



Matáv Minősített e-Szignó[®] hitelesítésszolgáltatás

***Nyilvános körben kibocsátott,
biztonságos aláírás-létrehozó eszköz
alkalmazását megkövetelő,
minősített tanúsítványokra vonatkozó
Tanúsítványtípus Szabályzat
(MTT+BALE)***

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.2.1.1

Verziószám: **1.2**

NHH azonosító: HL-9220-11/2004

Változáskezelés

Verzió	Dátum	A változás leírása
0.9	2003-09-5	Első tervezet
0.91	2003-09-15	Első belső munkaanyag
0.94	2003-11-21	Matáv műszaki szakértői vélemények beépítésével kibővített anyag
0.95	2004-01-23	Matáv jogi szakértői vélemények beépítésével pontosított anyag
0.96	2004-03-01	Szolgáltatási szabályzattal szinkronizált anyag
0.97	2004.03.11	Matáv WS változat
1.0	2004-03-30	Nemzeti Hírközlési Hatóság felé beadott változat
1.1	2004-07-16	Hatósági szemlét követő módosítások
1.2	2004-09-27	Hatóság felé beadott, elfogadott változat

		Aláírás
Készítette: HunGuard Kft.	Tanácsadó
Ellenőrizte: Tapasztó Balázs	Vezető termékmenedzser Matáv Rt.
Jóváhagyta: Bujáki József	Biztonsági tisztviselő Matáv Rt.

Tartalom

Változáskezelés	2
1. Bevezetés	7
1.1 Áttekintés	7
1.2 Azonosítás	7
1.3 Közösség és alkalmazhatóság	8
1.3.1 Hitelesítő szervezet	8
1.3.2 Regisztráló szervezet	8
1.3.3 Végfelhasználók	8
1.3.4 Alkalmazhatóság	8
1.4 Kapcsolattartás	9
2. Általános rendelkezések	9
2.1 Kötelezettségek	9
2.1.1 A hitelesítés-szolgáltató általános kötelezettségei	9
2.1.2 A hitelesítő szervezet kötelezettségei	10
2.1.3 A regisztrációs szervezet kötelezettségei -	13
2.1.4 Az aláíró és az előfizető kötelezettségei	15
2.1.5 Az érintett félre vonatkozó ajánlások	16
2.1.6 A címtár kötelezettségei	16
2.2 Felelősség	17
2.2.1 A hitelesítés-szolgáltató általános felelőssége	17
2.2.2 A hitelesítő szervezet felelőssége	17
2.2.3 A regisztráló szervezet felelőssége	18
2.2.4 Az aláíró felelőssége	18
2.2.5 Az előfizető felelőssége	18
2.2.6 Az érintett fél felelőssége	18
2.3 Pénzügyi felelősség	19
2.3.1 A hitelesítés-szolgáltatóval szembeni kártérítés	19
2.3.2 Adminisztratív folyamatok	19
2.4 Értelmezés és érvényesítés	19
2.4.1 Irányadó jog	19
2.4.2 Érvénytelenség, fennmaradás, megszűnés, értesítések	20
2.4.3 Vitás kérdések megoldására vonatkozó eljárások	21
2.5 Díjak	21
2.6 Közzététel és címtár	21
2.6.1 Hitelesítés-szolgáltatói információ közzététele	21
2.6.2 A közzététel gyakorisága	23
2.6.3 Hozzáférés ellenőrzések	23
2.6.4 Címtárak	23
2.7 A megfelelés vizsgálat	24
2.7.1 A megfelelés vizsgálatának gyakorisága	24
2.7.2 Az átvizsgáló szervezet megnevezése/jellemzői	24
2.7.3 Az átvizsgáló szervezet és a vizsgált fél kapcsolata	25
2.7.4 A vizsgálat által érintett területek	25
2.7.5 Hiányosságok esetén végrehajtandó tevékenységek	25
2.7.6 Az eredményekről való tájékoztatás	25
2.8 Bizalmasság	25
2.9 Szellemi tulajdonjogok	27
3. Azonosítás és hitelesítés	29
3.1 Kezdeti regisztrálás	29
3.1.1 Név típusok	29
3.1.2 Igény a nevek értelmezhetőségére	29

3.1.3	Különböző elnevezési formák értelmezési szabályai	29
3.1.4	A nevek egyedisége	29
3.1.5	Eljárások a nevekre vonatkozó vitás kérdések megoldására	29
3.1.6	Márkanév elismerése, hitelesítése és szerepe	29
3.1.7	A magánkulcs birtoklásának bizonyítási módszere	30
3.1.8	A szervezeti azonosság hitelesítése	30
3.1.9	Személyazonosság hitelesítése	30
3.2	Érvényes tanúsítvány megújítása	30
3.3	Érvénytelen tanúsítvány megújítása	30
3.4	Visszavonási és felfüggesztési kérelem	30
4.	Működésre vonatkozó követelmények	31
4.1	Tanúsítvány-kérelem	31
4.2	Tanúsítvány kibocsátás	31
4.3	Tanúsítvány elfogadás	31
4.4	Tanúsítvány felfüggesztés és visszavonás	31
4.5	A biztonsági naplózás folyamatai	31
4.5.1	A tárolt események típusai	32
4.5.2	A napló állomány feldolgozásának gyakorisága	32
4.5.3	A napló állomány megőrzési időtartama	32
4.5.4	A napló állomány védelme	32
4.5.5	A napló állomány mentési folyamatai	32
4.5.6	A napló gyűjtési rendszere	32
4.5.7	Az eseményeket kiváltó aláírók értesítése	32
4.5.8	Sebezhetőség felmérése	32
4.6	Adatok archiválása	33
4.6.1	A tárolt események típusai	33
4.6.2	Az archívum megőrzési időtartama	33
4.6.3	Az archívum védelme	33
4.6.4	Az archívum mentési folyamatai	34
4.6.5	A rekordok időbélyegzésére vonatkozó követelmények	34
4.6.6	Az archívum gyűjtési rendszere	34
4.6.7	Archív információ hozzáférését és ellenőrzését végző eljárások	34
4.7	Tanúsítványmegújítás	34
4.8	Helyreállítás rendkívüli üzemi helyzetek esetén	34
4.8.1	Sérült számítási erőforrások, szoftverek és/vagy adatok	35
4.8.2	A szolgáltatói egység nyilvános kulcsának visszavonása	35
4.8.3	Egy szolgáltatói egység kulcsának kompromittálódása	35
4.8.4	Működési képesség természeti vagy más katasztrófát követően	36
4.9	A hitelesítésszolgáltatás leállítás	36
5.	Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések	37
5.1	Fizikai óvintézkedések	38
5.1.1	A telephely elhelyezése és szerkezeti felépítése	38
5.1.2	Fizikai hozzáférés	39
5.1.3	Áramellátás, légkondicionálás	39
5.1.4	Beázás és elárasztódás veszélyeztetettsége	39
5.1.5	Tűzmegeelőzés és tűzvédelem	39
5.1.6	Adathordozók tárolása	40
5.1.7	Selejt kezelése, megsemmisítése	40
5.1.8	Fizikailag elkülönítetten őrzött mentési példányok	40
5.2	Eljárásbeli óvintézkedések	40
5.2.1	Bizalmi munkakörök	40
5.2.2	Az egyes feladatokhoz szükséges személyzeti létszámok	41
5.2.3	Az egyes munkakörökben elvárt azonosítás és hitelesítés	41
5.3	Személyzetre vonatkozó óvintézkedések	41
5.3.1	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények	41

5.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások	42
5.3.3 Kiképzési követelmények	42
5.3.4 Továbbképzési gyakoriságok és követelmények.....	42
5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje	42
5.3.6 A felhatalmazás nélküli tevékenységek büntető következményei	42
5.3.7 A szerződéses alkalmazottakra vonatkozó követelmények	42
5.3.8 A személyzet számára biztosított dokumentációk	43
6. Műszaki biztonsági óvintézkedések	44
6.1 Kulcspár előállítás és telepítés.....	44
6.1.1 Kulcspár előállítás	44
6.1.2 Magánkulcs eljuttatása a tulajdonoshoz.....	45
6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz	46
6.1.4 A szolgáltatói nyilvános kulcs közzététele	46
6.1.5 Kulcs méretek	46
6.1.6 A nyilvános kulcs paramétereinek előállítása	46
6.1.7 A paraméterek megfelelőségének ellenőrzése.....	46
6.1.8 Hardver/szoftver kulcselőállítás	47
6.1.9 A kulcs használat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően).....	47
6.2 A magánkulcsok védelme	47
6.2.1 Kriptográfiai modulra vonatkozó szabványok	47
6.2.2 A több-szereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése	49
6.2.3 Magánkulcs letétbe helyezése.....	49
6.2.4 Magánkulcs mentése	49
6.2.5 Magánkulcs archiválása	50
6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba.....	50
6.2.7 A magánkulcs aktivizálásának módja	51
6.2.8 A magánkulcs aktív állapotának megszüntetési módja.....	52
6.2.9 A magánkulcs megsemmisítésének módja	52
6.3 A kulcspár gondozásának egyéb szempontjai	53
6.3.1 A nyilvános kulcsok archiválása	53
6.3.2 A nyilvános és magánkulcsok használatának periódusa	53
6.4 Aktivizáló adatok.....	53
6.4.1 Aktivizáló adatok előállítása és telepítése.....	53
6.4.2 Az aktivizáló adatok védelme	53
6.4.3 Az aktivizáló adatok egyéb szempontjai.....	54
6.5 Számítógépbiztonsági óvintézkedések.....	54
6.5.1 Speciális számítógépbiztonsági műszaki követelmények	54
6.5.2 Informatikai biztonsági minősítés	55
6.6 Életciklusra vonatkozó műszaki óvintézkedések.....	55
6.6.1 Rendszerfejlesztési óvintézkedések	55
6.6.2 Biztonságkezelési óvintézkedések.....	56
6.6.3 Az életciklusra vonatkozó biztonság osztályozása	56
6.7 Hálózatbiztonsági óvintézkedések	56
6.8 A kriptográfiai modul ellenőrzése	57
7. Tanúsítvány és tanúsítvány visszavonási lista profilok	58
7.1 Tanúsítvány profil	58
7.1.1 Verzió szám(ok)	58
7.1.2 Tanúsítvány kiterjesztések	58
7.1.3 Algoritmus objektum azonosítók	58
7.1.4 Elnevezési formák.....	58
7.1.5 Elnevezésre vonatkozó korlátozások.....	58
7.1.6 Tanúsítványtípus objektum azonosító.....	58
7.1.7 A „tanúsítványtípus korlátozás” kiterjesztés használata	58
7.1.8 Szabályzat minősítő szintaxis és szemantika.....	59
7.1.9 A kritikus tanúsítványtípus kiterjesztés feldolgozása	59

7.2 Tanúsítvány visszavonási lista profil	59
7.2.1 Verzió szám(ok)	59
7.2.2 „Tanúsítvány visszavonási lista” és „Tanúsítvány visszavonási lista bejegyzési” kiterjesztések	59
8. Leírás adminisztráció.....	60
8.1 Leírás változtatási eljárások.....	60
8.2 Közzétételi és tájékoztatási elvek.....	60
8.3 Szolgáltatás szabályzat jóváhagyási eljárások	60
9. Hivatkozások.....	62
10. Jelölések, rövidítések és meghatározások	64

1. Bevezetés

1.1 Áttekintés

A Tanúsítványtípus Szabályzat egy „szabálygyűjtemény, mely egy Tanúsítványtípus Szabályzat felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára”.

A szabályokra vonatkozó követelményeit jelen dokumentum Tanúsítványtípus Szabályzat formájában határozza meg. A jelen dokumentumnak megfelelően kibocsátott tanúsítványok tartalmazzak egy Tanúsítványtípus Szabályzat azonosítót, amelyet az érintett felek arra használhatnak, hogy meghatározzák a tanúsítványok alkalmazhatóságát és megbízhatóságát egy adott alkalmazás tekintetében.

Jelen dokumentum az alábbi tanúsítványtípust határozza meg:

Nyilvános körben kibocsátott, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványtípus [MTT+BALE].

Erre a minősített tanúsítványtípusra teljesülnek az alábbiak:

megfelel az [1] törvény (Eat.) 2. számú mellékletében a minősített tanúsítvány tartalmára meghatározott követelményeknek;

olyan hitelesítés-szolgáltató adta ki, amely teljesíti az [1] Eat. 3. számú mellékletében a minősített hitelesítés-szolgáltatókra meghatározott követelményeket;

olyan biztonságos aláíró eszközzel kerül felhasználásra, amely eleget tesz az [1] (Eat.) 1. számú mellékletében a biztonságos aláírás-létrehozó eszközökre meghatározott követelményeknek;

nyilvános körben került kibocsátásra.

A minősített tanúsítványtípus határozatlan időre szól a változáskezelés táblázatban feltüntetett jelen verzióra érvényes **hatálybalépés dátumától** kezdődően. (A minősített tanúsítványtípus időbeli hatálya a szolgáltatás beszüntetésekor, illetve egy újabb verzió hatályba lépésekor szűnik meg.)

1.2 Azonosítás

A jelen dokumentumban meghatározott tanúsítványtípus azonosítója a fedőlapon található (Regisztrációs szám).

1.3 Közösség és alkalmazhatóság

1.3.1 Hitelesítő szervezet

A Matáv Rt. Minősített Hitelesítés Szolgáltató (továbbiakban: hitelesítés-szolgáltató) – saját szervezetén belül – egy hitelesítő szervezetet működtet, melynek feladatát, hatáskörét és felelősségét a Minősített Hitelesítés Szolgáltatási Szabályzat (továbbiakban: „mHSZSZ” vagy szolgáltatási szabályzat) ismerteti.

