Matáv Minősített e-Szignó®
hitelesítésszolgáltatás és
Időbélyegzés-szolgáltatás

Szolgáltatási Szabályzata

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.8.2.1.13.2.1

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.11.3.13.1.1

Verziószám:..... **1.2**

Változáskezelés

Verzió-szám	Dátum	A változás leírása
0.90	2003-10-10	Első változat (szakértői munkaanyagok)
0.91	2003-10-26	Javított tervezet (első változat)
0.92	2003-10-31	Javított tervezet (ellenőrzött változat)
0.93	2003-11-30	Javított tervezet (kiegészített és ellenőrzött harmadik változat)
0.94	2003-12-15	A kiviteli dokumentumokkal egyeztetett változat
0.95	2004-01-30	A tesztek és jogi ellenőrzések alapján módosított első változat
0.96	2004-03-05	A szolgáltatói ellenőrzések után javított változat
0,97	2004-03-11	Matáv Workshop utáni javított változat
1.0	2004-03-30	Hatósági kérelemben beadott szabályzat
1.1	2004-07-17	Hatósági szemlét követő változások átvezetése
1.2	2004-09-23	Hatóság részére átadott végső változat

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

TARTALOMJEGYZÉK

1. Bevezetés

Az **elektronikus aláírással** kapcsolatos szolgáltatások jellemzően az alábbiak lehetnek:

- *hitelesítésszolgáltatás* (teljes néven: elektronikus aláírás hitelesítésszolgáltatás),
- *időbélyegzés-szolgáltatás*,
- *aláírás-létrehozó eszköz szolgáltatás* (teljes néven: aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatás).

A ***hitelesítésszolgáltatás*** keretében a *hitelesítés-szolgáltató* jellemzően az alábbi szolgáltatásokat nyújtja:

- *azonosítja* az igénylő (*előfizető* és *aláíró*) személyét (regisztrációs szolgáltatás),
- *tanúsítvány*t hoz létre, (*tanúsítvány-előállítás szolgáltatás*),
- nyilvántartásokat vezet,
- fogadja a *tanúsítvány*okkal kapcsolatos változások adatait (*visszavonáskezelés-szolgáltatás*),
- *nyilvánosságra hozza* a tanúsítványhoz tartozó szabályzatokat,
- nyilvánosságra hozza az *aláírás-ellenőrző adat*okat (*tanúsítvány-kibocsátás szolgáltatás*),
- nyilvánosságra hozza a tanúsítvány aktuális állapotára vonatkozó információkat (*visszavonási állapot közzététele szolgáltatás*).

Az ***időbélyegzés-szolgáltatás*** során a hitelesítés-szolgáltató az *elektronikus dokumentum*hoz *időbélyegző*t kapcsol[1].

Az ***aláírás-létrehozó eszköz szolgáltatás*** keretében a hitelesítés-szolgáltató előkészíti és átadja az *aláírás-létrehozó eszköz*t az előfizetőknek. Ez a szolgáltatás történhet ***biztonságos aláíró-eszköz*** alkalmazásával is, amely külön kategória.

[1] Erre aláírásellenőrzési célokból lehet szükség.

Minden *hitelesítés-szolgáltató*nak vállalnia kell a fenti három alapszolgáltatás-csoport legalább egy elemét, de a *hitelesítés-szolgáltató*k (jellemzően) több alapszolgáltatást is **nyújtanak**.

Míg az [1] törvény[2] {ld. **9 *Hivatkozások***} többféle *elektronikus aláírás*ról szól ez a dokumentum viszont a következő feltételezéseken alapul:

- az elektronikus aláírások a *nyilvános kulcsú kriptográfia* **eszközeivel** készülnek,
- az elektronikusan aláíró egy magán és egy nyilvános komponensből álló kriptográfiai kulcspárt birtokol,
- a dokumentumban szereplő rendszer által létrehozott *tanúsítvány* egyedülállóan **kapcsolja össze** az aláíró nyilvános kulcsát az aláíró azonosítójával és esetleg más, az aláíróra vonatkozó információkkal egy olyan elektronikus aláírás segítségével, amelyet a *hitelesítés-szolgáltató* magánkulcsa (tanúsítvány aláíró kulcs) felhasználásával állítanak elő.

Az [1] törvény[3] az *elektronikus aláírás*ok alábbi három (biztonsági) szintjét nevezi meg:

- **Elektronikus aláírás**, amely „*elektronikus dokumentum*hoz azonosítás céljából végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt elektronikus adat, illetőleg dokumentum”.
- **Fokozott biztonságú elektronikus aláírás**, amely olyan „*elektronikus aláírás*, amely megfelel a következő követelményeknek:
  a) alkalmas az *aláíró azonosítására* és *egyedülállóan* hozzá köthető*,*
  b) olyan eszközzel hozták létre, mely *kizárólag* az *aláíró* befolyása alatt áll,
  c) a dokumentum *tartalmához* olyan módon *kapcsolódik*, hogy *minden* – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – *módosítás* érzékelhető.*”*
- **Minősített elektronikus aláírás**, mely „olyan – fokozott biztonságú – elektronikus aláírás, amely *biztonságos aláírás-létrehozó eszköz*zel készült, és amelynek hitelesítése céljából *minősített tanúsítvány*t bocsátottak ki.”

[2] 2001. évi XXXV. törvény az elektronikus aláírásról

[3] 2001. évi XXXV. törvény az elektronikus aláírásról

Jelen dokumentum a **minősített elektronikus aláírás**sal kapcsolatos hitelesítésszolgáltatásra **vonatkozik**.

1.1 Áttekintés

1.1.1 A Szabályzat

Ez a szabályzat a **Matáv Rt.** (ebben a dokumentumban: *Szolgáltató*) **minősített** *hitelesítés-szolgáltató*i tevékenységével[4] kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazza.

A dokumentum teljes neve: ***Matáv Minősített e-Szignó® hitelesítésszolgáltatás és Időbélyegzés-szolgáltatás Szolgáltatási Szabályzata.***

A dokumentum rövid neve: ***Matáv e-Szignó® mHSzSz***, vagy ebben a dokumentumban *Szabályzat*).

A Szabályzat célja, hogy összefogja azokat a dokumentumokat és információkat, melyeket a *Szolgáltató*val valamilyen módon kapcsolatba kerülő feleknek (elsősorban a végfelhasználóknak) a minősített hitelesítésszolgáltatással kapcsolatosan tudni érdemes. A Szabályzat biztosítja a *Szolgáltató* működésének átláthatóságát, s lehetővé teszi annak megállapítását, hogy a *Szolgáltató* gyakorlata, illetve a hitelesítésszolgáltatás keretében kiadott tanúsítványfajta mennyiben felel meg a felhasználói és törvényes elvárásoknak. A Szabályzat segítségével a tanúsítványok megrendelői és elfogadói egyértelműen megállapíthatják a tanúsítványok **kezelésének módját**, a garantált **biztonságot** és a szolgáltatásokra vonatkozó műszaki, üzleti, pénzügyi **garanciák**at és jogi **felelősségvállalások**at.

A Szabályzatban meghatározott hitelesítésszolgáltatást a jelen szabályzat és a [14] és [15] szerinti Matáv dokumentumok, valamint az aláíróval / előfizetővel megkötött szerződés ([16]) együttesen szabályozzák {ld. **9** ***Hivatkozások***}. Amennyiben a [14] vagy [15[szerinti szabályzatok valamint jelen szabályzat bármely vonatkozásban ellentmondással vagy eltérő kikötéssel élnének, akkor a Szabályzat előírásai tekintendők irányadónak.

A Szabályzat a [4] és [13] dokumentumok szerint készült {ld. **9** ***Hivatkozások***}.

[4] ld. [1] törvény 2. § (20)

1.1.2 A Szabályzat hatályai

A Szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya az {**1.1.4 *Szolgáltatások***} alfejezetben ismertetett **szolgáltatások** nyújtására és igénybevételére, illetve ezen szolgáltatásokkal kapcsolatos összes **objektum**ra és **tárgyi eszköz**re kiterjed.

A Szabályzat területi hatálya

A Szabályzat területi hatálya **Magyarország** teljes területe.

A Szabályzat időbeli hatálya

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

A Szabályzat személyi hatálya

A Szabályzat személyi hatálya a teljes **Közösség** {ld. **1.3 *Közösség és alkalmazhatóság***}, minden egyes tagjára, természetes, jogi személyiségű illetve jogi személyiséggel nem rendelkező személyekre egyaránt kiterjed.

1.1.3 A szolgáltató

A Szabályzatban *Szolgáltató* alatt a Matáv Rt. által – a saját szervezetén belül – létrehozott ***Matáv e-Szignó® Minősített Hitelesítésszolgáltatást*** (hitelesítő szervezetet és regisztrációs szervezetet együttesen) kell érteni. A *Szolgáltató*t jogi értelemben a **Matáv Rt.** képviseli.

A *Szolgáltató* **alvállalkozókat** is megbízhat egyes feladatok elvégzésével (regisztráció, ügyfélszolgálati, értékesítés stb.). Az alvállalkozók tevékenységéért a *Szolgáltató* teljes felelősséggel tartozik.

A *Szolgáltató* elérési adatai az {**1.4 „*Kapcsolattartás*”**} alfejezetben találhatók.

1.1.4 Szolgáltatások

A Matáv Rt. tevékenységi köre – egyebek mellett - a hitelesítésszolgáltatás és az ehhez kötődő fejlesztési és tanácsadási tevékenységek. A hitelesítésszolgáltatás tevékenység keretein belül a *Szolgáltató* a biztonságos aláíró eszközzel kapcsolatos kereskedelmi és megszemélyesítési feladatokat is ellátja.

A Matáv Rt. minősített **hitelesítésszolgáltatási tevékenysége** a következő elemekből áll:[5]

a) elektronikus aláírás hitelesítésszolgáltatás

- **regisztráció**,
- tanúsítvány-**előállítás** szolgáltatás,
- tanúsítvány-**kibocsátás** szolgáltatás,
- (tanúsítvány) **visszavonás-kezelés** szolgáltatás,
- (tanúsítvány) **visszavonási állapot közzététele** szolgáltatás,

b) **időbélyegzés** szolgáltatás

c) **biztonságos aláírás-létrehozó eszköz** szolgáltatás

A kötelezően vállalt *hitelesítésszolgáltatások* a következőeket jelentik:

a) **Regisztráció**: Ennek során a hitelesítés-szolgáltató ellenőrzi egy aláíró személyazonosságát, és ha alkalmazható, bármely más, egyedi jellemzőjét is. A szolgáltatás eredményeit a rendszer a *tanúsítvány-előállítás szolgáltatás* felé továbbítja.

b) **Tanúsítvány-előállítás szolgáltatás**: A hitelesítés-szolgáltató létrehozza és aláírja a regisztrációs szervezet által ellenőrzött, az aláíró személyazonosságán és más tulajdonságain alapuló, az aláíró nyilvános kulcsát is tartalmazó *tanúsítvány*okat.

[5] ld. [1] törvény 3. melléklet

c) **Tanúsítvány-kibocsátás szolgáltatás**: A hitelesítés-szolgáltató szétosztja a *tanúsítvány*okat az *aláírók* között, és közzé teszi az *érintett fel*ek részére is. A szolgáltatás a hitelesítés-szolgáltató hitelesítési politikájára és gyakorlatára vonatkozó adatokat az *aláírók* és az *érintett fel*ek rendelkezésére bocsátja.

d) **Visszavonás-kezelés szolgáltatás**: A hitelesítés-szolgáltató feldolgozza a visszavonással kapcsolatos kérelmeket és jelentéseket a szükséges teendők meghatározása érdekében. A szolgáltatás eredményei a visszavonási állapot *közzététele szolgáltatás*on keresztül kerülnek kiosztásra.

e) **Visszavonási állapot közzététele szolgáltatás**: A hitelesítés-szolgáltató *tanúsítvány-visszavonás státus információ*t szolgáltat az *érintett fel*eknek. Ez a szolgáltatás a rendszeres időközönként frissített *tanúsítvány visszavonási listákon* (CRL) alapul.

f) **Időbélyegzés-szolgáltatás:** Az *időbélyegzés-szolgáltatás* bizonyítékot nyújt arról, hogy egy adatelem létezett egy megadott időpontban (a **létezés** bizonyítéka). Ha az adatelemet az adatkérő azelőtt aláírta, mielőtt továbbította volna az *időbélyegzés-szolgáltató* számára (amely mindig egy hitelesítés-szolgáltató), akkor az időbélyegzés-szolgáltatás bizonyítékul szolgál arra nézve, hogy az adott adatelem létezett és ezen entitás birtokában volt abban a bizonyos időpontban (a **birtoklás** bizonyítéka). A hitelesítés-szolgáltató, mint harmadik fél megbízhatóan gondoskodik az *időbélyegzés-szolgáltatás*ról.

g) **Biztonságos aláírás-létrehozó eszköz szolgáltatás**: A hitelesítés-szolgáltató biztonságos *aláírás-létrehozó adat*ot (magánkulcsot) helyez el az *előfizető biztonságos aláírás-létrehozó eszköz*én, és ezt eljuttatja az aláíróhoz.

1.1.5 Szabványok és előírások

A Szabályzat a [10] hivatkozás, azaz „RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)” szabvány szerint készült, a *Matáv e-Szignó® Minősített Hitelesítésszolgáltatás* [**MTT+BALE**] *tanúsítványtípusainak* megfelelve (az egyes tanúsítványtípusok eltérő kezelését a Szabályzat jelöli).

A Szabályzat tartalmi vonatkozásokban eleget tesz az [1], [2] és [3] szerinti hazai jogszabályok előírásainak és ajánlásainak, továbbá felhasználja a [7] műszaki specifikáció, valamint a [12] ajánlásait {ld. **9 *Hivatkozások***}.

1.1.6 Tanúsítványfajták

A *Szolgáltató* által alkalmazott tanúsítványfajták főbb jellegzetességei az alábbiak:

Teszt tanúsítvány

A ***teszt tanúsítvány***ok esetében a *Szolgáltató* nem igényli a személyes regisztrációt a tanúsítvány *aláíró*jától. A ***teszt tanúsítvány***okat a *Szolgáltató* - egyedi elbírálást követően - ingyenesen biztosíthatja az igénylők számára. A teszt tanúsítvány jelzése a tanúsítvány tartalmában az erre utaló hivatkozással történik.

Mivel a ***teszt tanúsítvány***ok tartalma nem tekintendő ellenőrzött információnak, ezért ezek használata kizárólag tesztelési és oktatási célokra ajánlott, illetve olyan esetekben, mikor a biztonságról más módszerekkel is gondoskodnak.

Végfelhasználói minősített tanúsítvány

A ***végfelhasználói minősített tanúsítvány***ok igen erős biztosítékokkal szolgálnak a benne megnevezett személyek kilétét illetően. Ez esetben ugyanis követelmény az *aláíró* személyes megjelenése a *Regisztrációs Szervezet*nél**.** Emellett a Regisztrációs Szervezet az aláíró (és előfizető) adatait a hatósági adatbázisokkal is egyezteti ill. ellenőrzi. A ***végfelhasználói minősített tanúsítvány***okhoz kapcsolódó aláíró csak természetes személy lehet. **Előfizető** és **érintett fél** természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet is lehet. A szervezet azonosítása – a természetes személy azonosításához hasonlóan – szigorú módszerekkel történik.

A ***végfelhasználói minősített tanúsítvány***ok használata a magas összegű pénzügyi tranzakcióknál, továbbá a nagy biztonságú elektronikus dokumentumoknál ajánlott.

A *Szolgáltató* az egyes tanúsítványfajták tekintetében tranzakciós limiteket (aláíró által az aláírással egy alkalommal vállalható kötelezettség legmagasabb értéke) határozott meg. Az adott tanúsítvány ezt meghaladó összegű tranzakciókban nem használható fel. A tranzakciós limitek a következők:

Tanúsítványfajta	Tranzakciós limit
végfelhasználói minősített üzleti tanúsítvány - arany	**500 000 000 Ft. / tranzakció**
végfelhasználói minősített üzleti tanúsítvány - ezüst	**100 000 000 Ft. / tranzakció**
végfelhasználói minősített üzleti tanúsítvány - bronz	**10 000 000 Ft./tranzakció**

Az igénylőnek (*előfizető*, *aláíró*) mérlegelési joga és felelőssége, hogy a *Szolgáltató* szabályzatai alapján meghatározza, milyen tanúsítványt alkalmaz egy adott célra.

Ez a szabályzat a **végfelhasználói minősített üzleti tanúsítványfajta** kezelésére vonatkozik.

