

Minősített Alap Tanúsítvány Típus biztonságos aláírás létrehozó eszköz támogatásával minősített szolgáltatók számára



NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Nyilvántartási szám (OID): ----- 1.3.6.1.4.1.3555.1.14.030317

A Szabályzat hatályának kezdőnapja: ----- **2003. március 31.**

Oldalak száma: ----- **53, azaz ötvenhárom**

----- © Copyright 2003, NetLock Kft. - Minden jog fenntartva

Jóváhagyta: ----- **Rózsahegy Zsolt** ügyvezető

Jóváhagyás dátuma: ----- **2003. március 14.**

Jóváhagyom:

PH.

Hivatkozások

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

- [1] 2001. évi XXXV. Törvény az elektronikus aláírásról
- [2] 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről
- [3] 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- [4] ETSI TS 101 456 Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények
- [5] ETSI TS 101 862 Minősített tanúsítvány profil
- [6] RFC 2459 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány és tanúsítvány visszavonási lista profil)
- [7] RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)
- [8] RFC 3039 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)
- [9] International Telecommunication Union X.509 "Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer"
- [10] Minősített tanúsítványtípus minták minősített Hitelesítés Szolgáltatók számára, 1.2 verzió
- [11] FIPS PUB 140-1 (1994. január 11): "Kriptográfiai modulok biztonsági követelményei"

Tartalomjegyzék

1	BEVEZETÉS	9
1.1	Áttekintés	9
1.2	Azonosítás	9
1.3	Közösség és alkalmazhatóság	10
1.3.1	Regisztrációs egység	10
1.3.2	Hitelesítő egység	10
1.3.3	Szabályzatért felelős egység	10
1.3.4	Igénybevevők	10
1.3.5	Alkalmazhatóság	10
1.4	Kapcsolattartás	10
2	ÁLTALÁNOS RENDELKEZÉSEK	12
2.1	Kötelezettségek	12
2.1.1	A regisztrációs egység kötelezettségei	13
2.1.2	A hitelesítő egység kötelezettségei	16
2.1.3	Az alany és a felhasználó kötelezettségei	17
2.1.4	Az érintett fél kötelezettségei	17
2.1.5	A tanúsítványtár kötelezettségei	17
2.2	Felelősség	18
2.2.1	A hitelesítő egység felelőssége	18
2.2.2	A regisztrációs egység felelőssége	18
2.2.3	Az alany felelőssége	18
2.2.4	Az érintett fél felelőssége	18
2.3	Pénzügyi felelősség	19
2.3.1	A hitelesítés-szolgáltatóval szembeni kártérítés	19
2.3.2	Bizalmon alapuló kapcsolatok	19
2.3.3	Adminisztratív folyamatok	19
2.4	Értelmezés és érvényesítés	19
2.4.1	Irányadó jog	19
2.4.2	Érvénytelenség, fennmaradás, megszűnés, értesítések	19
2.4.3	Vitás kérdések megoldására vonatkozó eljárások	20
2.5	Díjak	20
2.5.1	Tanúsítvány kibocsátási és megújítási díjak	20
2.5.2	Tanúsítvány hozzáférési díjak	20
2.5.3	Visszavonási és állapot információ hozzáférési díjak	20

2.5.4	Egyéb szolgáltatásokra vonatkozó díjak	20
2.5.5	Visszatérítési elvek	20
2.6	Közzététel és tanúsítványtár	21
2.6.1	Hitelesítés-szolgáltató információ közzététele	21
2.6.2	A közzététel gyakorisága	21
2.6.3	Hozzáférés ellenőrzések	22
2.6.4	Tanúsítványtárak	22
2.7	A megfelelés vizsgálat	22
2.7.1	A megfelelés vizsgálatának gyakorisága	22
2.7.2	Az átvizsgáló egység és a vizsgált fél kapcsolata	22
2.7.3	Hiányosságok esetén végrehajtandó tevékenységek	22
2.8	Bizalmasság	22
2.8.1	Bizalmasan kezelendő információ típusok	23
2.8.2	Nem bizalmasnak tekintett információ típusok	23
2.8.3	Tanúsítvány visszavonására/felfüggesztésére vonatkozó információ felfedése	23
2.8.4	Információszoolgáltatás hatósági szervek részére	23
2.8.5	Információszoolgáltatás polgári eljárás keretében	23
2.8.6	A tulajdonos kérésére történő felfedés	24
2.8.7	Egyéb információ közzétételt eredményező körülmények	24
2.9	Szellemi tulajdonjogok	24
3	AZONOSÍTÁS ÉS HITELESÍTÉS	25
3.1	Kezdeti regisztrálás	25
3.1.1	Név típusok	25
3.1.2	Igény a nevek értelmezhetőségére	25
3.1.3	Különböző elnevezési formák értelmezési szabályai	25
3.1.4	A nevek egyedisége	25
3.1.5	Eljárások a nevekre vonatkozó vitás kérdések megoldására	25
3.1.6	Márkanevek elismerése, hitelesítése és szerepe	25
3.1.7	A magánkulcs birtoklásának bizonyítási módszere	25
3.1.8	A szervezeti azonosság hitelesítése	26
3.1.9	Személyazonosság hitelesítése	26
3.2	Érvényes tanúsítvány megújítása	26
3.3	Érvénytelen tanúsítvány megújítása	26
3.4	Visszavonási kérelem	26
4	MŰKÖDÉSRE VONATKOZÓ KÖVETELMÉNYEK	28
4.1	Tanúsítvány kérelem	28

4.2	Tanúsítvány kibocsátás	28
4.3	Tanúsítvány elfogadás	28
4.4	Tanúsítvány felfüggesztés és visszavonás	28
4.4.1	A visszavonás körülményei	28
4.4.2	Kik kérelmezhetik a visszavonást	29
4.4.3	Visszavonási kérelemre vonatkozó eljárás	29
4.4.4	Visszavonási kérelemre vonatkozó türelmi idő	29
4.4.5	A felfüggesztés körülményei	29
4.4.6	Kik kérelmezhetik a felfüggesztést	29
4.4.7	Felfüggesztési kérelemre vonatkozó eljárás	29
4.4.8	A felfüggesztés időtartamára vonatkozó korlátozások	30
4.4.9	A tanúsítvány visszavonási lista kibocsátási gyakorisága	30
4.4.10	Tanúsítvány visszavonási lista ellenőrzési követelményei	30
4.4.11	Valós idejű visszavonási állapot ellenőrzés elérhetősége	30
4.4.12	Valós idejű visszavonás ellenőrzési követelmények	30
4.4.13	A visszavonási hirdetmények egyéb elérhető formái	30
4.4.14	A visszavonási hirdetmények egyéb elérhető formáinak ellenőrzési követelményei	30
4.4.15	Kulcs kompromittálódás esetére vonatkozó speciális követelmények	30
4.5	A biztonsági naplózás folyamatai	31
4.5.1	A tárolt események típusai	31
4.5.2	A napló állomány feldolgozásának gyakorisága	31
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 alanyok értesítése	32
4.5.8	Sebezhetőség felmérése	32
4.6	Adatok archiválása	32
4.6.1	A tárolt események típusai	32
4.6.2	Az archívum megőrzési időtartama	33
4.6.3	Az archívum védelme	33
4.6.4	Az archívum mentési folyamatai	33
4.6.5	A rekordok időbélyegzésére vonatkozó követelmények	33
4.6.6	Az archívum gyűjtési rendszere	33
4.6.7	Archív információ hozzáférését és ellenőrzését végző eljárások	33
4.7	Kulcscsere.....	34
4.8	Helyreállítás kompromittálódás és katasztrófa esetén.....	34
4.8.1	Sérült számítási erőforrások, szoftverek és/vagy adatok	34
4.8.2	Egy szolgáltatói egység nyilvános kulcsának visszavonása	34
4.8.3	Egy szolgáltatói egység nyilvános kulcsának kompromittálódása	34
4.8.4	Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően	34

4.9	A hitelesítés-szolgáltató leállítása	35
5	FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK	36
5.1	Fizikai óvintézkedések	36
5.1.1	A telephely elhelyezése és szerkezeti felépítése	37
5.1.2	Fizikai hozzáférés	37
5.1.3	Áramellátás, légkondicionálás	38
5.1.4	Beázás és elárasztódás veszélyeztetettsége	38
5.1.5	Tűz megelőzés és tűzvédelem	38
5.1.6	Adathordozók tárolása	38
5.1.7	Selejt kezelése, megsemmisítése	38
5.1.8	Fizikailag elkülönítetten őrzött mentési példányok	38
5.2	Eljárásbeli óvintézkedések	38
5.2.1	Bizalmi munkakörök	39
5.2.2	Az egyes feladatokhoz szükséges személyzeti létszámok	39
5.2.3	Az egyes munkakörökben elvárt azonosítás és hitelesítés	39
5.3	Személyzetre vonatkozó óvintézkedések	39
5.3.1	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények	39
5.3.2	Biztonsági háttér ellenőrzésekre vonatkozó eljárások	39
5.3.3	Továbbképzési gyakoriságok és követelmények	40
5.3.4	A felhatalmazás nélküli tevékenységek büntető következményei	40
5.3.5	A szerződéses alkalmazottakra vonatkozó követelmények	40
5.3.6	A személyzet számára biztosított dokumentációk	40
6	MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	41
6.1	Kulcspár előállítás és telepítés	41
6.1.1	Kulcspár előállítás	41
6.1.2	Magánkulcs eljuttatása a tulajdonoshoz	41
6.1.3	A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz	42
6.1.4	A szolgáltatói nyilvános kulcs közzététele	42
6.1.5	Kulcs méretek	42
6.1.6	A nyilvános kulcs paramétereinek előállítása	42
6.1.7	A paraméterek megfelelőségének ellenőrzése	42
6.1.8	Hardver/szoftver kulcselőállítás	42
6.1.8.1	A kulcs használat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően).....	43
6.2	A magánkulcsok védelme.....	43
6.2.1	Kriptográfiai modulra vonatkozó szabványok	43
6.2.1.1	A több-szereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése	43
6.2.2	Magánkulcs letétbe helyezése	44
6.2.3	Magánkulcs mentése	44
6.2.4	Magánkulcs archiválása	44

6.2.5	Magánkulcs bejuttatása a kriptográfiai modulba	44
6.2.6	A magánkulcs aktivizálásának módja	45
6.2.7	A magánkulcs aktív állapotának megszüntetési módja	45
6.2.8	A magánkulcs megsemmisítésének módja	46
6.3	A kulcspár gondozásának egyéb szempontjai	46
6.3.1	Nyilvános kulcs archiválása	46
6.3.2	A nyilvános és magánkulcsok használatának periódusa	46
6.4	Aktivizáló adatok	46
6.4.1	Aktivizáló adatok előállítása és telepítése	46
6.4.1.1	Az aktivizáló adatok védelme	47
6.4.1.2	Az aktivizáló adatok egyéb szempontjai	47
6.5	Számítógépbiztonsági óvintézkedések	47
6.4.2	Speciális számítógépbiztonsági műszaki követelmények	47
6.4.3	Informatikai biztonsági minősítés	48
6.5	Életciklusra vonatkozó műszaki óvintézkedések	48
6.5.1	Rendszerfejlesztési óvintézkedések	48
6.5.2	Biztonságkezelési óvintézkedések	48
6.5.2.1	Az életciklusra vonatkozó biztonság osztályozása	48
6.6	Hálózatbiztonsági óvintézkedések	48
6.7	A kriptográfiai modul ellenőrzése	49
7	TANÚSÍTVÁNY ÉS TANÚSÍTVÁNY VISSZAVONÁSI LISTA PROFILOK	50
7.1	Tanúsítvány profil	50
7.1.1	Verzió szám(ok)	50
7.1.2	Tanúsítvány kiterjesztések	50
7.1.3	Algoritmus objektum azonosítók	50
7.1.4	Elnevezési formák	50
7.1.5	Elnevezésre vonatkozó korlátozások	50
7.1.6	Tanúsítványtípus objektum azonosító	50
7.1.7	A „tanúsítványtípus korlátozás” kiterjesztés használata	50
7.1.8	Szabályzat minősítő szintaxis és szemantika	50
7.1.9	A kritikus tanúsítványtípus kiterjesztés feldolgozása	51
7.2	Tanúsítvány visszavonási lista profil	51
7.2.1	Verzió szám(ok)	51
7.2.2	„Tanúsítvány visszavonási lista” és „Tanúsítvány visszavonási lista bejegyzési” kiterjesztések	51
8	LEÍRÁS ADMINISZTRÁCIÓ	52
8.1	Leírás változtatási eljárások	52

8.2	Közzétételi és tájékoztatási elvek	52
8.3	Szolgáltatás szabályzat jóváhagyási eljárások	52

1 Bevezetés

Jelen tanúsítványtípus célja, hogy egy olyan minősített alap tanúsítványtípusként, amelyhez szükséges biztonságos aláírás-létrehozó eszköz (továbbiakban: BALE) összefoglalja mindazon minimum követelményeket, amelyek ezen minősített tanúsítványtípus igénylésére, kibocsátására, használatára és életciklusára vonatkoznak. Jelen tanúsítványtípust alkalmazó hitelesítés-szolgáltatók a jelen dokumentumban nem szabályozott kérdésekben szolgáltatói szabályzatuknak megfelelően járnak el.