1.3.2 Regisztráló szervezet

A Szolgáltató – saját szervezetén belül – egy egyszintű regisztráló szervezetet működtet, melynek felépítését, feladatát, hatáskörét és felelősségét az mHSZSZ 1.3.2 pontja ismerteti.

1.3.3 Végfelhasználók

A hitelesítés-szolgáltató által nyújtott szolgáltatások végfelhasználói az alábbiak:

- előfizetők,
- aláírók és
- érintett felek.

Fentiek meghatározását az mHSZSZ 1.3.4 pontja tartalmazza.

1.3.4 Alkalmazhatóság

- a) Jelen Tanúsítványtípus Szabályzat érvényességi körében kibocsátott minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon kielégítik, ahogy egy kézírásos aláírás kielégíti ugyanazt a követelményt a papír-alapú adatok vonatkozásában¹.
- b) A kibocsátott minősített tanúsítványok kizárólag aláírási célra használhatók fel.
- c) A végfelhasználói tanúsítványokhoz tartozó aláírás létrehozó adat, tanúsítványok aláírására történő felhasználása, vagy bármilyen egyéb hitelesítésszolgáltatás nyújtásához történő alkalmazása tilos.
- d) A hitelesítés-szolgáltató a végfelhasználói tanúsítványok felhasználását a tanúsítványban jelzett módon tovább korlátozhatja.

¹ Lásd [1] 29.§ (1) bekezdését.

1.4 Kapcsolattartás

A kapcsolattartásra vonatkozó adatok az mHSZSZ 1.4 pontjában találhatóak meg.

2. Általános rendelkezések

2.1 Kötelezettségek

2.1.1 A hitelesítés-szolgáltató általános kötelezettségei

- a) A hitelesítés-szolgáltató (a hitelesítő szervezet, a regisztrációs szervezet(ek) és a címtár együttes tevékenységével) az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat biztosítja:
 - elektronikus aláírás hitelesítésszolgáltatás (a továbbiakban: hitelesítésszolgáltatás), ezen belül:
 - regisztráció,
 - tanúsítvány előállítás,
 - tanúsítvány kibocsátás,
 - visszavonás kezelés,
 - visszavonási állapot közzététele,
 - biztonságos aláírás-létrehozó eszköz szolgáltatás (biztonságos aláírás létrehozó eszközön az aláírás-létrehozó adat elhelyezése),
 - időbélyegzés szolgáltatás.
- b) A hitelesítés-szolgáltató gondoskodik a hitelesítés-szolgáltatóra vonatkozó valamennyi, a 3.-8. fejezetekben részletezett állítás teljesüléséről, amennyiben azok az adott tanúsítványtípusra alkalmazhatóak.
- c) A hitelesítés-szolgáltató szolgáltatásait hozzáférhetővé teszi minden olyan igénylő számára, akinek tevékenysége kinyilvánított működési területére esik.
- d) A hitelesítés-szolgáltató jogi személy.
- e) A hitelesítés-szolgáltató megfelelően dokumentált megállapodásokkal és szerződéses kapcsolatokkal rendelkezik azon esetekre, amikor a szolgáltatások nyújtása alvállalkozókat, illetve más, harmadik felekkel kötött megegyezéseket érint.
- f) A hitelesítés-szolgáltató olyan szabályzatokkal rendelkezik, mely a Tanúsítványtípus Szabályzatban azonosított valamennyi követelmény kielégítésére szolgáló gyakorlatra és eljárásra vonatkozik.
- g) A hitelesítés-szolgáltató szabályzatai meghatározzák a hitelesítés-szolgáltató szolgáltatásait támogató valamennyi külső szervezetre vonatkozó kötelezettségeket, beleértve az alkalmazandó szabályzatokat és gyakorlatokat is.

- h) A hitelesítés-szolgáltató valamennyi szolgáltatását szabályzataival összhangban nyújtja.
- i) A szabályzatokat a hitelesítés-szolgáltató felsőszintű irányító testülete hagyja jóvá.
- j) A szabályzatok megfelelő megvalósításáért a hitelesítés-szolgáltató felső vezetősége felel.
- k) A hitelesítés-szolgáltató szolgáltatási szabályzatát és egyéb fontos dokumentációját a Tanúsítványtípus Szabályzatnak való megfelelés felméréséhez szükséges mértékig az aláírók/előfizetők és az érintett felek rendelkezésére bocsátja.
- l) A hitelesítés-szolgáltató rendszeresen felülvizsgálja szabályzatait, az újra érvényesített szabályzat tartalmazza a szükséges módosításokat.
- m) A hitelesítés-szolgáltató időben értesítést tesz közzé a szolgáltatási szabályzatában tervezett változtatásokról és a fenti (i. pont szerint történő) jóváhagyást követően az átdolgozott szolgáltatási szabályzatát (a k. pontban előírtak szerint) haladéktalanul hozzáférhetővé teszi.
- n) Ha a hitelesítés-szolgáltató ellen felszámolási vagy végelszámolási eljárás indult, haladéktalanul köteles tájékoztatni a Hatóságot e tényről, megnevezve az eljárást lefolytató szervezetet.

2.1.2 A hitelesítő szervezet kötelezettségei

- a) A hitelesítő szervezet biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatást:
 - elektronikus aláírás hitelesítésszolgáltatáson belül : tanúsítvány előállítás és kibocsátás,
 - aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése,
 - időbélyegzés szolgáltatás.
- b) A hitelesítő szervezet közreműködik (a visszavonási listák aláírásával) az alábbi elektronikus aláírással kapcsolatos szolgáltatás biztosításában:
 - visszavonási állapot közzététele.

A hitelesítő szervezet a **tanúsítvány előállítás és kibocsátás** szolgáltatás keretén belül:

- c) ellenőrzi a regisztráló szervezettől érkező tanúsítvány-kérelmet, benne az aláírandó tanúsítvány adatokat tartalmazó üzenet sértetlenségét és hitelességét;
- d) feldolgozza a regisztráló szervezettől érkező hiteles és sértetlen tanúsítvány kérelmet, melynek keretén belül előállítja a tanúsítványt (aláírja az aláírandó tanúsítvány adatokat);

- e) a minősített tanúsítvány aláírására használt magánkulcsát alapvetően (de nem kizárólag) a minősített tanúsítványok és a visszavonási listák aláírására használja fel;
- f) csak olyan minősített tanúsítványokat állít elő, amelyek megfelelnek a szolgáltatási szabályzatban meghatározott, támogatott tanúsítványtípusoknak;
- g) csak olyan minősített tanúsítványokat bocsát ki, amelyek megfelelnek az [1] 2. számú mellékletében, valamint a [2] 162. pontjában meghatározott követelményeknek;
- h) gondoskodik arról, hogy a tanúsítványban foglalt „megkülönböztetett név” egyedi legyen a hitelesítés-szolgáltató szolgáltatási körén belül;
- i) gondoskodik arról, hogy a hitelesítés-szolgáltató teljes szolgáltatási körén belül kibocsátott tanúsítványokhoz tartozó kulcsok mindvégig egyediek maradjanak;
- j) megválaszolja a regisztráló szervezetnek a tőle kapott tanúsítvány-kérelmet, benne elküldve az előállított tanúsítványt, biztosítva a válaszüzenet sértetlenségét és hitelességét.

A hitelesítő szervezet az **aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése** szolgáltatás biztosítása keretén belül:

- k) gondoskodik valamennyi általa, az aláíró számára végrehajtott kulcs előállítás biztonságosságáról, az aláíró magánkulcsának titkosságáról;
- l) az aláíró részére előállított kulcspárt:
 - olyan kriptográfiai eszközön állíttatja elő, mely tanúsítvánnyal igazoltan megfelel az [1] Eat. 1. számú mellékletében meghatározott követelményeknek, egyben szerepel a Hatóság által nyilvántartásba vett biztonságos aláírás-létrehozó eszközök listáján is,
 - olyan algoritmus felhasználásával állíttatja elő, melyet a [2] 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő kulcsgeneráló algoritmusként ismer el,
 - olyan aláíró algoritmushoz és olyan kulcshosszúságban állítja elő, melyet a [2] 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő aláíró algoritmusként, illetve megfelelő paraméterként ismer el;
- m) gondoskodik az általa biztosított biztonságos aláírás-létrehozó eszköz kibocsátása során az eljárás biztonságáról;
- n) ellenőrzi a biztonságos aláírás-létrehozó eszköz kezelését;
- o) ellenőrzi, hogy a szolgáltatás során felhasznált aláírás-létrehozó eszköz a Nemzeti Hírközlési Hatóság (továbbiakban: Hatóság) által nyilvántartásba vett biztonságos aláírás-létrehozó eszköz-e;
- p) a biztonságos aláírás-létrehozó eszköz előkészítését megfelelően biztonságos környezetben (lásd 5.1 fejezet) hajtja végre;
- q) biztonságos konfigurációt alakít ki a biztonságos aláírás-létrehozó eszközön az inicializálás, formázás és fájl-struktúra kialakítás során;

- r) a biztonságos aláírás-létrehozó eszközt biztonságosan tárolja és továbbítja a regisztrációs szervezetnek;
- s) biztonságos módon előállítja a kezdeti aktivizáló adatokat, majd a biztonságos aláírás-létrehozó eszköztől elkülönítve továbbítja a regisztrációs szervezethez;
- t) biztosítja, hogy alkalmazottai nem élhetnek vissza a biztonságos aláírás-létrehozó eszközzel.

A hitelesítő szervezet az **időbélyegzés** szolgáltatás biztosítása keretén belül:

- u) biztosítja, hogy az időbélyeg adatelemeket a helyes időpont belefoglalásával, biztonságosan bocsátja ki;
- v) biztosítja órájának a koordinált univerzális időalaphoz (UTC) szinkronizálását a meghatározott pontosság tartományon belül.

A hitelesítő szervezet a **visszavonási állapot közzététele** szolgáltatásban való közreműködés keretén belül:

- w) ellenőrzi a regisztráló szervezettől érkező visszavonási lista aláírási kérelmet, s ebben az aláírandó tanúsítvány visszavonási lista sértetlenségét és hitelességét;
- x) feldolgozza a regisztráló szervezettől érkező hiteles és sértetlen visszavonási lista aláírási kérelmet, melynek során aláírja a tanúsítvány visszavonási listát;
- y) rendszeresen új tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, naponta egyszer, a szolgáltatási szabályzat 4.4 alfejezetében meghatározott frissítési időponthoz igazodóan, mely tartalmazza a következő lista tervezett kibocsátási idejét is;
- z) rendkívüli esetben² új tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, mely tartalmazza a következő lista tervezett kibocsátási idejét is;
- aa) aláírásra átküldi a hitelesítő szervezetnek az új tanúsítvány visszavonási listát (a visszavonási lista aláírási kérelemben), biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét;
- ab) elküldi a címtárnak az új tanúsítvány visszavonási listát, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét;
- ac) megválaszolja a regisztráló szervezettől kapott visszavonási lista aláírási kérelmet, elküldve az aláírt tanúsítvány visszavonási listát, biztosítva a válaszüzenet sértetlenségét és hitelességét.

² Rendkívüli esetnek számít a hitelesítés-szolgáltató szolgáltatói magánkulcsának kompromittálódása, illetve jelentős számú új tanúsítvány visszavonási kérelem beérkezése.

2.1.3 A regisztrációs szervezet kötelezettségei -

- a) A regisztráló szervezet biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:
 - regisztráció,
 - visszavonás kezelés.
- b) A regisztrációs szervezet egyúttal közreműködik az alábbi elektronikus aláírással kapcsolatos szolgáltatások biztosításában:
 - tanúsítvány előállítás,
 - kibocsátás,
 - visszavonás.

A regisztrációs szervezet a **regisztráció** szolgáltatás keretén belül:

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

A regisztráló szervezet a **visszavonás kezelés** szolgáltatás keretén belül:

- l) ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét (lásd még 4.4.2 és 4.4.6), valamint szabályosságát (lásd még 4.4.3 és 4.4.7);
- m) haladéktalanul³ végrehajtja a hiteles, érvényes és szabályos, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket (vagyis a kérelmezett változást átvezeti a tanúsítványtár alapját képező tanúsítvány állapot adatbázisába);
- n) visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket;
- o) haladéktalanul⁴ intézkedik egy tanúsítvány visszavonásáról, amennyiben olyan tényről szerez tudomást, ami a tanúsítvány felhasználhatóságának biztonságát fenyegeti;
- p) folyamatosan⁵ és állandó rendelkezésre állással biztosítja a visszavonás kezelési szolgáltatást minden érdekelt fél számára, egyúttal szolgáltatási szabályzat 4.4 alfejezetében leírt módon megadja az előre tervezett és rendkívüli leállások leghosszabb időtartamát.

A regisztráló szervezet a **tanúsítvány előállítás** szolgáltatásban való közreműködés keretén belül:

- q) a kezdeti tanúsítvány előállítás során a regisztráció szolgáltatás e) és f) pontjában leírt módon összegyűjtött és ellenőrzött, tanúsítványba kerülő adatokat ellenőrzi az adott tanúsítványtípushoz kapcsolódó hitelesítési/ellenőrzési eljárás szerint. A tanúsítvány kibocsátásához szükséges ellenőrzések és visszaigazolások sikeres befejeződése után a hitelesítő szervezet felé tanúsítvány kibocsátási kérelem üzenetet indít el;
- r) biztosítja az aláírandó tanúsítványt is tartalmazó tanúsítvány-kérelem üzenetsértetlenségét, hitelességét és bizalmasságát.

A regisztráló szervezet a (tanúsítvány és szabályzat) **kibocsátás** szolgáltatásban való közreműködés keretén belül:

- s) fogadja a hitelesítő szervezettől kapott új tanúsítványokat és a szabályzó szervezettől kapott szabályzatokat, valamint ellenőrzi ezek hitelességét és sértetlenségét;
- t) elküldi a címtárnak az új tanúsítványokat, , biztosítva az ezeket tartalmazó üzenet hitelességét és sértetlenségét.