Más tanúsítványfajta kezelését a *Szolgáltató* más szolgáltatási szabályzatai tárgyalhatják. Az egyes tanúsítványfajták nemcsak az azonosítás (a tanúsítvány és a benne megnevezett személyek közötti megfeleltethetőség) szintjében térhetnek el, hanem a *Szolgáltató* egyéb adminisztratív, algoritmikus, informatikai és fizikai biztonsági faktorokat is arányosan másképpen kezel velük kapcsolatban.

A tanúsítványok felhasználásának joghatásairól *a minősített hitelesítésszolgáltatására vonatkozó* ***Általános Szerződési Feltételek*** (ÁSzF) című dokumentum előírásai is rendelkeznek, amely megtalálható a http://www.eszigno.matav.hu internetcímen.

1.1.7 Biztonságos aláírás-létrehozó eszköz szolgáltatás

A *Szolgáltató* – a hitelesítésszolgáltatás keretében – nyilvános körben kibocsátott, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő, minősített tanúsítványtípust [**MTT+BALE**][6] kezel[7]. Ehhez a *Szolgáltató* alapvetően kétféle biztonságos aláírás-létrehozó eszközt alkalmaz:

- a **saját** biztonságos aláírás-létrehozó eszközét[8], melyet a *minősített tanúsítványok* aláírására és a *magánkulcsainak* tárolására használ és
- az **előfizetők** biztonságos aláírás-létrehozó eszközeit[9], melyeket a *biztonságos aláírás-létrehozó eszköz* szolgáltatás keretében kezel.

A biztonságos aláírás-létrehozó eszköz szolgáltatás (vagy teljes néven: **biztonságos aláírás-létrehozó adat elhelyezése a biztonságos aláírás-létrehozó eszközön szolgáltatás**) keretében a Szolgáltató *aláírás-létrehozó adat*ot (magánkulcsot) juttat el *biztonságos aláírás-létrehozó eszköz*ön az igénylő (*előfizető*, *aláíró*) számára. Az egyediséget biztosító megszemélyesítési folyamat két részből áll:

- a biztonságos aláírás-létrehozó eszköz **fizikai megszemélyesítése** (a *Szolgáltató* arculati elemeinek elhelyezése az eszközön) és
- a biztonságos aláírás-létrehozó eszköz **logikai megszemélyesítése** (tanúsítványok és magánkulcs[10] elhelyezése az eszközön).

A biztonságos aláírás-létrehozó eszköz szolgáltatás alapvetően három (biztonsági megoldások szempontjából elkülöníthető) folyamatot foglalhat magában:

---

[6] Nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványtípus

[7] Egy tárgyalt tevékenység (szolgáltatás) sokrétű, összetett folyamatait (beszerzés, létrehozás, átalakítás, szétosztás, nyilvántartás stb.) összefoglalóan „kezelés”-nek hívjuk ebben a dokumentumban.

[8] Ez egy kriptográfiai hardver modul.

[9] Ezek intelligens kártyák.

[10] A jogszabályok ezt a szolgáltatást „aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése” néven nevezik.

(1) a biztonságos aláírás-létrehozó eszköz **beszerzése és előkészítése** a felhasználó számára (opció),

(2) az aláíró **kulcspár előállításának kiváltása** az *aláírás-létrehozó eszköz*ön és

(3) a biztonságos aláírás-létrehozó eszköz (megfelelően biztonságos módon történő) **eljuttatása** a regisztrált aláíróhoz.

1.1.8 Időbélyegzés-szolgáltatás

A hiteles időadathoz kétféle tevékenység köthető:

- **időjel ellátás**, amelyet a *Szolgáltató* a belső és külső ügyfelei részére egyaránt biztosít azért, hogy azok hitelesített időforráshoz szinkronizálhassák a rendszereiket[11] és
- **időbélyegzés-szolgáltatás**, amellyel a *Szolgáltató* minősített időbélyegzés-szolgáltatásként (előfizetéses alapon) támogatja a külső ügyfeleit.

Az időbélyegek használata során ***kétféle alapműveletet*** kell elvégezni:

- **időbélyegzést** (folyamatot), amely az adatokat időértékekkel kapcsolja össze kriptográfiai eszközök segítségével és
- **időbélyeg-ellenőrzést** (folyamatot), amely kiértékeli ezeknek az összekötéseknek a megfelelőségét.

Az időbélyegzéshez használt kulcspárhoz tartozó tanúsítvány kiállítása a *Hitelesítő Szervezet* feladata.

Az időbélyegzés-szolgáltatás során a *Szolgáltató* (bizonyíthatóan) nem ismeri meg az időbélyegzett dokumentum tartalmát, és csak az abból képzett lenyomatot kezeli.

A *Szolgáltató* időbélyegző infrastruktúrája pontosság és biztonság tekintetében **megfelel** a *Nemzeti Hírközlési Hatóság* (röviden: NHH, a továbbiakban: *Hatóság*) vonatkozó előírásainak.

[11] Mivel a tanúsítványok kibocsátása és azok menedzselése időhöz kötött tevékenység, ezért biztosítani kell a hiteles időadatot a Szolgáltató megbízható rendszereinek szinkronizálásához is.

A *Szolgáltató* két fázisban fejleszti ki az időbélyegzés-szolgáltatást:

- első fázisban csak a *nagy forgalmú ügyfelek* részére szolgáltat[12],
- második fázisban az előzőt kiterjeszti a lehető *legszélesebb felhasználói kör*re.

1.2 Azonosítás

A Szabályzat azonosítása

A dokumentum teljes neve ***A Matáv Minősített e-Szignó® hitelesítésszolgáltatás és Időbélyegzés-szolgáltatás Szolgáltatási Szabályzata***, röviden: *mHSzSz*. A *Szabályzat* az alábbi adatokkal azonosítható[13]:

Egyedi objektum-azonosító (OID): ..... a *Szabályzat* fedőlapján található

Regisztrációs szám: ..... a *Szabályzat* fedőlapján található

Verziószám: ..... a *Szabályzat* fedőlapján található

A **hatályba lépés dátuma**[14]:..... a *Szabályzat* fedőlapján található

A szolgáltatások védett **márkaneve**:..... *Matáv e-Szignó®*

A *PKI-alkalmazás* **technikai azonosítója**: *Matáv e-Szignó® QCA v1.0.*

Az *időbélyegző-alkalmazás* **technikai azonosítója**: *Matáv e-Szignó ® TSA v1.0.*

A Szabályzat hivatalos és aktuális verziója a Szolgáltató elektronikus aláírásával ellátva, megtalálható és letölthető a *Szolgáltató* internetes honlapjának következő oldalairól:

http://www.eszigno.matav.hu

A tanúsítványtípus azonosítása

[12] Ez bizonyos technikai korlátozásokat jelent, például megkövetelheti a *bérelt vonali* kommunikációs csatornák vagy egyéb egyedi megoldásokhasználatát.

[13] A 16/2001. (IX. 1.) MeHVM rendelet 1. számú melléklet a)-e) pontjait

[14] A *Szabályzat* aktuális verziójára vonatkozik.

A Szabályzat a következő tanúsítványtípusra vonatkozik:

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

A [14] dokumentum további adatokat tartalmaz a tanúsítványtípusra vonatkozóan.

A *Szolgáltató* minősített szolgáltatókénti nyilvántartásba vételének napja: 2004. október 01.

1.3 Közösség és alkalmazhatóság

A *Szolgáltató* -szolgáltatásaihoz (tanúsítvány-szolgáltatás, időbélyegzés-szolgáltatás és biztonságos aláírás-létrehozó eszköz-szolgáltatás) tartozó közösség (a továbbiakban: **Közösség**) az alábbiakból áll:

- a *Matáv e-Szignó® Minősített Hitelesítésszolgáltatás* szervezetei (ezen belül regisztrációs és hitelesítő szervezet),
- a *Matáv Termék- és Megoldásmenedzsment szervezet, Termékmenedzsment osztálya* (mint a hitelesítés-szabályozásért felelős szervezet a továbbiakban: TM),
- a *végfelhasználók* (előfizető, aláíró és érintett fél).

A Szabályzat keretei között végzett szolgáltatói tevékenységekért a *Matáv Rt.* a felelős {ld. még a **2.1** és **2.2** alfejezeteket}.

1.3.1 Hitelesítő szervezet

A *Szolgáltató* – a saját szervezetén belül – hitelesítő szervezetet (teljes név: *Matáv e-Szignó® Minősített Hitelesítésszolgáltatás Hitelesítő Szervezete*, és ebben a dokumentumban *Hitelesítő Szervezet* vagy **HSz**) működtet, melynek feladata a tanúsítványok központi előállítása és menedzsmentje (a *Regisztrációs Szervezet*től {**RSz**} kapott kérelmeknek megfelelően, a hitelesítés-szabályozásért felelős szervezet, a *Matáv SKH* által meghatározott eljárások szerint), valamint az időbélyegzés és az aláírás-létrehozó eszköz szolgáltatások nyújtása.

A minősített tanúsítványok kibocsátását végző *Hitelesítő Szervezet* a következő **hitelesítő egységekből** áll:

- *Gyökér Hitelesítő Egység* (önhitelesített) és
- *Felhasználói Hitelesítő Egység* (amelyet a Gyökér Hitelesítő Egység hitelesít).

A *Szolgáltató* a **végfelhasználói minősített tanúsítványfajta** kibocsátását, továbbá az időbélyegzés szolgáltatását a Szabályzat és más kapcsolódó szabályzatok előírásainak megfelelően végzi (lásd a http://www.eszigno.matav.hu internetoldalak).

A *Gyökér Hitelesítő Egység* tanúsítványának lenyomata: 691D 25F1 298B 8ECC EF4E FC77 04CE D79F BDCA AE2D

Ezt a lenyomatot a Matáv Rt. hivatalos formában a Magyar Hírlapban teszi közzé {ld. még a **2.6.1** alfejezetet}.

1.3.2 Regisztrációs szervezet

A *Szolgáltató* – a saját szervezetén belül – egyszintű **regisztrációs szervezetet** (teljes neve: *Matáv e-Szignó® Minősített Hitelesítésszolgáltatás Regisztrációs Szervezete*, ebben a dokumentumban *Regisztrációs Szervezet* vagy **RSz**) működtet, melyek feladatai az alábbiak:

- a ***végfelhasználói minősített tanúsítványok*** alanyainak kezdeti regisztrációja,
- a tanúsítványok kibocsátásához kapcsolódó adminisztrációs és regisztrációs tevékenység,
- ügyfélszolgálati teendők: a felhasználókkal való kapcsolattartás és további tanúsítványmenedzsment feladatok ellátása,
- visszavonási nyilvántartásokkal kapcsolatos adminisztrációs és regisztrációs tevékenység.

A Regisztrációs Szervezet a feladatait a Szabályzat előírásainak megfelelően végzi. Az aktuális ügyek kezelését távolról az interneten és telefonon keresztül, illetve (az ügyfélszolgálaton) személyes közreműködéssel látja el.

A *Szolgáltató* a későbbiekben egyéb szervezetekkel is szerződést köthet a **regisztráció** elvégzésére.

A *Szolgáltató* külföldön nem tart fenn regisztráló, képviseleti vagy ügyfélszolgálati irodákat.

1.3.3 A hitelesítés-szabályozási szervezet

A *Szolgáltató* –szervezetén belül – hitelesítés-szabályozási szervezetet működtet (ebben a dokumentumban *Szabályozási Egység* vagy **SzE**)-, amely a Szolgáltató tevékenységéhez elengedhetetlen szabályozási feladatokat látja el, beleértve a szabályzatok elkészítésével, harmonizálásával, kiegészítésével, aktualizálásával stb., azaz kezelésével kapcsolatos **összes feladatot**.

1.3.4 Végfelhasználók

A *Szolgáltató* által nyújtott szolgáltatások végfelhasználói az alábbiak lehetnek {ld. **10 *Jelölések és meghatározások***}:

- az *előfizető*, aki a kibocsátott tanúsítvány és az ehhez tartozó kulcspár tulajdonosa,
- az *aláíró*, aki a kibocsátott tanúsítványhoz tartozó kulcspár teljes jogú, kizárólagos használója és
- az *érintett fél.*

Az *aláíró* csak természetes személy lehet, aki a tanúsítványban foglalt (nyilvános kulcsnak megfelelő) **magánkulcsot** aláírásra **felhasználja**.

Az **előfizető** olyan tetszőleges természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet lehet, aki/amely elfogadja a Szolgáltató szabályzataiban (különösképpen jelen Szabályzat **2.1.4** alfejezetében {„A szabályozó szervezet kötelezettségei”}) meghatározott kötelezettségeket, és aki fizet a szolgáltatásért.

Az előfizető és aláíró szerződéses viszonyban áll a *Szolgáltatóval* a vonatkozó Szolgáltatói Szerződésben (**SzSz**)[15], Általános Szerződési Feltételekben (**ÁSzF**)[16], Minősített Tanúsítványtípus Szabályzat (**mTT**)[17] dokumentumban és a Minősített HitelesítésSzolgáltatási Szabályzatban (**mHSzSz**) – utóbbi a jelen dokumentum – foglaltak szerint. A *Szolgáltató* az aláíróval és előfizetővel elsősorban a *Regisztrációs Szervezet*en keresztül tart kapcsolatot.

[15] ld. a [16] dokumentumot

[16] ld. a [15] dokumentumot

[17] ld. a [14] dokumentumot

A Szolgáltató szabályzatai csak a tanúsítványfajták meghatározásával korlátozzák az *aláírók* és *előfizető*k körét, a *Szolgáltató* szerződéses feltételeinek teljesítésével, a szabályzatokban leírt jellemzőknek megfelelve bárki lehet *aláíró*, illetve *előfizető*.

Az **érintett fél** (Szolgáltatóval szerződéses viszonyban nem álló harmadik személy) a Közösség olyan tagja, aki az elektronikus dokumentum fogadója és a *Szolgáltató* által kibocsátott (tanúsítvánnyal megerősített) elektronikus aláírásra, illetve egy hitelesített időpontra hagyatkozva jár el az aláírás és/vagy az időbélyeg hitelességének ellenőrzésekor.

Az *érintett fél* természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet lehet, és a *Szolgáltató*val nem áll szerződéses viszonyban. Az *érintett fél* tevékenységére vonatkozó ajánlásokat a Szabályzat és az abban megnevezett egyéb szabályzatok tartalmazzák.

Az *érintett fél* elfogadja a Szabályzat **2.1.7** alfejezetében szereplő ajánlásokat. A *Szolgáltató* az *érintett fél*lel elsősorban a címtáron keresztül tart kapcsolatot. A *Szolgáltató* szabályzatai semmilyen formában sem korlátozzák az *érintett fel*ek körét.

Az *aláíró* és (vagy) az *előfizető* érdeke annak mérlegelése, hogy **milyen tanúsítványt alkalmaz** egy adott célra. Az *érintett fél*nek is mérlegelési joga és felelőssége, hogy meghatározza, **milyen tanúsítványt fogad el** egy adott célra, ezért fontos, hogy a *Szolgáltató* által karbantartott publikus nyilvántartásokat és szabályzatokat ismerje és az aktualitást ellenőrizze.

1.3.5 Alkalmazhatóság

A Szabályzat érvényességi körében kibocsátott minősített tanúsítványok olyan **elektronikus aláírások igazolására** használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon kielégítik, ahogy egy kézírásos aláírás kielégíti ugyanazt a követelményt a papír-alapú adatok vonatkozásában.

Engedélyezett alkalmazási lehetőségek

A kibocsátott végfelhasználói tanúsítványok magánkulcsai az elektronikus dokumentumokkal kapcsolatos elektronikus aláírások megtételére, a tanúsítványokban található nyilvános kulcsok (melybe más nyilvános kulcs nem értendő bele) az elektronikus aláírások ellenőrzésére használhatók fel a tanúsítványba foglaltaknak megfelelően.

Korlátozott alkalmazási lehetőségek

A *Szolgáltató* a szabályzataiban szereplő feltételekkel korlátozza a kibocsátott tanúsítványok felhasználhatóságát a pénzügyi tranzakciós limit vagy az egyéb vonatkozásokban. A kibocsátott végfelhasználói tanúsítványokra vonatkozó korlátozásokat az **1.1.6** ***Tanúsítványfajták***, illetve a **7** ***Tanúsítvány-, CRL- és időbélyeg-profilok*** alfejezetek ismertetik ebben a dokumentumban. A *Szolgáltató* egyéb módon nem korlátozza a kibocsátott végfelhasználói tanúsítványok felhasználhatóságát. Az ***előfizető*** élhet korlátozásokkal az *aláíró* és az *érintett felek* tanúsítvány felhasználási tevékenységével kapcsolatosan.

