikailag biztonságos környezetben legyenek és konfigurációikat időszakonként auditálják.

f) Folyamatos felügyelő és riasztó eszközöket kell biztosítani, hogy a hitelesítés-szolgáltató képes legyen felismerni, regisztrálni az erőforrásaihoz (hálózatról) történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre[21].

A tanúsítvány nyilvánosságra hozatalával kapcsolatosan:

g) A nyilvánosságra hozatal alkalmazásnak (hálózati) hozzáférés ellenőrzést kell érvényesítenie a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információk módosítására irányuló kísérletekre vonatkozóan.

A visszavonás állapot szolgáltatásával kapcsolatosan:

h) A visszavonás állapot alkalmazásnak hozzáférés ellenőrzést kell érvényesítenie a visszavonás állapot információ (hálózati) módosítására irányuló próbálkozások esetében.

6.8 Időbélyegzés

Az archiválásra vonatkozó 5.5.5, valamint a leállás előtti mentésre vonatkozó 5.8 elvárásait leszámítva nincs megkötés.

[21] A hitelesítés-szolgáltató erre használhat például egy behatolás észlelő rendszert, vagy hozzáférés ellenőrzést felügyelő és riasztási eszközöket.

7. Tanúsítvány-, tanúsítvány visszavonási lista- és OCSP-profilok

7.1 Tanúsítványprofilok

A kibocsátott tanúsítványok feleljenek meg a [6]-ban leírt X.509 3-as verziójú tanúsítványoknak, ezen belül különösen az alábbiaknak:

7.1.1 Verzió szám(ok)

a) A [6]-ban leírt X.509 3-as verziójú tanúsítvány verziójának értékszáma: 2

7.1.2 Tanúsítvány kiterjesztések

A kiterjesztések részletes leírását [7] tartalmazza.

7.1.3 Az algoritmus objektum azonosítója

a) A hitelesítés-szolgáltatónak az alábbi névfa azonosítót kell használnia a tanúsítványok és a visszavonási listák (CRL) aláíró algoritmusának algoritmus meghatározásához:

- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)

7.1.4 Névformák

a) A hitelesítés-szolgáltatónak jelen hitelesítési irányelvek alapján kibocsátott tanúsítványok alanyaként egy megkülönböztetett nevet kell belefoglalnia a tanúsítványba. Ezen név formájának az X.520 szerinti részletes meghatározását lásd a 3.1.1 pontban.

7.1.5 Névhasználati megkötöttségek

a) A Subject (alany) és Issuer (kibocsátó) megkülönböztetett neveket minden tanúsítványban meg kell adni, és ezeknek meg kell felelni a [7]-ban előírtaknak. Minden névnek meg kell felelni a 3.1. alatt előírtaknak is.

7.1.6 A Hitelesítési rend objektum azonosítója

a) A hitelesítés-szolgáltató minden jelen Hitelesítési rend szerint kibocsátott tanúsítványba köteles felvenni a nem kritikus Hitelesítési rend kiterjesztést. Ez a kiterjesztés tartalmazza az 1.2 pontban meghatározott névfa azonosítót. Amennyiben a szolgáltató hitelésítési rendjében jóváhagyottan eltér jelen előírásoktól, akkor más OID-et kell azonosítóként feltüntetnie.

7.1.7 A Hitelesítési rend megkötöttségek kiterjesztés használata

Nincs megkötés.

7.1.8 A Hitelesítési rend jellemzők szintaktikája és szemantikája

a) A hitelesítés-szolgáltatónak a „policyQualifiers” kiterjesztést a Hitelesítési rend URI-jével együtt kell telepítenie.

7.1.9 A kritikus Hitelesítési rend kiterjesztések feldolgozási szemantikája

A kritikus kiterjesztéseket a [6]-ban meghatározottak szerint kell értelmezni.

7.2 Tanúsítvány visszavonási lista profil

A kibocsátott tanúsítvány visszavonási listák feleljenek meg a [6]-ban leírt X.509 2-es verziójú visszavonási listáknak, ezen belül különösen az alábbiaknak:

7.2.1 Verziószám(ok)

a) A [7] szabványban leírt X.509 2-as verziójú tanúsítvány visszavonási lista verziójának értékszáma: 1

7.2.2 Tanúsítvány visszavonási lista kiterjesztések

A Szolgáltatási Szabályzatban meghatározott.

7.3 OCSP-profil

a) Amennyiben a hitelesítés-szolgáltató valós idejű tanúsítvány állapot protokoll (OCSP) szolgáltatást biztosít, az abban alkalmazott OCSP profilt a Szolgáltatási Szabályzatban kell meghatároznia.

8. Megfelelőségi audit és egyéb ellenőrzések

8.1 Az ellenőrzések körülményei és gyakorisága

a) A megfelelőségi ellenőrzéseket 2 évente meg kell ismételni. Ezek az ellenőrzések lehetnek belső auditok is.

8.2 Az auditor és szükséges képesítése

a) A külső és belső auditálást végző személyeknek függetlennek kell lenniük a hitelesítés-szolgáltató üzemeltetését végző személyektől.

b) A külső és belső auditálást csak a megfelelő szakmai ismeretek birtokában lévő, tapasztalt szakemberek végezhetik.

8.3 Az auditor és az auditált rendszerelem függetlensége

a) Az auditornak függetlennek kell lennie az általa ellenőrzött rendszertől.

8.4 Az auditálás által lefedett területek

a) Az auditálásnak le kell fedni az alábbi területeket

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

8.5 A hiányosságok kezelése

Nincs megkötés.

8.6 Az eredmények közzététele

Nincs megkötés.