³ A szolgáltatási szabályzatban meghatározott időn belül.

⁴ A szolgáltatási szabályzatban meghatározott időn belül.

⁵ a hét 7 napján, a nap 24 órájában

2.1.4 Az aláíró és az előfizető kötelezettségei

2.1.4.1 Az aláíró kötelezettségei

A hitelesítés-szolgáltató az aláírókat megállapodáson keresztül (lásd a 2.6.1 és 4.1 alfejezeteket) különösen az alábbiakra kötelezi:

- a) pontos és teljes információt adjon be a regisztráló szervezethez jelen Tanúsítványtípus Szabályzat követelményeinek megfelelően, különös tekintettel a regisztrációra;
- b) a kulcspárt csak a vele közölt valamennyi korlátozásnak megfelelően használja;
- c) teljes gonddal járjon el, hogy megelőzze aláíró magánkulcsának illetéktelen felhasználását;
- d) magánkulcsát aláírásra csak a biztonságos aláírás-létrehozó eszközzel használja,
- e) késedelem nélkül értesítse a hitelesítés-szolgáltatót, amennyiben az alábbiak közül bármelyik bekövetkezik a tanúsítványban megadott érvényességi időszak vége előtt:
 - aláíró magánkulcsa elveszett, azt ellopták, esetlegesen kompromittálták,
 - aláíró elvesztette ellenőrzését magánkulcsa felett, aktivizálási adatai (például PIN kód) kompromittálódása, illetve más okokból kifolyólag,
- f) kompromittálódás esetén aláíró magánkulcsának használatát azonnal és véglegesen szakítsa meg.

2.1.4.2 Az előfizető kötelezettségei

A hitelesítés-szolgáltató az előfizetőt megállapodáson keresztül (lásd a 2.6.1 és 4.1 alfejezeteket) különösen az alábbiakra kötelezi:

- a) a regisztráló szervezetnél személyesen megjelenő, a minősített tanúsítványt és az ezzel kapcsolatos műveleteket igénylő aláírót lássa el meghatalmazással;
- b) pontos és teljes információt nyújtson be a regisztráló szervezethez jelen Tanúsítványtípus Szabályzat követelményeinek megfelelően, különös tekintettel a regisztrációra;
- c) teljes gonddal járjon el, hogy megelőzze az aláíró magánkulcsának illetéktelen felhasználását;
- d) késedelem nélkül értesítse a hitelesítés-szolgáltatót, amennyiben az alábbiak közül bármelyik bekövetkezik a tanúsítványban megadott érvényességi időszak vége előtt:
 - az aláíró magánkulcsa elveszett, azt ellopták, esetlegesen kompromittálták,

- az aláíró elvesztette ellenőrzését magánkulcsa felett, aktivizálási adatai (például PIN kód) kompromittálódása, illetve más okokból kifolyólag,
 - az előfizető tudomására jutott, hogy a tanúsítvány tartalmában vagy egyéb regisztrációs adatokban pontatlanság van, illetve változás következett be;
- e) A hitelesítés-szolgáltatás díjait a hatályos szabályzatok és Szolgáltatási Szerződés szerint fizesse meg.

2.1.5 Az érintett félre vonatkozó ajánlások

Az érintett felek számára rendelkezésre bocsátott kikötések és feltételek (lásd 2.6.1 alfejezetet) tartalmaznak egy megjegyzést, miszerint, ha ésszerű módon egy tanúsítványra kívánnak hagyatkozni, az alábbiakat szükséges tenniük:

- a) ellenőrizzék a tanúsítvány érvényességét az érvényes visszavonási állapot információ felhasználásával, a szabályzatoknak megfelelően;
- b) vegyék figyelembe a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, melyek a tanúsítványban és a szabályzatokban szerepelnek;
- c) tegyenek meg minden, megállapodásokban, illetve máshol előírt egyéb óvintézkedést.

2.1.6 A címtár kötelezettségei

- a) A címtár a hitelesítő szervezet részeként biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:
 - tanúsítvány **kibocsátás**,
 - **visszavonási állapot közzététele**.

A címtár a **kibocsátás** szolgáltatás keretén belül:

- b) közzé teszi a végfelhasználói tanúsítványokat;
- c) biztosítja a b) alatt szereplő információ folyamatos⁶ elérhetőségét, A címtár a **visszavonási állapot közzététele** szolgáltatás keretén belül;
- e) közzé teszi a hiteles és sértetlen új tanúsítvány visszavonási listát;
- f) biztosítja a legfrissebb tanúsítvány visszavonási lista folyamatos⁷ elérhetőségét,

⁶ A hét 7 napján, a nap 24 órájában.

⁷ A hét 7 napján, a nap 24 órájában.

2.2 Felelősség

2.2.1 A hitelesítés-szolgáltató általános felelőssége

- a) A hitelesítés-szolgáltató felelősséget vállal az általa támogatott Tanúsítványtípus Szabályzatban leírt eljárásoknak való megfeleléséért, még abban az esetben is, amikor a hitelesítés-szolgáltató egyes tevékenységeit alvállalkozók végzik⁸.
- b) A hitelesítés-szolgáltató a vele szerződéses jogviszonyban álló felekkel (ilyen az aláíró és az előfizető) szemben a Magyar Köztársaság Polgári Törvénykönyve (Ptk.) szerződésszegésért való felelősség szabályai szerint felelős.
- c) A hitelesítés-szolgáltató a vele szerződéses jogviszonyban nem álló harmadik féllel (ilyen az érintett fél) szemben a Ptk. szerződésen kívüli károkozásról szóló szabályai (Ptk. 339. §) szerint felelős.
- d) A hitelesítés-szolgáltató nem felelős az olyan kárért, mely abból adódott, hogy az érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és hitelesítés-szolgáltató szabályzatai szerint járt el, illetve nem úgy járt el, ahogyan az adott helyzetben általában elvárható.
- e) A hitelesítés-szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helyt állni.
- f) A hitelesítés-szolgáltató pénzügyi felelősségének korlátozását az ÁSZF 11. fejezete tartalmazza.

2.2.2 A hitelesítő szervezet felelőssége

- a) A hitelesítő szervezet felelős:
 - az általa kibocsátott tanúsítványok hitelességéért,
 - az általa kibocsátott szabályzatokért, azok jogszabályi megfeleléséért és betartásáért,
 - a generált kulcspárok megfeleléséért, a magánkulcs- nyilvános kulcs és tanúsítvány összetartozásáért,
 - az aláírás-létrehozó eszköz aktivizáló kódjának és az eszközre töltött kulcsok összetartozásáért,
 - általában kötelezettségei betartásáért.
- b) A hitelesítő szervezet nem felelős:

⁸ A hitelesítés-szolgáltató általánosan felelős a hitelesítő szervezet, a regisztráló szervezet, valamint a címtár kötelezettségeiért, tevékenységeiért.

- az előfizetők és aláírók magánkulccsal, illetve aláírás-létrehozó eszközzel kapcsolatos tevékenységeiért,
- az érintett felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért.
- az előfizetők, érintett felek, és mások által kibocsátott szabályzatokért.

2.2.3 A regisztráló szervezet felelőssége

- a) A regisztráló szervezet felelős:
- az aláírók és előfizetők személyes, illetve szervezeti azonosságának megállapításáért,
 - a felvett regisztrációs adatok valódiságáért,
 - általában kötelezettségei betartásáért.

2.2.4 Az aláíró felelőssége

- a) Az aláíró felelős:
- regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért,
 - az adatokban bekövetkezett változások bejelentéséért,
 - magánkulcsának és aláírás-létrehozó eszközének a szabályzatoknak megfelelő felhasználásáért,
 - magánkulcsának és aktivizáló kódjának biztonságáért,
 - a biztonságos aláírás-létrehozó eszköz biztonságáért,
 - általában kötelezettségei betartásáért.

2.2.5 Az előfizető felelőssége

- a) Az előfizető felelős:
- regisztráció során megadott, szervezetére vonatkozó adatai valódiságáért, pontosságáért és érvényességéért,
 - az adatokban bekövetkezett változások bejelentéséért,
 - a szolgáltatási díjak megfizetéséért.
 - általában kötelezettségei betartásáért.

2.2.6 Az érintett fél felelőssége

- a) Az érintett fél felelős:
- a tanúsítványok elfogadása során tanúsított körültekintő eljárásért,
 - általában kötelezettségei betartásáért.
- b) Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a Tanúsítványtípus Szabályzat, a szolgáltatási szabályzat illetve a hatályos jogszabályok szerint jár el.

2.3 Pénzügyi felelősség

- a) A hitelesítés-szolgáltató megfelelő megoldásokkal rendelkezik a műveleteiből és tevékenységeiből származó kötelezettségek fedezésére, különösképpen a kárfelelősség kockázatára vonatkozóan.
- b) A hitelesítés-szolgáltató rendelkezik a jelen dokumentumban foglaltakkal összhangban álló üzemeltetéshez szükséges pénzügyi stabilitással és erőforrásokkal.

2.3.1 A hitelesítés-szolgáltatóval szembeni kártérítés

- a) Az előfizetők és az érintett felek kártérítési felelősséggel tartoznak a hitelesítés- szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket kötelezettségeik be nem tartásával okoznak számára.

2.3.2 Adminisztratív folyamatok

- a) A hitelesítés-szolgáltató a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) azokat. (Részletesebben lásd a 4.5. és 4.6 alfejezeteket.)

2.4 Értelmezés és érvényesítés

2.4.1 Irányadó jog

A hitelesítés-szolgáltató tevékenységét a következő jogszabályok szabályozzák⁹:

- a) 2001. évi XXXV. törvény az elektronikus aláírásról¹⁰.
- b) 100/2000. (VI. 23.) Korm. rendelet az információs társadalom megvalósításával összefüggő feladatokról, az informatikai kormánybiztos feladat- és hatásköréről.
- c) 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.
- d) 1014/2001. (III.5.) Korm. határozat az elektronikus aláírásról szóló törvény alapelveiről és az ezzel kapcsolatban szükséges intézkedésekről szóló 1075/2000. (IX.13.) Korm. határozat módosításáról.

⁹ A jogszabályok szövege elérhető a Hatóság honlapján keresztül, a www.nhh.hu címen.

¹⁰ A törvényt kiegészítő, alább felsorolt alacsonyabb szintű jogszabályok a 2003 december 31.-i állapotot tükrözik. A lista folyamatos nyomon követése, és érdemi változás esetén frissítése a szolgáltatási szabályzat készítőinek feladata.

- e) 151/2001. (IX. 1.) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat-és hatásköréről, valamint eljárásainak részletes szabályairól.
- f) 20/2001. (XI.15.) MeHVM rendelet a Nemzeti Hírközlési Hatóság az elektronikus aláírással összefüggő minősítéssel nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról.
- g) 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- h) 15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
- i) 1026/2002. (III. 26.) Kormányhatározat a kormányzati elektronikus aláírási rendszer kiépítésével összefüggő egyes feladatokról és a kormányzati központi kormányzati hitelesítés-szolgáltató felállításáról.
- j) 47/2002. (III. 26.) Korm. rendelet a kormányzati elektronikus aláírási rendszer kiépítésével összefüggő egyes kormányrendeletek módosításáról.
- k) 2/2002 (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.
- l) 7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről.

2.4.2 Érvénytelenség, fennmaradás, megszűnés, értesítések

Érvénytelenség

- a) Amennyiben jelen Tanúsítványtípus Szabályzat valamely pontja érvénytelen lenne, jelen dokumentum egészének és más pontjainak érvényességét nem érinti.

Fennmaradás

- b) Jelen Tanúsítványtípus Szabályzat 2. fejezete érvényben marad a jelen dokumentum hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, melyet jelen szabályzat hatálya alatt bocsátott ki a hitelesítés-szolgáltató.

Megszűnés

- c) Jelen Tanúsítványtípus Szabályzat a Közösség (lásd 1.3) valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A Tanúsítványtípus Szabályzat egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében. A Tanúsítványtípus Szabályzat csak

írott és hitelesített formában módosítható, a Hatóság által vezetett Tanúsítványtípus Szabályzat nyilvántartásban való átvezetés mellett.

Értesítések

- d) Az előfizető és aláíró jognyilatkozatait hitelesítés-szolgáltató felé, kizárólag írásban, hivatalosan aláírt módon teheti meg. Az előfizető és az aláíró egyéb esetekben a hitelesítés-szolgáltatót írásban, elektronikus levél vagy fax formájában is értesítheti. A hitelesítés-szolgáltató értesítési címei a szolgáltatási szabályzat 1.4 alfejezetben találhatóak.
- e) A hitelesítés-szolgáltató ügyfeleit a honlapján történő közzététel útján vagy elektronikus levélben tájékoztathatja.

2.4.3 Vitás kérdések megoldására vonatkozó eljárások

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

2.5 Díjak

A hitelesítés-szolgáltató szolgáltatásainak díjazására vonatkozó információt a hitelesítés-szolgáltató szabályzatai tartalmazzák.

2.6 Közzététel és címtár

2.6.1 Hitelesítés-szolgáltatói információ közzététele

Kikötések és feltételek közzététele:

A hitelesítés-szolgáltató gondoskodik arról, hogy kikötései és egyéb feltételei az aláírók, előfizetők és az érintett felek rendelkezésére álljanak.