Tiltott alkalmazási lehetőségek

A tanúsítványtípusnak megfelelő korlátozások megtalálhatók a [14] Tanúsítványtípus Szabályzat dokumentumban.

1.4 Kapcsolattartás

Szolgáltató

A *Szolgáltató* (Matáv Rt.) elérési adatai a következők:

Név: Matáv Rt. Magyar Távközlési Részvénytársaság
Cégjegyzékszám: CG 01-10041928
Székhely: 1013 Budapest, Krisztina krt. 55.
Postacím: 1541 Budapest
Telefon: +36-1-458 0000
Fax: +36-1-458 7176
Honlap: www.matav.hu

Regisztrációs szervezet

A *Regisztrációs Szervezet* elérési adatai a következők:

Név: Matáv Üzleti Megoldások Üzletág, Termék- és Megoldásmenedzsment szervezet, Megoldásmenedzsment osztály, Helpdesk csoport

Cím: 1122 Budapest Maros u. 32.

Telefon: +36-80-20-44-51

Fax: +36-1-458-0215

Postacím: 1541 Budapest

Honlap: http://www.eszigno.matav.hu

E-levélcím:eszigno_help@ln.matav.hu

A *Regisztrációs Szervezet* általában munkanapokon **8 és 16 óra között** tart nyitva, de egyes napokon ettől eltérő nyitvatartási időpont is lehetséges. A visszavonással kapcsolatos regisztrációs és adminisztrációs szolgáltatás folyamatosan – **0 és 24 óra között** – elérhető az alábbi telefon ill. faxszámon:

24 órás ügyelet telefonszáma: +36-80-204-165

24 órás ügyelet e-mail címe: bzh@ln.matav.hu

A *Regisztrációs Szervezet* aktuális adatai a *Szolgáltató* fenti internetes honlapján megtekinthetők.

Megjegyzés: a minősített Hitelesítésszolgáltatásnak a Regisztrációs Szervezete eltér a Matáv Fokozott Hitelesítésszolgáltatás Regisztrációs Szervezetétől.

Hitelesítő Szervezet

A *Hitelesítő Szervezet* elérése a Regisztrációs Szervezeten keresztül történik.

Szabályzó szervezet

A *Szabályozási Egység* adatai a következők:

Név: Matáv Üzleti Megoldások Üzletág, Termék- és Megoldásmenedzsment szervezet (jelen dokumentumban: Szabályozó Egység: SZe)

Cím: 1013 Budapest, Krisztina krt. 55.

Telefon: +36-1-457-4137

Fax: +36-1-458-0755
Postacím: 1541 Budapest

Ügyfélszolgálat

A szolgáltatással kapcsolatos kérdéseikkel, problémákkal a végfelhasználók rendszerint a Regisztrációs Szervezethez fordulnak szóban vagy írásban.

Illetékes fogyasztóvédelmi felügyelőség

A *Szabályzat* szerinti szolgáltatással kapcsolatban illetékes fogyasztóvédelmi felügyelőség adatai a következők:

Név: *Budapest Főváros Közigazgatási Hivatal Fogyasztóvédelmi Felügyelőség*
Cím: 1088 Budapest, József krt. 6.
Postacím: 1364 Budapest, Pf. 234
Telefon: +36-1-4594-918
Fax: +36-1-4594-870

2. Általános rendelkezések

A Szabályzat hatálya alá eső teljes **Közösség** {ld. **1.3** ***Közösség és alkalmazhatóság***} kötelezettségeit és felelősségeit, illetve az érintett félre vonatkozó ajánlásokat a vonatkozó Szolgáltatói Szerződés (**SzSz**)[18], az Általános Szerződési Feltételek (**ÁSzF**)[19], a vonatkozó Tanúsítványtípus Szabályzat[20] és a jelen hitelesítésszolgáltatási szabályzat tartalmazzák.

2.1 Kötelezettségek

A *Szolgáltató* elsődleges feladata a *Hitelesítő Szervezet*, a *Regisztrációs Szervezet* és a címtár működtetése. A *Szolgáltató*nak szolgáltatásait a hatályos jogi szabályozással, szolgáltatási szabályzatával és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban kell nyújtania.

2.1.1 Szolgáltató általános kötelezettségei

A *Szolgáltató* alapvető kötelezettsége, hogy vállalt szolgáltatásait a jelen és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a vállalati és biztonsági belső szabályzatokkal összhangban nyújtsa; ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. **keretek megteremtése**,
- **magas színvonalú** és **biztonságos** szolgáltatások {ld. **1.1.4** ***Szolgáltatások***} nyújtása a vonatkozó **szabályzatok szerint**,
- a hitelesítés-szolgáltató **szervezetek** (hitelesítő-, regisztrációs- és szabályozó-szervezetek, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése,
- a szabályzatokban előírt **eljárások betartása**, és az esetleg bekövetkező helytelen működés megszüntetése

[18] ld. a [16] hivatkozást

[19] ld. a [15] hivatkozást

[20] ld. a [14] hivatkozást

- a szolgáltatások biztosítása minden olyan **igénylő számára**, aki elfogadja a szabályzatokban rögzített feltételeket,
- a jogszabály szerinti **publikus nyilvántartások** és előírt saját szabályzatok karbantartása (pl. a **Címtár** aktualizált működtetése) és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

A **Szolgáltató** általános kötelezettségeit a [14] Tanúsítványtípus Szabályzat dokumentum részletesen tartalmazza.

2.1.2 A Hitelesítő Szervezet kötelezettségei

A *Hitelesítő Szervezet* alapvető feladata a *Szolgáltató* hitelesítő egységeinek (a Gyökér Hitelesítő Egység és a Felhasználói Hitelesítő Egység) felállítása és működtetése, valamint az időbélyegzés és biztonságos aláírás-létrehozó eszköz szolgáltatás nyújtása.

A hitelesítő egységek belső működtetését szolgáltatói operatív szabályzatok határozzák meg. A hitelesítő egységek által kibocsátott ***szolgáltatói tanúsítványok*** (regisztrációs egységek, ügyintézők stb. felé) kezelése az operatív szabályzatok előírásainak megfelelően kell, hogy történjen.

Ez a szabályzat csak a ***végfelhasználói tanúsítványokkal*** kapcsolatban tartalmaz előírásokat.

A **Hitelesítő Szervezet** kötelezettségeit a [14] Tanúsítványtípus Szabályzat dokumentum részletesen tartalmazza.

2.1.3 A Regisztrációs Szervezet kötelezettségei

A *Regisztrációs Szervezet* alapvető kötelezettsége a *Szolgáltató* képviselete a szolgáltatások kapcsán a végfelhasználónál, amelyhez az alábbi főbb feladatok tartoznak:

- a hitelesítésszolgáltatás**ok értékesítésében történő közreműködés**,
- az **ügyféladatok** (az előfizető és az aláíró adatainak) kezelése (beleértve a valódiság ellenőrzését is), azaz *regisztrációs szolgáltatás*,

- a **tanúsítvány-kérelmek** intézése, továbbá a tanúsítvány-felfüggesztés és -*visszavonás kezelés*e (felfüggesztés, visszavonás),
- a tanúsítványok **nyilvántartásba vétele**, elbírálása, továbbítása, ,
- közreműködés a visszavonási állapot **közzétételében** (a címtár-szolgáltatásban),

A *Regisztrációs Szervezet* kötelezettségeit a [14] **tanúsítványtípus dokumentum** részletesen tartalmazza.

2.1.4 A szabályozó szervezet kötelezettségei

Szabályozási Egység főbb kötelezettségei az alábbiak:

- az alkalmazott tanúsítványfajták {ld. **1.1.6** ***Tanúsítványfajták***} specifikálása, jóváhagyása és karbantartása,
- a hitelesítésszolgáltatási nyilvános szabályzatainak és a vonatkozó belső (nem nyilvános) előírásoknak előkészítése, egyeztetése jogszabályokkal és a belső (nem nyilvános) Matáv-szabályzatokkal, továbbá az aktualizálások elvégzése,
- a hitelesítésszolgáltatási szabályzatokkal kapcsolatos észrevételek rögzítése és javaslatok elbírálása,
- a szolgáltatási eljárások és ügyviteli folyamatok szabályzatok szerint ellenőrzése.

2.1.5 Az Ügyfélszolgálat kötelezettségei

Az Ügyfélszolgálat ügyfélkapcsolati információs tevékenység nyújt az *igénylő*k (előfizetők, aláírók), az *érintett fel*ek részére a

- *regisztrációs* szolgáltatás,
- *visszavonás-kezelés* szolgáltatás,
- *tanúsítvány-előállítás* szolgáltatás,
- *biztonságos aláírás-létrehozó eszköz szolgáltatás* és
- *időbélyegzés-szolgáltatás* területén.

2.1.6 Az aláíró és előfizető kötelezettségei

Az *előfizető*nek és az *aláíró*nak kötelessége a *Szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatások felhasználása során, beleértve a tanúsítvány és magánkulcs igénylését és alkalmazását.

A kötelezettségek értelemszerűen alkalmazandók a tanúsítvány és a kulcs érvényességi időszaka alatt, és ha szükséges azt követően is.

Az *előfizető* és *az aláíró* kötelezettségeit a [14] **Tanúsítványtípus Szabályzat dokumentum** külön-külön részletezi.

2.1.7 Az érintett félre vonatkozó ajánlások

Az *érintett fél* a *Szolgáltató* szabályzatainak megfelelően járjon el a szolgáltatások igénybevétele során. A tanúsítványok érvényességének ellenőrzése kapcsán ez különösen így van, kiegészítve a lehető legnagyobb gondosság és körültekintés követelményével, amely az összes rendelkezésre álló információ alapján történő ésszerű mérlegelést jelenti[21].

A tanúsítványra vonatkozó ellenőrzéseket *érintett fél*nek ajánlott elvégeznie a teljes tanúsítási láncra vonatkozóan. Ha a tanúsítvánnyal kapcsolatos tranzakció[22], a tanúsítvány vagy a tanúsítási lánc tanúsítványainak valamely adata a művelet érvénytelenségére utal, illetve ha az adott kontextusban nem elfogadható, akkor a tranzakciót és a tanúsítvány elfogadását az *érintett fél*nek vissza kell utasítania.

Az *érintett* félre vonatkozó ajánlásokat a [14] **Tanúsítványtípus Szabályzat dokumentum** részletesen tartalmazza.

2.1.8 A címtárra vonatkozó kötelezettségek

A *címtár - a hitelesítő szervezet részeként* - feladata tanúsítványok és tanúsítvány visszavonási listák és szabályzatok minden *érintett fél* által elérhető módon történő közzététele {ld. a **2.6.4** sz. alfejezetet).

[21] Ez nem csak a *Szolgáltató*tól származó információkat jelenti, hanem a rendelkezésre álló összes óvintézkedés foganatosítását is.

Az erre vontakozó kötelezettségeket a [14] **Tanúsítványtípus Szabályzat dokumentum** tartalmazza.

2.2 Felelősség

2.2.1 A Szolgáltató általános felelőssége

a) A *Szolgáltató* felelősséget vállal az általa támogatott Tanúsítványtípus Sazbályzatokban leírt eljárásoknak való megfelelőségért, még abban az esetben is, amikor a Szolgáltató egyes tevékenységeit alvállalkozók végzik[23].

b) A *Szolgáltató* a vele szerződéses jogviszonyban álló felekkel (ilyen az *aláíró* és az *előfizető*) szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésszegésért való felelősség szabályai szerint felelős.

c) A *Szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik féllel (ilyen az *érintett fél*) szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésen kívüli károkozásról szóló szabályai (Ptk. 339. §) szerint felelős.

d) A *Szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az előfizetővel / aláíróval megkötött szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet {ld. később „***Pénzügyi felelősség korlátozása***"}. Felelősség korlátozása

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

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

---

[22] Például egy bizonyos típusú elektronikus aláírás.

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

Pénzügyi felelősség korlátozása

A *Szolgáltató* a kártérítés felső határát tanúsítványonként és összességében is (az összes tanúsítvánnyal és káreseménnyel kapcsolatban) korlátozza. A *Szolgáltató* pénzügyi felelősségével kapcsolatos további részleteket az **ÁSzF** dokumentum tartalmazza.

2.2.2 A Hitelesítő Szervezet felelőssége

a) A *Hitelesítő Szervezet* **felelős**:
   - az általa kibocsátott tanúsítványok hitelességéért,
   - az általa kibocsátott szabályzatokért, azok jogszabályi megfelelőségéért és betartásáért,
   - a generált **kulcspárok megfelelőségéért**, a magánkulcs-nyilvános kulcs és tanúsítvány összetartozásáért,
   - a biztonságos aláírás-létrehozó eszközt aktivizáló kód és az eszközre töltött **kulcsok összetartozásáért**,
   - általában a kötelezettségei betartásáért.

b) A *Hitelesítő Szervezet* **nem felelős**:
   - az *előfizető*k és *aláírók* magánkulccsal, illetve aláírás-létrehozó eszközzel kapcsolatos tevékenységeiért,
   - az *érintett fel*ek tanúsítvány ellenőrzési és felhasználási tevékenységeiért,
   - az *előfizető*k, *érintett fel*ek, és mások által kibocsátott szabályzatokért.

2.2.3 A Regisztrációs Szervezet felelőssége

A *Regisztrációs Szervezet* felelős:
   - az *aláírók* és *előfizető*k személyes és szervezeti **azonosságának megállapításáért**,
   - a felvett **regisztrációs adatok valódiságáért**,

- a hitelesítésszolgáltatás igénybevevőjének tájékoztatásáért a *Szabályzat* tartalmáról és elérhetőségéről a *Szolgáltatói Szerződés* megkötését megelőzően,
- általában kötelezettségei betartásáért.

2.2.4 Az aláíró felelőssége

Az *aláíró* felelős:

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

2.2.5 Az előfizető felelőssége

Az *előfizető* felelős:

- a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért,
- az adatokban bekövetkezett változások haladéktalan bejelentéséért,
- a Szolgáltatási Szerződés betartásáért,
- a számára kibocsátott tanúsítványok és az ehhez tartozó kulcspár tulajdonosi kötelezettségeiért,
- a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása vitás ügyekben,

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

2.2.6 Az érintett fél felelőssége

a) Az *érintett fél* felelős:
   - a tanúsítványok elfogadása során tanúsított körültekintő eljárásért,
   - általában a kötelezettségei betartásáért.

b) Az *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, az aláírás szabályzat, illetve a hatályos jogszabályok szerint jár el.

2.3 Bankgaranciák, felelősségbiztosítás

A *Szolgáltató* pénzügyi felelőssége, valamint a megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében **25.000.000** Ft (huszonöt-millió forint) feltétel nélküli és visszavonhatatlan **bankgaranciával** rendelkezik..[24]

A *Szolgáltató* ezen felül, a megbízhatóság biztosítása érdekében teljes körű felelősségbiztosítással is rendelkezik az OTP Garancia Biztosító Rt-nél. A felelősségbiztosítási szerződés kiterjed a *Szolgáltató* által a szolgáltatások nyújtásával összefüggésben okozott valamennyi kárra. A **biztosítás** egy biztosítási esemény vonatkozásában káreseményenként **50.000.000** Ft (ötvenmillió forint)[25], összességében **évente 240.000.000** Ft (kétszáznegyvenmillió forint) összegig **fedezetet** biztosít az összes károsultnak okozott károkra. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

[24] ld. [3] 8-11. §

[25] ld. a [3] 15. § (3)

A felelősségbiztosítás egy biztosítási áresemény vonatkozásában **50.000.000** Ft (ötvenmillió forint) összegig fedezetet nyújt a károsultnak a *Szolgáltató* károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták. Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.[26]

2.3.1 A hitelesítés szolgáltatóval szembeni kártérítés

Az *előfizető*k, *aláírók* és *érintett fel*ek kártérítési felelősséggel tartoznak a *Szolgáltató*val szemben azokért a veszteségekért és károkért, melyeket kötelezettségeik be nem tartásával okoznak számára.

2.3.2 Adminisztratív folyamatok

A *Szolgáltató* a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) a naplóadatokat {ld. még a [14] hivatkozás szerinti Tanúsítványtípus Szabályzat dokumentum **4.5** és **4.6** alfejezeteit}.

2.4 Értelmezés és érvényesítés

2.4.1 Irányadó jog

A *Szolgáltató* tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A *Szolgáltató* szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

A hatályos jogszabályokat lásd a **Tanúsítványtípus Szabályzatban**.

[26] ld. [3] 15. §

2.4.2 Érvénytelenség, fennmaradás, megszűnés és értesítések

Érvénytelenség

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

Fennmaradás

A Szabályzat 2. fejezete érvényben marad a Szabályzat hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, melyet a *Szolgáltató* a Szabályzat hatálya alatt bocsátott ki.