1.1 Áttekintés

A tanúsítványtípus „szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára”. Jelen tanúsítványtípus az [7] RFC 2527 szabványa és a [10] Minősített tanúsítványtípus minta alapján készült. A dokumentum tartalmi vonatkozásokban eleget tesz az [1] Elektronikus aláírás törvény, és egyéb hazai jogszabályok ([2] és [3]) előírásainak és ajánlásainak, és felhasználja az [4] ETSI követelmények műszaki specifikációját, valamint egyéb nemzetközi ajánlásokat.

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

Jelen dokumentumban meghatározott tanúsítványtípus a nyilvános körben kibocsátott minősített alap tanúsítványtípus biztonságos aláírás létrehozó eszköz támogatásával. [MATT+BALE.], mely nyilvános körben kibocsátott minősített tanúsítvány és biztonságos aláírás-létrehozó eszköz alkalmazását megköveteli. Így:

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

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

1.2 Azonosítás

A jelen dokumentumban meghatározott tanúsítványtípusra vonatkozó azonosító az alábbi:

- **MATT+BALE.** (Nyilvános körben kibocsátott minősített alap tanúsítványtípus biztonságos aláírás létrehozó eszköz támogatásával.)

1.3 Közösség és alkalmazhatóság

1.3.1 Regisztrációs egység

A hitelesítés-szolgáltató – saját egységén belül – regisztrációs egységet működtessen, melynek pontos feladatát, hatáskörét és felelősségét a szolgáltatási szabályzat ismertesse.

1.3.2 Hitelesítő egység

A hitelesítés-szolgáltató – saját egységén belül – hitelesítő egységet működtessen, melynek pontos felépítését, feladatát, hatáskörét és felelősségét a szolgáltatási szabályzat ismertesse.

1.3.3 Szabályzatért felelős egység

A hitelesítés-szolgáltató szabályzatainak kibocsátását, karbantartását a hitelesítés-szolgáltató szabályzatért felelős egysége végezze. A hitelesítés-szolgáltató a szabályzatért felelős egységet saját egységén belül működtesse, s ennek pontos felépítését, feladatát, hatáskörét és felelősségét a szolgáltatási szabályzat ismertesse.

1.3.4 Igénybevevők

A szolgáltatások nyilvánosak legyenek, vagyis az alábbi korlátozásokkal bárki lehessen igénybevevő:

- alany: tetszőleges természetes személy, aki a kibocsátott vagy kibocsátandó tanúsítványban szerepelni fog,
- felhasználó: tetszőleges természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki/amely elfogadja a szolgáltatási szabályzatban számára meghatározott kötelezettségeket,
- érintett fél: tetszőleges természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki/amely elfogadja a szolgáltatási szabályzatban (Az érintett fél kötelezettségei) meghatározott kötelezettségeket.

1.3.5 Alkalmazhatóság

Az ezen dokumentumban meghatározott tanúsítványtípus érvényességi körében kibocsátott minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon kielégítik, ahogy egy kézírásos aláírás kielégíti ugyanazt a követelményt a papír-alapú adatok vonatkozásában. A tanúsítványtípus területi hatályát a Szolgáltató a konkrét tanúsítványban határozza meg. A kibocsátott minősített tanúsítványok kizárólag aláírási célra használhatók fel.

1.4 Kapcsolattartás

A hitelesítés-szolgáltató adatai:

A hitelesítés-szolgáltató kapcsolattartáshoz szükséges adatait, szolgáltatási szabályzatában ismertesse.

Szabályzatért felelős egység:

A szabályzatokkal kapcsolatos kérdésekkel és észrevételekkel közvetlenül a szabályzatért felelős egység legyen megkereshető.

2 Általános rendelkezések

2.1 Kötelezettségek

A hitelesítés-szolgáltató általában:

A hitelesítés-szolgáltató (a regisztrációs egység, hitelesítő egység, szabályzatért felelős egység, és a tanúsítványtár együttes tevékenységével) legalább az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat biztosítsa:

- regisztráció,
- tanúsítvány előállítás,
- kibocsátás,
- visszavonás kezelés,
- visszavonási állapot közzététele

A hitelesítés-szolgáltató gondoskodjon a hitelesítés-szolgáltatóra vonatkozó valamennyi, a 3–8. fejezetekben részletezett állítások teljesüléséről.

A hitelesítés-szolgáltató szolgáltatásait tegye hozzáférhetővé minden olyan igénylő számára, akinek tevékenysége kinyilvánított működési területére esik.

A hitelesítés-szolgáltató jogi személy legyen, melynek székhelye Magyarországon legyen.

A hitelesítés-szolgáltató megfelelően dokumentált megállapodásokkal és szerződéses kapcsolatokkal rendelkezzen azon esetekre, amikor a szolgáltatások nyújtása alvállalkozókat, illetve más, harmadik felekkel kötött megegyezéseket érint.

A hitelesítés-szolgáltató olyan (szolgáltatási) szabályzattal rendelkezzen, mely e tanúsítványtípusban azonosított valamennyi követelmény kielégítésére szolgáló gyakorlatra és eljárásra vonatkozik.

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg a hitelesítés-szolgáltató szolgáltatásait támogató valamennyi külső egységre vonatkozó kötelezettségeket, beleértve az alkalmazandó szabályzatokat és gyakorlatokat is.

A hitelesítés-szolgáltató valamennyi szolgáltatását szolgáltatási szabályzatával összhangban nyújtsa.

A szolgáltatási szabályzatot a hitelesítés-szolgáltató felsőszintű irányító testülete hagyja jóvá.

A szolgáltatási szabályzat megfelelő megvalósításáért a hitelesítés-szolgáltató felső vezetősége feleljen.

A hitelesítés-szolgáltató bocsássa szolgáltatási szabályzatát és egyéb fontos dokumentációit a tanúsítványtípusnak való megfelelés felméréséhez szükséges mértékig az igénybevevők rendelkezésére.

A hitelesítés-szolgáltató rendszeresen vizsgálja felül szolgáltatási szabályzatát, az újra érvényesített szabályzat tartalmazza a szükséges módosításokat.

A hitelesítés-szolgáltató időben tegyen közzé értesítést a szolgáltatási szabályzatában tervezett változtatásokról és a fenti jóváhagyást követően az átdolgozott szolgáltatási szabályzatát haladéktalanul tegye hozzáférhetővé.

2.1.1 A regisztrációs egység kötelezettségei

A regisztrációs egység biztosítsa az elektronikus aláírás hitelesítés-szolgáltatáson (a továbbiakban hitelesítés-szolgáltatás) belül:

- regisztrációt,
- visszavonás kezelést.

A regisztrációs egység ezen kívül működjön közre az alábbi elektronikus aláírással kapcsolatos szolgáltatások biztosításában:

- tanúsítvány előállítás,
- kibocsátás,
- visszavonási állapot közzététele.

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

- gondoskodjon a tanúsítványt igénylő megfelelő azonosításáról, illetve arról, hogy a tanúsítványt igénylő formanyomtatványok teljeseek, pontosak és kellőképpen hitelesek legyenek;
- ellenőrizze a tanúsítványt igénylő ügyfél személyazonosságát és a leendő alany azon egyedi jellemzőit, melyet a minősített tanúsítvány igazol;
- gyűjtse össze, illetve határozza meg a regisztráció során valamennyi, az [1] Törvény 2. számú mellékletében meghatározott, tanúsítványba kerülő adatot;
- ellenőrizze a tanúsítványt igénylő ügyfél által átadott személyazonosító és egyéb igazoló dokumentumok valóságát, érvényességét, sértetlenségét és hitelességét. Vesse össze egymással és a valósággal az egyes iratokon szereplő adatokat. Lehetőség szerint ellenőrizze a dokumentumok érvényességét, valóságát valós idejű nyilvántartásokban is;
- írásbeli indoklással utasítsa vissza 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;
- vegyen nyilvántartásba minden, a tanúsítványok kiadásához kapcsolódó, a [2] irányelv 152. pontjában meghatározottat;
- őrizze meg a nyilvántartásokat a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig;
- bizalmas információként kezelje a felhasználó és az alany 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 kezelje, s csak a 2.8 fejezet megfelelő pontjaiban, illetve a hitelesítés szolgáltató szabályzataiban említett esetekben és személyek részére fedje fel őket;
- korlátozás nélkül biztosítsa az alany számára a rá vonatkozó regisztrációs és egyéb információhoz történő hozzáférést.

A regisztrációs egység a **visszavonás kezelés** szolgáltatás keretén belül:

- ellenőrizze 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);

- a szolgáltatási szabályzatban meghatározott időn, de legkésőbb 24 órán belül hajtsa végre a hiteles, érvényes és szabályos, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket (vagyis a kérelmezett változást vezesse át a tanúsítványtár alapját képező tanúsítvány állapot adatbázisába);
- utasítsa vissza (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket;
- a szolgáltatási szabályzatban meghatározott időn, de legkésőbb 24 órán belül intézkedjen egy tanúsítvány visszavonásáról, amennyiben olyan tényről szerez tudomást, ami a tanúsítvány felhasználhatóságának biztonságát fenyegeti;
- tájékoztassa a visszavont, illetve felfüggesztett tanúsítvány tulajdonosát tanúsítványa állapotának változásáról;
- a szolgáltatási szabályzatban meghatározott mértékben, de minimum 99%-os rendelkezésre állással biztosítsa a visszavonás kezelési szolgáltatást minden érdekelt fél számára, egyúttal ugyanott adja meg az előre tervezett és rendkívüli leállások leghosszabb időtartamát.

A regisztrációs egység az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:

- gondoskodjon valamennyi általa, az alany számára végrehajtott kulcs előállítás biztonságosságáról, az alany magánkulcsának titkosságáról;
- az alany részére előállított kulcspárt:
- olyan kriptográfiai eszközzel állítsa elő, mely tanúsítvánnyal igazoltan megfelel a [11] szabvány 3-as szintjének és egyben szerepel a Hírközlési Felügyelet által nyilvántartásba vett, tanúsított elektronikus aláírási termékek listáján is,
- olyan algoritmus felhasználásával állítsa elő, melyet a [2] 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő kulcs generáló algoritmusként ismer el,
- olyan aláíró algoritmushoz és olyan kulcshosszúságban állítsa elő, melyet a [2] 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő aláíró algoritmusként, illetve megfelelő paraméterként ismer el;
- biztonságos módon juttassa el az alany részére előállított kulcspárt a biztonságos aláírás-létrehozó eszközbe, egy a kriptográfiai eszköz és a biztonságos aláírás létrehozó eszköz közötti olyan biztonságos útvonal kiépítésével, mely megfelelő kriptográfiai mechanizmusok felhasználásával forráshitelesítést, sértetlenséget és bizalmasságot biztosít;
- biztonságos módon semmisítse meg az alany részére előállított magánkulcs biztonságos aláírás-létrehozó eszközön kívüli összes példányát, miután az alany részére előállított kulcspárt elhelyezte a biztonságos aláírás-létrehozó eszközben;
- gondoskodjon az általa biztosított biztonságos aláírás-létrehozó eszköz kibocsátása során az eljárás biztonságáról;
- ellenőrizze a biztonságos aláírás-létrehozó eszköz kezelését;
- ellenőrizze, hogy a szolgáltatáshoz felhasznált biztonságos aláírás-létrehozó eszköz a Hírközlési Felügyelet által nyilvántartásba vett biztonságos aláírás-létrehozó eszköz-e;
- a biztonságos aláírás-létrehozó eszköz előkészítését megfelelően biztonságos környezetben hajtsa végre;
- biztonságos konfigurációt alakítson ki a biztonságos aláírás-létrehozó eszközön az inicializálás, formázás és fájl-struktúra kialakítás során;

- a biztonságos aláírás-létrehozó eszközt biztonságosan tárolja és juttassa el a szándék szerinti, hitelesített alanyhoz;
- biztonságos módon állítsa elő a kezdeti aktivizáló adatokat, majd a biztonságos aláírás-létrehozó eszköztől elkülönítve juttassa el az előfizetőhöz;
- biztosítsa, hogy alkalmazottai nem élhetnek vissza a biztonságos aláírás-létrehozó eszközzel.