Különösképpen:

- a) A hitelesítés-szolgáltató az aláírók/előfizetők és az érintett felek rendelkezésére bocsátja a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, köztük az alábbiakat:
 - az alkalmazott Tanúsítványtípus Szabályzatot, beleértve egy egyértelmű nyilatkozatot arra vonatkozóan, hogy a Tanúsítványtípus Szabályzat a nyilvánosság részére kibocsátott tanúsítványokra vonatkozik, és hogy megköveteli-e bármilyen speciális termék, alkalmazás vagy eszköz

használatát¹¹ a kibocsátandó tanúsítvánnyal összekapcsolt kulcspár alkalmazására;

- a tanúsítványok használatára vonatkozó bárminemű korlátozást;
- az előfizető kötelezettségeit a 2.1.3 alfejezetben meghatározottaknak megfelelően;
- a tanúsítvány ellenőrzésének mikéntjére vonatkozó információt, beleértve a tanúsítvány visszavonási állapot ellenőrzésére vonatkozó követelményeket, oly módon, hogy az érintett fél "ésszerű módon hagyatkozhatson" a tanúsítványra (lásd 2.1.4);
- a felelősségvállalásra vonatkozó bármilyen korlátozást, beleértve azokat az okokat/használatokat, melyek esetén a hitelesítés-szolgáltató elfogadja, illetve visszautasítja a felelősség vállalását (lásd 2.2);
- információt arról az időtartamról, amíg a regisztrációs információt (lásd 3.1) megőrzik;
- információt arról az időtartamról, amíg a hitelesítés-szolgáltató eseménynaplóját (lásd 4.5) megőrzik;
- információt reklamációkról és viták rendezésére vonatkozó eljárásokról (lásd 2.4.3);
- információt az alkalmazandó jogról (lásd 2.4.1); és
- az, hogy a hitelesítés-szolgáltatónak az adott Tanúsítványtípus Szabályzatnak való megfelelése értékelésre került-e, s hogy ez milyen tanúsító rendszeren keresztül történt (lásd 2.7).

- b) A hitelesítés-szolgáltató elérhetővé teszi a fenti a) pontban meghatározott információt Internetes honlapján keresztül, közérthetően megfogalmazva, elektronikusan továbbítható formában.

Tanúsítványok nyilvánosságra hozatala:

A hitelesítés-szolgáltató gondoskodik arról, hogy a tanúsítványok szükség esetén az előfizetők, aláírók és az érintett felek rendelkezésre álljanak. Részletesebben:

- c) az előállítás után a teljes és pontos tanúsítvány rendelkezésre áll azon aláíró számára, akinek a tanúsítvány kibocsátásra került;
- d) a tanúsítványok csak azokban az esetekben nem érhetőek el más számára, ha az előfizető és az aláíró ill. a hitelesítés-szolgáltató így állapodtak meg;
- e) a hitelesítés-szolgáltató az érintett felek rendelkezésére bocsátja a tanúsítvány használatával kapcsolatos kikötéseket és feltételeket;
- f) egy adott tanúsítvánnyal kapcsolatban a vonatkozó kikötések és feltételek könnyen azonosíthatók.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala:

A hitelesítés-szolgáltató gondoskodik arról, hogy hiteles és érvényes tanúsítvány visszavonási és felfüggesztési kérelmek esetén a tanúsítványok időben visszavonásra,

¹¹ Ezek közt jelen tanúsítványtípusra szerepel a biztonságos aláírás-létrehozó eszköz használatának követelménye.

illetve felfüggesztésre kerüljenek, egyúttal ezen információ nyilvánosságra kerüljön. Részletesebben:

- g) a hitelesítés-szolgáltató szolgáltatási szabályzat 4.4 alfejezetében dokumentálja a tanúsítványok visszavonásának és felfüggesztésének eljárásait, beleértve az alábbiakat:
 - a visszavonási állapot információk nyilvánosságra hozatalánál használt mechanizmusok,
 - a legnagyobb késedelem a visszavonási és felfüggesztési kérelem fogadása, és az összes érintett fél rendelkezésére álló információk állapotának megváltozása között.
- h) biztosítja, hogy a tanúsítvány visszavonási listákra teljesüljenek az alábbiak:
 - minden egyes visszavonási lista tartalmazza a következő visszavonási lista kibocsátási időpontját,
 - új visszavonási lista közzétehető a következő visszavonási lista kibocsátására megadott időpont előtt is,
 - a visszavonási listát a hitelesítő szervezet a hitelesítés-szolgáltató nevében elektronikusan aláírja.

2.6.2 A közzététel gyakorisága

Lásd a szolgáltatási szabályzat 2.6.2 pontját.

2.6.3 Hozzáférés ellenőrzések

- a) A hitelesítés-szolgáltató a nyilvánosságnak bocsát ki tanúsítványt, ezért a tanúsítványok, valamint a tanúsítványok használatára vonatkozó kikötések és feltételek nyilvánosak, szabványos felületen bárki által elérhetők;
- b) A visszavonásra és felfüggesztésre vonatkozó kérelmeket hitelesíteni kell, a hitelesítés-szolgáltató feldolgozás előtt ellenőrzi, hogy hiteles forrásból származnak-e. A nem írásban tett visszavonási kérelmeket, írásban hivatalos aláírással ellátva is meg kell erősíteni.
- c) A hitelesítés-szolgáltató a nyilvánosságnak bocsát ki tanúsítványt, ezért a visszavonási állapotokat tartalmazó tanúsítvány visszavonási listák nyilvánosak, szabványos felületen bárki által elérhetők.

2.6.4 Címtárak

- a) A hitelesítés-szolgáltató a tanúsítványokat, valamint a tanúsítvány visszavonási listákat címtárán, a tanúsítványok használatára vonatkozó kikötéseket és feltételeket honlapján, keresztül teszi hozzáférhetővé.
- b) A honlap ill. címtár elérhetőségét, valamint az általa biztosított szabványos felületeket és támogatott lekérdezési műveleteket a szolgáltatási szabályzat 2.6 alfejezete határozza meg.

2.7 A megfelelés vizsgálat

- a) A hitelesítés-szolgáltatót fokozott biztonságú szolgáltatóként 2001. december 21-én a Hírközlési Felügyelet nyilvántartásba vette, minősített szolgáltatóként való nyilvántartásba vételét 2004. március 25.-én kezdeményezte, és a hatósági nyilvántartásba vételtől kezdve működik nyilvántartott minősített hitelesítés-szolgáltatóként.
- b) A Hatóság a hitelesítés-szolgáltató bejelentése alapján a jelen dokumentumban megnevezett Tanúsítványtípus Szabályzatot nyilvántartásába felvette.
- c) A hitelesítés-szolgáltató olyan elektronikus aláírási termékeket használ „elektronikus aláírás hitelesítésszolgáltatás” szolgáltatásához (a szolgáltatói kulcspárok előállításához, a kibocsátott tanúsítványok és tanúsítvány visszavonási listák aláírásához, valamint az ehhez szükséges magánkulcsok tárolásához), mely szerepel a Hatóság „tanúsított elektronikus aláírási termékek” listáján.
- d) A hitelesítés-szolgáltató az „aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése” szolgáltatásához olyan biztonságos aláírás-létrehozó eszközt használ fel, mely szerepel a Hatóság „tanúsított elektronikus aláírási termékek” listáján.

2.7.1 A megfelelés vizsgálatának gyakorisága

- a) A minősített szolgáltatókra vonatkozó követelményeknek, valamint a Tanúsítványtípus Szabályzat való megfelelés rendszeres felülvizsgálata érdekében a Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart hitelesítés-szolgáltatónál.
- b) A hitelesítés-szolgáltató által felhasznált elektronikus aláírási termékek megfelelés vizsgálatának gyakoriságát, illetve egyéb más megfelelési vizsgálatok gyakoriságát a szolgáltatási szabályzat 2.7 alfejezete határozza meg.

2.7.2 Az átvizsgáló szervezet megnevezése/jellemzői

- a) A minősített szolgáltatókra vonatkozó követelményeknek, valamint a Tanúsítványtípus megfelelés vizsgálatát a Hatóság végzi.
- b) A hitelesítés-szolgáltató által felhasznált elektronikus aláírási termékek megfelelés vizsgálatát, illetve tanúsítását végző szervezeteket, illetve az egyéb megfelelési vizsgálatokat végző szervezeteket a szolgáltatási szabályzat 2.7 alfejezete nevezi meg.

2.7.3 Az átvizsgáló szervezet és a vizsgált fél kapcsolata

- a) A Hatóság minősítési eljárásában résztvevő szakértők a Matáv Rt. hitelesítés-szolgáltatótól függetlenek, tevékenységüket befolyástól mentesen végzik.

2.7.4 A vizsgálat által érintett területek

- a) Az elektronikus aláírással kapcsolatos szolgáltatásokra vonatkozó minősítő eljárás az [1] törvény 3. számú mellékletének, a [3] rendelet előírásainak, valamint a hitelesítés-szolgáltató szabályzatainak (való megfelelés vizsgálatára irányul.

2.7.5 Hiányosságok esetén végrehajtandó tevékenységek

- a) A minősítő eljárás, vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a hitelesítés-szolgáltató késlekedés nélkül megszünteti a vizsgálatot végző Hatóság kapott információ és ajánlások alapján.

2.7.6 Az eredményekről való tájékoztatás

- a) Lásd a szolgáltatási szabályzat 2.7.6 pontját.

2.8 Bizalmasság

A hitelesítés-szolgáltató az adatok bizalmas kezelésével kapcsolatban gondoskodik a jogszabályoknak való megfelelésről. Ennek keretén belül:

- a) a fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól. A jogszabályoknak való megfelelés, valamint az alapvető üzleti tevékenységek támogatása érdekében szükség van bizonyos bejegyzések biztonságos megőrzésére is. (lásd 4.5 és 4.6);
- b) gondoskodik az adatvédelmi törvényeknek való megfelelésről;
- c) megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen kezelése ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen;
- d) nyilvántartásba veszi az előfizetővel és az aláíróval aláírt megállapodást, beleértve az alábbiakat:
 - hozzájárulás az alábbi szolgáltatások során felhasznált információ hitelesítés-szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az aláírók eszközzel való ellátása, időbélyegzés,
 - a hitelesítés-szolgáltató szolgáltatásainak leállítása esetén hozzájárulás a nyilvántartásba vett információ harmadik félhez történő továbbításához a vonatkozó szabályzat megkövetelt feltételei szerint,

- hogy az előfizető vagy aláíró megköveteli-e a tanúsítvány közzétételének mellőzését.
- e) gondoskodik az aláíróra és az előfizetőre vonatkozó információ bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk¹² hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja;
- f) védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az előfizetővel/aláíróval folytatott, illetve a hitelesítő szervezet – regisztráló szervezet – címtár rendszerkomponensek közötti adatcsere során is.

2.8.1 Bizalmasan kezelendő információ típusok

- a) A hitelesítés-szolgáltató bizalmas információként kezeli az előfizető és az aláíró minden adatát, kivéve azokat, amelyeket a 2.8.2 alfejezet tárgyal.
- b) A hitelesítés-szolgáltató a birtokába jutott bizalmas információt a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvénynek megfelelően kezeli, s csak a 2.8.3-2.8.7 alfejezetekben említett esetekben és személyek/szervezetek részére fedi fel őket.
- c) Szolgáltató ezen kívül bizalmas információként kezeli a következő adatokat és dokumentumokat:
 - magánkulcsok és aktivizáló kódok,
 - tanúsítványigénylések és előfizetői szerződések,
 - tranzakciós és napló adatok,
 - nem nyilvános szabályzatok,
 - minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

2.8.2 Nem bizalmasnak tekintett információ típusok

- a) A hitelesítés-szolgáltató nem bizalmas információként kezeli mindazon adatokat, melyet a tanúsítványba belefoglal. Ezek az adatok a tanúsítványigénylő úrlapon egyértelműen jelölve vannak.

2.8.3 Tanúsítvány visszavonására/felfüggesztésére vonatkozó információ felfedése

- a) A hitelesítés-szolgáltató az általa kibocsátott tanúsítványok visszavonását és felfüggesztését tanúsítvány-visszavonási listákban teszi közzé, a szolgáltatási szabályzat 2.6 alfejezetében meghatározott tartalommal, jellemzőkkel, illetve általa támogatott keresési lehetőségekkel.

2.8.4 Információszolgáltatás hatósági szervek részére

- a) A hitelesítés-szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre meghatározott jogszabályi

¹² vagy nevükben az előfizető

feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak feltárhat jogszabályban meghatározott bizalmas felhasználói információkat az [1] törvény 11.§ (2) bekezdése szerint.

- b) A hitelesítés-szolgáltató rögzíti az a) pontbeli adatátadás tényét, de arról nem tájékoztatja sem az előfizetőt, sem az aláíró.

2.8.5 Információszolgáltatás polgári eljárás keretében

- a) A hitelesítés-szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során – az érintettség igazolása esetén – az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhat jogszabályban meghatározott bizalmas felhasználói információkat az [1] törvény 11.§ (3) bekezdése szerint.
- b) A hitelesítés-szolgáltató rögzíti az a) pontbeli adatátadás tényét, és arról tájékoztatja az előfizetőt és az aláíró.

2.8.6 A tulajdonos kérésére történő felfedés

- a) Az aláíró és az előfizető hozzáférhet a rá vonatkozó regisztrációs és egyéb információhoz.

2.8.7 Egyéb információ közzététel eredményező körülmények

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

2.9 Szellemi tulajdonjogok

- a) A hitelesítés-szolgáltató által kibocsátott végfelhasználói tanúsítvány és az ennek megfelelő kulcspár tulajdonosa az előfizető, teljes jogú kizárólagos használója pedig az aláíró, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.
- b) A hitelesítés-szolgáltató a tanúsítványt a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja, s egyéb módon kezelheti.
- c) A visszavonási információ a hitelesítés-szolgáltató tulajdonát képezi.
- d) A hitelesítés-szolgáltató által az aláíró részére kibocsátott egyedi azonosító a hitelesítés-szolgáltató tulajdonát képezi.
- e) A tanúsítványban szereplő megkülönböztető név használatára a megnevezett aláíró jogosult.
- f) Az aláíró egyedi azonosítójában szereplő bármilyen védjegy, szervezeti- és személy név, egyéb adat az előfizető vagy aláíró tulajdonát képezheti.