Megszűnés

A Szabályzat a Közösség valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A Szabályzat egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében, beleértve a *Szolgáltató* és más szervezet jövőbeli esetleges összeolvadásának esetét is. A Szabályzat csak írott és hitelesített formában módosítható, a *Hatóság* által vezetett szabályzat-nyilvántartásban való átvezetés mellett.

Értesítések

Az előfizető és aláíró jognyilatkozatait hitelesítés szolgáltató felé, kizárólag írásban, hivatalosan aláírt módon teheti meg. Az előfizető és az aláíró egyéb esetekben a hitelesítés szolgáltatót írásban, elektronikus levél vagy fax formájában is értesítheti. A hitelesítés-szolgáltató értesítési címei a szolgáltatási szabályzat 1.4 alfejezetben találhatóak.

A hitelesítés szolgáltató ügyfeleit a honlapján történő közzététel útján vagy elektronikus levélben tájékoztathatja.

2.4.3 Vitás kérdések megoldására vonatkozó eljárások

A szolgáltatással kapcsolatos bármely vitás kérdés vagy panasz felmerülése esetén a vita jogi útra terelése előtt az *aláíró*nak és az *előfizető*nek kötelessége a *Szolgáltató* haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően. A felek vitáikat mindenkor megkísérlik békés, tárgyalásos úton rendezni.

A *Szolgáltató* (beleértve a *Regisztrációs Szervezet*et is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az 1.4 Kapcsolattartás fejezetben rögzített elérhetőségeken lehet megtenni.

A *Szolgáltató* az érkeztetést követő egy munkanapon **belül** (a megjelölt címen) értesíti a panaszos felet a panasz kézhezvételéről az ügy kivizsgálásához szükséges idő megjelölésével. A jelzett időn belül, mely nem lehet több mint **10 munkanap**, a *Szolgáltató* írásban válaszol a bejelentőnek. Ha a választ bejelentő nem fogadja el, egyeztetést kell kezdeményeznie a *Szolgáltató*val. Ha a *Szolgáltató* ezt megtagadja, vagy ha a felek közötti egyeztetés annak megkezdésétől számított **20 munkanapon belül** nem vezetne eredményre, akkor a bejelentő peres útra terelheti az ügyet. Ez esetben felek kölcsönösen alávetik magukat a *Kereskedelmi és Iparkamara* mellett működő választott bíróság kizárólagos illetékességének.

2.5 Díjak

A *Szolgáltató* meghirdetett díjait előzetes értesítés nélkül bármikor módosíthatja. Mindazonáltal, a tanúsítvány kezelésének költségei a tanúsítvány érvényességének teljes időtartama alatt érvényesek, a tanúsítvány kibocsátásának idején érvényes árlista szerint. Bármilyen költség számlázására csak közvetlenül a *Szolgáltató* jogosult.

2.5.1 Aláírás hitelesítésszolgáltatásához kapcsolódó díjak

A *Szolgáltató* a vonatkozó szolgáltatási szerződés szerint kibocsátott tanúsítványokért az ÁSZF-ben megjelölt díjelemekből álló díjat számol fel az előfizető felé.

2.5.2 Időbélyegzés szolgáltatási díjak

A *Szolgáltató* az időbélyegzés szolgáltatásért **díjat számol fel** a vonatkozó Szolgáltatói Szerződésben (**SzSz**) foglaltak szerint.

2.5.3 A biztonságos aláírás-létrehozó eszköz szolgáltatás díja

A *Szolgáltató* a vonatkozó szolgáltatási szerződés szerint átadott és megszemélyesített eszközökért az ÁSZF-ben megjelölt díjelemekből álló díjat számol fel az előfizető felé.

2.5.4 Tanúsítvány hozzáférési díjak

A *Szolgáltató* a közzétett tanúsítványok eléréséért **nem számol fel** díjat az *érintett fel*ek irányában.

2.5.5 Visszavonási és állapot-információ hozzáférési díjak

A *Szolgáltató* a közzétett visszavonási vagy státus-információ eléréséért **nem számol fel** díjat az *érintett fel*ek irányában.

2.5.6 Egyéb szolgáltatásokra vonatkozó díjak

A *Szolgáltató* a kibocsátott tanúsítványok **visszavonásá**ért, **felfüggesztésé**ért és újra**érvényesítésé**ért eljárási díjat nem számol fel az *előfizető* felé.

Visszatérítési elvek

Az *előfizető* jogosult a számára kibocsátott tanúsítvány éves fenntartási díjának visszatérítésére a következő esetekben:

- a kibocsátott tanúsítvány valamely **adata** nem megfelelő a *Szolgáltató* hibájából fakadóan,
- a kibocsátott **tanúsítvány**, a **magánkulcs** és az **aktivizáló adat** {ld. **10** ***Jelölések és meghatározások***} nem összetartozóak a *Szolgáltató* hibájából fakadóan,

- a kibocsátott *biztonságos aláírás-létrehozó eszköz*ön szereplő **adatok**,[27] hibásak a *Szolgáltató* tevékenysége következtében,
- a kibocsátott **biztonságos aláírás-létrehozó eszköz**, az **aktivizáló adat** és a **kulcsok** nem összetartozóak a *Szolgáltató* hibájából fakadóan,
- az *előfizető* vagy *aláíró* a *Szolgáltató* hibájából fakadó műszaki okok miatt - nem képes felhasználni a kibocsátott **tanúsítványt**,
- az *előfizető* vagy *aláíró* nem képes felhasználni a **biztonságos aláírás-létrehozó eszköz**t a *Szolgáltató* hibájából fakadó műszaki okok miatt.

Az *előfizető*nek kérvényt kell beadnia a *Szolgáltató* részére írásban a díj visszatérítése céljából a tanúsítvány kibocsátását követő **30 naptári napon belül** a regisztrációt végző *Regisztrációs Szervezet*nél. A kérvény pozitív elbírálása esetén a *Szolgáltató* a tanúsítványt díjmentesen visszavonja, és a fenntartási díjat előfizető számára a megjelölt bankszámlaszámra a visszavonástól számított **20 naptári napon belül** visszautalja.

A tanúsítvány kibocsátását követő **30 naptári napon túl** előfizető kizárólag csak a *Szolgáltató* bizonyított szerződés- vagy kötelezettségszegése esetén jogosult a díjak visszafizetésre.

A *Szolgáltató* egyéb esetekben díj-visszafizetésre nem köteles.

2.6 Közzététel és címtár szolgáltatás

2.6.1 A szolgáltatói információ közzététele

Kikötések és feltételek közzététele

A *Szolgáltató* szerződéses feltételeit és szabályzatait elektronikus formában (MS-Word és / vagy Adobe Acrobat formátumokban) hozza nyilvánosságra az internetes honlapjának oldalain.

[27] pl. a kártya fizikai megszemélyesítése nem megfelelő

Elérhetőség: http://www.eszigno.matav.hu.

A dokumentumok korábban érvényben lévő változatai is megtalálhatóak itt az aktuális verziók mellett.. A dokumentumok nyomtatott változatai semmilyen formában sem tekinthető hivatalos példánynak vagy hiteles másolatnak.

Rendkívüli információk közzététele

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

- új szolgáltatás beindítása,
- valamely szolgáltatás tervezett beszüntetése vagy tartós (**24 órát** meghaladó) szüneteltetése,
- tevékenységének befejezése {ld. még **4.9** ***A hitelesítésszolgáltatás leállítása***},
- valamely, általa működtetett hitelesítő egység magánkulcsának kompromittálódása.

Tanúsítványok nyilvánosságra hozatala

A *Szolgáltató* az általa működtetett **hitelesítő egységek tanúsítványá**t a következő módszerekkel teszi közzé:

- A *Gyökér Hitelesítő Egység* (önhitelesített) tanúsítványát egy országos terjesztésű napilapban teszi közzé.
- Az összes *hitelesített* tanúsítványt (gyökér-tanúsítvány, felhasználói- tanúsítvány, az időbélyeg aláíró kulcs tanúsítványát, a tanúsítvány visszavonási listákat) a **Címtárban**, valamint a *Szolgáltató* honlapján keresztül teszi közzé.
- Az *előfizető* részére a végfelhasználói tanúsítvánnyal együtt átadja (lásd ott).

A *Szolgáltató* az általa kibocsátott **végfelhasználói tanúsítvány**okat a következő módszerekkel teszi közzé:

- az *aláíró*nak átadja a biztonságos aláírás-létrehozó eszközön,

- az *érintett fel*ek részére közzéteszi a nyilvános **Címtárban**. A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala

A *Szolgáltató* az általa működtetett *hitelesítő egység*ek tanúsítványával kapcsolatos **állapot-információ**kat a következő módszerekkel teszi közzé:

- A *Gyökér Hitelesítő Egység* tanúsítványának állapotváltozásáról egy országos terjesztésű **napilap**ban tesz közzé hirdetést. A gyökér-tanúsítványok esetében ez az egyetlen módszer tekinthető hivatalos formának.
- A *Felhasználói Hitelesítő Egység* tanúsítványának állapotváltozását a **Címtár**ban hozza nyilvánosságra.

A *Szolgáltató* az általa kibocsátott **végfelhasználói tanúsítvány**okkal kapcsolatos állapot-információkat a következő módszerekkel teszi közzé:

- a **Címtár**ban hozza nyilvánosságra.

A végfelhasználói tanúsítvány visszavonását és felfüggesztését a *Szolgáltató* akkor is nyilvánosságra hozza, ha a tanúsítvány közzétételéhez az *előfizető* nem járult hozzá.

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

2.6.2 A közzététel gyakorisága

Kikötések és feltételek közzétételi gyakorisága

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

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

Rendkívüli információk közzétételi gyakorisága

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

Tanúsítványok nyilvánosságra hozatalának gyakorisága

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

- Az általa működtetett *Gyökér Hitelesítő Egység* tanúsítványát a kibocsátást követő **10 munkanapon belül** teszi közzé.
- Az általa működtetett *Felhasználói Hitelesítő Egység* tanúsítványa a *Címtárban* **24 órán belül**, internetes honlapján pedig **5 munkanapon belül** megjelenik.
- A *Szolgáltató* a végfelhasználói tanúsítványokat a kibocsátást követően, a regisztrációs eljárás részeként, a biztonságos aláírás-létrehozó eszközön átadja az *aláíró* vagy az *előfizető* részére.
- A *Szolgáltató* a végfelhasználói tanúsítványokat a *Címtárban* az előállítást követően **24 órán belül** teszi közzé.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

Szolgáltató az általa működtetett *hitelesítő egység*ek és *aláírók* / *előfizetők* tanúsítványával kapcsolatos állapot-információkat a {**4.4.9** „***A tanúsítvány-visszavonási lista kibocsátási gyakorisága***”} alfejezetben tárgyalt gyakorisággal teszi közzé.

2.6.3 Hozzáférés-ellenőrzések

A *Szolgáltató* által közzétett kikötések és feltételek, rendkívüli információk, tanúsítványok és állapot információk nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közzététel sajátosságainak megfelelően. A tanúsítványok és állapot-információk elérése a megfelelő Tanúsítványtípus Szabályzat és a szolgáltatási szabályzat kikötéseinek és feltételeinek elfogadását jelenti.

A *Szolgáltató* által közölt információkat kizárólag csak a *Szolgáltató* egészítheti ki, törölheti vagy módosíthatja. A *Szolgáltató* különböző védelmi mechanizmusokkal igyekszik megakadályozni az információk jogosulatlan módosítását.

2.6.4 A címtár

A *Szolgáltató* címtára egy X.500-as **címtár**kiszolgáló alkalmazás, ami szabványos **X.500, LDAP** és **HTTP** lekérdezésekkel, érhető el.

A **címtár** elérhetőségét a *Szolgáltató* folyamatosan (az év minden napján, **0-24 óra** között) biztosítja, a karbantartáshoz szükséges idők kivételével. A *Szolgáltató* a tervezett karbantartásokat munkaidőn kívüli időszakokra ütemezi, és ezekről a karbantartás megelőzően **24 órával** értesítést tesz közzé a honlapján.[28]

2.7 A megfelelőség vizsgálata

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

- a *minősített tanúsítványok* aláírására, az időbélyeg előállítására, valamint *magánkulcsainak* tárolására használt kriptográfiai hardver modult (nShield F3 PCI hardver kriptográfiai modul),
- a saját informatikai rendszerén belül, az infrastrukturális és megbízható rerndszervezérlési kulcsok generálására, tárolására és felhasználására alkalmazott intelligens kártyát (CosmopolIC intelligens kártya)
- a **biztonságos aláírás-létrehozó eszközöket**[29], melyeket az *aláírók* számára biztosít (P8WE5032v0G mikrochip-ből, STARCOS SPK 2.3 v7.0 operációs rendszerből, valamint a StarCert digitális aláírás alkalmazásból álló intelligens kártya),
- a végfelhasználói és szolgáltatói minősített tanúsítványok kezeléshez használt **rendszereit és módszereit**.

[28] ld. [3] 14. §

[29] Intelligens kártyák

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

A *Szolgáltató* minősített hitelesítés-szolgáltatóként történő önkéntes minősítési (akkreditációs) eljárásban a nyilvántartásba vétel kezdeményezésének időpontjáig nem volt minősítve.

2.7.1 A megfelelőség-vizsgálat gyakorisága

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

A minősített tanúsítványok kezeléshez használt rendszerek és módszerek tanúsítására hatósági minősítési eljárás keretében kerül sor, s a jogszabályoknak megfelelően legalább ***évente*** átfogó helyszíni ellenőrzéssel jár együtt.[30]

2.7.2 Az átvizsgáló szervezet megnevezése és jellemzői

A kriptográfiai hardver modulok, a saját informatikai rendszerén belül alkalmazott intelligens kártyák és a biztonságos aláírás létrehozó eszközöktanúsítását egy erre feljogosított *tanúsító szervezet* {ld. [1] törvény[31] 24. §} végezte, melynek kijelölésére a [3] rendelet[32] előírásainak megfelelően került sor. Mindhárom tanúsított elektronikus aláírási terméket a Hatóság nyilvántartásba vette.

A minősített tanúsítványok kezeléshez használt rendszerek és módszerek tanúsítására hatósági minősítési eljárás (akkreditáció) keretében, a **Hatóság** által kijelölt szakértők által került sor.

[30] ld. [1] 8, 18, 20. §

[31] 2001. évi XXXV. törvény az elektronikus aláírásról

[32] 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

2.7.3 Az átvizsgáló szervezet és a vizsgált fél kapcsolata

A *Szolgáltató*val kapcsolatban tanúsítást végző szervezetek a *Szolgáltató*tól függetlenek, és befolyástól mentesen végzik tevékenységüket. A vizsgálatot végző szervezet nem rendelkezik tulajdonrésszel vagy érdekeltséggel a *Szolgáltató*t illetően, és *Szolgáltató* nem tulajdonosa közvetlenül vagy közvetve a vizsgálatot végző szervezetnek. A tanúsító szervezet díjazása nem függött a tanúsítás során végzett tevékenységének megállapításaitól.

2.7.4 A vizsgálat által érintett területek

A biztonságos aláírás-létrehozó eszközök tanúsítása az [1] törvény[33] 1. mellékletének való megfelelőség vizsgálatára irányult.

A kriptográfiai hardver modulok tanúsítása a [2] harmadik részének 1. fejezetében maghatározott követelményeknek való megfelelőség vizsgálatára irányul.

A minősített tanúsítványok kezeléshez használt rendszerek és módszerek tanúsítása az [1] törvény 3. mellékletének és a [3] rendelet előírásainak, valamint a *Szolgáltató* saját tanúsítványtípus dokumentumának és egyéb szabályzatainak való megfelelőség vizsgálatára irányul.

2.7.5 Hiányosságok esetén végrehajtandó tevékenységek

A minősítő eljárás, vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a *Szolgáltató* késlekedés nélkül megszünteti a vizsgálatot végző Hatóságtól kapott információ és ajánlások alapján.

2.7.6 Az eredményekről való tájékoztatás

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

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

[33] 2001. évi XXXV. törvény az elektronikus aláírásról

2.8 Bizalmasság

A *Szolgáltató* az *előfizető* és *aláíró* adatait a jogszabályoknak megfelelően kezeli. A *Szolgáltató* **adatkezelési szabályzat**tal rendelkezik, mely a személyes adatok kezelésével kiemelten foglalkozik. A *Szolgáltató* belső (nem nyilvános) iratkezelési szabályzata operatív szinten tárgyalja az adatkezelési szabályzatban megfogalmazott elveket és követelményeket.