A regisztrációs egység a **tanúsítvány előállítás** szolgáltatásban való közreműködés keretén belül:

- kezdeti tanúsítvány előállítás esetén a regisztrációs szolgáltatás által összegyűjtött, tanúsítványba kerülő adatokat ellenőrizze ezen tanúsítványtípushoz kapcsolódó hitelesítési/ellenőrzési eljárás szerint. A tanúsítvány kibocsátásához szükséges ellenőrzések és visszaigazolások sikeres befejeződése után a hitelesítő egység felé tanúsítvány kibocsátási kérelem üzenetet indítson el;
- tanúsítvány kulcscsere kérelem esetén ellenőrizze a már korábban nyilvántartásba vett alanytól érkező tanúsítvány megújítási kérelem teljességét, pontosságát, hitelességét és, hogy a megújítási kérelem megfelel-e a szolgáltatási szabályzatban meghatározott feltételeknek;
- a hitelesség ellenőrzéséhez nem minden esetben kell megkövetelni az alany ismételt személyes megjelenését, elfogadhat, illetve feldolgozhat minősített elektronikus aláírással hitelesített elektronikus kérelmet is;
- dolgozza fel a teljes, pontos, hiteles és teljesíthető tanúsítvány megújítási kérelmeket az alábbi módon:
 - Tanúsítványfrissítés kérelme esetén az alany korábbi tanúsítványában szereplő adataiból és nyilvános kulcsából összeállítja az aláírandó új tanúsítványt. Ezt megelőzően a regisztráció szolgáltatással együttműködve ellenőrzi, hogy a tanúsítványtulajdonos azonosságának és jellemzőinek igazolására használt információ érvényes-e még.
 - Tanúsítvány aktualizálás kérelme esetén vegye nyilvántartásba az alany megváltozott új adatait, majd ezekből és az alany régi nyilvános kulcsából összeállítja az aláírandó új tanúsítványt. Ezt megelőzően a regisztráció szolgáltatással együttműködve ellenőrzi, hogy a tanúsítványtulajdonos azonosságának és jellemzőinek igazolására használt információ érvényes-e még.
 - Tanúsítvány kulcscsere kérelme esetén az alany korábbi tanúsítványában szereplő adataiból és az új nyilvános kulccsal állítsa össze az aláírandó új tanúsítványt;
- a tanúsítvány megújítási kérelem sikeres feldolgozása után sikeres befejeződése után a hitelesítő egység felé tanúsítvány kérelem üzenetet indítsa el;
- biztosítsa az aláírandó tanúsítványt is tartalmazó tanúsítvány kérelem üzenetet sértetlenségét, hitelességét és bizalmasságát.

A regisztrációs egység a (tanúsítvány és szabályzat) **kibocsátás** szolgáltatásban való közreműködés keretén belül:

- fogadja a hitelesítő egységtől kapott új tanúsítványokat, illetve új szabályzatokat, valamint ellenőrizze ezek hitelességét és sértetlenségét;
- küldje el a tanúsítványtárnak az új tanúsítványokat (amennyiben az alany hozzájárult ehhez), illetve új szabályzatokat, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét.

A regisztrációs egység a **visszavonási állapot közzététele** szolgáltatásban való közreműködés keretén belül:

- rendszeresen készítsen új tanúsítvány visszavonási listát tanúsítvány állapot adatbázisából, naponta egyszer, a szolgáltatási szabályzatban meghatározott frissítési időponthoz igazodóan, mely tartalmazza a következő lista tervezett kibocsátási idejét is;

- rendkívüli esetben készítsen új tanúsítvány visszavonási listát tanúsítvány állapot adatbázisából, mely tartalmazza a következő lista tervezett kibocsátási idejét is;
- aláírás céljából küldje el a hitelesítő egységnek az új tanúsítvány visszavonási listát, (a visszavonási lista aláírási kérelemben), biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét;

küldje el a tanúsítványtárnak az új tanúsítvány visszavonási listát, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét.

2.1.2 A hitelesítő egység kötelezettségei

A hitelesítő egység biztosítsa az alábbi elektronikus aláírással kapcsolatos szolgáltatást:

- tanúsítvány előállítás,

egyúttal működjön közre (a visszavonási listák aláírásával) az alábbi elektronikus aláírással kapcsolatos szolgáltatás biztosításában:

- visszavonási állapot közzététele.

A hitelesítő egység a **tanúsítvány előállítás** szolgáltatás biztosítása keretén belül:

- ellenőrizze a regisztrációs egységtől érkező tanúsítvány kérelmet, benne az aláírandó tanúsítvány adatokat tartalmazó üzenet sértetlenségét és hitelességét;
- dolgozza fel a regisztrációs egységtől érkező hiteles és sértetlen tanúsítvány kérelmet, melynek keretén belül állítsa elő a tanúsítványt (aláírja az aláírandó tanúsítvány adatokat);
- csak minősített tanúsítványok és azok visszavonási listáinak aláírására használja fel a minősített szolgáltatói magánkulcsát;
- csak olyan tanúsítványokat állítson elő, amelyek megfelelnek a szolgáltatási szabályzatában meghatározott, támogatott tanúsítványtípusoknak;
- csak olyan minősített tanúsítványokat bocsásson ki, amelyek megfelelnek az Eat. 2. számú mellékletében, valamint a [2] irányelv 162. pontjában meghatározott követelményeknek;
- gondoskodjon arról, hogy a tanúsítványban foglalt megkülönböztetett név alanyonként egyedi legyen a hitelesítés-szolgáltató szolgáltatási körén belül;
- gondoskodjon arról, hogy a hitelesítés-szolgáltató teljes szolgáltatási körén belül kibocsátott tanúsítványokhoz tartozó kulcsok mindvégig egyediek maradjanak;
- válaszolja meg a regisztrációs egységnek a tőle kapott tanúsítvány kérelmet, benne elküldve az előállított tanúsítványt, biztosítva a válaszüzenet sértetlenségét és hitelességét.

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

- ellenőrizze a regisztrációs egységtől érkező visszavonási lista aláírási kérelmet, s ebben az aláírandó tanúsítvány visszavonási lista sértetlenségét és hitelességét;
- dolgozza fel a regisztrációs egységtől érkező hiteles és sértetlen visszavonási lista aláírási kérelmet, melynek során írja alá a tanúsítvány visszavonási listát;
- válaszolja meg a regisztrációs egységtől kapott visszavonási lista aláírási kérelmet, elküldve az aláírt tanúsítvány visszavonási listát, biztosítva a válaszüzenet sértetlenségét és hitelességét.

2.1.3 Az alany és a felhasználó kötelezettségei

A hitelesítés-szolgáltató az alanyokat és a felhasználót megállapodáson (lásd 2.6.1 pont és 4.1 alfejezet) keresztül az alábbiakra kötelezze:

- a felhasználó a regisztrációs egységnél személyesen megjelenő, a minősített tanúsítványt és az ezzel kapcsolatos műveleteket igénylő alanyt lássa el meghatalmazással, hozzájáruló nyilatkozattal;
- pontos és teljes információt adjon be a regisztrációs egységhez jelen tanúsítványtípus követelményeinek megfelelően, különös tekintettel a regisztrációra;
- a kulcspárt csak a vele közölt valamennyi korlátozásnak megfelelően használja;
- ésszerű gonddal járjon el, hogy megelőzze az alany magánkulcsának illetéktelen felhasználását;
- késedelem nélkül értesítse a hitelesítés-szolgáltatót, amennyiben az alábbiak, illetve a szolgáltatási szabályzatban meghatározottak közül bármelyik bekövetkezik a tanúsítványban megadott érvényességi időszak vége előtt:
 - az alany magánkulcsa elveszett, azt ellopták, esetlegesen kompromittálták,
 - az alany elvesztette ellenőrzését magánkulcsa felett, aktivizálási adatai (például PIN kód) kompromittálódása, illetve más okokból kifolyólag,
 - a felhasználó tudomására jutott, hogy a tanúsítvány tartalmában vagy egyéb regisztrációs adatokban pontatlanság van, illetve változás következett be;
- kompromittálódás esetén az alany magánkulcsának használatát azonnal és véglegesen szakítsa meg;
- az alany magánkulcsát aláírásra csak a biztonságos aláírás-létrehozó eszközzel használja.

2.1.4 Az érintett fél kötelezettségei

Az érintett felek számára rendelkezésre bocsátott (lásd a 2.6.1 pont) kikötések és feltételek tartalmazzanak egy megjegyzést, miszerint, ha ésszerű módon egy tanúsítványra kívánnak hagyatkozni, az alábbiakat, illetve a szolgáltatási szabályzatban meghatározottakat kell tenniük:

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

2.1.5 A tanúsítványtár kötelezettségei

A tanúsítványtár biztosítsa az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:

- (tanúsítvány és szabályzat) kibocsátás,
- visszavonási állapot közzététele.

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

- tegye közzé a végfelhasználói tanúsítványokat, amennyiben az alany hozzájárult ehhez;
- hozza nyilvánosságra a szolgáltatási szabályzatot, általános szerződési feltételeket és egyéb ezekhez kapcsolódó információt;

- biztosítsa a szolgáltatási szabályzatban meghatározott mértékű, de minimum 99 %-os rendelkezésre állását, még rendkívüli üzemeltetési helyzet esetén is.

A tanúsítványtár a **visszavonási állapot közzététele** szolgáltatás keretén belül:

- tegye közzé a hiteles és sértetlen új tanúsítvány visszavonási listát;
- biztosítsa a legfrissebb tanúsítvány visszavonási lista a szolgáltatási szabályzatban meghatározott mértékű, de minimum 99 %-os rendelkezésre állását, még rendkívüli üzemeltetési helyzet esetén is.

2.2 Felelősség

A hitelesítés-szolgáltató általában:

A Szolgáltató az általánostól eltérő felelősségi szabályairól a szolgáltatási szabályzatában nyilatkozzon.

2.2.1 A hitelesítő egység felelőssége

Lásd 2.2 pont

2.2.2 A regisztrációs egység felelőssége

Lásd 2.2 pont

2.2.3 Az alany felelőssége

Az alany felelős:

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

Az alanynak büntetőjogi felelőssége áll fenn szolgáltatóval szemben az általa megadott adatok tekintetében.

2.2.4 Az érintett fél felelőssége

Az érintett fél felelős:

- a tanúsítványok elfogadása során tanúsított körütekintő eljárásért,
- általában kötelezettségei betartásáért.

Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a tanúsítványtípus, a szolgáltatási szabályzat, illetve a hatályos jogszabályok szerint jár el.

2.3 Pénzügyi felelősség

A hitelesítés-szolgáltató megfelelő megoldásokkal rendelkezzen a műveleteiből és tevékenységeiből származó kötelezettségek fedezésére, különösképpen a kárfelelősség kockázatára vonatkozóan.