-
- g) A hitelesítés-szolgáltató szabályzatai, szerződéses feltételei a hitelesítés-szolgáltató tulajdonát képezik.
- h) A tanúsítványban szereplő hitelesítő azonosító a hitelesítés-szolgáltató tulajdonát képezi.

3. Azonosítás és hitelesítés

3.1 Kezdeti regisztrálás

A hitelesítés-szolgáltató a kezdeti regisztrálás során:

- a) gondoskodik arról, hogy az aláíró és az előfizető tanúsítvány kérelmei pontosak, hitelesek és teljeseek legyenek;
- b) megfelelő, hiteles források (hatósági adatbázisok) igazolásán alapulva megvizsgálja az aláírók és előfizetők azonosságára vonatkozó bizonyítékokat, valamint nevük és a hozzá kapcsolódó adatok pontosságát.

3.1.1 Név típusok

Lásd a szolgáltatási szabályzat 3.1.1 pontjában.

3.1.2 Igény a nevek értelmezhetőségére

Lásd a szolgáltatási szabályzat 3.1.2 pontjában.

3.1.3 Különböző elnevezési formák értelmezési szabályai

Lásd a szolgáltatási szabályzat 3.1.3 pontjában.

3.1.4 A nevek egyedisége

- a) A hitelesítés-szolgáltató gondoskodik arról, hogy, a tanúsítványban általa használt megkülönböztetett nevet annak teljes élettartama alatt nem rendeli egy másik személyhez.

A részletekért lásd a szolgáltatási szabályzat 3.1.4 pontját.

3.1.5 Eljárások a nevekre vonatkozó vitás kérdések megoldására

Lásd a szolgáltatási szabályzat 3.1.5 pontját.

3.1.6 Márkanevek elismerése, hitelesítése és szerepe

Lásd a szolgáltatási szabályzat 3.1.6 pontját.

3.1.7 A magánkulcs birtoklásának bizonyítási módszere

Lásd a szolgáltatási szabályzat 3.1.7 pontját.

3.1.8 A szervezeti azonosság hitelesítése

Lásd a szolgáltatási szabályzat 3.1.8 pontját.

3.1.9 Személyazonosság hitelesítése

Lásd a szolgáltatási szabályzat 3.1.9 pontját.

3.2 *Érvényes tanúsítvány megújítása*

- a) A hitelesítés-szolgáltató nem teszi lehetővé az érvényes tanúsítványok megújítását.

3.3 *Érvénytelen tanúsítvány megújítása*

- a) A hitelesítés-szolgáltató nem teszi lehetővé lejárt, visszavont vagy felfüggesztett tanúsítvány megújítását.

3.4 *Visszavonási és felfüggesztési kérelem*

- a) A hitelesítés-szolgáltató lehetővé teszi érvényes tanúsítvány visszavonásának és felfüggesztésének személyes megjelenést nem igénylő megvalósítását a szolgáltatási szabályzat 4.4 alfejezetében meghatározott módon és feltételekkel.
- b) A hitelesítés-szolgáltató gondoskodik arról, hogy az a) pontban meghatározott, egy már korábban nála nyilvántartásba vett aláírótól származó tanúsítvány visszavonási vagy felfüggesztési kérelem teljes, pontos és kellőképpen hiteles legyen. Ennek érdekében a hitelesítés-szolgáltató szolgáltatási szabályzatának részeként (a 4.4 alfejezetben) dokumentálja a tanúsítványok visszavonásának, felfüggesztésének eljárásait, beleértve az alábbiakat:
 - ki adhat be és milyen formában visszavonási, felfüggesztési kérelmeket,
 - mik a visszavonási kérelmek megerősítésére vonatkozó esetleges követelmények,
 - milyen okból vonható vissza és milyen okból függeszthető fel egy tanúsítvány,
 - mi a felfüggesztett állapot maximális időtartama.

4. Működésre vonatkozó követelmények

4.1 Tanúsítvány-kérelem

Lásd a szolgáltatási szabályzat 4.1 pontját.

4.2 Tanúsítvány kibocsátás

Lásd a szolgáltatási szabályzat 4.2 pontját.

4.3 Tanúsítvány elfogadás

Lásd a szolgáltatási szabályzat 4.3 pontját.

4.4 Tanúsítvány felfüggesztés és visszavonás

Lásd a szolgáltatási szabályzat 4.4 pontját.

4.5 A biztonsági naplózás folyamatai

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

Jelen dokumentum csak a tanúsítványokra vonatkozó adatok (regisztrációs információ, a hitelesítés-szolgáltató kulcsgondozási és tanúsítványgondozási eseményeire vonatkozó fontosabb információ) naplózási folyamatának általános jellegzetességeit adja meg az alábbiakban:

- b) A hitelesítés-szolgáltató a környezetére, kulcs- és tanúsítvány gondozására vonatkozó események pontos időpontját is rögzíti¹³.
- c) A hitelesítés-szolgáltató biztosítja személyzete felelősségre vonhatóságát tevékenységéért, többek között az eseménynapló megőrzésén és védelmén keresztül (lásd 4.5.1, 4.5.4, 4.5.5).

¹³ A szolgáltatási szabályzat ismerteti az események időzítéséhez használt óra pontosságát, és azt, hogy ez a pontosság hogyan van biztosítva.

4.5.1 A tárolt események típusai

Lásd a szolgáltatási szabályzat 4.5.1 pontját.

4.5.2 A napló állomány feldolgozásának gyakorisága

Lásd a szolgáltatási szabályzat 4.5.2 pontját.

4.5.3 A napló állomány megőrzési időtartama

Lásd a szolgáltatási szabályzat 4.5.3 pontját.

4.5.4 A napló állomány védelme

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

4.5.5 A napló állomány mentési folyamatai

Lásd a szolgáltatási szabályzat 4.5.5 pontját.

4.5.6 A napló gyűjtési rendszere

Lásd a szolgáltatási szabályzat 4.5.6 pontját.

4.5.7 Az eseményeket kiváltó aláírók értesítése

- a) A hitelesítés-szolgáltató nem értesíti a naplóbejegyzéseket kiváltó érintetteket, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába.

4.5.8 Sebezhetőség felmérése

Lásd a szolgáltatási szabályzat 4.5.8 pontját.

4.6 Adatok archiválása

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

4.6.1 A tárolt események típusai

- a) A hitelesítés-szolgáltató gondoskodik arról, hogy rögzítésre kerüljön az összes regisztrációs információ.
- b) A tanúsítványokra vonatkozó valamennyi naplóbejegyzés archiválásra kerül.
- c) Azon eseményeket, melyek a fent említett naplóbejegyzéseken túl kerülnek archiválásra (a biztonságos környezet fenntartásának és utólagos ellenőrizhetősége és bizonyíthatósága céljából), a hitelesítés-szolgáltató szolgáltatási szabályzat 4.6.1 pontjában határozza meg.

4.6.2 Az archívum megőrzési időtartama

- a) A hitelesítés-szolgáltató a 4.1. d) és e) pontjában megnevezett nyilvántartásokat megőrzi a tanúsítvány érvényességének lejártától számított tíz évig, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig.
- b) A hitelesítés-szolgáltató az a) pontban meghatározott adatokon kívüli napló adatokat (lásd 4.5.1.a)-g) pontokat) a keletkezésüktől számított tíz évig megőrzi.
- c) A hitelesítés-szolgáltató Tanúsítványtípus Szabályzatait és szolgáltatási szabályzatait hatályon kívül helyezésüktől számított tíz évig megőrzi.

4.6.3 Az archívum védelme

- a) A hitelesítés-szolgáltató fenntartja a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét.
- b) A hitelesítés-szolgáltató a tanúsítványokra vonatkozó naplóadatokat teljes körűen és a bizalmasságot garantáló módon archiválja a szolgáltatási szabályzat 4.6.3 pontjában leírt üzleti gyakorlatnak megfelelően.
- c) A hitelesítés-szolgáltató a bejegyzéseket megvédi az elveszéstől, tönkretételtől és hamisítástól.
- d) A hitelesítés-szolgáltató megfelelő műszaki és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen feldolgozása ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen.

4.6.4 Az archívum mentési folyamatai

- a) Az archívum mentési folyamatait a hitelesítés-szolgáltató szolgáltatási szabályzat 4.6.4 pontja határozza meg.

4.6.5 A rekordok időbélyegzésére vonatkozó követelmények

Lásd a szolgáltatási szabályzat 4.6.5 pontját.

4.6.6 Az archívum gyűjtési rendszere

Lásd a szolgáltatási szabályzat 4.6.6 pontját.

4.6.7 Archív információ hozzáférését és ellenőrzését végző eljárások

- a) A hitelesítés-szolgáltató a tanúsítványokra vonatkozó adatokat rendelkezésre bocsátja, ha arra jogi eljárásokban bizonyíték nyújtása céljából szükség van.
- b) Az aláíró, és az adatvédelmi követelmények korlátozásain belül az előfizető hozzáférhet az aláíróra vonatkozó regisztrációs és egyéb információhoz.

4.7 Tanúsítványmegújítás

- a) A hitelesítés-szolgáltató nem teszi lehetővé az érvényes tanúsítványok megújítását.

4.8 Helyreállítás rendkívüli üzemi helyzetek esetén

- a) A hitelesítés-szolgáltató a rendkívüli üzemeltetési helyzetek esetére olyan eljárásokat dolgozott ki, amely lehető teszi a megbízható üzemmenet mielőbbi helyreállítását.
- b) A hitelesítés-szolgáltató gondoskodik arról, hogy rendkívüli üzemeltetési helyzet bekövetkezése esetén, beleértve a saját magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, a visszavonási nyilvántartások megbízható helyreállítása maradéktalanul megtörténjen.
- c) Rendkívüli üzemeltetési helyzet bekövetkezése esetén a hitelesítés-szolgáltató haladéktalanul értesíti a Hatóság, valamint a szolgáltatást igénybe vevő mindazon személyeket, akiket a rendkívüli üzemeltetési helyzet érint.

4.8.1 Sérült számítási erőforrások, szoftverek és/vagy adatok

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

4.8.2 A szolgáltatói egység nyilvános kulcsának visszavonása

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

4.8.3 Egy szolgáltatói egység kulcsának kompromittálódása

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

4.8.4 Működési képesség természeti vagy más katasztrófát követően

- a) Természeti vagy más katasztrófát követően a hitelesítés-szolgáltató életbe lépteti az üzlet folytonossági terve (illetve katasztrófa utáni helyreállítási terve) által előírt eljárásokat annak érdekében, hogy az üzemeltetés helyreálljon a szolgáltatási szabályzat 4.8 alfejezetében megjelölt időn belül.
- b) Katasztrófát követően a hitelesítés-szolgáltató ésszerű lépéseket tesz a katasztrófa ismételt bekövetkezésének megakadályozására.

4.9 A hitelesítésszolgáltatás leállítása

Lásd a szolgáltatási szabályzat 4.9 alfejezetét.

5. Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A biztonsági óvintézkedésekről általában:

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

- a) A hitelesítés-szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározása érdekében.
- b) A hitelesítés-szolgáltató felelősséget vállal minden elektronikus aláírással kapcsolatos szolgáltatásért még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki. c) A hitelesítés-szolgáltató vezetősége (mely felelős a hitelesítés-szolgáltató informatikai biztonság politikájának meghatározásáért, és e politika által érintett valamennyi alkalmazott részére történő közzétételért) az információ biztonságára vonatkozó útmutatót hagyott jóvá és adott ki.
- d) A hitelesítés-szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bármilyen változtatást a hitelesítés-szolgáltató vezetősége hagyja jóvá.
- e) A hitelesítés-szolgáltató (rendszerbiztonsági szabályzatában) dokumentálta, majd megvalósította és folyamatosan fenntartja a hitelesítési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait.
- f) A hitelesítés-szolgáltató gondoskodik az informatika biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez, illetve egységhez lettek kiadva.
- g) A hitelesítés-szolgáltató biztonsági műveleteiért a végső felelősség a hitelesítés-szolgáltatót terheli. Ezen biztonsági műveletek közé az alábbiak tartoznak:
 - üzemeltetési eljárások és felelősségek,
 - biztonsági rendszerek tervezése és elfogadása,
 - káros szoftver elleni védelem,
 - erőforrás gazdálkodás,
 - hálózat menedzselés,
 - a biztonsági napló aktív felügyelete, eseményelemzések és nyomkövetések,
 - adathordozó eszköz kezelése és biztonsága,
 - adat és szoftver csere.

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

Az értékek osztályozása és kezelése

A hitelesítés-szolgáltató gondoskodik arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek. Különösképpen:

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

5.1 Fizikai óvintézkedések

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

5.1.1 A telephely elhelyezése és szerkezeti felépítése

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

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

Tanúsítvány előállítással, aláírók eszközzel való ellátásával, visszavonás kezeléssel kapcsolatosan:

- c) A hitelesítés-szolgáltató egy egyértelműen meghatározott biztonsági körlet létrehozásával fizikai védelmet biztosít az alábbi szolgáltatások számára:
 - tanúsítvány előállítás,
 - az aláírók eszközzel való ellátása,
 - visszavonás kezelés,
 - időpecsét kibocsátás.
- d) A hitelesítés-szolgáltató óvintézkedéseket valósít meg a fizikai és környezetbiztonsági rendszer erőforrások, illetve a működésük támogatására használt berendezések megvédése érdekében. A hitelesítés-szolgáltató a:
 - tanúsítvány előállítás,
 - az aláírók eszközzel való ellátása,
 - visszavonás kezelés,

- időpecsét kibocsátás.

szolgáltatásainak fizikai- és környezetbiztonsági programjai foglalkoznak a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelem és tűzbiztonság tényezőivel, a támogató eszközök (ezen belül az áram és klíma berendezések) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, katasztrófa utáni helyreállítással, stb.