Az *előfizető* és *aláíró* a tanúsítvány igénylésével a hozzájárul ahhoz, hogy a személyes adatait a *Szolgáltató* (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A hozzájárulás egyaránt vonatkozik az adatok *aláíró*val és *előfizető*vel való megosztására (ha a két fél különbözik), a törvény által meghatározott és nyilvántartásba vett információk harmadik félhez történő továbbítására a *Szolgáltató* szolgáltatásainak leállítása esetén[34]. A **Szolgáltatási Szerződéshez tartozó tanúsítványigénylő űrlap**on az *előfizető*nek és (vagy) az *aláíró*nak jeleznie kell a tanúsítvány nyilvánosságra hozatalának mellőzését. A *Szolgáltató* az előfizetői adatokat kizárólag csak a hitelesítésszolgáltatással összefüggésben használja fel.

Az **előfizető illetve aláíró tanúsítványban megjelenő adatai**a tanúsítványba foglalva {ld. ***7 Tanúsítvány-, CRL- és időbélyeg-profilok***}, valamint a *Szolgáltató* címtárán keresztül nyilvánosságra kerülnek a nyilvános kulcs tulajdonosának azonosítása céljából, a tanúsítványba nem kerülő adataikat a *Szolgáltató* védett módon tárolja az *előfizető* és az *aláíró* azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

[34] ld. [1] 16. § (2)

A *Szolgáltató* a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi, majd a bizalmasnak számító információkat vissza nem állítható módon megsemmisíti. A *Szolgáltató* a felhasználói adatok megőrzése során gondoskodik az információk **sértetlenség**éről, **bizalmasság**áról és **biztonságos tárolás**áról. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja. A felhasználói adatok papír alapú eredeti példányát és az elektronikus másolatokat a **Matáv Üzleti Inteligencia és Dokumentációs Igazgatóság** (ebben a dokumentumban Adattár) tárolja. A *Szolgáltató* gondoskodik a nem nyilvános információk **bizalmasság**áról és **sértetlenség**éről a felhasználói adatok továbbítása során, továbbá – megbízható rendszerek alkalmazásával és az adatok rendszeres archiválásával – a megfelelő **rendelkezésre állásról**.

2.8.1 Bizalmasan kezelendő információ-típusok

a) A *Szolgáltató* bizalmas információként kezeli az *előfizető* és az *aláíró* minden adatát, kivéve azokat, amelyeket a **2.8.2** alfejezet tárgyal.

b) A *Szolgáltató* a birtokába jutott bizalmas információt a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény rendelkezéseinek megfelelően kezeli, s csak a **2.8.3**-**2.8.7** alfejezetekben említett esetekben és személyek/szervezetek részére fedi fel őket.

c) A *Szolgáltató* bizalmas információként kezeli a következő adatokat és dokumentumokat az előbbieken kívül:

- magánkulcsok és aktivizáló kódok,
- tanúsítványigénylések és szolgáltatási szerződések,
- tranzakciós és napló adatok,
- nem nyilvános szabályzatok,
- minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

2.8.2 Nem bizalmasnak tekintett információ típusok

A *Szolgáltató* nem bizalmas információként kezeli mindazon adatokat, melyet a tanúsítványba belefoglal[35]. Ezek az adatok a Szolgáltatási Szerződéshez kapcsolódó **tanúsítványigénylő űrlap**on egyértelmű jelöléssel szerepelnek.

2.8.3 Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése

A *Szolgáltató* az általa kibocsátott tanúsítványok visszavonását és felfüggesztését a **tanúsítvány-visszavonási listá**ban teszi közzé, a tanúsítvány sorszámának és opcionálisan a visszavonás/felfüggesztés okának a jelölésével. Bővebb információ a **7.2** alfejezetben található.

2.8.4 Információszolgáltatás a hatóságok részére

a) A *Szolgáltató* az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat az [1] törvény[36] 11.§ (2) bekezdése szerinti körben.

b) A *Szolgáltató* rögzíti az a) pontbeli adatátadás tényét, de arról nem tájékoztatja sem az *előfizető*t, sem az *aláíró*t.

2.8.5 Információszolgáltatás polgári eljárás keretében

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

[35] Függetlenül attól, hogy az előfizető hozzájárul-e (az alany nevében) a tanúsítvány nyilvánosságra hozásához.
[36] 2001. évi XXXV. törvény az elektronikus aláírásról

b) A *Szolgáltató* rögzíti az a) pontbeli adatátadás tényét, és arról tájékoztatja az *előfizető*t és az *aláíró*t.

2.8.6 A tulajdonos kérésére történő felfedés

A *Szolgáltató* az *előfizető* vagy *aláíró* hivatalos – írásban adott – felhatalmazása alapján tárja fel a rájuk vonatkozó bizalmas felhasználói információkat *harmadik fél* részére.

2.8.7 Egyéb információ-közzétételt eredményező körülmények

A *Szolgáltató* a nyilvántartásait (a jogszabályban meghatározott bizalmas felhasználói adatokkal együtt) a tevékenysége befejezésekor átadja más – szintén minősített – hitelesítés-szolgáltató részére az [1] törvény[37] 16. § 2. bekezdése szerint.

2.9 Szellemi tulajdonjogok

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

b) A *Szolgáltató* a **tanúsítvány**t a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.

c) A **visszavonási információ** a *Szolgáltató* tulajdonát képezi.

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

e) A tanúsítványban szereplő **megkülönböztető név** használatára a megnevezett *aláíró* jogosult.

f) Az *aláíró* egyedi azonosítójában szereplő bármilyen védjegy, szervezeti- és személynév, egyéb adat az *előfizető* vagy *aláíró* tulajdonát képezi.

[37] 2001. évi XXXV. törvény az elektronikus aláírásról

g) A *Szolgáltató* szabályzatai, szerződéses feltételei *Szolgáltató* tulajdonát képezik.

3. Azonosítás és hitelesítés

3.1 Kezdeti regisztrálás

3.1.1 Név típusok

A tanúsítvány **azonosító mezői** (Kibocsátó és Alany) a [12] szerinti egyedi név formátum előírásainak felelnek meg.

A tanúsítvány-**kibocsátó azonosító**ja (a „*Kibocsátó*” mező tartalma) a következő módon épül fel[38]:

Jelölés	Jelentés	Adat
CN	a tanúsítvány kibocsátását végző szervezet neve (*Common name*)	Matav Minositett CA
O	a szolgáltató szervezet neve (*Organization*)	Matáv Matav
OU	a szolgáltató szervezeti egység neve (*Organizational* unit)	Matav Trust center
C	ország név (*Country*)[39]	HU
L	a szervezet székhelye - városnév (*Locality*)	Budapest

[38] ld. [1] törvény 2. számú melléklet b) pontját

[39] A [5] szabvány szerinti két karakter hosszóságú országkódokat kell alkalmazni.

A tanúsítvány tulajdonosának **azonosító**ja (az „*Alany*” mező tartalma) a következő módon épül fel:

Jelölés	Jelentés	Adat / Kitöltési szabály
CN	az *aláíró* családi- és keresztneve.[40] (*Common name*[41]*)*	A személyazonosító okmányban szereplő adat.
O	az előfizető szervezet hivatalos neve (*Organization*[42])	A szervezet alapító okirata szerint. Gazdasági társaság esetében a cégbejegyzésben szereplő név (rövid alakban) és a szervezet típusa.
OU	az *aláíró* szervezeti egységének neve az *előfizető* szervezetben (*Organizational unit*[43]*)*	A *Tanúsítványigénylő űrlap*nak megfelelően.[44] Opcionális adat
C	az *előfizető* szervezet székhelye szerinti ország (*Country*[45]*)*.	A *Tanúsítványigénylő űrlap*nak megfelelően.
L	az *előfizető* szervezet székhelye szerinti város (*Locality)*	A *Tanúsítványigénylő űrlap*nak megfelelően.
E-mail	az *aláíró* e-levél címe az *előfizető* szervezeten belül (*E-mail*)	A *Tanúsítványigénylő űrlap*nak megfelelően.
UID	egyedi azonosító (*Unique identifier*)	A szervezet adószáma : az aláírót azonosító okmány száma:opcionálisan aláíró egyéb azonosítója
Title	az *aláíró* szervezeti pozíciója (Title)	Ez egy opcionális adat, Megrendelőlapnak megfelelő

[40] A természetes személy családi,- elő- és utóneve olyan sorrendben szerepel ebben a mezőben, ahogyan a személyazonosító okmányában.

[41] ld. [1] törvény 2. számú melléklet c) pont

[42] ld. [1] törvény 2. számú melléklet k) pont

[43] Az „Organizational unit” mezőt igen gyakran használják (a szervezeten belüli szervezeti egység jelölésére). Ha ilyenre kerül sor, akkor azt jelezni kell.

[44] A Megrendelőlapon külön-külön szerepelnek azok az adatok, amelyeket az alany illetve a szervezet, továbbá azok, amelyeket *Szolgáltató* tölti ki.

[45] Célszerű az [5] szabvány szerinti két karakter hosszú országkódot alkalmazni.

3.1.2 Igény a nevek értelmezhetőségére

A **tulajdonos-azonosító**ra ("Alany" mezőre)a következő szabályok érvényesek:

- Az azonosítónak értelmezhetőnek kell lenni.
- Álnév használata megengedett. Ebben az esetben igénylő az általa választott tetszőleges álnevet használhatja, amely a tanúsítványban megjelenik. Álnév használata esetén Szolgáltató nem vállal felelősséget a tanúsítvány használata során az esetleges visszaélésekért és az így keletkezett károkért.
- Magyar állampolgárok nevének felvétele során a személyi igazolványban szereplő írásmódot - ékezetmentes formában - kell követni.
- Nem magyar állampolgárok esetében az útlevélben szereplő írásmódot kell (ékezetmentes formában) követni.

3.1.3 Különböző elnevezési formák értelmezési szabályai

Kibocsátó-azonosító a következő módon értelmezendő:

- A tanúsítványt a *Matáv e-Szignó® Minősített Hitelesítésszolgáltatás* minősített tanúsítványokat kibocsátó *Hitelesítő Szervezete* adta ki.

A **tulajdonos-azonosító** a következő módon értelmezendő:

- A tanúsítvány **aláírója** a „Common Name” mező szerinti természetes személy, **előfizetője** „Organization” mező szerinti szervezet. Amennyiben a szervezet gazdasági társaság, akkor ez a szervezet típusából látható.

Az *aláíró* a szervezet „Organizational unit” mező szerinti **egységéhez** tartozik. Az előfizető szervezet **székhelye** a „Country” mező szerinti ország „Locality” mező szerinti városában található. Az *aláíró* **e-levél** címe (az előfizető szervezettel összefüggésben) az „Email” mezőben található.

A **tulajdonos-azonosító mező**nek az a célja, hogy a tanúsítvány *aláírój*át az *előfizető* szervezetén belül azonosítani lehessen, valamint az, hogy az előfizető szervezet a Közösség számára egyértelműen azonosítható legyen. Az *aláíró* az *előfizető* szervezetén belüli pozíciójának és jogosultságainak meghatározása a tanúsítványnak nem célja, ezért erre vonatkozóan információt nem tartalmaz.

Az *aláíró* és az *előfizető* szervezet együttes megjelenítése a tanúsítványban azt jelenti, hogy az *előfizető* hozzájárult az *aláíró* és a szervezet nevének együttes feltüntetéséhez. A két fél közti viszony mikéntjére (munkavállalói, tagsági, támogatói, szimpatizánsi, előfizetői, aláírói, partneri stb. viszony) vonatkozóan információt semmilyen formában nem fejez ki.

Az azonosítók értelmezése érdekében az *érintett fel*eknek a jelen szolgáltatási szabályzatban leírtak alapján kell eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az *érintett fél*nek segítségre lenne szüksége, akkor a *Szolgáltató*val közvetlen is felveheti a kapcsolatot. A *Szolgáltató* ilyen esetben az *aláíró* és az *előfizető* egyéb adatairól többlettájékoztatást nem ad, csak a tanúsítványban feltüntetett adatok értelmezését segítő információt szolgáltatja.

3.1.4 A nevek egyedisége

A **tulajdonos-azonosító** a *Szolgáltató* címtárában egyedi. Erről elsődlegesen az *aláíró* e-levél címének azonosítóban való szerepeltetése gondoskodik. A *Szolgáltató* az azonosító kiosztásakor ellenőrzi, hogy az adott e-levél cím nem szerepel-e egy más személy részére korábban kibocsátott tanúsítványban. Ha szerepel, és a tanúsítvány azonosítójának egyéb mezői sem biztosítják az egyediséget, akkor pl. az azonosító „Common Name” mezőjében az *aláíró* családi és keresztnevét egy sorszámmal egészíti ki (ez abban a nagyon ritka esetben fordulhat elő, ha egy szervezet ugyanazon szervezeti egységében egymást követően két ugyanolyan nevű *aláíró* kap szerepet, és ők ugyanazt az e-levél címet kapják a szervezettől).

3.1.5 Eljárások a nevekre vonatkozó vitás kérdések megoldására

Az előfizetői azonosítók kiosztása a beérkezett tanúsítvány-kérelmek elbírálásának sorrendje szerint történik. Ha a kérelmezett azonosító már korábban kiosztásra került, a *Szolgáltató* az egyediséget szolgáló eljárásait követve eltérő azonosítót oszt ki.

A *Szolgáltató* – lehetőségei szerint ellenőrzi az *aláíró* jogosultságát a feltüntetett nevek használatára vonatkozóan a névkiosztás során. A *Szolgáltató* fenntartja magának a jogot az igényelt nevek kiosztásának visszautasítására. Jogszerűtlen név- vagy adathasználat miatt, amennyiben erre bíróság kötelezi, vagy másik fél megalapozott módon bizonyítani tudja jogosultságát, *Szolgáltató*nak jogában áll visszavonni a kérdéses tanúsítványt.

3.1.6 Márkanevek elismerése, hitelesítése és szerepe

A Szolgáltató a szolgáltatása során az „Matáv **e-Szignó**®" **védjegyet** alkalmazza. A védjegy a **Matáv Rt.** tulajdona.

A *Szolgáltató* a közölt adatok alapján – lehetőségei szerint – ellenőrizheti ezek jogos használatát, de nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában. A *Szolgáltató* ezért nem garantálja az előfizetők számára a **védjegy**e és **márkanev**e(i) feltüntetését a tanúsítványban. Az előfizető részéről egy védjegy vagy márkanév megszerzése nem tekintendő olyan eseménynek, mely alapján a tanúsítvány megújítását kell kezdeményeznie.

3.1.7 A magánkulcs birtoklása

A *Szolgáltató* saját sszervezetén belül maga generáltatja a kulcsokat a biztonságos aláírás-létrehozó eszközökön, ezért nem kell ellenőriznie azt, hogy az *aláíró* rendelkezik-e egy (*harmadik fél* részére) hitelesítendő nyilvános kulcs magánkulcs-párjával.

3.1.8 A szervezeti azonosság hitelesítése

A *Szolgáltató* által kibocsátott tanúsítványokban szerepel az előfizető **szervezet neve**, és opcionálisan szerepelhet az előfizető szervezet egy megnevezett **szervezeti egységének neve** is.

Az *igénylő*nek (*előfizető*, *aláíró*) ehhez **adatok**at és **bizonyítékok**at kell nyújtani a következőkről:

- létezik-e az előfizető szervezet és annak szervezeti egysége,

- hivatalos azonosító adatok a szervezetről {ld. **1. melléklet**: ***A regisztrációhoz szükséges adatok***},
- az előfizető szervezet és szervezeti egység viszonya az igénylőhöz,
- az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:
  - a tanúsítvány kibocsátásra kerüljön,
  - a szervezet és szervezeti egysége neve a tanúsítvány tulajdonos-azonosító "alany" mezőjében feltüntetésre kerüljön,
  - az *aláíró* neve a tanúsítvány tulajdonos-azonosító mezőjében feltüntetésre kerüljön;
- az előfizető szervezet kötelezettségvállalása melyben:
  - a tanúsítvány kibocsátásával és fenntartásával kapcsolatos és minden egyéb járulékos költséget vállal,
  - a *Szolgáltató* szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, és elfogadja azokat.

Ennek érdekében az igénylőnek megrendeléskor csatolnia kell a *Szolgáltató* által a szolgáltatási szerződés részét képező **Tanúsítványigénylő űrlap**ot kitöltve, és a szervezet képviseletre jogosult vezető tisztségviselőinek az aláírásával ellátva.

A tanúsítvány-igényléshez csatolni kell a szervezet **aláírási címpéldány**át vagy más hivatalos dokumentumot, mely a szervezet aláírásra jogosult vezetőinek nevét és aláírását tartalmazza. Gazdasági társaságok esetében a **cégkivonatot** (új bejegyzésű szervezet esetében a hatósági tanúsítást), más szervezetek esetében a szervezet hivatalos bejegyzését tanúsító okiratot is mellékelni kell a kérelemhez. A regisztrációhoz szükséges iratokról részletes tájékoztatás található az **1. melléklet**ben.