A hitelesítés-szolgáltató rendelkezzen a jelen dokumentumban foglaltakkal összhangban álló üzemeltetéshez szükséges pénzügyi stabilitással és erőforrásokkal.

2.3.1 A hitelesítés-szolgáltatóval szembeni kártérítés

Az igénybevevők kártérítési felelősséggel tartoznak a hitelesítés- szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket kötelezettségeik be nem tartásával okoztak számára.

2.3.2 Bizalmon alapuló kapcsolatok

A hitelesítés-szolgáltató, illetve annak bármely egysége a hitelesítési szolgáltatással összefüggésben semmilyen körülmények között nem tekinthető a felhasználó vagy az érintett fél megbízottjának, képviselőjének vagy partnerének.

2.3.3 Adminisztratív folyamatok

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, védje a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon őrizze meg (archiválja) azokat. (Részletesebben lásd a 4.5 és 4.6 alfejezeteket.)

2.4 Értelmezés és érvényesítés

2.4.1 Irányadó jog

Az alkalmazandó jogszabályokat a szolgáltatási szabályzat tartalmazza.

2.4.2 Érvénytelenség, fennmaradás, megszűnés, értesítések

Érvénytelenség

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

Fennmaradás

Szolgáltató vállalja, hogy jelen tanúsítványtípus 2. fejezete érvényben marad a tanúsítványtípus hatályának végét követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, melyet jelen tanúsítványtípus hatálya alatt bocsátott ki a hitelesítés-szolgáltató.

Megszűnés

Jelen tanúsítványtípus a közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A tanúsítványtípus egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében, beleértve a hitelesítés-szolgáltató és más egység jövőbeli esetleges összeolvadásának esetét is. A tanúsítványtípus csak írott és hitelesített formában módosítható, a Hírközlési Felügyelet által vezetett tanúsítványtípus nyilvántartásban való átvezetés mellett.

Értesítések

A hitelesítés-szolgáltatót az ügyfél és bármely más fél legalább elektronikus levélben, írásban vagy faxon értesítheti, hivatalosan aláírt módon (a hitelesítés-szolgáltató értesítési címei annak szolgáltatási szabályzatában legyenek megtalálhatóak).

A hitelesítés-szolgáltató ügyfeleit a web oldalain történő közzététel útján, elektronikus levélben, írásban és faxon is tájékoztathatja.

2.4.3 Vitás kérdések megoldására vonatkozó eljárások

A hitelesítés-szolgáltató szabályzatokkal és eljárásokkal rendelkezzen 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 szolgáltatási szabályzatok tartalmazzák. A díjakról a szolgáltatás igénybevételét megelőzően is kellő információt kell hogy biztosítson a szolgáltató.

2.5.1 Tanúsítvány kibocsátási és megújítási díjak

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

2.5.2 Tanúsítvány hozzáférési díjak

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

2.5.3 Visszavonási és állapot információ hozzáférési díjak

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

2.5.4 Egyéb szolgáltatásokra vonatkozó díjak

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

2.5.5 Visszatérítési elvek

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

2.6 Közzététel és tanúsítványtár

2.6.1 Hitelesítés-szolgáltató információ közzététele

Kikötések és feltételek közzététele:

A hitelesítés-szolgáltató gondoskodjon arról, hogy kikötései és egyéb feltételei az igénybevevők rendelkezésére álljanak. Különösképpen:

- A hitelesítés-szolgáltató bocsássa az igénybevevők rendelkezésére a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, köztük az alábbiakat:
 - az alkalmazott tanúsítványtípusok HÍF azonosítóit;
 - szolgáltatási szabályzatát
 - általános szerződési feltételeit
- A hitelesítés-szolgáltató tegye elérhetővé a fenti pontban meghatározott információt web oldalain keresztül, elektronikusan továbbítható formában is.

Tanúsítványok nyilvánosságra hozatala:

A hitelesítés-szolgáltató gondoskodjon arról, hogy a tanúsítványok szükség esetén az igénybevevők rendelkezésére álljanak.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala:

A hitelesítés-szolgáltató gondoskodjon arról, hogy hiteles és érvényes tanúsítvány visszavonási és felfüggesztési kérelmek esetén a tanúsítványok időben visszavonásra, s ezen információ nyilvánosságra kerüljön.

Részletesebben:

- a hitelesítés-szolgáltató szolgáltatási szabályzatában dokumentálja a tanúsítványok visszavonásának eljárásait,
- tájékoztassa a visszavont, illetve felfüggesztett tanúsítvány tulajdonosát (ahol ez alkalmazható, a felhasználót is) tanúsítványa állapotának megváltozásáról;
- biztosítsa, 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 egység a hitelesítés-szolgáltató nevében elektronikusan aláírja.

2.6.2 A közzététel gyakorisága

Tanúsítványok nyilvánosságra hozatalának gyakorisága:

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága:

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást, de maximum 24 óránként.

2.6.3 Hozzáférés ellenőrzések

A hitelesítés-szolgáltató a nyilvánosságnak bocsásson ki tanúsítványt, ezért a tanúsítványok, valamint a tanúsítványok használatára vonatkozó kikötések és feltételek nyilvánosak, szabványos felületen bárki által elérhetők legyenek.

A visszavonásra vonatkozó kérelmeket hitelesíteni kell, a hitelesítés-szolgáltató feldolgozás előtt ellenőrizze, hogy hiteles forrásból származnak-e. Az ilyen jellegű kérelmeket meg kell erősíteni.

A hitelesítés-szolgáltató a nyilvánosságnak bocsát ki tanúsítványt, ezért a visszavonási állapotokat tartalmazó tanúsítvány visszavonási listák nyilvánosak, szabványos felületen bárki által elérhetők legyenek.

2.6.4 Tanúsítványtárak

A hitelesítés-szolgáltató a tanúsítványokat, a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, valamint a tanúsítvány visszavonási listákat tanúsítványtárán keresztül tegye hozzáférhetővé.

A tanúsítványtár elérhetőségét, valamint az általa biztosított szabványos felületeket és támogatott lekérdezési műveleteket a szolgáltatási szabályzat határozza meg.

2.7 A megfelelés vizsgálat

A hitelesítés-szolgáltató olyan elektronikus aláírási termékeket használjon elektronikus aláírás hitelesítés-szolgáltatás szolgáltatásához (kulcspárok előállításához, a kibocsátott tanúsítványok és tanúsítvány visszavonási listák aláírásához, valamint az ehhez szükséges magánkulcsok tárolásához), amely kellően biztonságos és megfelel az alkalmazható iparági szabványoknak, illetve egyéb jogszabályi előírásoknak. Konkrét ismertetésük a szolgáltatási szabályzatban szerepeljen.

2.7.1 A megfelelés vizsgálatának gyakorisága

A minősített szolgáltatókra vonatkozó követelményeknek, valamint a tanúsítványtípusnak való megfelelés rendszeres felülvizsgálata érdekében a Hírközlési Felügyelet évente legalább egyszer tartson átfogó helyszíni ellenőrzést hitelesítés-szolgáltatónál.

2.7.2 Az átvizsgáló egység és a vizsgált fél kapcsolata

A Hírközlési Felügyelet minősítési eljárásában résztvevő kijelölt szakértőknek a vizsgált hitelesítés-szolgáltatótól függetlennek kell lenniük, s befolyástól mentesen kell tevékenységüket végezniük.

2.7.3 Hiányosságok esetén végrehajtandó tevékenységek

A minősítő eljárás vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a hitelesítés-szolgáltató késlekedés nélkül szüntesse meg a vizsgálatot végző Hírközlési Felügyelettől kapott információ és ajánlások alapján.

2.8 Bizalmasság

A hitelesítés-szolgáltató gondoskodjon a jogszabályoknak való megfelelésről. Ennek keretén belül:

- a fontos bejegyzéseket védje 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 alfejezet);
- gondoskodjon az adatvédelmi törvényeknek való megfelelésről;
- megfelelő technikai és egységi intézkedéseket hozzon a személyes adatok felhatalmazás nélküli, illetve törvénytelen kezelése ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen;
- gondoskodjon az alanyra vonatkozó információ bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk (vagy nevükben a felhasználó) hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja.

2.8.1 Bizalmasan kezelendő információ típusok

A hitelesítés-szolgáltató bizalmas információként kezelje a felhasználó és az alany minden adatát, kivéve azokat, amelyeket a 2.8.2 pont tárgyal.

Szolgáltató ezen kívül bizalmas információként kezelje a következő adatokat és dokumentumokat:

- magánkulcsok és aktivizáló kódok,
- tanúsítványigénylések és 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 hitelesítés-szolgáltató kezelheti nem bizalmas információként mindazon adatokat, melyet a tanúsítványba belefoglal függetlenül attól, hogy a felhasználó vagy az alany hozzájárul-e a tanúsítvány nyilvánosságra hozásához. Ezek az adatok a tanúsítványigénylő űrlapon egyértelműen jelölve vannak.

2.8.3 Tanúsítvány visszavonására/felfüggesztésére vonatkozó információ felfedése

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

2.8.4 Információszoolgáltatás hatósági szervek részére

Nincs rá külön előírás.

2.8.5 Információszoolgáltatás polgári eljárás keretében

Nincs rá külön előírás.

2.8.6 A tulajdonos kérésére történő felfedés

Nincs rá külön előírás.

2.8.7 Egyéb információ közzététel eredményező körülmények

Nincs rá külön előírás.

2.9 Szellemi tulajdonjogok

A hitelesítés-szolgáltató által ügyfelei részére kibocsátott tanúsítvány és az ennek megfelelő kulcspár tulajdonosa az alany, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

A hitelesítés-szolgáltató a tanúsítványt a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja, s egyéb módon kezelheti.

A visszavonási információ a hitelesítés-szolgáltató tulajdonát képezi.

A hitelesítés-szolgáltató által az alany részére kibocsátott egyedi azonosító a hitelesítés-szolgáltató tulajdonát képezi.

A tanúsítványban szereplő megkülönböztető név használatára a megnevezett alany jogosult.

Az alany egyedi azonosítójában szereplő bármilyen védjegy, egységi és személy név, egyéb adat a felhasználó vagy alany tulajdonát képezheti.

A hitelesítés-szolgáltató szabályzatai, szerződéses feltételei a hitelesítés-szolgáltató tulajdonát képezik.

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:

- gondoskodjon arról, hogy az alany tanúsítvány kérelmei pontosak, hitelesek és teljeseek legyenek;
- megfelelő, illetékes források igazolásán alapulva vizsgálja meg az alanyok és felhasználók azonosságára vonatkozó bizonyítékokat, valamint nevük és a hozzá kapcsolódó adatok pontosságát.

3.1.1 Név típusok

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

3.1.2 Igény a nevek értelmezhetőségére

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

3.1.3 Különböző elnevezési formák értelmezési szabályai

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

3.1.4 A nevek egyedisége

A hitelesítés-szolgáltató gondoskodjon arról, hogy teljes élettartama alatt a tanúsítványban általa használt megkülönböztetett nevet sohasem fogja egy másik egyedhez rendelni.

3.1.5 Eljárások a nevekre vonatkozó vitás kérdések megoldására

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

3.1.6 Márkanevek elismerése, hitelesítése és szerepe

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

3.1.7 A magánkulcs birtoklásának bizonyítási módszere

A tanúsítvány kérelem eljárásnak biztosítania kell, hogy az alany a tanúsításra bemutatott nyilvános kulcsnak megfelelő magánkulcsot birtokolja. Vagyis azt, hogy a tanúsítvány igénylője ne érhesse el egy olyan nyilvános kulcs hitelesítését, amelynek a magánkulcs párjával nem rendelkezik.

Aláíró-eszköz szolgáltatás esetén a hitelesítés-szolgáltató maga generálja az alany számára a nyilvános-magán kulcspárt, az alanyak ekkor nem kell bizonyítania a magánkulcs birtoklását.

3.1.8 A szervezeti azonosság hitelesítése

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást, de a szolgáltató legalább a hiteles, eredeti és valódi dokumentumok ellenőrzésével végezze az azonosítást.

3.1.9 Személyazonosság hitelesítése

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást, de a szolgáltató legalább a hiteles, eredeti és valódi dokumentumok ellenőrzésével végezze az azonosítást.