- e) A hitelesítés-szolgáltató óvintézkedéseket valósít meg annak megakadályozása érdekében, hogy az elektronikus aláírással kapcsolatos szolgáltatáshoz szükséges berendezést, információt, adathordozót vagy szoftvert jogosulatlanul elvigyék a helyszínről.

5.1.2 Fizikai hozzáférés

- a) A hitelesítés-szolgáltató a
- tanúsítvány előállítás,
 - az aláírók eszközzel való ellátása,
 - visszavonás kezelés

szolgáltatásokkal kapcsolatos eszközökhöz történő fizikai hozzáférést megfelelően felhatalmazott egyénekre korlátozza.

- b) A hitelesítés-szolgáltató a
- tanúsítvány előállítás,
 - az aláírók eszközzel való ellátása,

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

5.1.3 Áramellátás, légkondicionálás

Lásd az 5.1.1. d) pontot, illetve a szolgáltatási szabályzat 5.1.3 pontját.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

Lásd az 5.1.1. d) pontot, illetve a szolgáltatási szabályzat 5.1.4 pontját.

5.1.5 Tűzmegelőzés és tűzvédelem

Lásd az 5.1.1. d) pontot, illetve a szolgáltatási szabályzat 5.1.5 pontját.

5.1.6 Adathordozók tárolása

- a) A hitelesítés-szolgáltató az adathordozó eszközöket biztonságosan kezeli a sérülés, eltulajdonítás és jogosulatlan hozzáférés elleni védelem érdekében¹⁴.
- b) A hitelesítés-szolgáltató az összes adathordozó eszközt biztonságosan kezeli az adat-minősítési rendszer követelményeinek megfelelően (lásd 5. h.).

5.1.7 Selejt kezelése, megsemmisítése

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

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

Lásd a szolgáltatási szabályzat 5.1.8. pontját.

5.2 Eljárásbeli óvintézkedések

A hitelesítés-szolgáltató gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék.

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

5.2.1 Bizalmi munkakörök

Hitelesítés-szolgáltató a következő bizalmi munkaköröket határozza meg:

- Biztonsági tisztviselő,
- Rendszeradminisztrátor,
- Regisztráció tisztviselő,
- Regisztrációs ügyeleti operátor,
- Rendszeroperátor,
- Rendszervizsgáló.

Bizalmi munkakörökkel kapcsolatos részletes leírást a szolgáltatási szabályzat 5.2.1 pontja tartalmazza.

¹⁴ A személyzet minden irányítói felelősséggel rendelkező tagja felelős a tanúsítványtípus és a vele kapcsolatos gyakorlatok tervezéséért, valamint a szolgáltatási szabályzatban dokumentáltaknak megfelelő, hatékony megvalósításáért.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Lásd a szolgáltatási szabályzat 5.2.2 pontját.

5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

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

5.3 Személyzetre vonatkozó óvintézkedések

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

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

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

- a) A hitelesítés-szolgáltató olyan személyzetet alkalmaz, amely rendelkezik a kínált szolgáltatáshoz szükséges szakértői tudással, tapasztalattal és minősítésekkel.

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

5.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások

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

5.3.3 Kiképzési követelmények

- a) A hitelesítés-szolgáltató személyzete rendelkezik a kínált szolgáltatásokhoz szükséges szakértői tudással, tapasztalattal és minősítésekkel.

5.3.4 Továbbképzési gyakoriságok és követelmények

A szolgáltatási szabályzat 5.3.4 pontjának előírásai szerint.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

A szolgáltatási szabályzat 5.3.5 pontjának előírásai szerint.

5.3.6 A felhatalmazás nélküli tevékenységek büntető következményei

Lásd a szolgáltatási szabályzat 5.3.6 pontját.

5.3.7 A szerződéses alkalmazottakra vonatkozó követelmények

Lásd a szolgáltatási szabályzat 5.3.7 pontját.

5.3.8 A személyzet számára biztosított dokumentációk

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

6. Műszaki biztonsági óvintézkedések

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

6.1 Kulcspár előállítás és telepítés

A hitelesítés-szolgáltató gondoskodik valamennyi általa (saját maga, egyes szervezeti egységei /pl. címtár, regisztrációs szervezetek/, illetve aláírók számára) generált magánkulcs biztonságos és szabványos előállításáról.

6.1.1 Kulcspár előállítás

A hitelesítés-szolgáltató saját kulcspár előállítása:

- a) A hitelesítés-szolgáltatónál történő kulcselőállítást fizikailag védett környezetben (lásd 5.1), bizalmi munkakört betöltő személyzet (lásd 5.2.1) végzi, legalább kettős ellenőrzés¹⁵ mellett. A kulcselőállítás funkció végrehajtására felhatalmazott személyzet körét a hitelesítés-szolgáltató szolgáltatási szabályzatának még megfigyelve, a lehető legkisebbre korlátozza.
- b) A hitelesítés-szolgáltató a kulcselőállítást olyan biztonságos kriptográfiai modulban hajtja végre, amely tanúsítvánnyal igazoltan megfelel az alábbi követelményeknek:
 - a modul garantálja a kulcsok bizalmosságát és sértetlenségét azok teljes életciklusa során,
 - a modul képes felhasználói azonosítására és hitelesítésére,
 - a modul a felhasználó és annak szerepköre alapján azokra a szolgáltatásokra korlátozza a hozzáférést, amelyek az adott felhasználó adott szerepköréhez vannak rendelve,
 - a modul képes egy teszt sorozat lefuttatására, mely ellenőrzi működése helyességét, és hiba észlelése esetén egy biztonságos állapotba lép,
 - a modul észleli a fizikai módosítási kísérleteket, s ilyenkor egy biztonságos állapotba lép,
 - a modul naplóbejegyzéseket készít minden biztonság-kritikus változtatásról,
 - amennyiben a modul támogatja a kulcsok mentését és visszaállítását¹⁶, megvédi a mentési adatok bizalmosságát és sértetlenségét, s legalább kettős ellenőrzést követel meg mind a mentés, mind a visszaállítás műveleténél

¹⁵ Két személy együttes jelenlétével

¹⁶ Lévéen ez csak egy opcionális elvárás

- amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között. c) A hitelesítés-szolgáltató a kulcs előállítását olyan algoritmussal valósítja meg, melyet jogszabály ismer el erre a célra alkalmasnak.¹⁷

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

- d) A hitelesítés-szolgáltató által saját szervezeti egységei /címtár, regisztrációs szervezetek/ számára előállított kulcsokat biztonságos módon, olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak¹⁸.
- e) A hitelesítés-szolgáltató által az aláírók számára előállított kulcsokat biztonságos módon, olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak¹⁹.
- f) A biztonságos aláírás-létrehozó eszköz elkészítését (logikai és fizikai megismerését) a hitelesítés-szolgáltató ellenőrzi.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

Amikor a hitelesítés-szolgáltató kulcsokat generál más felek (regisztrációs szervezetek és aláírók) számára:

- a) az általa más felek számára előállított kulcsokat a címzett félhez történő továbbításig biztonságos módon tárolja;
- b) az általa más felek számára előállított magánkulcsot a címzett félhez olyan módon továbbítja, hogy a magánkulcs titkossága ne sérüljön;
- c) a szállítást követően csak az aláíró férhet hozzá saját magánkulcsához;
- d) a hitelesítés-szolgáltató biztonságosan ellenőrzi a biztonságos aláírás-létrehozó eszköz elkészítését;
- e) a hitelesítés-szolgáltató a biztonságos aláírás-létrehozó eszközt biztonságosan tárolja és osztja szét;
- f) A hitelesítés-szolgáltató ellenőrzi a biztonságos aláírás-létrehozó eszköz kiiktatását és újraaktivizálását;
- g) A hitelesítés-szolgáltató a biztonságos aláírás-létrehozó eszköz aktivizálási adatait (PIN kód) biztonságosan készíti el és biztonságosan osztja szét.

¹⁷ Az említett jogszabály a következő: „2/2002 (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről” jogszabály 1. sz. melléklete, mely felsorolja a megfelelőnek elismert kulcselőállítási algoritmusokat.

¹⁸ Az említett jogszabály a következő: „2/2002 (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről” jogszabály 1. sz. melléklete, mely felsorolja a kulcs előállítására vonatkozó, megfelelőnek elismert algoritmusokat.

¹⁹ Az említett jogszabály a következő: „2/2002 (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről” jogszabály 1. sz. melléklete, mely felsorolja a kulcs előállítására vonatkozó, megfelelőnek elismert algoritmusokat.

6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

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

6.1.4 A szolgáltatói nyilvános kulcs közzététele

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

6.1.5 Kulcs méretek

A hitelesítés-szolgáltató saját kulcsának mérete:

- a) A hitelesítés-szolgáltató aláíró kulcsára olyan kulcshosszúságot és algoritmust választ, melyet jogszabály ismer el erre a célra alkalmasnak²⁰.

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

- b) A hitelesítés-szolgáltató által más felek (regisztráló szervezetek és az aláírók) számára generált kulcsok olyan hosszúságúak és olyan algoritmushoz tartozók, melyet jogszabály ismer el erre a célra alkalmasnak²¹.

6.1.6 A nyilvános kulcs paramétereinek előállítása

- a) A hitelesítés-szolgáltató a nyilvános kulcs paramétereinek előállítása során /beleértve az ehhez szükséges véletlenszám generálást is/ olyan szabványos megoldást használ, melyet jogszabály ismer el erre a célra alkalmasnak²².

6.1.7 A paraméterek megfelelőségének ellenőrzése

- a) A hitelesítés-szolgáltató ellenőrzi valamennyi kulcspár előállítása során a paraméterek minőségét.²³

²⁰ Az említett jogszabály a következő: „2/2002 (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről” jogszabály 1. sz. melléklete, mely felsorolja az aláíró kulcsokra vonatkozó, megfelelőnek elismert kulcshosszúságokat és algoritmusokat.

²¹ Lásd 2/2002 (IV.26) MeHVM irányelve, 1. sz. melléklete.

²² Lásd 2/2002 (IV.26) MeHVM irányelve, 1. sz. melléklete.

²³ A szolgáltatási szabályzatban ismertetett módon.

6.1.8 Hardver/szoftver kulcselőállítás

- a) A hitelesítés-szolgáltató valamennyi kulcspár előállítását olyan biztonságos kriptográfiai modulban hajtja végre, amely tanúsítvánnyal igazoltan megfelel a 6.1.1 alatt felsorolt követelményeknek, s amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között. A tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelményrendszer szerint, azzal egyenértékű értékeli szinten végezték.

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

- a) A hitelesítés-szolgáltató saját kulcsainak használati célja az alábbiak egyike lehet:
 - tanúsítvány aláírás,
 - visszavonási lista aláírás,
 - titkosítás.
- b) A hitelesítés-szolgáltató által az aláírók számára előállított kulcsok használati célja kizárólag aláírás (nonrepudiation) lehet²⁴.

6.2 A magánkulcsok védelme

- a) A hitelesítés-szolgáltató gondoskodik valamennyi általa (saját maga, a regisztráló szervezetek, illetve az aláírók számára) előállított magánkulcs titkosságáról és sértetlenségéről.
- b) A hitelesítés-szolgáltató külön aláíró magánkulcsot használ tanúsítvány aláírásra, és tanúsítvány visszavonási lista aláírásra, egyúttal ezen kulcsokat semmilyen más célra nem használja.
- c) A hitelesítés-szolgáltató a tanúsítványokat, illetve a tanúsítvány visszavonási listákat aláíró magánkulcsait fizikailag biztonságos helyszínen használja.

6.2.1 Kriptográfiai modulra vonatkozó szabványok

Hitelesítő szervezet

- a) A hitelesítés-szolgáltató a tanúsítványokat és tanúsítvány visszavonási listákat aláíró magánkulcsait olyan biztonságos kriptográfiai modulban állítja elő, amely tanúsítvánnyal igazoltan megfelel a 6.1.1 alatt felsorolt követelményeknek, s amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között. A

²⁴ Ez a tanúsítványtípus kizárólag elektronikus aláírásra használható kulcsokkal, tanúsítványokkal foglalkozik. A titkosításra, illetve hitelesítésre is használható kulcsokkal hitelesítés-szolgáltató egy másik tanúsítványtípusa foglalkozik.

tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelményrendszer szerint, azzal egyenértékű értékelési szinten végezték.

- b) A Hitelesítő Szervezet tanúsítványokat és tanúsítvány visszavonási listákat aláíró magánkulcsait olyan biztonságos kriptográfiai modulban tárolja és használja, amely tanúsítvánnyal igazoltan megfelel a 6.1.1 alatt felsorolt követelményeknek, s amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között. A tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelményrendszer szerint, azzal egyenértékű értékelési szinten végezték.
- c) A hitelesítés-szolgáltató a regisztráló szervezettel folytatott biztonságos kommunikációjában felhasznált aláíró magánkulcsait egy olyan hardver kriptográfiai eszközben állítja elő amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között.
- d) A hitelesítő szervezet a regisztráló szervezettel folytatott biztonságos kommunikációjában felhasznált aláíró magánkulcsait egy olyan hardver kriptográfiai eszközben tárolja és használja, amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között.

Regisztráló szervezet

- e) A regisztráló szervezet magán aláíró kulcsait olyan hardver kriptográfiai eszközben állítja elő, amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között.
- f) A regisztráló szervezet magán aláíró kulcsait olyan hardver kriptográfiai eszközben tárolja és használja, amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között.