Szolgáltató a bemutatott iratok és okmányok érvényességét és hitelességét hatósági adatbázisokban ellenőrzi. A *Szolgáltató* a **tanúsítvány** kibocsátását visszautasítja, amennyiben:

- az átadott adatok hiányosak,

- a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a hatósági adatbázisokkal végzett adategyeztetés a bemutatott adatoktól eltérő eredményt ad,
- a személy szervezethez tartozása nem egyértelmű,
- a szervezet nem állapítható meg minden kétséget kizáróan,
- nem egyértelmű a szervezet felhatalmazása a tanúsítvány kibocsátására.

és az igénylő a Szolgáltató által megadott határidőn (hiánypótlási határidő) belül nem pótolta illetve nem helyesbítette a szolgáltatói felhívásban szereplő adatokat, dokumentumokat. A hiánypótlási határidő minden esetben 15 munkanap.

3.1.9 A személyazonosság hitelesítése

A *Szolgáltató* a tanúsítványban megnevezésre kerülő természetes **személy** azonosítását követeli meg a tanúsítvány igénylésekor.

A *Szolgáltató* az igénylő személyazonosságáról személyazonosításra alkalmas okmányok alapján {ld. **1. melléklet**: ***A regisztrációhoz szükséges adatok***} győződik meg. Amennyiben ezek a dokumentumok nem tartalmazzák a szükséges adatokat, akkor a *Szolgáltató* további hivatalos iratokat is kérhet, melyben hatóság igazolja az *igénylő* nevét, állandó lakcímét[46], születésének dátumát és helyét, valamint az anyja nevét.

A személyi igazolványban, illetve útlevélben szereplő fénykép alapján igénylőnek egyértelműen felismerhetőnek kell lennie, és a benne szereplő aláírásnak meg kell egyezni a tanúsítványigénylő űrlapon igénylő által tett aláírással.

A **bemutatott dokumentumok**nak eredetinek, valódinak és érvényesnek kell lenniük. A *Szolgáltató* ezt hagyományos módszerekkel, valamint a személyi adat- és lakcímnyilvántartással, az úti-okmány nyilvántartással és a gépjárművezetői nyilvántartással történő adategyeztetéssel ellenőrzi.

A *Szolgáltató* a bemutatott dokumentumokról fénymásolatot készít és archiválja azokat, vagy jegyzőkönyvet vesz fel.

A *Szolgáltató* a **tanúsítvány** kibocsátását **megtagadja** az alábbi esetekben:

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

[46] például lakcímigazoló kártyával

és az igénylő a Szolgáltató által megadott határidőn (hiánypótlási határidő) belül nem pótolta illetve nem helyesbítette a szolgáltatói felhívásban szereplő adatokat, dokumentumokat. A hiánypótlási határidő minden esetben 15 munkanap.

A *Szolgáltató* nem fogad el **elektronikus dokumentum**ot az egyéni azonosság hitelesítésére a kezdeti regisztráció során.

3.2 Érvényes tanúsítvány megújítása

A *Szolgáltató* **nem teszi lehetővé** az érvényes tanúsítványok megújítását.

A tanúsítvány lejárta után az *aláíró*nak új tanúsítványt kell igényelnie a kezdeti regisztráció módszerével.

3.3 Érvénytelen tanúsítvány megújítása

A *Szolgáltató* az érvénytelen tanúsítványok megújítását **nem teszi lehetővé**.

Ha az aláírónak / előfizetőnek a tanúsítvány visszavonása után új tanúsítványra van szüksége, akkor új tanúsítványt kell igényelnie {ld. 4.1 Tanúsítvány-kérelem}. Visszavonási és felfüggesztési kérelem

Szolgáltató tanúsítvány visszavonási és felfüggesztési szolgáltatásokat egyaránt nyújt. Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait a **4.4.3** ***Visszavonási kérelemre vonatkozó eljárás*** alfejezet tárgyalja.

4. Működésre vonatkozó követelmények

4.1 Tanúsítvány-kérelem

Új végfelhasználói tanúsítvány kibocsátása – az értékesítői szervezet által történt kezdeményezést követően – a *Szolgáltató* regisztrációs szervezeténél igényelhető.

Az igénylési eljárás lépései a következők:

a) Az igénylő tájékozódik a Szolgáltató tanúsítványtípusairól és a Megrendelőlap kitöltésével és aláírásával, valamint annak a Szolgáltató részére való eljuttatásával Tanúsítvány kibocsátását kérelmezi,

b) A Szolgáltató Mobil regisztrációs tisztviselője elvégzi az igénylő személyes ellenőrzését. Az igénylő a regisztráció során a Szolgáltatóval és annak regisztrációs tisztviselőjével köteles együttműködni,

c) Szolgáltató a Szolgáltatási Szabályzatban foglaltaknak megfelelően ellenőrzi az űrlapon szereplő előfizetői és aláírói adatokat és hitelesíti a személyes és szervezeti identitásokat,

d) Szolgáltató elfogadja a tanúsítvány megrendelést, rögzíti az adatokat az informatikai rendszerében, létrehozza az aláírás ellenőrző és létrehozó adatot a Biztonságos aláírás létrehozó eszközön, előállítja és kibocsátja a Tanúsítványt.

e) Szolgáltató átadja a Biztonságos aláírás létrehozó eszközt az Aláírónak vagy Aláíró kijelölt képviselőjének.

E lépéseket megelőzően az igénylő szóban is jelezheti tanúsítványigényét, és a *Szolgáltató* képvelőjével közösen választhatják ki a számára legmegfelelőbb tanúsítványtípust, illetve egyéb tanúsítvány és biztonságos aláírás-létrehozó eszköz-jellemzőket a *Szolgáltató* kínálatából. Amennyiben az igényelő kéri, a szolgáltatás nyilvános dokumentumainak helyszíni tanulmányozására is lehetősége van, valamint szóban történő tájékoztatást is kaphat a szolgáltatással kapcsolatban.

A Megrendelőlap valamint a Szolgáltató szabályzatai és termékismertetői megtalálhatók a *Szolgáltató* honlapján is, így előzetesen is áttekinthető és kitölthető.

A személy- és szervezeti azonosság, valamint a szervezethez tartozás megállapítása a **3.1.7** és **3.1.8** alfejezetekben leírtak alapján történik. A *Szolgáltató* rögzít minden, az *aláíró* és *előfizető* azonosságának igazolására használt információt, és a dokumentációkról másolatot készít.

Az *aláíró* azonosítójának (egyedi nevének) megállapítása a **3.1.4** alfejezetben tárgyaltaknak megfelelően történik.

A szolgáltatási szerződés ezt követő aláírásával születik meg szolgáltató és igénylő között az előfizetői szerződés, az ***Általános Szerződési Feltételek*** (ÁSzF) rendelkezéseinek megfelelően.

Az igénylő aláírásával egyúttal nyilatkozik arról is, hogy *Szolgáltató* feltételei és kikötései, saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Az aláírással igénylő hozzájárul a szolgáltatások során felhasznált információ *Szolgáltató* által történő nyilvántartásba vételéhez, tanúsítványa és az azzal kapcsolatos állapot információ **szolgáltatói címtárban** való közzétételéhez, s ezen információ harmadik félhez történő továbbításához *Szolgáltató* szolgáltatásainak leállítása esetén, illetve egyéb jogszabályok által meghatározott esetekben, *Szolgáltató* szabályzatai által meghatározott módon.

Az aláírás igazolja azt is, hogy az igénylő:

- vállalja a biztonságos aláírás-létrehozó eszköz használatát és védelmét,
- garantálja feltüntetett adatainak valódiságát,
- az adatok későbbi változásairól szolgáltatót értesíti.

A **Szolgáltatási szerződés** és **Megrendelőlap tartalma** ezt követően *Szolgáltató* nyilvántartásába kerül mind elektronikus, mind papír formában.

4.2 Tanúsítvány-kibocsátás

Végfelhasználói tanúsítványok kibocsátására a tanúsítványigénylő eljárás lefolytatását követően kerül sor. A tanúsítvány elkészítésére az új tanúsítványigénylés során (a MEgrendelőlapon) megadott, érvényesnek elismert adatok alapján kerül sor.

A Megrendelőlapon megadott adatok rögzítésre kerülnek, a *Regisztrációs Szervezet által a Szolgáltató* információs rendszerébe.

A *Regisztrációs Szervezet* összeállítja a tanúsítványigénylés elektronikus formátumát és továbbítja a hitelesítő szervezet rendszerébe. Itt megtörténik az egyedi név képzése, a kulcspár előállítása, majd az aláírt tanúsítvány-kérelem eljut a *Hitelesítő Szervezet* tanúsítványkiadó egységébe. A *Hitelesítő Szervezet* aláírja a tanúsítványt saját magánkulcsával. Ezt követően a tanúsítvány 24 órán belül kerül közzétételre anyilvános címtárban.

Az elkészült tanúsítványt *Szolgáltató* a biztonságos aláírás-létrehozó eszközön juttatja el *aláíró*hoz.

Amennyiben *Szolgáltató* az igényelt tanúsítványkérelmet visszautasítja, akkor a kérelmezőnek a *Regisztrációs Szervezet* értesítést küld, a visszautasítás okának megjelölésével.

4.3 Tanúsítvány-elfogadás

A tanúsítványkérelem beadását követően egy későbbi időpontban az űrlapon megjelölt felhatalmazott személy vagy az *aláíró* **személyesen** veheti át a magánkulcsot a biztonságos aláírás-létrehozó eszközön (az ennek aktivizáló adatát tartalmazó zárt borítékkal együtt) a regisztrációs szervezettől.

A magánkulcs használatba vétele előtt az *aláíró*nak kötelessége ellenőrizni a tanúsítványban feltűntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál, a magánkulcsot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonása érdekében.

A kibocsátott **tanúsítvány elfogadása** a kulcs első felhasználásával történik meg.

4.4 Tanúsítvány-felfüggesztés és -visszavonás

Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatásokat nyújt. A tanúsítvány visszavonása a tanúsítvány állapotát végérvényesen érvénytelenre állítja.. A felfüggesztett tanúsítvány mindaddig, amíg felfüggesztett állapotban van, ugyanúgy érvénytelenként kezelendő, mint a visszavont.

A visszavont/felfüggesztett tanúsítványhoz tartozó magánkulcs használatát az eljárás után azonnal **meg kell szüntetni**, illetve fel kell függeszteni. Felelősségi szabályok a visszavont/visszavonandó tanúsítvány elfogadásából eredendő károkra[47]:

- a visszavonási/felfüggesztési kérelem Szolgáltatóhoz történő megérkezéséig az *aláíró* és *előfizető* felelős a felmerülő károkért az *Általános Szerződési Feltételek*nek (**ÁSzF**) megfelelően,
- a visszavonási/felfüggesztési kérelem megérkezésétől az érvénytelen állapot címtárban való megjelenésig *Szolgáltató* felelős a felmerülő károkért,
- az érvénytelen állapot címtárban való megjelenése után az *érintett fél* felelős a felmerülő károkért.

4.4.1 A visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásához a következő körülmények vezetnek.

Aláíró és előfizető (képviselt) kezdeményezése alapján az alábbi esetekben:

- az Aláíró magánkulcsának kompromittálódása,
- biztonságos aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása,
- a biztonságos aláírás-létrehozó eszköz aktivizáló adatának kompromittálódása,
- az Aláíró Tanúsítványban feltűntetett adatainak érvénytelensége,
- az előfizető Tanúsítványban feltűntetett adatainak érvénytelensége,
- a Tanúsítványban feltűntetett Aláíró és előfizető kapcsolatának megváltozása,

[47] ld. [1] törvény 14. § (4)

- az Aláíró visszavonási kérelme,
- az előfizető visszavonási kérelme.

Szolgáltató kezdeményezése alapján az alábbi esetekben:

- az előfizetői szerződés feltételeinek megszegése Aláíró, illetve előfizető által,
- az előfizetői szerződés megszűnése,
- az Aláíró és az előfizető kötelezettségeinek be nem tartása (különösen azonnali felmondás, fizetési késedelem esetén),
- a hitelesítés-szolgáltató tudomására jutott tény a regisztráció során megadott adatok valótlanságáról,
- a Tanúsítványban feltűntetett Szolgáltatói adatok érvénytelensége,
- a hitelesítés-szolgáltató valamely magánkulcsának kompromittálódása,
- a hitelesítési szolgáltatás megszűnése.

Egyéb visszavonáshoz vezető körülmények:

- az Aláíró halála, az előfizető halála vagy megszűnése,
- a Hatóság jogerős és végrehajtható határozata,
- jogszabály rendelkezik így.

4.4.2 Kik kérelmezhetik a visszavonást?

Végfelhasználói tanúsítvány visszavonását az *aláíró*, *előfizető*, *Szolgáltató*, vagy egy hatóság is kezdeményezheti.[48] Az *aláíró*nak, *előfizető*nek és *Szolgáltató*nak kötelessége a **4.4.1** {***A visszavonás körülményei***} alfejezetben feltűntetett esetekben a visszavonás azonnali kezdeményezése, illetve végrehajtása.

4.4.3 Visszavonási kérelemre vonatkozó eljárás

A tanúsítvány visszavonási kérelmét aláírónak telefonon kell bejelentenie a regisztrációs szervezetnél.

Aláírót az regisztrációs szervezet munkatársa a visszavonási jelszava alapján azonosítja (amennyiben ezt aláíró elfelejtette, személyes adatai alapján kerül azonosításra).

[48] Előfordulhat, hogy *Szolgáltató* bizonyos esetekben kívülálló felek számára is engedélyezi a visszavonást (lásd felfüggesztés).

Sikeres azonosítást követően az operátor csak felfüggeszti a tanúsítvány; a visszavonáshoz aláírónak írásban kell megerősítenie visszavonási kérelmét. Az így felfüggesztett tanúsítvány csak akkor kerül visszavonásra, amikor aláíró írásos kérelme a regisztrációs szervezethez beérkezett.

Üzleti tanúsítvány esetén előfizető részéről a törvényes képviselő kezdeményezheti a visszavonást, a visszavonási kérelmet írásban (faxon) kell benyújtsa a regisztrációs szervezethez.

A faxon beküldött kérelem alapján a regisztrációs szervezet munkatársa csak felfüggeszti a tanúsítvány; a visszavonáshoz előfizetőnek írásban kell megerősítenie visszavonási kérelmét. Az így felfüggesztett tanúsítvány csak akkor kerül visszavonásra, amikor előfizető írásos kérelme a regisztrációs szervezethez beérkezett.

A visszavonási kérelemnek a következő adatokat kell tartalmaznia:

- A Tanúsítvány sorozatszáma, referencia száma, típusa,
- Aláíró neve, email címe,
- a visszavonást kérő megnevezése
- a visszavonást kérő beosztása (Üzleti Tanúsítvány esetén),
- a visszavonási kódszó (telefonos visszavonás esetén),
- a visszavonás oka.

A visszavonási kérelem alapján Szolgáltató regisztrációs szervezete ellenőrzi a visszavonási kérelemben szereplő adatokat. Ha az adatok helytelenek, a kérelmező kiléte vagy a visszavonásra való jogosultság nem állapítható meg, akkor Szolgáltató a tanúsítvány visszavonást megtagadja.

Helyes és hiteles kérelem esetén a Szolgáltató további mérlegelés nélkül intézkedik a tanúsítvány visszavonása érdekében: a visszavonást a regisztrációs szervezet a kérelem beérkeztétől számított 1 órán belül végrehajtja. A visszavont tanúsítvány bekerül a következő alkalommal kibocsátott visszavonási listába.

4.4.4 Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási kérelmet azonnal be kell nyújtani az ezért felelős személynek, amikor valamelyik visszavonáshoz vezető körülményről {ld. **4.4.1** ***A visszavonás körülményei***} értesül.

4.4.5 A felfüggesztés körülményei

A tanúsítvány érvényességének felfüggesztése az alábbi esetekben történhet: Aláíró és előfizető (képviselt) kezdeményezése alapján az alábbi esetekben:

- az aláíró felfüggesztési kérelme,
- az előfizető felfüggesztési kérelme.

Szolgáltató kezdeményezése alapján az alábbi esetekben:

- fennálló gyanú a tanúsítványban feltűntetett Szolgáltatói adatok érvénytelenségére vagy a hitelesítés-szolgáltató valamely magánkulcsának kompromittálódására,
- megalapozottan feltételezhető, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy az aláírás-létrehozó adat nem az aláíró kizárólagos birtokában van.