3.2 Érvényes tanúsítvány megújítása

A hitelesítés-szolgáltató lehetővé teheti az érvényes tanúsítvány megújítások elektronikus üzenetváltáson alapuló, személyes megjelenést nem igénylő megvalósítását a szolgáltatási szabályzatban meghatározott módon és feltételekkel. Tekintettel a kulcsok előállításának egyszerűségére, illetve a kulcspárok összetartozásának ellenőrzési kötelezettségére (ld. 3.1.7 pont) ajánlott a kulcscsere nélküli megújítás támogatása.

A hitelesítés-szolgáltató gondoskodjon arról, hogy amennyiben támogatja a tanúsítvány megújítás elektronikus üzenetváltáson alapuló, személyes megjelenést nem igénylő megvalósítását úgy, egy már korábban nála nyilvántartásba vett és érvényes tanúsítvánnyal rendelkező alanytól származó tanúsítvány megújítás kérelem teljes, pontos és kellőképpen hiteles legyen. Ennek érdekében a hitelesítés-szolgáltató:

- ellenőrizze a tanúsítvány létezését és érvényességét, valamint, hogy az alany azonosságának és jellemzőinek igazolására használt információ még mindig érvényes-e,
- amennyiben bármely feltétele, illetve kikötése megváltozott, közölje azokat az alanyal, és egyezzen meg vele a 4.1 pontoknak megfelelően.

3.3 Érvénytelen tanúsítvány megújítása

A hitelesítés-szolgáltató ne tegye lehetővé visszavont, felfüggesztett tanúsítvány megújításának személyes megjelenést nem igénylő megvalósítását.

3.4 Visszavonási kérelem

A hitelesítés-szolgáltató tegye lehetővé érvényes tanúsítvány visszavonásának és felfüggesztésének elektronikus üzenetváltáson alapuló, személyes megjelenést nem igénylő megvalósítását a szolgáltatási szabályzatban meghatározott módon és feltételekkel.

A hitelesítés-szolgáltató gondoskodjon arról, hogy egy már korábban nála nyilvántartásba vett alanytól származó, tanúsítvány visszavonási vagy felfüggesztési kérelem teljes, pontos és kellőképpen hiteles legyen. Ennek érdekében a hitelesítés-szolgáltató szolgáltatási szabályzatának részeként (Tanúsítvány felfüggesztés és visszavonás című pont) dokumentálja a tanúsítványok visszavonásának, felfüggesztésének eljárásait, beleértve az alábbiakat:

- ki adhat be visszavonási kérelmeket,
- hogyan lehet ezeket beadni,
- mik a visszavonási kérelmek megerősítésére vonatkozó esetleges követelmények,
- milyen okból kifolyólag függeszthető fel egy tanúsítvány,

A felfüggesztett állapot maximális időtartamát „a felfüggesztés időtartamára vonatkozó korlátozások” című pont tartalmazza.

4 Működésre vonatkozó követelmények

4.1 Tanúsítvány kérelem

A hitelesítés-szolgáltató vegyen nyilvántartásba minden, az alany azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat.

A hitelesítés-szolgáltató vegye nyilvántartásba az alannal aláírt megállapodást.

4.2 Tanúsítvány kibocsátás

A hitelesítés-szolgáltató biztonságosan tartsa fenn az általa kibocsátott tanúsítványok hitelességét.

Különösképpen:

- Előállítás után a teljes és pontos tanúsítvány álljon rendelkezésére azon alany számára, akinek a tanúsítvány kibocsátásra került,
- A tanúsítvány kibocsátás eljárása biztonságosan kapcsolódjon a megfelelő regisztrációhoz, illetve a különböző tanúsítvány megújítási eljárásokhoz,
- A hitelesítés-szolgáltató csak akkor bocsásson ki egy új tanúsítványt az alany korábbiakban tanúsított nyilvános kulcsának felhasználásával (tanúsítvány frissítés), ha annak kriptográfiai biztonsága még megfelelő az új tanúsítvány tervezett élettartamára, és nincsenek arra utaló jelek, hogy az alany magánkulcsa kompromittálódott. A hitelesítés-szolgáltató legfeljebb egy alkalommal újíthat meg egy tanúsítványt ily módon.

Aláíró-eszköz szolgáltatás esetén az alany számára a hitelesítés-szolgáltató által megvalósított kulcselőállításra vonatkozóan:

- a tanúsítvány kibocsátás eljárása biztonságosan kapcsolódjon a hitelesítés-szolgáltató általi kulcspár előállításához;
- az alany magánkulcsát tartalmazó biztonságos aláírás-létrehozó eszközt biztonságosan továbbítsák az alanyhoz.

4.3 Tanúsítvány elfogadás

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

4.4 Tanúsítvány felfüggesztés és visszavonás

A hitelesítés-szolgáltató gondoskodjon arról, hogy hiteles és érvényes tanúsítvány visszavonási, illetve felfüggesztési kérelmek esetén a tanúsítványok a szolgáltatási szabályzatban meghatározott időn belül, de legkésőbb a visszavonásról, illetve felfüggesztéstől született hitelesítés-szolgáltatói döntéstől számított legközelebb kibocsátásra kerülő visszavonási listán szerepeljenek.

4.4.1 A visszavonás körülményei

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg, hogy a [1] törvényben felsorolt eseteken túl milyen körülmények között lehet, illetve kell visszavonási kérelmet benyújtani.

4.4.2 Kik kérelmezhetik a visszavonást

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg, hogy a [1] törvényben felsorolt eseteken túl ki adhat be visszavonási kérelmet.

4.4.3 Visszavonási kérelemre vonatkozó eljárás

A hitelesítés-szolgáltató szolgáltatási szabályzata dokumentálja a tanúsítványok visszavonásának eljárásait.

A hitelesítés-szolgáltató a tanúsítványok visszavonásra vonatkozó kérelmeket fogadásuk után haladéktalanul dolgozza fel.

A visszavonásra vonatkozó kérelmeket hitelesíteni kell, a hitelesítés-szolgáltató ellenőrizze, hogy hiteles forrásból származnak-e.

A hitelesítés-szolgáltató tájékoztassa a visszavont tanúsítvány alanyát, és ahol ez alkalmazható a felhasználót, a tanúsítvány állapotának megváltozásáról.

A hitelesítés-szolgáltató nem állíthatja vissza érvényesre a már egyszer véglegesen visszavonásra (azaz nem felfüggesztésre) került tanúsítványokat.

4.4.4 Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási kérelem megérkezésétől – amennyiben az hiteles és megalapozott - számított a szolgáltatási szabályzatban meghatározott időn, de legkésőbb 24 órán belül, a hitelesítés-szolgáltató köteles új visszavonási listát kiadni.

4.4.5 A felfüggesztés körülményei

A hitelesítés-szolgáltató megerősítést igénylő visszavonási kérelem esetén, melynek esetleges eseteit a szolgáltatási szabályzat tartalmazza a tanúsítvány visszavonási állapotát „felfüggesztett”-re állítja, amíg a visszavonás megerősítésre nem kerül.

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg, hogy a tanúsítványok milyen okból kifolyólag függeszthetők fel.

4.4.6 Kik kérelmezhetik a felfüggesztést

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg, hogy kik kérelmezhetik a tanúsítványok felfüggesztését.

4.4.7 Felfüggesztési kérelemre vonatkozó eljárás

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg a felfüggesztési kérelemre vonatkozó pontos eljárást, beleértve azt is, hogyan lehet ezen kérelmeket beadni.

A hitelesítés-szolgáltató a tanúsítványok felfüggesztésére vonatkozó kérelmeket fogadásuk után haladéktalanul dolgozza fel.

A hitelesítés-szolgáltató tájékoztassa a felfüggesztett tanúsítvány alanyát, és ahol ez alkalmazható a felhasználót, a tanúsítvány állapotának megváltozásáról.

4.4.8 A felfüggesztés időtartamára vonatkozó korlátozások

A hitelesítés-szolgáltató gondoskodjon arról, hogy egy tanúsítvány ne legyen hosszabb ideig felfüggesztve, mint amennyi állapotának megerősítéséhez szükséges. A felfüggesztett állapot maximum 5 nap, ha ezen idő alatt nem változik a tanúsítvány státusza automatikusan felkerül az 5. nap lejártát követő legközelebbi visszavonási listára visszavont tanúsítványként.

4.4.9 A tanúsítvány visszavonási lista kibocsátási gyakorisága

A hitelesítés-szolgáltató a visszavonási állapot információt legalább tanúsítvány visszavonási listák egy adattáron keresztül történő nyilvánosságra hozatalán keresztül nyújtja. Ezen információt a szolgáltató egyéb módon is nyújthatja, amelyről a szolgáltatási szabályzata rendelkezhet.

A hitelesítés-szolgáltató a tanúsítvány visszavonási listákat legalább 24 óránként közzé teszi.

4.4.10 Tanúsítvány visszavonási lista ellenőrzési követelményei

A hitelesítés-szolgáltató védje meg a tanúsítvány visszavonási lista sértetlenségét és hitelességét.

4.4.11 Valós idejű visszavonási állapot ellenőrzés elérhetősége

[1] törvényben felsorolt körülményeken túl a szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

4.4.12 Valós idejű visszavonás ellenőrzési követelmények

[1] törvényben felsorolt körülményeken túl a szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

4.4.13 A visszavonási hirdetések egyéb elérhető formái

Nincs rá külön előírás.

4.4.14 A visszavonási hirdetések egyéb elérhető formáinak ellenőrzési követelményei

Nincs rá külön előírás.

4.4.15 Kulcs kompromittálódás esetére vonatkozó speciális követelmények

Nincs rá külön előírás.

4.5 A biztonsági naplózás folyamatai

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg, hogy a biztonságos környezet fenntartása érdekében a hitelesítés-szolgáltató milyen eseménynaplózó és ellenőrző rendszereket valósít meg.

A jelen dokumentumban leírt tanúsítványtípus csak a tanúsítványokra vonatkozó adatok (regisztrációs információ, a hitelesítés-szolgáltató kulcsgondozási és tanúsítványgondozási eseményeire vonatkozó fontosabb információ) naplózási folyamatának alábbi általános jellegzetességeit adja meg:

- A hitelesítés-szolgáltató a környezetére, kulcs- és tanúsítvány gondozására vonatkozó fontosabb események pontos időpontját is rögzítse. A szolgáltatási szabályzat ismertesse az események időzítéséhez használt óra pontosságát, és azt, hogy ez a pontosság hogyan van biztosítva.
- A hitelesítés-szolgáltató biztosítsa személyzete felelősségre vonhatóságát tevékenységéért, többek között az eseménynapló megőrzésén és védelmén keresztül.

4.5.1 A tárolt események típusai

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

A naplózandó speciális eseményeket és adatokat a hitelesítés-szolgáltató dokumentálja szolgáltatási szabályzatában.

A regisztrációval kapcsolatosan:

A hitelesítés-szolgáltató gondoskodjon arról, hogy naplózásra kerüljön valamennyi regisztrációval kapcsolatos esemény, beleértve a tanúsítvány megújítására (tanúsítványfrissítésre, tanúsítvány aktualizálására és kulcscserére) vonatkozó kérelmet is.

A tanúsítvány előállítással kapcsolatosan:

A hitelesítés-szolgáltató naplózza a szolgáltatói kulcsok életciklusával kapcsolatos összes eseményt.

A hitelesítés-szolgáltató naplózza a tanúsítványok életciklusával kapcsolatos összes eseményt.

Az alanyok eszközzel való ellátásával kapcsolatosan:

A hitelesítés-szolgáltató naplóz minden általa gondozott kulcs életciklusával kapcsolatos eseményt.

A hitelesítés-szolgáltató naplózza a biztonságos aláírás-létrehozó eszközök készítésével kapcsolatos valamennyi eseményt.

A visszavonás kezeléssel kapcsolatosan:

A hitelesítés-szolgáltató gondoskodjon a visszavonással kapcsolatos összes kérés, valamint az ezek eredményét képező összes tevékenység naplózásáról.

4.5.2 A napló állomány feldolgozásának gyakorisága

A napló állományok feldolgozásának gyakoriságát a hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg.