Aláírók

- g) A aláírók magán aláíró kulcsát a hitelesítés-szolgáltató állítja elő olyan kriptográfiai hardver modulban, amely tanúsítvánnyal igazoltan megfelel az alábbi követelményeknek:
 - a modul garantálja a kulcsok bizalmosságát és sértetlenségét mindaddig, míg a kulcsok a modul ellenőrzése alatt állnak,
 - a modul garantálja a modulból a biztonságos aláírás-létrehozás eszközbe továbbított magánkulcsok bizalmosságát,
 - a modul garantálja a modulból más rendszerekbe vagy alkalmazásokba exportált nyilvános kulcsok sértetlenségét,
 - a modul képes felhasználói azonosítására és hitelesítésére,
 - a modul korlátozza a szolgáltatásaihoz való hozzáférést,
 - a modul képes egy teszt sorozat lefuttatására, mely ellenőrzi működése helyességét, és hiba észlelése esetén egy biztonságos állapotba lép,

- a modul észleli a fizikai módosítási kísérleteket, s ilyenkor egy biztonságos állapotba lép,
 - amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között. A tanúsítást a CEN CMCKG-PP [6] vagy más, alkalmas követelményrendszer szerint, azzal egyenértékű értékelési szinten végezték.
- h) Az aláíró magán aláíró kulcsát olyan biztonságos aláírási-létrehozó eszközben tárolja, illetve használja, amely nem kompromittálja a magánkulcs biztonságát, megfelel a [4] szabvány szerint kidolgozott SSCD-PP²⁵ védelmi profil [15] követelményeinek, s amely szerepel a Hatóság elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között.

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

Hitelesítő szervezet

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

Regisztráló szervezet

- b) A regisztráló szervezet magán aláíró kulcsa nem kerül mentésre, így visszaállítása nem lehetséges.

Aláírók

- c) Az aláírók magán aláíró kulcsa nem kerül mentésre, így visszaállítása nem lehetséges.

6.2.3 Magánkulcs letétbe helyezése

- a) A hitelesítés-szolgáltató az aláíró magán aláíró kulcsait nem tárolja, és nem tartja olyan módon sem, mely lehetővé tenné a (kulcs)adatok későbbi visszaállítását.

6.2.4 Magánkulcs mentése

Hitelesítő szervezet

²⁵ A védelmi profil pontos megnevezése: Protection Profile – Secure Signature-Creation Device Type 2, verzió száma: 1.05, regisztrációs száma: BSI-PP-0005-2002, értékelés garancia szintje: emelt EAL4

- a) A hitelesítő szervezet magán aláíró kulcsát csak bizalmi munkakört betöltő személyzet másolhatja le, illetve tárolhatja le, legalább kettős ellenőrzés mellett, fizikailag biztonságos környezetben (lásd az 5.2.2 pontot).
- b) A hitelesítő szervezet magán aláíró kulcsainak mentett másolataira ugyanolyan szintű biztonsági előírások vonatkoznak, mint a használatban levő kulcsokra.

Regisztráló szervezet

- c) A regisztráló szervezet magán aláíró kulcsának mentése nem lehetséges.

Aláírók

- d) A hitelesítés-szolgáltató által az aláíróknak előállított magánkulcsok mentése nem lehetséges.

6.2.5 Magánkulcs archiválása

- a) A hitelesítés-szolgáltató magánkulcsot nem archivál.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

Hitelesítő szervezet

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

Regisztráló szervezet

- d) A regisztráló szervezet magánkulcsait az ezeket felhasználó kriptográfiai hardver modul állítja elő, így ezeket nem kell külön a modulba juttatni.
- e) A regisztráló szervezet magán aláíró kulcsa teljes életciklusában a biztonságos kriptográfiai eszközben marad, azt semmilyen célból nem hagyja el.
- f) A regisztráló szervezet kriptográfiai hardver modulja kikapcsolt állapotban a magánkulcsokat kódolva tárolja, olyan algoritmust és kulcs hosszát alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs teljes hátralévő életciklusában.

Aláírók

- g) A hitelesítés-szolgáltató az általa előállított magánkulcsoknak a biztonságos aláírás-létrehozó eszközbe való bejuttatása (áttöltése) során²⁶ a magánkulcsokat kódolja, olyan protokollt, algoritmust és kulcs hosszát alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt magánkulcs teljes hátralévő életciklusában.
- h) Az aláíró magán aláíró kulcsa a feltöltést követően a biztonságos aláírás-létrehozó eszközben marad, azt semmilyen célból nem hagyja el.
- i) Az aláíró biztonságos aláírás-létrehozó eszköze kikapcsolt állapotban a magánkulcsokat kódolva tárolja, olyan algoritmust és kulcs hosszát alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs teljes hátralévő életciklusában.

6.2.7 A magánkulcs aktivizálásának módja

Hitelesítő szervezet

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

Regisztráló szervezet

- c) A regisztráló szervezet (az archiválandó regisztrációs adatokat és tranzakciókat aláíró) magánkulcsa aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.
- d) A regisztráló szervezet egyéb (a hitelesítés-szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsai aktivizálását az erre felhatalmazott felhasználó²⁷ tudáson alapuló hitelesítési eljárással aktivizálhatja.

Aláírók

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

²⁶ Az „aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése” szolgáltatás keretén belül.

²⁷ a rendszerüzemeltető

6.2.8 A magánkulcs aktív állapotának megszüntetési módja

Hitelesítő és regisztráló szervezet

- a) A magánkulcsok aktív állapotának megszüntetése (deaktivizálása) akkor lehetséges, ha a magánkulcsot tároló kriptográfiai hardver modulok szabályos vagy szabálytalan módon kikerülnek az aktivizálást és felhasználást lehetővé tevő állapotból. (Az erre vonatkozó részleteket a szolgáltatási szabályzat 6.2 alfejezete tartalmazza.)

Aláírók

- b) A magánkulcsok deaktivizálása akkor lehetséges, ha a magánkulcsot tároló biztonságos aláírás-létrehozó eszköz szabályos vagy szabálytalan módon kikerül az aktivizálást és felhasználást lehetővé tevő állapotból. (Az erre vonatkozó részleteket a szolgáltatási szabályzat 6.2 alfejezete tartalmazza.)

6.2.9 A magánkulcs megsemmisítésének módja

Hitelesítő és regisztráló szervezet magánkulcsainak megsemmisítése

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

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

A hitelesítés-szolgáltató által az aláírók számára generált magánkulcsok megsemmisítése

- d) A hitelesítés-szolgáltató – közvetlenül az aláíró magánkulcsának előállítása és az aláíró aláírás-létrehozó eszközére töltése után – a magánkulcsot (s annak minden esetleges másolatát) megsemmisíti.
- e) A hitelesítés-szolgáltató által végrehajtott kulcscsere során – az aláíró új magánkulcsának biztonságos aláírás-létrehozó eszközre töltése utáni megsemmisítésén túlmenően – hitelesítés-szolgáltató gondoskodik arról is,

hogy a régi magánkulcs az aláíró biztonságos aláírás-létrehozó eszközén is megsemmisüljön.

- f) Az aláíró magánkulcsának élelciklus végén történő megsemmisítése kívül esik a hitelesítés-szolgáltató felelősségi körén.

6.3 A kulcspár gondozásának egyéb szempontjai

6.3.1 A nyilvános kulcsok archiválása

- a) A hitelesítés-szolgáltató archiválja az aláírók nyilvános kulcsait, a szolgáltatási szabályzat 6.3 alfejezetében meghatározott időtartamig.

6.3.2 A nyilvános és magánkulcsok használatának periódusa

Hitelesítő és regisztráló szervezet

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

Aláírók

- b) Az aláíró magánkulcsának használati periódusa nem haladhatja meg a tanúsítvány érvényességi idejét, ennek betartása viszont kívül esik a hitelesítés-szolgáltató felelősségi körén. Ennek betartása az előfizető és az aláíró kötelessége (lásd 2.1.4.1 c. és 2.1.4.2 c. pontok), ellenőrzése pedig az érintett felek kötelessége (lásd 2.1.5 b. pontja).

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

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

6.4.2 Az aktivizáló adatok védelme

- a) A hitelesítés- szolgáltató az általa kibocsátott biztonságos aláírás-létrehozó eszközök aktivizáló adatait biztonságos módon állítja elő és osztja szét.

6.4.3 Az aktivizáló adatok egyéb szempontjai

- a) A hitelesítés-szolgáltató az általa kibocsátott biztonságos aláírás-létrehozó eszközök kiiktatását és újraaktivizálását biztonságosan ellenőrzi.

6.5 Számítógépbiztonsági óvintézkedések

6.5.1 Speciális számítógépbiztonsági műszaki követelmények

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

- a) A hitelesítés-szolgáltató védi rendszerei és információi sértetlenségét vírusok, káros és engedély nélküli szoftverek ellen.
- b) A hitelesítés-szolgáltató biztonságosan kezeli adathordozó eszközeit a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.
- c) A hitelesítés-szolgáltató gondoskodik a felhasználói²⁸ hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.
- d) A hitelesítés-szolgáltató gondoskodik arról, hogy az információhoz és az alkalmazói rendszer funkciókhoz történő hozzáférés, a hozzáférés ellenőrzési szabályzatnak megfelelően korlátozott legyen, és hogy a hitelesítés-szolgáltató rendszere megfelelő számítógépbiztonsági ellenőrzéseket nyújtson a hitelesítés-szolgáltató szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében, beleértve a biztonsági, adminisztrátori és üzemeltetési funkció elkülönítését. Különösképpen a rendszer szolgáltatási programok használatát korlátozza és ellenőrzi szigorúan.
- e) A hitelesítés-szolgáltató gondoskodik arról, hogy személyzetét sikeresen azonosítsák és hitelesítsék, mielőtt a tanúsítvány gondozásával kapcsolatos kritikus alkalmazásokat használhatnák.
- f) A hitelesítés-szolgáltató eljárásokat dolgoztat ki és hajtat végre valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására.
- g) A hitelesítés-szolgáltató műszaki óvintézkedéseket juttat érvényre, hogy a hitelesítés-szolgáltató belső hálózati tartományai védettek legyenek a harmadik felek számára elérhető külső hálózati tartományoktól.
- h) A hitelesítés-szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a

²⁸ A felhasználó fogalma itt felöleli a rendszer operátorokat, rendszer adminisztrátorokat és bármely olyan felhasználót, akinek közvetlen hozzáférése van a rendszerhez.

biztonság megsértésének hatásait. Valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.

- i) A hitelesítés-szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni és regisztrálni az erőforrásaihoz való jogosulatlan és/vagy szabálytalan hozzáférési kísérleteket, valamint képes legyen ezekre időben reagálni.
- j) A hitelesítés-szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.
- k) A hitelesítés-szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ (hálózatról történő) módosítására vonatkozóan.
- l) A hitelesítés-szolgáltató gondoskodik arról, hogy az érzékeny adatokat²⁹ megvédjék az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.
- m) A hitelesítés-szolgáltató biztosítja a személyzet tevékenységéért való felelősségre vonhatóságát.

6.5.2 Informatikai biztonsági minősítés

- a) A hitelesítés-szolgáltató szolgáltatásaira vonatkozóan végrehajtott kockázat elemzés (lásd 5. a.) azonosította azokat a kritikus szolgáltatásokat, amelyekhez megbízható informatikai rendszerek kellene, egyben meghatározta a szükséges értékelési garanciaszinteket.
- b) A hitelesítés-szolgáltató megbízható informatikai rendszereket alkalmaz.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

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

²⁹ Az érzékeny adatok közé tartoznak a regisztrációs információk is.

6.6.2 Biztonságkezelési óvintézkedések

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

6.6.3 Az életciklusra vonatkozó biztonság osztályozása

- a) A hitelesítés-szolgáltató által alkalmazott megbízható informatikai rendszerek magukban foglalnak életciklusra vonatkozó független biztonsági értékelést is.

6.7 Hálózatbiztonsági óvintézkedések

A hitelesítés-szolgáltató gondoskodik arról, hogy informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerüljön sor. Különösképpen:

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

- a) Az érzékeny adatokat³⁰ megvédi, amikor azok átvitele (cseréje) nem biztonságos hálózatokon keresztül történik.
- b) A hitelesítés-szolgáltató biztosítja általános informatikai biztonságát még akkor is, ha a hitelesítés-szolgáltató egyes funkciót más szervezet (pl. a regisztráló szervezet) valósítja meg.

A regisztrálással kapcsolatosan:

- c) A regisztrációs adatok bizalmasságát és sértetlenségét megvédik, különösen az előfizetővel/alannal folytatott külső, illetve a hitelesítés-szolgáltató egyes komponensei közötti belső adatcsere során.
- d) A hitelesítés-szolgáltató (a hitelesítő szervezeten keresztül) ellenőrzéssel biztosítja, hogy regisztrációs adatokat csak általa elismert, azonosságában hitelesített regisztrációs szolgáltatókkal cserél.

A tanúsítvány előállítással és visszavonás kezeléssel kapcsolatosan:

- e) A hitelesítés-szolgáltató gondoskodik arról, hogy a helyi hálózati komponensek (például routerek) fizikailag biztonságos környezetben legyenek és konfigurációikat időszakonként auditálják.
- f) A hitelesítés-szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni, regisztrálni az erőforrásaihoz (hálózatról) történő

³⁰ Az érzékeny adatok közé tartoznak a regisztrációs információk is.

hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre.

A tanúsítvány kibocsátásával kapcsolatosan:

- g) A hitelesítés-szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.

A tanúsítvány visszavonás kezeléssel kapcsolatosan:

- h) A hitelesítés-szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ (hálózatról történő) módosítására vonatkozóan.

6.8 A kriptográfiai modul ellenőrzése

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

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

7. Tanúsítvány és tanúsítvány visszavonási lista profilok

7.1 Tanúsítvány profil

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

7.1.1 Verzió szám(ok)

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.1 pontját.