Egyéb visszavonáshoz vezető körülmények:

- a Hatóság jogerős és végrehajtható határozata,
- jogszabály rendelkezik így.

4.4.6 Kik kérelmezhetik a felfüggesztést?

A felfüggesztést ugyanazok kérelmezhetik, akik a visszavonást {ld. **4.4.2** ***Kik kérelmezhetik a visszavonást?***}

4.4.7 Felfüggesztési kérelemre vonatkozó eljárás

A felfüggesztési kérelem a visszavonási kérelemhez hasonlóan nyújtható be szolgáltatóhoz. *Szolgáltató* a felfüggesztési kérelmet írásbeli megerősítés nélkül, az aláíró visszavonási jelszava alapján történő ellenőrzést követően hajtja végre..Előfizető részéről a felfüggesztést a szervezet törvényes képviselője kérheti faxon eljuttatott kérelem formájában.

4.4.8 A felfüggesztés időtartama

Szolgáltató általi kezdeményezés esetén: tanúsítvány addig lehet felfüggesztett állapotban, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 3 napig. Ezt követően a tanúsítvány visszavonásáról, illetve újbóli érvényesítéséről szolgáltatónak a lehető leghamarabb intézkednie kell.

Amennyiben a felfüggesztést a *Hatóság*, az *aláíró* vagy az *előfizető* kérelmezte, úgy a felfüggesztés időtartama legfeljebb 3 nap lehet, vagy a *Hatóság*, az *aláíró* ill. az *előfizető* kérésére ettől rövidebb. A felfüggesztés nem határozatlan idejű és 3 napon belül az aláíró, előfizető vagy a Hatóság írásbeli kérelme alpján történhet meg a tanúsítvány ismételt érvénybe helyezése. Ennek hiányában a 3 nap elteltével Szolgáltató automatikusan visszavonja a tanúsítványt.

4.4.9 A tanúsítvány-visszavonási lista kibocsátási gyakorisága

Szolgáltató a tanúsítványok érvényességének ellenőrzésére tanúsítvány visszavonási listát bocsát ki. A visszavonási listában a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok az újbóli érvényesítés hatására kikerülnek a listából. A visszavont tanúsítványokat is törlik a listából, a tanúsítvány lejártát követően.

A visszavonási lista kibocsátása *Szolgáltató* **Címtár**ából történik. A kibocsátások legfeljebb **24 óránként** követik egymást. A visszavonási lista mindig tartalmazza a következő lista kibocsátásnak idejét, de *Szolgáltató* ennél korábban is kibocsáthat új listát.

4.4.10 Tanúsítvány-visszavonási lista ellenőrzési követelményei

A visszavonási lista ellenőrzése az *érintett fel*ek részére javasolt a tanúsítványok elfogadását megelőzően. A tanúsítványhoz tartozó visszavonási lista elérhetősége bele van foglalva a tanúsítványba. A lista ellenőrzésének arra kell vonatkozni, hogy a kérdéses tanúsítványt a lista tartalmazza-e, a lista hiteles és sértetlen, s a kérdéses tranzakció szempontjából időben releváns-e.

*Szolgáltató*t nem terheli felelősség a visszavonási listában közzétett tanúsítványok elfogadásából keletkező esetleges károkért.

4.4.11 Valós idejű visszavonási állapot ellenőrzés elérhetősége

Szolgáltató valós idejű visszavonási állapot-szolgáltatást nem nyújt.

4.4.12 Valós idejű visszavonás-ellenőrzési követelmények

Szolgáltató valós idejű visszavonási állapot-szolgáltatást nem nyújt.

4.4.13 A visszavonási hirdetmények egyéb elérhető formái

A visszavonási hirdetmények csak *Szolgáltató* címtárán keresztül érhetők el.

4.4.14 A visszavonási hirdetmények egyéb elérhető formáinak ellenőrzési követelményei

Ilyen követelmények nincsenek.

4.4.15 Kulcs kompromittálódás esetére vonatkozó speciális követelmények

Az *aláíró* kötelessége a kompromittálódott magánkulcs által esetlegesen az *érintett fel*ek értesítése, és minden intézkedés megtétele az esetleges károk megelőzése vagy enyhítése érdekében.

4.5 A biztonsági naplózás folyamatai

Szolgáltató hitelesítési rendszere széleskörű naplózási tevékenységet folytat a tanúsítványokra vonatkozó műveletek és az ezek során felhasznált adatok megőrzése érdekében. A naplóbejegyzések a bejegyzés pontos idejét, a tevékenység időpontját (ha az a bejegyzés idejétől eltér) és végrehajtóját is tartalmazzák. A pontos időt *Szolgáltató* pontosidő-egysége biztosítja, ami legfeljebb **1 másodperces** eltérést engedélyez a valódi időhöz képest. Az esetleges ennél nagyobb eltérések szintén naplózásra kerülnek.

Szolgáltató egyéb rendszerei szintén naplóznak. E naplózások tulajdonságai az adott alkalmazások függvényei. A naplózások elemei elkülönülten keletkeznek a különböző modulokban.

Az egyes ***rendszerek üzemeltetési leírásai*** operatív szinten szabályozzák a napló adatok kezelését.

4.5.1 A tárolt események típusai

A hitelesítési rendszer által a hitelesítő és a regisztrációs egységekhez történő valamennyi hozzáférés és tevékenység naplózásra kerül. Így naplózásra kerül:

- valamennyi regisztrációval kapcsolatos esemény,
- a tanúsítványok életciklusával kapcsolatos összes esemény,
- a kulcsok életciklusával kapcsolatos események,
- a biztonságos aláírás-létrehozó eszközök kezelése (BALE-előkészítés, kulcs felírás, BALE-szétosztás stb. kapcsolatos valamennyi esemény,
- az esetleges hibaesemények.

4.5.2 A napló állomány feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása **napi rendszerességgel** megtörténik. *Szolgáltató* hálózati védelmi riasztás funkciókkal is rendelkeznek az erőforrásokhoz történő jogosulatlan hozzáférés észlelésének jelzésére. Ilyen riasztási esetekben a naplóbejegyzéseket soron kívül átvizsgálják. Rendellenességek észleléskor, reklamáció esetén, vagy egyéb megkeresések kapcsán szintén sor kerülhet a napló adatok rendkívüli átvizsgálására.

4.5.3 A napló-állomány megőrzési időtartama

A napló-állományokat **90 napig** tárolják a keletkezésük helyén. Ezek után az adatokat egyszer írható médiára archiválják, és a napló-állományok archív adathordozóit biztonságosan megőrzik a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított **10 évig**, illetőleg a velük kapcsolatban esetleg felmerült jogvita jogerős lezárásáig.[49]

4.5.4 A napló állomány védelme

Szolgáltató hitelesítési rendszerének naplóbejegyzései *Szolgáltató* elektronikus aláírásával ellátva, a törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A napló állományt a véletlen és szándékos rongálások ellen **biztonsági mentés**ek védik {ld. **4.5.5** ***A napló állomány mentési folyamatai***}. A személyes adatokat tartalmazó naplóbejegyzések esetében *Szolgáltató* gondoskodik az adatok bizalmas tárolásáról. A napló állományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán szükségük van. *Szolgáltató* a hozzáféréseket biztonságos módon ellenőrzi.

4.5.5 A napló állomány mentési folyamatai

A naplóállományok **napi rendszerességgel** (az átvizsgálást megelőzően) mentésre kerülnek egyszer írható médiára aláírt formában. A média elzárva és fizikailag is elkülönítetten megőrzésre kerül (lásd **5.1.6** és **5.18**).

A mentés és visszaállítás operatív folyamatait *Szolgáltató* ***mentési szabályzatai*** írják le részletesen.

4.5.6 A napló gyűjtési rendszere

A naplóbejegyzéseket az alkalmazások automatikusan gyűjtik és tárolják a napló állományokban. A mentett médiákat *Szolgáltató* napi rendszerességgel begyűjti. A médiákat *Szolgáltató* saját munkatársai szállítják a megőrzési helyre.

[49] ld. [1] törvény 9. § (7)

4.5.7 Az eseményeket kiváltó aláírók értesítése

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

4.5.8 Sebezhetőség felmérése

A naplóbejegyzések feldolgozása során *Szolgáltató* a naplózott események alapján a sebezhetőségre vonatkozó felméréseket végez. A napi rendszerességgel végzett feldolgozáson túl *Szolgáltató* szakemberei **havonta áttekintik** a rendkívüli eseményeket és ezek alapján a sebezhetőségre vonatkozó elemzéseket végeznek. Ezen elemzések alapján *Szolgáltató* lépéseket tesz a rendszer biztonságának javítására.

4.6 Adatok archiválása

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

4.6.1 A tárolt események típusai

Szolgáltató regisztrációs szervezete valamennyi regisztrációs eljárás során keletkező iratot tárol és megőriz. Így tárolják:

- a *Szolgáltató*hoz benyújtott valamennyi papír alapú kérelmet (tanúsítvány kibocsátás, -megújítás, -visszavonás stb.),
- az igénylő személyes és szervezeti identitásának igazolására bemutatott valamennyi dokumentum fénymásolatát,
- *Szolgáltató,* az *aláíró* és az *előfizető* között megkötött valamennyi megállapodást.

Szolgáltató központi ügyfélszolgálata és regisztrációs szervezete ezen túl hangszalagra veheti, az összes telefonos megkeresés során elhangzott párbeszédet.

4.6.2 Az archívum megőrzési időtartama

Szolgáltató valamennyi (papíralapú vagy elektronikus) iratot és hangfelvételt a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított **10 évig**, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrzi.[50]

4.6.3 Az archívum védelme

Az iratok biztonságos megőrzéséről és tárolásáról *Szolgáltató* egy ***Adattár*** segítségével gondoskodik, amelyhez a Szolgáltatónak a meghatározott munkatársairendelkeznek hozzáférési engedéllyel (adattár felelős).

A *Szolgáltató* a hitelesítésszolgáltatás során elektronikus formában tárolt archivált adatállományt **minősített aláírás**sal és **időbélyegző**vel látja el."

4.6.4 Az archívum mentési folyamatai

Az elektronikus másolati példányban létező iratokat egyszer írható médiára rendszeresen mentik..

4.6.5 A rekordok időbélyegzésére vonatkozó követelmények

Lásd a **4.6.3** ***Az archívum védelme*** alfejezetet.

4.6.6 Az archívum gyűjtési rendszere

A regisztráció során keletkezett papíralapú iratokat az *Adattár*ban tárolják és őrzik. Az elektronikus másolatok elektronikus adathordozón, biztonságos formában kerülnek az *Adattár* archívumába[51].

[50] ld. [1] törvény 9. § (7)

[51] Bármilyen továbbítás és tárolás során gondoskodni kell az adatok bizalmasságáról és sértetlenségéről.

4.6.7 Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz *Szolgáltató* ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés *aláíró*nak és előfizetőnek a rá vonatkozó adatokhoz lehetséges, más feleknek a **2.8.4**, **2.8.5** és **2.8.6** alfejezetek szerint. *Szolgáltató* a jogosultságot minden esetben ellenőrzi, és azt naplózza.

4.7 Tanúsítványmegújítás

Szolgáltató által kibocsátott végfelhasználói tanúsítványok érvényességi ideje **1 év**. Az érvényesség kezdete a tanúsítvány "érvényesség" mezőjében megadott kezdeti (not before) érték által mutatott dátum. A magánkulcs érvényességi ideje megegyezik a tanúsítvány érvényességi idejével. *Szolgáltató* a **tanúsítványok megújítását nem támogatja**.

4.8 Helyreállítás rendkívüli üzemi helyzetek esetén

Rendkívüli üzemeltetési helyzet bekövetkezése esetén a szolgáltató haladéktalanul értesíti a Hatóságos a rendkívüli üzemeltetési helyzet bekövetkezéséről, annak hatásáról, várható időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről. A Szolgáltató a rendkívüli üzemeltetési helyzetről értesíti a szolgáltatást igénybe vevő azon szerződött ügyfeleit, akiket a rendkívüli üzemeltetési helyzet érint, valamint az erről szóló tájékoztatást az interneten elérhetővé teszi.”

A *Szolgáltató* katasztrófa elhárítási tervben részletesen szabályozza a különböző sérülések és katasztrófahelyzetek (beleértve valamely szolgáltatói magánkulcs kompromittálódását, vagy kritikus hardver/szoftver elem meghibásodását is) esetén követendő eljárásokat. A következő fejezetekben e **katasztrófa elhárítási irányelveket** foglaljuk össze.

4.8.1 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltató **megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik**, a hardver- és szoftver-meghibásodások valamint az adatsérülések minimalizálása érdekében. A szolgáltatások helyreállíthatóságát *Szolgáltató* háttérszerződései és saját tartalékeszközei garantálják. *Szolgáltató* rendszeres mentései és tranzakció naplózása biztosítja az adatok visszaállíthatóságát valamely adattároló eszköz kiesésének esetére. Ez a rendszer a legrosszabb esetben az előző napi adatok helyreállítására képes.

Szolgáltató katasztrófa elhárítási terve eseményjelentési előírásokkal rendelkezik valamennyi eszköze meghibásodása, illetve rendellenes működése tekintetében (ezek egy része automatizált, más része a kezelőszemélyzet felelőssége). A jelentéseket szakértő személyzet értékeli ki, és válaszadás eljárásokat foganatosítva minimalizálja az esetleges károkat és szolgáltatás kieséseket.

4.8.2 A szolgáltatói egység nyilvános kulcsának visszavonása

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

4.8.3 Egy szolgáltatói egység kulcsának kompromittálódása

Szolgáltató katasztrófa elhárítási terve a szolgáltatói magánkulcsok[52] kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik az ez által érintett valamennyi fél értesítéséről (a **2.6.1** alfejezettől függetlenül, de arra tekintettel), megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet.

[52] Ide nem csak a hitelesítő egységek tartoznak, de egyéb - a hitelesítési szolgáltatásban részt vevő - alkalmazások és személyek kulcsai is.

4.8.4 Biztonsági képesség természeti vagy más katasztrófát követően

Szolgáltató **elsődleges működési helyszín**ein kívül másodlagos helyszínekkel is rendelkezik[53]. Természeti vagy más katasztrófát követően, illetve *Szolgáltató* berendezéseinek olyan mértékű meghibásodását illetően, mely a **4.8.1** alfejezet szerint nem kezelhető, *Szolgáltató* a másodlagos helyszínen is képes szolgáltatásainak beindítására.

Ilyen esetekben *Szolgáltató* a következő szolgáltatások legfeljebb **3 órán belüli** elindítását vállalja:

- visszavonás kezelés szolgáltatás,
- visszavonási állapot közzététele szolgáltatás.

Minden egyéb szolgáltatás elindítását *Szolgáltató* **24 órán belül** vállalja.

4.9 A hitelesítésszolgáltatás leállítása

A *Szolgáltató* a szolgáltatás tervezett megszűntetése esetén legkevesebb **60 nappal** a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a *Hatóság*ot[54]. A *Szolgáltató* a bejelentéssel egyidejűleg leállítja a következő szolgáltatásait:

- tanúsítvány-előállítás szolgáltatás (ezen belül a tanúsítvány megújítása),
- kezdeti regisztrációs szolgáltatás (az egyéb regisztrációs szolgáltatások tovább élnek),
- tanúsítvány-kibocsátás szolgáltatás (ezen belül a tanúsítvány archiválása),
- az aláírás-létrehozó adat elhelyezése biztonságos aláírás-létrehozó eszközön szolgáltatás.

[53] A *Hitelesítő Szervezet* másodlagos helyszíne a *Regisztrációs Szervezet* helyszíne, és fordítva.

[54] ld. [1] törvény 16. § (1)

Szolgáltató a tervezett megszűnés előtt legalább **20 nappal** intézkedik a végfelhasználói tanúsítványok visszavonásáról[55]. Ezzel egyidejűleg leállítja a következő szolgáltatást:

- visszavonás-kezelési szolgáltatás,
- időbélyegzés szolgáltatás.

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

- visszavonási állapot közzététele szolgáltatás.

Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású szolgáltatókkal **szolgáltatásainak átvételéről**. Nyilvántartásait, a bizalmas felhasználói adatokkal együtt a **2.8.7** alfejezet szerint mindenképpen átadja egy ilyen szolgáltatónak, egyéb szolgáltatásait a tárgyalások eredményétől függően.

A szolgáltatói tanúsítványok visszavonásáról (és a magánkulcsok megsemmisítéséről) - a tárgyalások eredményétől függően - *Szolgáltató* fokozatosan intézkedik a 60 napos időszakban.