4.5.3 A napló állomány megőrzési időtartama

[1] törvényben felsorolt eseteken túl a szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

4.5.4 A napló állomány védelme

A hitelesítés-szolgáltató az eseményeket oly módon naplózza, ami nem törölhető, illetve nem tehető könnyen tönkre azon időtartam alatt, amíg azokat meg kell őrizni.

A hitelesítés-szolgáltató biztosítsa a tanúsítványok és kulcsok gondozására vonatkozó napló rekordok bizalmasságát és sértetlenségét.

4.5.5 A napló állomány mentési folyamatai

A napló állomány mentési folyamatait a hitelesítés-szolgáltató szolgáltatási szabályzatában határozza meg.

4.5.6 A napló gyűjtési rendszere

A napló gyűjtési rendszerét a hitelesítés-szolgáltató szolgáltatási szabályzatában határozza meg.

4.5.7 Az eseményeket kiváltó alanyok értesítése

A hitelesítés-szolgáltató nem köteles értesíti a naplóbejegyzéseket kiváltó alanyokat, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában közreműködőknek ilyen esetben legyen kötelessége a hitelesítés-szolgáltatóval való együttműködés.

4.5.8 Sebezhetőség felmérése

A sebezhetőség felmérésére végzett tevékenységeket a hitelesítés-szolgáltató szolgáltatási szabályzatában határozza meg.

4.6 Adatok archiválása

A hitelesítés-szolgáltató gondoskodjon 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 hitelesítés-szolgáltató gondoskodjon arról, hogy rögzítésre kerüljön az összes regisztrációs információ.

A tanúsítványokra vonatkozó valamennyi naplóbejegyzés kerüljön archiválásra.

Azon eseményeket, mely a fent említett naplóbejegyzéseken túl kerülnek archiválásra (a biztonságos környezet fenntartásának és utólagos ellenőrizhetősége és bizonyíthatósága céljából), a hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg.

4.6.2 Az archívum megőrzési időtartama

A hitelesítés-szolgáltató a nyilvántartásait őrizze meg a vállalt időtartamig (amelyet a hitelesítés-szolgáltató szerződéses feltételei (kikötések és feltételek) jelöljenek meg, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig).

A hitelesítés-szolgáltató a tanúsítványokra vonatkozó napló adatokat őrizze meg addig az időtartamig, amelyet a hitelesítés-szolgáltató szerződéses feltételei (kikötések és feltételek) megjelöltek.

A biztonságos környezet fenntartásának utólagos ellenőrizhetősége és bizonyíthatósága érdekében archivált egyéb naplóbejegyzések megőrzési időtartamát a hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg.

4.6.3 Az archívum védelme

A hitelesítés-szolgáltató tartsa fenn a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmosságát és sértetlenségét.

A hitelesítés-szolgáltató a tanúsítványokra vonatkozó naplóadatokat teljes körűen és a bizalmosságot garantáló módon archiválja a szolgáltatás szabályzatban leírt üzleti gyakorlatnak megfelelően.

A hitelesítés-szolgáltató a fontos bejegyzéseket védje meg az elveszéstől, tönkretételtől és hamisítástól.

A hitelesítés-szolgáltató hozzon megfelelő műszaki és szervezeti intézkedéseket 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

Az archívum mentési folyamatait a hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg.

4.6.5 A rekordok időbélyegzésére vonatkozó követelmények

Az archívum időbélyegzésére vonatkozó követelményeit és gyakorlatát a hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg.

4.6.6 Az archívum gyűjtési rendszere

Az archívum gyűjtési rendszerét a hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg.

4.6.7 Archív információ hozzáférését és ellenőrzését végző eljárások

A hitelesítés-szolgáltató a tanúsítványokra vonatkozó adatokat bocsássa rendelkezésre, ha arra jogi eljárásokban bizonyíték nyújtása céljából szükség van.

Az alany és az adatvédelmi követelmények korlátozásain belül a felhasználó férhessen hozzá az alanyra vonatkozó regisztrációs és egyéb információhoz.

4.7 Kulcscsere

A végfelhasználói tanúsítványok kulcscseréjét a hitelesítés-szolgáltató szolgáltatási szabályzata tárgyalja.

4.8 Helyreállítás kompromittálódás és katasztrófa esetén

A hitelesítés-szolgáltató gondoskodjon arról, hogy katasztrófa esetén, beleértve a saját aláírás-létrehozó magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, az üzemeltetés, amint csak lehetséges, helyreálljon.

4.8.1 Sérült számítási erőforrások, szoftverek és/vagy adatok

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

A hitelesítés-szolgáltató minimalizálja a biztonsági események és hibás működések által okozott kárt, eseményjelentés és válaszadás eljárások használatán keresztül.

A hitelesítés-szolgáltató időben és összehangoltan lépjen fel annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Ennek érdekében valamennyi eseményt jelentse az esemény bekövetkezte után, amint az lehetséges.

4.8.2 Egy szolgáltatói egység nyilvános kulcsának visszavonása

Egy szolgáltatói kulcs visszavonása esetén a hitelesítés-szolgáltató az alábbiakat vállalja:

- a visszavonásról tájékoztassa az összes igénybevevőt,
- jelezze, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes(ek).

A hitelesítés-szolgáltató a szolgáltatói kulcs visszavonását előidéző okok megszüntetése érdekében állítsa helyre a biztonságos környezetet, valamint az alanyok számára új tanúsítvány kiadásával biztosítson új nyilvános kulcsot.

4.8.3 Egy szolgáltatói egység nyilvános kulcsának kompromittálódása

Lásd 4.8.2 pont

4.8.4 Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően

Természeti vagy más egyéb katasztrófát követően a hitelesítés-szolgáltató léptesse életbe az üzletmenet folytonossági terve (illetve katasztrófa utáni helyreállítási terve) által megtervezett eljárásokat annak érdekében, hogy az üzemeltetés helyreálljon a szolgáltatási szabályzatban megjelölt időn belül.

Egy katasztrófát követően a hitelesítés-szolgáltató (ha ez ésszerű) tegyen lépéseket a katasztrófa ismételt bekövetkezésének megakadályozására.

4.9 A hitelesítés-szolgáltató leállítása

Nincs rá külön előírás.

5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A biztonsági óvintézkedésekről általában:

A hitelesítés-szolgáltató gondoskodjon 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 hitelesítés-szolgáltató az egységein belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan tartsa fenn. A biztonság szintjére hatást gyakorló bármilyen változtatást a hitelesítés-szolgáltató vezetőségének kelljen jóváhagynia.
- A hitelesítés-szolgáltató (rendszerbiztonsági szabályzatában) dokumentálja, majd valósítsa meg és folyamatosan tartsa fenn a hitelesítési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait.
- A hitelesítés-szolgáltató gondoskodjon az informatika biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más egységhez, illetve egységhez lettek kiadva.
- A hitelesítés-szolgáltató biztonsági műveleteiért a végső felelősség a felső vezetőségé legyen.

A biztonsági műveletek közé az alábbiak tartoznak:

- üzemeltetési eljárások és felelőségek,
- 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.

E felelőségeket a hitelesítés-szolgáltató biztonsági műveletei kezeljék, de azokat ténylegesen nem szakértő üzemeltető személyzet végrehajthatja.

Az értékek osztályozása és kezelése

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

- A hitelesítés-szolgáltató valamennyi informatikai értékéről vezessen leltárt, ezek védelmi követelményeit sorolja osztályokba és minősítse kockázatelemzésével összhangban.

5.1 Fizikai óvintézkedések

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

5.1.1 A telephely elhelyezése és szerkezeti felépítése

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

A hitelesítés-szolgáltató biztosítsa az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.

A hitelesítés-szolgáltató óvintézkedéseket valósítson meg az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

Tanúsítvány előállítással, alanyok eszközzel való ellátással, visszavonás kezeléssel kapcsolatosan:

A hitelesítés-szolgáltató egy egyértelműen meghatározott biztonsági körlet létrehozásával fizikai védelmet biztosítson az alábbi szolgáltatások számára:

- tanúsítvány előállítás,
- az alanyok eszközzel való ellátása,
- visszavonás kezelés.

Bármely más egységgel megosztott rész e körleten kívül essen.

A hitelesítés-szolgáltató óvintézkedéseket valósítson meg a fizikai és környezetbiztonsági rendszer erőforrások, illetve a működésük támogatására használt berendezések megvédése érdekében. A hitelesítés-szolgáltató

- tanúsítvány előállítás,
- az alanyok eszközzel való ellátása,
- visszavonás kezelés,

szolgáltatásainak fizikai- és környezetbiztonsági programjai foglalkozzanak 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.

A hitelesítés-szolgáltató óvintézkedéseket valósítson 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 hitelesítés-szolgáltató

- tanúsítvány előállítás,
- az alanyok eszközzel való ellátása,
- visszavonás kezelés,

szolgáltatásokkal kapcsolatos eszközökhöz történő fizikai hozzáférést megfelelően felhatalmazott egyénekre korlátozza.

A hitelesítés-szolgáltató a

- tanúsítvány előállítás,

- az alanyok eszközzel való ellátása,
- visszavonás kezelés,

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

5.1.3 Áramellátás, légkondicionálás

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

5.1.5 Tűzmegelőzés és tűzvédelem

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

5.1.6 Adathordozók tárolása

A hitelesítés-szolgáltató az adathordozó eszközöket biztonságosan kezelje a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében. A személyzet minden irányítói felelősséggel rendelkező tagja legyen felelős a tanúsítványtípus és a vele kapcsolatos gyakorlatok tervezéséért, valamint a szolgáltatási szabályzatban dokumentáltaknak megfelelő, hatékony megvalósításáért.

A hitelesítés-szolgáltató az összes adathordozó eszközt biztonságosan kezelje az adat-minősítési rendszer követelményeinek megfelelően.

5.1.7 Selejt kezelése, megsemmisítése

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

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

5.2 Eljárásbeli óvintézkedések

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

A hitelesítés-szolgáltató személyzete olyan adminisztratív és kezelési eljárásokat és folyamatokat végezzen, amely szinkronban van a hitelesítés-szolgáltató rendszerbiztonsági szabályzatának eljárásaival.

5.2.1 Bizalmi munkakörök

A hitelesítés-szolgáltató a biztonsági munkaköröket és felelőségeket munkaleírásokban dokumentálja.

A bizalmi munkakörökbe a hitelesítés-szolgáltató felső vezetése nevezze ki a munkatársakat.

Valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására, előzetesen kidolgozott eljárások kerüljenek végrehajtásra.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

A hitelesítés-szolgáltató (ideiglenes és állandó) munkatársainak munkaleírásai támogassák a feladatok szétválasztását. A munkaleírások többek között határozzák meg az egyes feladatokhoz szükséges létszámot is.

Csak bizalmi munkakört betöltő személyzet végezheti legalább kettős ellenőrzés mellett az alábbi funkciókat:

- a hitelesítés-szolgáltató saját (szolgáltatói) kulcsának előállítása,
- a hitelesítés-szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktivizálása,
- a hitelesítés-szolgáltató magán aláíró kulcsának másolása, letárolása, visszaállítása,
- a hitelesítés-szolgáltató magán aláíró kulcsának megsemmisítése.

A fenti funkciók végrehajtására felhatalmazott személyzet köre a hitelesítés-szolgáltató szolgáltatási szabályzatának megfelelően, a lehető legkisebbre legyen korlátozva.

5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

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 gondoskodjon arról, hogy személyzeti, illetve a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a hitelesítés-szolgáltató működésének megbízhatóságát.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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

A vezető személyzet tapasztalattal rendelkezzen az elektronikus aláírási technológia terén, ismerje a biztonsági felelősséggel tartozó munkatársakra vonatkozó biztonsági eljárásokat, valamint gyakorlattal rendelkezzen az informatika biztonság és a kockázatelemzés területein.

5.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások

A hitelesítés-szolgáltató ne nevezzen ki bizalmi munkakörbe, illetve a vezetőségbe olyan személyt, aki bűncselekményért, illetve más olyan vétségért el lett ítélve, amely beosztást illető alkalmasságát befolyásolja. A

munkatársak ne férhessenek biztonsági funkciókhoz a szükséges, személyükre és alkalmasságukra vonatkozó ellenőrzések végrehajtása előtt.