9. Egyéb üzleti és jogi kérdések

9.1 Díjak

Nincs megkötés.

9.2 Anyagi felelősségvállalás

a) A hitelesítés-szolgáltatónak a megbízhatóság biztosítása érdekében felelősségbiztosítással kell rendelkeznie.

b) A felelősségbiztosítási szerződésnek ki kell terjednie az alábbi károkra:

- a szolgáltatások nyújtása során a szolgáltató hibájából bekövetkező károkra,
- ha a hitelesítés-szolgáltató tevékenységének befejezését előzetesen nem jelenti be az NHH-nak, és nem gondoskodik arról, hogy egy vele azonos besorolású másik hitelesítés-szolgáltató átvegye nyilvántartásait (ezen belül különösen a visszavont tanúsítványok nyilvántartásait), akkor az NHH által végrehajtott visszavonási, értesítési és adatmegőrzésre kijelölő tevékenységek költségeivel az NHH-nak okozott károkra.

c) A felelősségbiztosítási szerződésnek egy biztosítási esemény vonatkozásában káreseményenként a tanúsítványban, illetve a Szolgáltatási Szabályzatban vállalt felelősségvállalási érték legalább háromszorosáig kell fedezetet biztosítania az összes károsultnak okozott károkra. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

d) A felelősségbiztosításnak a c) pontban meghatározott összeg erejéig fedezetet kell nyújtania a károsultnak a hitelesítés-szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.

e) Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

9.3 Az üzleti információk bizalmassága

Nincs megkötés.

9.4 A személyes adatok védelme

a) A hitelesítés-szolgáltatónak gondoskodnia kell az adatvédelem és az adatbiztonság területén a szabályszerű működésről, a jogok, kötelezettségek és felelősségek meghatározásáról

b) A hitelesítés-szolgáltató működésének és szabályzatainak meg kell felelniük a Személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992 évi XLIII. törvény követelményeinek.

9.5 Szellemi tulajdonjogok

Nincs megkötés.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 A hitelesítés-szolgáltató felelőssége és helytállása

a) A hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy a rá vonatkozó vonatkozó valamennyi, a jelen dokumentumban részletezett követelmény teljesüljön, amennyiben azok alkalmazhatók.

b) A hitelesítés-szolgáltató a felelős az általa támogatott Hitelesítési rendben és Szolgáltatási Szabályzatban leírt eljárásoknak való megfelelőségért, még abban az esetben is, ha a hitelesítés-szolgáltató egyes funkcionalitásait alvállalkozók végzik.

9.6.2 A regisztrációs szervezet felelőssége és helytállása

Nincs megkötés.

9.6.3 Az előfizető felelőssége és helytállása

Nincs megkötés.

9.6.4 Az érintett fél felelőssége

a) Az érintett felek számára rendelkezésre bocsátott kikötéseknek és feltételeknek tartalmazniuk kell egy megjegyzést, miszerint: „Ha ésszerű módon egy tanúsítványra kívánnak hagyatkozni, az alábbiakat kell tenniük:

- ellenőrizzék a tanúsítvány érvényességét, azt, hogy a tanúsítvány nincs felfüggesztve, illetve visszavonva az érvényes visszavonási állapot információ szerint, a Hitelesítési rendben és a Szolgáltatási Szabályzatnak megfelelően;
- vegyék figyelembe a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban, a Hitelesítési rendben és a Szolgáltatási Szabályzatban szerepel;
- tegyenek meg minden, megállapodásokban, máshol előírt, illetve az adott helyzetben általában elvárható egyéb óvintézkedést.”

9.6.5 Egyéb szereplők tevékenységért viselt felelősség és helytállás

Nincs megkötés.

9.7 Helytállás érvénytelenségi köre

Nincs megkötés.

9.8 Felelősségi korlátozások

Nincs megkötés.

9.9 Kártérítési kötelezettségek

Nincs megkötés.

9.10 Érvényesség

Jelen Hitelesítési rend visszavonásig érvényes.

9.11 A felek közötti kommunikációra vonatkozó előírások

Nincs megkötés.

9.12 Kiegészítések

Nincs megkötés.

9.13 Vitás kérdések megoldása

Nincs megkötés.

9.14 Irányadó jog

A hitelesítés-szolgáltató működésének jogi vonatkozásaira a Magyar Köztársaság törvényei az irányadók.

9.15 Az érvényben lévő jogszabályoknak való megfelelőség

A jelen dokumentumban megfogalmazott Hitelesítési rend az alábbi törvényeknek, rendeleteknek és irányelveknek való megfelelőséget tűzi célul:

a) Személyes adatok védelméről és a közhasznú adatok nyilvánosságáról szóló 1992 évi XLIII. Tv.

b) Az elektronikus aláírásról szóló 2001:XXXV. törvény

c) 9/2005 (VII.21.) IHM rendelet

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

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

f) 20/2001 (XI. 15.) MeHVM rendelet a Hírközlési Főfelügyeletnek az elektronikus aláírással összefüggő minősítéssel és nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

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

h) 2/2002 (IV. 26.) MeHVM irányelv A minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.

i) Az Európai Parlament és a Tanács 1999/93/EK számú irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről

j) A közigazgatási hatósági eljárás és szolgáltatás szabályairól szóló 2004. évi CXL. törvény és az elektronikus ügyintézéshez kapcsolódó végrehajtási rendeletek, azaz a 193/2005 (IX.22.), 194/2005 (IX.22.) és 195/2005 (IX.22.) számú kormányrendeletek.

9.16 Vegyes rendelkezések

Nincs megkötés.

9.17 Egyéb rendelkezések

Nincs megkötés.