7.1.2 Tanúsítvány kiterjesztések

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.2 pontját.

7.1.3 Algoritmus objektum azonosítók

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.3 pontját.

7.1.4 Elnevezési formák

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.4 pontját.

7.1.5 Elnevezésre vonatkozó korlátozások

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.5 pontját.

7.1.6 Tanúsítványtípus objektum azonosító

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.6 pontját.

7.1.7 A „tanúsítványtípus korlátozás” kiterjesztés használata

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.7 pontját.

7.1.8 Szabályzat minősítő szintaxis és szemantika

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.8 pontját.

7.1.9 A kritikus tanúsítványtípus kiterjesztés feldolgozása

Lásd a 7.1 a. b. és c. állításokat, valamint a szolgáltatási szabályzat 7.1.9 pontját.

7.2 Tanúsítvány visszavonási lista profil

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

7.2.1 Verzió szám(ok)

Lásd a 7.2 a. és b. állításokat, valamint a szolgáltatási szabályzat 7.2.1 pontját.

7.2.2 „Tanúsítvány visszavonási lista” és „Tanúsítvány visszavonási lista bejegyzési” kiterjesztések

Lásd a 7.2 a. és b. állításokat, valamint a szolgáltatási szabályzat 7.2.2 pontját.

8. Leírás adminisztráció

- a) A hitelesítés-szolgáltató rendelkezik egy olyan szolgáltatási szabályzattal, mely a jelen Tanúsítványtípus Szabályzatban (MTT+BALE) leírt valamennyi állításra tartalmazza a megvalósítás gyakorlatát és eljárását.
- b) A hitelesítés-szolgáltató szolgáltatási szabályzata meghatározza a hitelesítés-szolgáltató szolgáltatásait támogató valamennyi külső szervezetre vonatkozó kötelezettségeket is, beleértve az alkalmazandó szabályzatokat is.

8.1 Leírás változtatási eljárások

- a) A hitelesítés-szolgáltató egy felülvizsgálati folyamattal gondozza jelen Tanúsítványtípus Szabályzatot és a hozzá tartozó szolgáltatási szabályzatot.
- b) A hitelesítés-szolgáltató időben értesítést tesz közzé a jelen Tanúsítványtípus Szabályzatban, illetve az ehhez tartozó szolgáltatási szabályzatában tervezett változtatásokról, majd a (8.3 a) pont szerint történő jóváhagyást követően az átdolgozott Tanúsítványtípus Szabályzatot (vagy szolgáltatási szabályzatot) - a 8.2 a) pontban előírtak szerint - haladéktalanul hozzáférhetővé teszi.

8.2 Közzétételi és tájékoztatási elvek

- a) A hitelesítés-szolgáltató a jelen Tanúsítványtípus Szabályzatot, valamint az ehhez tartozó szolgáltatási szabályzatát és egyéb más fontos dokumentációját az aláírók/előfizetők és az érintett felek rendelkezésére bocsátja, az előírásoknak való megfelelés felméréséhez szükséges mértékig.
- b) A hitelesítés-szolgáltató a tanúsítvány használatával kapcsolatos kikötéseit és feltételeit az összes végfelhasználó számára megismerhetővé teszi, a 2.6.1-ben meghatározottak szerint.

8.3 Szolgáltatás szabályzat jóváhagyási eljárások

A tanúsítványtípusra vonatkozóan:

- a) Jelen Tanúsítványtípus Szabályzat tartalmilag megfelel a [7] MTT+BALE tanúsítványtípusokkal szemben támasztott minimális követelményeknek.
- b) Jelen Tanúsítványtípus Szabályzat formailag megfelel a [10] szabványnak.
- c) A hitelesítés-szolgáltató jóváhagyás előtt megvizsgálja a Tanúsítványtípus Szabályzat (fenti a.-b. pontokban meghatározott) követelményeknek való megfelelését.
- d) A Tanúsítványtípus Szabályzat jóváhagyására a hitelesítés-szolgáltató felsőszintű irányító testülete rendelkezik végső hatáskörrel és felelősséggel.

- e) A Hatóság nyilvántartásba vette a hitelesítés-szolgáltató által jóváhagyott és bejelentett Tanúsítványtípus Szabályzatot.

A szolgáltatási szabályzatra vonatkozóan:

- f) A jelen Tanúsítványtípus Szabályzathoz tartozó szolgáltatási szabályzat tartalmilag és formailag is megfelel e Tanúsítványtípus Szabályzatnak³¹.
- g) A hitelesítés-szolgáltató jóváhagyás előtt megvizsgálja a szolgáltatási szabályzatot a Tanúsítványtípus Szabályzatnak való megfelelés szempontjából.
- h) A szolgáltatási szabályzat jóváhagyására a hitelesítés-szolgáltató felsőszintű irányító testülete rendelkezik végső hatáskörrel és felelősséggel.
- i) A szolgáltatási szabályzat megfelelését a Hatóság is megvizsgálja³² a hitelesítés-szolgáltató minősítési eljárása során.

³¹ A tartalmi és formai megfelelés azt jelenti, hogy a tanúsítványtípus „mit valósít meg a hitelesítés-szolgáltató” típusú állításait a szolgáltatási szabályzat „hogyan valósítja meg ezeket” típusú leírásai ellentmondás mentesen és hasonló szerkezeti felépítéssel részletezik.

³² És értékeli: jóváhagyja, vagy módosítja.

9. Hivatkozások

- [1] 2001. évi XXXV. Törvény az elektronikus aláírásról /Eat.
- [2] 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről
- [3] 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- [4] ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1. 2. és 3. rész)
- [5] CEN 14167-2 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató aláíró műveleteit megvalósító kriptográfiai modulra” (CMCSO-PP, HSM-PP)
- [6] CEN 14167-3 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató kulcs előállítási szolgáltatásait megvalósító kriptográfiai modulra” (CMCKG-PP, HSM-PP)
- [7] ETSI TS 101 456 Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények
- [8] ETSI TS 101 862 Minősített tanúsítvány profil
- [9] RFC 3280 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány és tanúsítvány visszavonási lista profil)
- [10] RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – Tanúsítványtípus Szabályzat és szolgáltatási szabályzat keretrendszer)
- [11] RFC 3039 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)
- [12] International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer”
- [13] FIPS PUB 140-1 (1994. január): "Kriptográfiai modulok biztonsági követelményei"
- [14] FIPS PUB 140-2 (2001. május): "Kriptográfiai modulok biztonsági követelményei"
- [15] Biztonságos aláírás-létrehozó eszköz védelmi profil /Protection Profile – Secure Signature-Creation Device Type 2, v1.05, BSI-PP-0005-2002/

-
- [16] CEN 14167-1 munkacsoport egyezmény: „Biztonsági követelmények elektronikus aláírásokkal kapcsolatos tanúsítványokat kezelő rendszerek megbízható rendszereire”
- [17] ITU-R Ajánlás TF 460-5 (1997) "Szabványos frekvencia- és időjel kibocsátás".

10. Jelölések, rövidítések és meghatározások

Jelen Tanúsítványtípus Szabályzat az alábbi fogalmakat az alábbi értelemben használja:

Fogalom	Meghatározás (magyarázat)
aktivizáló adatok	a kriptográfiai modul működtetéséhez szükséges adatok, melyeket védeni kell (pl. PIN kód, jelmondat vagy manuálisan birtokolt kulcs-részlet)
aláírás-ellenőrző adat (az aláíró nyilvános kulcsa)	olyan egyedi adat, (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ
aláírás-létrehozó adat (az aláíró magánkulcsa)	olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ
aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön	az aláírás-létrehozó eszközök elkészítése és az aláíró részére történő átadása
aláírás-létrehozó eszköz	olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza
aláíró (aláíró fél)	az a természetes személy, akihez az elektronikus aláírás hitelesítés-szolgáltató (hitelesítés-szolgáltató) által közzétett aláírás-ellenőrző adatok jegyzéke szerint az aláírás-ellenőrző adat kapcsolódik
biztonságos aláírás-létrehozó eszköz	a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény (Eat.) 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz
elektronikus aláírás	elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum
elektronikus dokumentum	elektronikus eszköz útján értelmezhető adat, mely elektronikus aláírással van ellátva
elektronikus aláírás ellenőrzése	az elektronikus dokumentum tartalmának összevetése aláíráskor, illetve ellenőrzéskor, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, valamint a <i>tanúsítvány</i> felhasználásával
elektronikus aláírás felhasználása	elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése

Fogalom	Meghatározás (magyarázat)
elektronikus irat	olyan elektronikus dokumentum, mely szöveget és más olyan adatot (pl. fejléceket) tartalmaz, amely legfeljebb a szöveg illusztrálására, azonosítására szolgál, továbbá digitális jeleket is tartalmaz (az olvasó számára közvetlenül nem érzékelhető módon) a szöveggel összefüggő informatikai funkciók megvalósítása érdekében
elektronikus okirat	olyan elektronikus irat, mely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy nyilatkozat kötelezőnek elismerését foglalja magában. Az elektronikus okirat fogalmát az eljárási törvényekben szereplő okirati bizonyítási eszközök virtuális megfelelőjeként hozza létre a Javaslat, azok hagyományos meghatározásával összhangban
elektronikusan történő aláírás	elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz
előfizető	szolgáltatónál egy vagy több aláíró nevében előfizető entitás, aki közvetlenül vagy közvetve elfogadja szolgáltató kikötéseit és feltételeit
érintett fél	az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el
eszköz-szolgáltató	olyan hitelesítés-szolgáltató, amely a hitelesítésszolgáltatás mellett az aláírás-létrehozó adat elhelyezése az aláírás-létrehozó eszközön szolgáltatást is felvállalja
fogadó fél (elfogadó fél)	az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el
fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető, olyan eszközökkel hozták létre, melyek kizárólag az aláíró befolyása alatt állnak és a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető. Az ilyen fajta elektronikus aláírást is hitelesítés-szolgáltató tanúsítja, de az aláírás technológiája, biztonsági foka vagy a hitelesítés-szolgáltató körülményei nem valósítják meg a minősített elektronikus aláírás követelményeit
időbélyeg adatelem	olyan adat objektum, mely adatok egy reprezentációját összeköti egy meghatározott időponttal, bizonyítékot szolgáltatva ezzel arra, hogy az adatok léteztek az adott időpont előtt
időbélyegző egység	szabályok összessége, mely egy időbélyeg adatelem alkalmazhatóságát jelzi egy adott közösség és/illetve közös biztonsági követelményekkel rendelkező alkalmazás osztály esetében
időbélyegzés szolgáltató	szervezet, mely időbélyeg adatelemeket bocsát ki.
időbélyegzés-szolgáltató nyilatkozat	egy időbélyegzés-szolgáltató időbélyegző típusára és szolgáltatási szabályzatára vonatkozó állítások összessége, melyet az előfizetők és érintett felek számára kíván hangsúlyozni, illetve közzétenni, például a kötelező

	követelmények kielégítésére nézve
koordinált univerzális időalap (UTC)	másodpercen alapuló időmérték, melyet [17] határoz meg.

Fogalom	Meghatározás (magyarázat)
hitelesítésszolgáltatási szabályzat	a 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat
hitelesítés-szolgáltató	személy (szervezet), amely a hitelesítésszolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványokhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány visszavonási listát
időbélyeg (időbélyegző)	elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját, és amely a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető
időbélyegzés-szolgáltató	olyan szolgáltató, amely az időbélyegzés szolgáltatást felvállalja
igénylő	Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki e-szignó minősített hitelesítés szolgáltatást <i>aláíróként</i> vagy <i>előfizetőként</i> kíván igénybe venni.
kriptográfiai kulcs	olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges
kulcsgondozás	a kriptográfiai kulcsok előállítása, a felhasználókhöz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, szoros kapcsolatban az alkalmazott biztonsági eljárásmóddal
minősített elektronikus aláírás	olyan – fokozott biztonságú – elektronikus aláírás, amely biztonságos aláírás-létrehozó eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki
nyilvános (publikus) kulcsú infrastruktúra	tanúsítványok létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is

Fogalom	Meghatározás (magyarázat)
regisztrációs szervezet	szervezet, amely ellenőrzi a tanúsítvány aláírójának személyazonosságát. Egy Hitelesítő Szervezet több ilyen szervezettel is együttműködhet.
tanúsítvány	hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot a 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát
tanúsítvány-előállítás	tanúsítványok létrehozása és a hitelesítés-szolgáltató által történő aláírása (a regisztrációs szolgáltatásra alapozva).
tanúsítvány kibocsátás	egy tanúsítvány rendelkezésre bocsátása az aláíró számára, valamint a tanúsítvány közzététele a hitelesítés-szolgáltató nyilvántartásában
tanúsítvány megújítás	új tanúsítvány biztosítása, melyben az aláíró megváltozott új nyilvános kulcsát és régi adatait a hitelesítés-szolgáltató (új érvényességi időtartamra) érvényes magánkulcsával aláírja
tanúsítvány visszavonási közzététele	Információ nyújtása az elfogadó fél számára a tanúsítványok visszavonásáról. A szolgáltatás lehet valós idejű, vagy az információk előre meghatározott időközönkénti aktualizálásán kell alapulnia.
tanúsítvány visszavonási lista	valamely okból visszavont, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a hitelesítés szolgáltató bocsát ki
tanúsítvány visszavonási nyilvántartás	nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját
Tanúsítványtípus Szabályzat	szabályok összessége, amely megmutatja adott tanúsítványok alkalmazhatóságát egy bizonyos közösségre, illetve alkalmazások olyan csoportjára, ahol azonosak a biztonsági követelmények
végfelhasználó	az aláíró, az előfizető, valamint az elfogadó fél