5.3.3 Továbbképzési gyakoriságok és követelmények

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

5.3.4 A felhatalmazás nélküli tevékenységek büntető következményei

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

5.3.5 A szerződéses alkalmazottakra vonatkozó követelmények

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

5.3.6 A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentáció tartalmazza a szolgáltató rendszerbiztonsági szabályzatát.

6 Műszaki biztonsági óvintézkedések

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

6.1 Kulcspár előállítás és telepítés

A hitelesítés-szolgáltató gondoskodjon valamennyi általa (saját maga, egyes egységi egységei /pl. tanúsítványtár, regisztrációs egységek, illetve alanyok számára) generált magánkulcs biztonságos és szabványos előállításáról.

6.1.1 Kulcspár előállítás

A hitelesítés-szolgáltató saját kulcspár előállítása:

A hitelesítés-szolgáltató a kulcselőállítást olyan eszközön belül hajtsa végre, amely kellően biztonságos és megfelel a jogszabályi előírásoknak, azaz rendelkezik a kijelölt tanúsító szervezet által kibocsátott, megfelelő tanúsítvánnyal és szerepel a Felügyelet nyilvántartásában.

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

A hitelesítés-szolgáltató által saját egységi egységei /tanúsítványtár, regisztrációs egységek/ számára előállított kulcsokat biztonságos módon, olyan algoritmussal állítsa elő, melyet a „2/2002 (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről” jogszabály 1. sz. melléklete sorol fel.

Amennyiben a hitelesítés-szolgáltató „Aláírás-létrehozó adat elhelyezése” szolgáltatást nyújt, úgy az alany számára előállított kulcsokat olyan eszközön belül állítsa elő, melyek

- a) kellően biztonságosak és megfelelnek a jogszabályi előírásoknak, azaz rendelkeznek a kijelölt tanúsító szervezet által kibocsátott, megfelelő tanúsítvánnyal és szerepelnek a Felügyelet nyilvántartásában;
- b) alkalmasak arra, hogy biztonságos módon juttassák az alany számára átadandó biztonságos aláírás-létrehozó eszközbe az előállított kulcsokat, amennyiben az alany számára előállított kulcsok nem az alany számára átadandó eszközben keletkeztek.

Az alany számára átadandó eszköz kellően biztonságos legyen és rendelkezzen a kijelölt tanúsító szervezet által kibocsátott, megfelelő tanúsítvánnyal és mint minősített biztonságos aláírás-létrehozó eszköz szerepeljen a Felügyelet elektronikus aláírás termékek nyilvántartásában.

Az alany által előállított kulcspár előállítás:

Az alany a kulcselőállítást olyan eszközön belül hajtsa végre, amely kellően biztonságos és rendelkezik kijelölt tanúsító szervezet által kibocsátott, megfelelő tanúsítvánnyal és mint minősített biztonságos aláírás-létrehozó eszköz szerepel a Felügyelet elektronikus aláírás termékek nyilvántartásában. A hitelesítés-szolgáltató tegyen meg mindent azért, hogy az alany csak olyan nyilvános kulcsát foglalja tanúsítványba, melynek magán párja az alany biztonságos aláírás-létrehozó eszközében keletkezett.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

A hitelesítés-szolgáltató amikor kulcsokat generál más felek számára:

- a) az általa más felek számára előállított kulcsokat, illetve az azt tartalmazó biztonságos aláírás-létrehozó eszközt a címzett félhez történő továbbításig biztonságos módon tárolja;
- b) az általa más felek számára előállított magánkulcsot, illetve az azt tartalmazó biztonságos aláírás-létrehozó eszközt a címzett félhez olyan módon továbbítsa, hogy a magánkulcs titkossága ne sérüljön;
- c) a szállítást követően csak az alany férhessen hozzá saját magánkulcsához;
- d) a hitelesítés-szolgáltató biztonságosan felügyelje a biztonságos aláírás-létrehozó eszköz elkészítését;
- e) a hitelesítés-szolgáltató biztonságosan ellenőrizze a biztonságos aláírás-létrehozó eszköz kiiktatását és újraaktivizálását;
- f) a hitelesítés-szolgáltató a biztonságos aláírás-létrehozó eszköz aktivizálási adatait (PIN kód) biztonságosan készítse el és az aláírás-létrehozó modultól elkülönítve ossza szét.

6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A hitelesítés-szolgáltató biztosítsa a nyilvános kulcs sértetlenségét a kulcspár nyilvános részének a tanúsítvány kibocsátásának helyszínére történő továbbítás során.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

A hitelesítés-szolgáltató saját aláírás-ellenőrző (szolgáltatói) nyilvános kulcsait tegye elérhetővé 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:

RSA algoritmus használata esetén minimum 2048 bit legyen.

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

RSA algoritmus használata esetén minimum 1024 bit legyen.

6.1.6 A nyilvános kulcs paramétereinek előállítása

A hitelesítés-szolgáltató a nyilvános kulcs paramétereinek előállítása során /beleértve az ehhez szükséges véletlen szám generálást is/ olyan szabványos megoldást használjon, melyet a [2] irányelv 1. sz. melléklete elismer erre a célra alkalmasnak.

6.1.7 A paraméterek megfelelőségének ellenőrzése

A hitelesítés-szolgáltató ellenőrizze valamennyi kulcspár előállítása során a paraméterek minőségét a szolgáltatási szabályzatban ismertetett módon.

6.1.8 Hardver/szoftver kulcselőállítás

Lásd 6.1.1 pont.

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

A hitelesítés-szolgáltató saját kulcsai használati célja az alábbiak lehetnek:

- tanúsítvány aláírás,
- visszavonási lista aláírás,
- időbélyeg válasz aláírása.

Azalany számára előállított kulcsok használati célja kizárólag aláírás lehet. Ez a tanúsítványtípus kizárólag elektronikus aláírásra használható kulcsokkal, tanúsítványokkal foglalkozik. A titkosításra, illetve hitelesítésre is használható kulcsokkal hitelesítés-szolgáltató egy másik tanúsítványtípusa foglalkozzon.

6.2 A magánkulcsok védelme

A hitelesítés-szolgáltató gondoskodjon valamennyi általa (saját maga, regisztrációs egységek) előállított magánkulcs titkosságáról és sértetlenségéről.

A hitelesítés-szolgáltató nem köteles külön aláíró magánkulcsot tanúsítvány aláírásra, és tanúsítvány visszavonási lista aláírásra használni, de ezen kulcsokat semmilyen más célra ne használja.

A hitelesítés-szolgáltató a tanúsítványokat, illetve a tanúsítvány visszavonási listákat aláíró magánkulcsait fizikailag biztonságos helyszínen használja.

6.2.1 Kriptográfiai modulra vonatkozó szabványok

Hitelesítő egység

Lásd 6.1.1 pont.

Regisztrációs egység

Lásd 6.1.1 pont.

Igénybevevők (alanyok)

Lásd 6.1.1 pont.

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

Hitelesítő egység

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

Regisztrációs egység

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

Igénybevevők (alanyok)

Az alanyok magán aláíró kulcsa nem kerül mentésre, így visszaállítása nem lehetséges.

6.2.2 Magánkulcs letétbe helyezése

A hitelesítés-szolgáltató az alany magán aláíró kulcsait ne helyezze letétbe, és ne tartsa olyan módon sem, mely lehetővé tenné a (kulcs)adatok későbbi dekódolását.

6.2.3 Magánkulcs mentése

Hitelesítő egység

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

Regisztrációs egység

A regisztrációs egység magán aláíró kulcsainak mentett másolataira ugyanolyan szintű biztonsági előírások vonatkoznak, mint a használatban levő kulcsokra.

Igénybevevők (alanyok)

A hitelesítés-szolgáltató által az alanyoknak vagy az alanyok saját maguknak előállított magánkulcsok mentése nem lehetséges.

6.2.4 Magánkulcs archiválása

Lásd 6.2.2, illetve 6.2.3 pont.

6.2.5 Magánkulcs bejuttatása a kriptográfiai modulba

Hitelesítő egység

A hitelesítő egység magánkulcsait az ezeket felhasználó kriptográfiai hardver modul állítsa elő, így ezeket első használat előtt nem kell külön a modulba juttatni.

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) a hitelesítő egység 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.

A hitelesítő egység 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.

Regisztrációs egység

A regisztrációs egység magánkulcsait az ezeket felhasználó kriptográfiai hardver modul állítsa elő, így ezeket első használat előtt nem kell külön a modulba juttatni.

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) a regisztrációs egység 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.

A regisztrációs egység 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.

Igénybevevők (alanyok)

Amennyiben a hitelesítés-szolgáltató „Aláírás-létrehozó adat elhelyezése” szolgáltatást nyújt és az alany számára előállított kulcsok nem az alany számára átadandó biztonságos aláírás-létrehozó eszközben keletkeztek, úgy a hitelesítés-szolgáltató az alany számára magánkulcsoknak a biztonságos aláírás-létrehozó eszközbe való bejuttatása (áttöltése) során kódolja a magánkulcsokat, olyan protokollt, algoritmust és kulcs hosszát alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt magánkulcs teljes hátralévő életciklusában.

Az alany magán aláíró kulcsa a feltöltést követően maradjon a biztonságos aláírás-létrehozó eszközben, azt semmilyen célból ne hagyja el.

Az alany biztonságos aláírás-létrehozó eszköze kikapcsolt állapotban a magánkulcsokat tárolja kódolva, olyan algoritmust és kulcs hosszát alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs teljes hátralévő életciklusában.

6.2.6 A magánkulcs aktivizálásának módja

Hitelesítő egység

A hitelesítő egység (tanúsítványokat és tanúsítvány visszavonási listákat aláíró) magánkulcsait bizalmi munkakört betöltő személy aktivizálhassa megfelelően biztonságos hitelesítési eljárással.

A hitelesítő egység egyéb (a hitelesítés-szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsait bizalmi munkakört betöltő személy aktivizálhassa megfelelően biztonságos hitelesítési eljárással.

Regisztrációs egység

A regisztrációs egység (az archiválandó regisztrációs adatokat és tranzakciókat aláíró) magánkulcsait bizalmi munkakört betöltő személy aktivizálhassa megfelelően biztonságos hitelesítési eljárással.

A regisztrációs egység egyéb (a hitelesítés-szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsait bizalmi munkakört betöltő személy aktivizálhassa megfelelően biztonságos hitelesítési eljárással.

Igénybevevők (alanyok)

Az alany magánkulcsa illetéktelen felhasználásának megakadályozása érdekében a biztonságos aláírás-létrehozó eszközben tárolt magánkulcs használatát az alany megfelelően biztonságos hitelesítési eljárással aktivizálhassa.

6.2.7 A magánkulcs aktív állapotának megszüntetési módja

Hitelesítő és regisztrációs egység

A szolgáltató erről a szolgáltatási szabályzatában adjon tájékoztatást.

Igénybevevők (alanyok)

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

6.2.8 A magánkulcs megsemmisítésének módja

Hitelesítő és regisztrációs egység magánkulcsainak megsemmisítése

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

A hitelesítés-szolgáltató által az alanyok számára generált magánkulcsok megsemmisítése

A hitelesítés-szolgáltató – közvetlenül az alany magánkulcsának előállítására és az alany aláírás-létrehozó eszközére töltése után – a magánkulcsot (s annak minden esetleges másolatát) semmisítse meg.

A hitelesítés-szolgáltató által végrehajtott kulcscsere során – az alany új magánkulcsának biztonságos aláírás-létrehozó eszközre töltése utáni megsemmisítésén túlmenően – hitelesítés-szolgáltató gondoskodjon arról is, hogy a régi magánkulcs az alany biztonságos aláírás-létrehozó eszközén is megsemmisüljön.

6.3 A kulcspár gondozásának egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

A hitelesítés-szolgáltató - tanúsítvány archiválási szolgáltatása keretén belül – archiválhatja az alanyok nyilvános kulcsait.

6.3.2 A nyilvános és magánkulcsok használatának periódusa

Hitelesítő és regisztrációs egység

A hitelesítés-szolgáltató saját magánkulcsainak használati periódusa ne haladhatta meg az azokhoz tartozó tanúsítvány érvényességi idejét.

Igénybevevők (alanyok)

Az alany magánkulcsának használati periódusa nem haladhatja meg a tanúsítvány érvényességi idejét, ennek betartása viszont kívül esik a hitelesítés-szolgáltató felelősségi körén. Ennek betartása az alany kötelessége, ellenőrzése pedig az érintett felek kötelessége.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

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

6.4.1.1 Az aktivizáló adatok védelme

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

6.4.1.2 Az aktivizáló adatok egyéb szempontjai

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

6.5 Számítógépbiztonsági óvintézkedések

6.4.2 Speciális számítógépbiztonsági műszaki követelmények

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

- A hitelesítés-szolgáltató védje meg rendszerei és információi sértetlenségét vírusok, káros és engedély nélküli szoftverek ellen.
- A hitelesítés-szolgáltató kezelje biztonságosan adathordozó eszközeit a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.
- A hitelesítés-szolgáltató gondoskodjon a felhasználói (a felhasználó fogalma itt felöleli a rendszer operátorokat, rendszer adminisztrátorokat és bármely olyan felhasználót, akinek közvetlen hozzáférése van a rendszerhez) hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.
- A hitelesítés-szolgáltató gondoskodjon 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 számítógép biztonsági ellenőrzéseket nyújtson a hitelesítés-szolgáltató szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében. Különösképpen a rendszer szolgáltatási programok használatát korlátozza és ellenőrizze szigorúan.
- A hitelesítés-szolgáltató gondoskodjon arról, hogy személyzetét sikeresen azonosítsák és hitelesítsék, mielőtt a tanúsítvány gondozásával kapcsolatos kritikus alkalmazásokat használhatnák.
- A hitelesítés-szolgáltató műszaki óvintézkedéseket juttasson érvényre (például tűzfalak segítségével), hogy a hitelesítés-szolgáltató belső hálózati tartományai védettek legyenek a harmadik felek számára elérhető külső hálózati tartományoktól.
- A hitelesítés-szolgáltató időben és összehangoltan lépjen fel annak érdekében, hogy gyorsan válaszoljon tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Valamennyi eseményt jelentsen az esemény bekövetkezése után, amint az lehetséges.
- A hitelesítés-szolgáltató folyamatos felügyelő és riasztó eszközöket biztosítson, hogy képes legyen felismerni és regisztrálni az erőforrásaihoz való jogosulatlan és/vagy szabálytalan hozzáférési kísérleteket, valamint képes legyen ezekre időben reagálni.
- A hitelesítés-szolgáltató gondoskodjon 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 hitelesítés-szolgáltató gondoskodjon arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzését érvényesítsen a visszavonás állapot információ (hálózatról történő) módosítására vonatkozóan.
- A hitelesítés-szolgáltató gondoskodjon arról, hogy az érzékeny adatokat megvédjék az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.
- A hitelesítés-szolgáltató biztosítsa a személyzet tevékenységéért való felelősségre vonhatóságát.

6.4.3 Informatikai biztonsági minősítés

A hitelesítés-szolgáltató szolgáltatásaira vonatkozóan hajtson végre kockázatelemzést, azonosítsa azokat a kritikus szolgáltatásokat, amelyekhez megbízható informatikai rendszerek kellene, egyben határozza meg a szükséges értékelési garanciaszinteket.

6.5 Életciklusra vonatkozó műszaki óvintézkedések

6.5.1 Rendszerfejlesztési óvintézkedések

A hitelesítés-szolgáltató gondoskodjon 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.

6.5.2 Biztonságkezelési óvintézkedések

A hitelesítés-szolgáltató olyan eszközöket és eljárásokat alkalmazzon, melyek garantálják a kritikus szolgáltatásait megvalósító megbízható informatikai rendszereire az operációs rendszer beállítások, valamint a hálózati konfiguráció biztonságát, egyúttal az alkalmazott biztonsági mechanizmusok sérteletlenségének, helyes működésének ellenőrzését.

6.5.2.1 Az életciklusra vonatkozó biztonság osztályozása

A hitelesítés-szolgáltató által alkalmazott megbízható informatikai rendszerek biztonsági értékelései foglalják magukba az életciklusra vonatkozó független biztonsági értékelési szempontokat is.

6.6 Hálózatbiztonsági óvintézkedések

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

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

Az érzékeny adatokat, melyek közzé a regisztrációs információk is tartoznak, védjék meg, amikor azok átvitele (cseréje) nem biztonságos hálózatokon keresztül történik.

A hitelesítés-szolgáltató biztosítsa általános informatikai biztonságát még akkor is, ha a hitelesítés-szolgáltató egyes funkciót más egység (pl. a regisztrációs egység) valósítja meg.

A regisztrálással kapcsolatosan:

A regisztrációs adatok bizalmosságát és sértetlenségét védjük meg, különösen a felhasználóval/alannyal folytatott külső, illetve a hitelesítés-szolgáltató egyes komponensei közötti belső adatcsere során.

A hitelesítés-szolgáltató (a hitelesítő egységen keresztül) ellenőrzéssel biztosítsa, hogy regisztrációs adatokat csak általa elismert, azonosságában hitelesített regisztrációs szolgáltatókkal cserél.

A tanúsítvány előállításával és visszavonás kezelésével kapcsolatban:

A hitelesítés-szolgáltató gondoskodjon arról, hogy a helyi hálózati komponensek (például routerek) fizikailag biztonságos környezetben legyenek és konfigurációikat időszakonként auditálják.

A hitelesítés-szolgáltató folyamatos felügyelő és riasztó eszközöket biztosítson, hogy képes legyen felismerni, regisztrálni az erőforrásaihoz (hálózatról) történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre.

A tanúsítvány kibocsátásával kapcsolatban:

A hitelesítés-szolgáltató gondoskodjon 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 kezelésével kapcsolatban:

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

6.7 A kriptográfiai modul ellenőrzése

A hitelesítés-szolgáltató gondoskodjon az általa kezelt kriptográfiai hardverek biztonságáról annak teljes élettartama alatt. Különösképpen gondoskodjon arról, hogy:

- a tanúsítványt, visszavonási állapotot és időbélyeget aláíró, valamint az eszköz szolgáltatás során kulcsgenerálásra használt, illetve az alannak átadott kriptográfiai hardvereket ne manipulálják szállítás és tárolás közben;
- a tanúsítványt, visszavonási állapotot és időbélyeget aláíró, valamint az eszköz szolgáltatás során kulcsgenerálásra használt, illetve az alannak átadott kriptográfiai hardverek helyesen működjenek;
- a hitelesítés-szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktivizálása, mentése és visszaállítása legalább két bizalmi munkakört betöltő alkalmazott együttes jelenlétét kívánja meg;
- a hitelesítés-szolgáltató kriptográfiai hardverén tárolt hitelesítés-szolgáltatói magán aláíró kulcsokat az eszköz visszavonásakor megsemmisítsék.

7 Tanúsítvány és tanúsítvány visszavonási lista profilok

7.1 Tanúsítvány profil

A hitelesítő-szolgáltató által kibocsátott tanúsítványok feleljenek meg a [6] szabványban leírt X.509 3-as verziójú tanúsítványoknak.

A hitelesítő-szolgáltató által az alanyoknak kibocsátott tanúsítványok feleljenek meg az [5], illetve a [8] szabványban leírt minősített tanúsítványoknak.

A tanúsítványprofil a szolgáltató tegye közzé a szolgáltatási szabályzatában.

7.1.1 Verzió szám(ok)

Lásd 7.1 pont.

7.1.2 Tanúsítvány kiterjesztések

Lásd 7.1 pont.

7.1.3 Algoritmus objektum azonosítók

Lásd 7.1 pont.

7.1.4 Elnevezési formák

Lásd 7.1 pont.

7.1.5 Elnevezésre vonatkozó korlátozások

Lásd 7.1 pont.

7.1.6 Tanúsítványtípus objektum azonosító

Lásd 7.1 pont.

7.1.7 A „tanúsítványtípus korlátozás” kiterjesztés használata

Lásd 7.1 pont.

7.1.8 Szabályzat minősítő szintaxis és szemantika

Lásd 7.1 pont.

7.1.9 A kritikus tanúsítványtípus kiterjesztés feldolgozása

Lásd 7.1 pont.

7.2 Tanúsítvány visszavonási lista profil

A hitelesítő-szolgáltató által kibocsátott tanúsítvány visszavonási listák feleljenek meg a [9] ajánlásának.

A hitelesítő-szolgáltató által kibocsátott tanúsítvány visszavonási listák feleljenek meg a [6] szabványban leírt X.509 2-as verziójú tanúsítvány visszavonási listáknak.

7.2.1 Verzió szám(ok)

Lásd 7.2 pont.

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

Lásd 7.2 pont.

8 Leírás adminisztráció

A hitelesítés-szolgáltató rendelkezzen olyan szolgáltatási szabályzattal, mely vonatkozik az általa támogatott, kielégítésre felvállalt tanúsítványtípusban azonosított, valamennyi állítást megvalósító gyakorlatra és eljárásra.

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg a hitelesítés-szolgáltató szolgáltatásait támogató valamennyi külső egységre vonatkozó kötelezettségeket, beleértve az alkalmazandó szabályzatokat is.

8.1 Leírás változtatási eljárások

A hitelesítés-szolgáltató határozzon meg egy felülvizsgálati folyamatot, mely kiterjed a tanúsítványtípus és szolgáltatási szabályzat gondozására is.

A hitelesítés-szolgáltató időben tegyen közzé értesítést az általa támogatott tanúsítványtípusban, illetve szolgáltatási szabályzatában tervezett változtatásokról, majd a jóváhagyást követően az átdolgozott tanúsítványtípust / szolgáltatási szabályzatot haladéktalanul tegye hozzáférhetővé.

8.2 Közzétételi és tájékoztatási elvek

A hitelesítés-szolgáltató az általa támogatott tanúsítványtípust, valamint szolgáltatási szabályzatát és egyéb más fontos dokumentációját bocsássa az igénybevevők rendelkezésére, a tanúsítványtípusnak való megfelelés felméréséhez szükséges mértékig.

A hitelesítés-szolgáltató a tanúsítvány használatával kapcsolatos kikötéseit és feltételeit az összes igénybevevő számára tegye megismerhetővé.

8.3 Szolgáltatás szabályzat jóváhagyási eljárások

A tanúsítványtípusra vonatkozóan:

A tanúsítványtípus tartalmilag meg kell feleljen a [4] MTT+ BALE tanúsítványtípusokkal szemben támasztott minimális követelményeknek.

A tanúsítványtípus formailag meg kell feleljen a [7] szabványnak.

A hitelesítés-szolgáltató elfogadás előtt vizsgálja meg a tanúsítványtípus fenti követelményeknek való megfelelését.

A tanúsítványtípus elfogadására vagy esetlegesen a Hírközlési Felügyelet által már nyilvántartásba vett tanúsítványtípusok közül történő kiválasztására a hitelesítés-szolgáltató felsőszintű irányító testülete rendelkezzen végső hatáskörrel és felelősséggel.

A Hírközlési Felügyelet vegye nyilvántartásba a hitelesítés-szolgáltató által jóváhagyott és bejelentett tanúsítványtípust.

A szolgáltatási szabályzatra vonatkozóan:

A szolgáltatási szabályzat tartalmilag és formailag feleljen meg a tanúsítványtípusnak.

A hitelesítés-szolgáltató jóváhagyás előtt vizsgálja meg a szolgáltatási szabályzatot a tanúsítványtípusnak való megfelelés szempontjából.

A szolgáltatási szabályzat jóváhagyására a hitelesítés-szolgáltató felsőszintű irányító testülete rendelkezzen végső hatáskörrel és felelőséggel.

A szolgáltatási szabályzat megfelelését a Hírközlési Felügyelet is vizsgálja meg és értékeli (hagyja jóvá vagy módosíttassa) a hitelesítés-szolgáltató minősítési eljárása során.