A *Szolgáltató* a tárgyalások végeredményéről tájékoztatja a végfelhasználókat és a *Hatóság*ot. A *Szolgáltató* az *aláíró*kat és az *előfizető*ket elektronikus levélben, az *érintett fel*eket az internetes honlapon történő közzététel útján tájékoztatja. A *Szolgáltató* a *Gyökér Hitelesítő Egység* tanúsítványának visszavonását **5 nappal megelőzően** a **2.6.1** alfejezetnek megfelelően hirdetményt tesz közzé.

A *Szolgáltató* hitelesítésszolgáltatási tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, **minősített időbélyegzővel** ellátott **mentést** készít

A *Szolgáltató* - annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak - az adatokat az új szolgáltató által fogadóképes médián és formátumban helyezi el vagy biztosítja az új szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, melyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

[55] ld. [1] törvény 16. § (1)

5. Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

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

5.1 Fizikai óvintézkedések

Szolgáltató gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások nyújtásához szükséges eszközök használatából eredő kockázatot minimalizálják.

A fizikai óvintézkedések célja a *Szolgáltató* információira és fizikai körleteire irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A biztosított védelem arányban áll a *Szolgáltató* által végzett kockázat elemzésben megállapított kockázatokkal.

A leginkább veszélyeztetett szolgáltatásokat a *Hitelesítő Szervezet* védett számítógép termeiben valósítják meg. Ezek a számítógép termek speciálisan erre a célra lettek tervezve és kialakítva, és tervezésénél több különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés /beléptetés ellenőrzése és felügyelete/, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, stb.) érvényesítésére is sor került.

A *Hitelesítő Szervezet* valamennyi kritikus szolgáltatását biztonsági körletben valósítja meg, és az ehhez szükséges valamennyi eszközt a biztonsági körletek részét képező védett számítógép termekben helyezte el. A termek túlmelegedés elleni védelmére kialakításra kerül helyiségenként elektromos hőérzékelő berendezés mely a kritikus hőmérséklet elérése előtt riasztási jelzést továbbít a létesítmény épület-felügyeleti rendszeréhez. A helyiségekben gyengeáramú szükség-megvilágítás került telepítésre mely egyben a menekülési útvonalat is jelöli. A padló burkolata csúszásmentes, antisztatikus és terhelő nyomásnak ellenálló.

A *Regisztrációs Szervezet* számítógép terme úgy lett kialakítva, hogy a fenti szempontoknak szintén megfeleljen, alacsonyabb kialakítási és fenntartási költségek mellett, tekintetbe véve az itt megvalósított szolgáltatások fontosságát és centralizált jellegét, egyúttal a *Hitelesítő Szervezet* védett számítógép termeiben megvalósított szolgáltatásokhoz képest kevésbé kritikus jellegét.

A *Regisztrációs Szervezet* (és benne a címtár) számítógép terme önálló biztonsági körletnek minősül. Ezen belül valósulnak meg a kritikus szolgáltatások, és itt került elhelyezésre az ezekhez szükséges valamennyi eszköz.

5.1.1 A telephely elhelyezése és szerkezeti felépítése

A *Hitelesítő Szervezet* védett számítógép terme a befogadó épület területén elkülönítetten került kialakításra (Budapest XII. kerület, Schweidel út 6.). Az elkülönített biztonsági körlet három egymásba nyíló, összesen egy bejárattal rendelkező ablaktalan helyiségből áll, melyben elhelyezésre kerültek a számítógépszerverek és az üzemeltetésükhöz szükséges teljes infrastruktúra.

A *Regisztrációs Szervezet* számítógép terme a Horváth M.-tér 17-19. „B” épület kiemelt földszintjén foglal helyet. A körlet három egymásba nyíló helyiségből áll, melyből a regisztrációs szervezet eszközei egy helyiségben kerültek elhelyezésre, a működtetésükhöz szükséges infrastruktúrával együtt.

5.1.2 Fizikai hozzáférés

A *Hitelesítő Szervezet* védett számítógép terme úgy lett kialakítva, hogy illetéktelen személyek egyáltalán ne juthassanak be, a biztonsági őrség viszont rövid idő alatt meg tudja közelíteni riasztás esetén. A biztonsági körletnek nincs ablaka, a bejárati ajtón kívül csak falbontással lehet behatolni ide. A biztonsági körlet integráltan megvalósított behatolás jelző (riasztó) és beléptető (ujjlenyomat azonosító) rendszerrel van ellátva.

A védett számítógép termekbe az ott dolgozó bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és kísérettel léphetnek be.

A *Regisztrációs Szervezet* számítógép termébe csak az erre feljogosított személyek léphetnek be, egy proximity kártyás beléptető rendszer felügyelete alatt. A gépterem behatolás jelző (riasztó) rendszerrel is el van látva.

A számítógép terembe az ott dolgozó bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és kísérettel léphetnek be.

5.1.3 Áramellátás, légkondicionálás

Áramellátás

A *Hitelesítő Szervezet* védett számítógép termeinek zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében. A helyiségek betáplálására 3x60 amper tápellátás áll rendelkezésre, fáziselosztással, bemeneti zavarszűrűvel és érintésvédelemmel.

A következő védelmi megoldások együttese biztosított:

- szünetmentes energia ellátás a gépekbe szerelt UPS-egységek által,
- villamos zavar, villám és túlfeszültség védelem,

Az alkalmazott üzemmód pedig az alábbi:

- az üzemi táp kimaradása vagy csökkenése esetén a rendszer átkapcsol a tartalék tápra,
- ha a tartalék táp sem használható, akkor a rendszer fokozatosan leállítja a szervereket,

Zárlati leoldásra szelektív áramkörök segítségével a gépteremben több egymástól független működésű rendszer lett kialakítva a folyamatos üzemeltetés támogatására. A villamos zavar, villám és túlfeszültség védelem szempontjából a gépterem nagy értékű, kritikus szolgáltatásokat biztosító berendezései védve vannak a különböző vezetett és sugárzott villamos zavarok, villámok miatt bekövetkező túlfeszültség hatásai ellen:

- a rendszert külön mechanizmusok védik a villámok által keltett elektromágneses impulzusok (EMI) hatása ellen,

- az üzemeltetett berendezések a sugárzott elektromágneses zavarás elleni védelem mindkét elvárását teljesítik: egyrészt védettek az üzemelési környezetükben jelen levő hatások ellen, másrészt nem bocsátanak ki olyan zavaró elektromágneses jeleket, amely a környezetükben üzemelő többi berendezés működését zavarhatná.

A *Regisztrációs Szervezet* számítógép termének zavartalan áramellátását szünetmentes energia ellátás biztosítja.

Külön akkumulátoros **szünetmentes tápegységek** biztosítják az alábbi berendezések áramellátását áramszünet esetén:

- tűzjelző berendezés (**24 órás** üzemképességgel teljes áramszünet esetén),
- telefonközpont (**6 órás** áramszüneti üzemképességgel).

Légkondicionálás

A *Hitelesítő Szervezet* védett számítógép terme hűtésigényének kiszolgálását helyiségenkénti levegő hűtését egy split klíma biztosítja. Mivel a létesítmény föld alatti, a friss levegő utánpótlásról, illetve elszívásról egy központi rendszer gondoskodik.

A *Regisztrációs Szervezet* számítógép termében a hőmérséklet állandó szinten tartását split klímaberendezések együttes működése biztosítja.

A klímaberendezések elhelyezésének módja biztosítja, hogy azok karbantartása ne okozzon zavart a géptermek működésében.

5.1.4 Beázás és elárasztás veszélyeztetettsége

A *Hitelesítő Szervezet* biztonsági körleteinek kialakítása során figyelembe vették az elárasztás veszélyének minimalizálását. A biztonsági körletek teljes területe mentes a vizesblokkoktól, illetve a közelben nincs sem csatorna, sem vízvezeték.

A *Regisztrációs Szervezet* számítógép termében és körzetében nincsenek vizesblokkok, vízvezeték és csatorna.

5.1.5 Tűzmegelőzés és tűzvédelem

A *Hitelesítő Szervezet* géptermét befogadó épületben a helyiségek védelmére kiépített tűzvédelmi rendszer működik.

A helyiségek tűzvédelmét egy tűzjelző és oltóközpont biztosítja. A tűzvédelmi jelzések az épület felügyeleti rendszerre kerültek beintegrálásra, mely a jelzéseket a Matáv Rt. **24 órás** diszpécserszolgálatához továbbítja, ahol a szükséges intézkedéseket megteszik. Tűzriasztás esetén az épület-felügyeleti rendszer a légbefújást automatikusan leállítja.

A helyiségek bejáratát tűzgátló ajtó választja el a létesítménytől, így a kialakított termek önálló tűzszakaszt képeznek.

A *Regisztrációs Szervezet* biztonsági körletének kialakítása során az építési engedély tűzvédelmi fejezetét az illetékes tűzoltó parancsnokság jóváhagyta.

A kiépített tűzvédelmi rendszert (melynek fő elemei: füstérzékelő- és tűzjelző rendszerek, oltókapszulák) az illetékes tűzoltó parancsnokság engedélyezte.

5.1.6 Adathordozók tárolása

A *Hitelesítő Szervezet* biztonsági körletében egy kódzáras és egy rekeszenként külön-külön zárható lemezszekrény szolgál az adathordozók biztonságos tárolására.

Az első lemezszekrényben a *Regisztrációs Szervezet* mentési példányait tárolják {ld. **5.1.8 *Fizikailag elkülönítetten őrzött mentési példányok***}.

A kódzár nyitási kódját csak a *Hitelesítő Szervezet* biztonsági tisztviselője ismeri. A nyitási kód egy példányban papíron is rögzítésre kerül, egy lezárt borítékban (a boríték külső oldalán a kódzár azonosítójának feltüntetésével), melyet a *Regisztrációs Szervezet* biztonsági tisztviselője őriz (rendkívüli esetekre).

A második lemezszekrényben (külön elzárható rekeszekben) a *Hitelesítő Szervezet* adminisztrálásához, üzemeltetéséhez szükséges adathordozókat tárolják a bizalmi munkakört betöltő munkatársak (központi adminisztrátorok, rendszeroperátorok). Itt tárolják az egyes munkatársak számára készült, illetve általuk készített bizalmas minősítésű papíralapú dokumentumokat is. A kulcsokat (mindenki a sajátját) pecsételhető kulcsdobozva zárva, lepecsételve, távozáskor a biztonsági őrség szobájában elhelyezett tároló szekrénybe kell rakni. Innen vehető fel érkezéskor (mind a felvétel, mind a leadás aláíráshoz kapcsolódik).

Egy külön lepecsételt kulcsdobozban tárolódnak a lemezszekrény kulcsok másodpéldányai. Ezt (rendkívüli esetben) a pecséttel rendelkező biztonsági tisztviselő veheti fel, de ő is csak a biztonsági őrség egyik tagjának jelenlétében használhatja. Az írásban is rögzített használat után, lepecsételve vissza kell rakni a tároló szekrénybe.

Bizalmas adatokat tartalmazó adathordozót, jogosult felhasználója nem hagyhatja felügyelet nélkül, köteles lemezszekrényébe elzárni.

A *Regisztrációs Szervezet* biztonsági körletében (a gépteremben) egy kódzáras és több zárható lemezszekrény szolgál az adathordozók biztonságos tárolására.

A kódzáras lemezszekrényben a *Hitelesítő Szervezet* mentési példányait tárolják {ld. **5.1.8 *Fizikailag elkülönítetten őrzött mentési példányok***}.

A kódzár nyitási kódját csak a *Regisztrációs Szervezet* biztonsági tisztviselője ismeri. A nyitási kód egy példányban papíron is rögzítésre kerül, egy lezárt borítékban (a boríték külső oldalán a kódzár azonosítójának feltüntetésével), melyet a *Hitelesítő Szervezet* biztonsági tisztviselője őriz (rendkívüli esetekre).

A zárható lemezszekrényekben a *Regisztrációs Szervezet* adminisztrálásához, üzemeltetéséhez szükséges adathordozókat tárolják a bizalmi munkakört betöltő munkatársak (központi adminisztrátorok, rendszeroperátorok). Itt tárolják az egyes munkatársak számára készült, illetve általuk készített bizalmas minősítésű papíralapú dokumentumokat is. A kulcsokat (mindenki a sajátját) pecsételhető kulcsdobozva zárva, lepecsételve, távozáskor az épület portaszolgálatán elhelyezett tároló szekrénybe kell rakni. Innen vehető fel érkezéskor (mind a felvétel, mind a leadás aláíráshoz kapcsolódik).

Egy külön lepecsételt kulcsdobozban tárolódnak a lemezszekrény kulcsok másodpéldányai. Ezt (rendkívüli esetben) a pecséttel rendelkező biztonsági tisztviselő veheti fel, de ő is csak egy másik bizalmi munkakört betöltő munkatárs jelenlétében használhatja. Az írásban is rögzített használat után, lepecsételve vissza kell rakni a tároló szekrénybe.

Bizalmas adatokat tartalmazó adathordozót, jogosult felhasználója nem hagyhatja felügyelet nélkül, köteles lemezszekrényébe elzárni.

5.1.7 Selejt kezelése és megsemmisítése

A *Hitelesítő Szervezet* biztonsági körleteiben a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat, még tartalmuk törlése után sem használják fel nem minősített adatok tárolására. A feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat fizikailag megsemmisítik:

- a papíralapú dokumentumokat zúzógéppel felaprítják,
- a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprítják,
- a merev lemezeket (a befogadó épületben központilag biztosított célberendezés felhasználásával) demagnetizálás után fizikailag összetörik.

A *Regisztrációs Szervezet* biztonsági körletében a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat, még tartalmuk törlése után sem használják fel nem minősített adatok tárolására. A feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat fizikailag megsemmisítik:

- a papíralapú dokumentumokat zúzógéppel felaprítják,
- a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprítják,
- a merev lemezeket (a befogadó épületben központilag biztosított célberendezés felhasználásával) demagnetizálás után összetörik.

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

A *Hitelesítő Szervezet* biztonság-kritikus szolgáltatásaira vonatkozó adatok mentési példányait a *Regisztrációs Szervezet* biztonsági körletében tárolják.

A *Regisztrációs Szervezet* biztonság-kritikus szolgáltatásaira vonatkozó adatok mentési példányait a *Hitelesítő Szervezet* biztonsági körletében tárolják.

5.2 Eljárásbeli óvintézkedések

Az eljárásbeli óvintézkedések célja, hogy a **bizalmi munkakörök** kijelölésével és elkülönítésével, az egyes *munkakörök felelősségének* dokumentálásával, az egyes feladatokhoz szükséges *személyzeti létszámok*, valamint az *egyes munkakörökben elvárt azonosítás és hitelesítés* meghatározásával kiegészítse, egyúttal fokozza a fizikai és személyzetre vonatkozó óvintézkedések hatásosságát.

5.2.1 Bizalmi munkakörök

Szolgáltató a következő bizalmi munkaköröket határozza meg az alábbi felelősségkörökkel:

- biztonsági tisztviselő,
- rendszer (vagy központi) adminisztrátor,
- regisztrációs tisztviselő
- regisztrációs ügyeleti operátor,
- rendszeroperátor,
- rendszervizsgáló.

A ***Hitelesítő Szervezettel munkaviszonyban álló***, változó helyszínen dolgozó **biztonsági tisztviselő(k)** a tanúsítvány előállítását, kibocsátását, felfüggesztését és visszavonását ***nem végezhetik*,** de jóváhagyják azok kérését.

A ***Hitelesítő Szervezettel munkaviszonyban álló,*** változó helyszínen dolgozó **biztonsági tisztviselők** általánosan (a *Hitelesítő Szervezet*nél és a *Regisztrációs Szervezetnél egyaránt*) felelnek:

- a különböző biztonsági óvintézkedések kidolgozásáért,
- a különböző biztonsági óvintézkedések rendszeres felülvizsgálatáért, a szükségessé váló módosítások kezdeményezéséért,

- a biztonsági óvintézkedések érvényre jutásáért, betartatásáért,
- az informatikai rendszerek biztonsági szintjének megőrzéséért (rendszeres auditok szervezésével).

A ***Hitelesítő Szervezettel munkaviszonyban álló,*** változó helyszínen dolgozó **biztonsági tisztviselők** közreműködnek (egy másik, bizalmi munkakört betöltő társuk jelenlétében) az alábbi tevékenységeknél:

- *a Szolgáltató* első saját kulcsának generálásánál,
- *a Szolgáltató* későbbi saját kulcsgenerálásánál,
- *a Szolgáltató* magán aláíró kulcsának biztonsági mentésénél,
- *a Szolgáltató* magán aláíró kulcsának visszaállításánál,
- *a Szolgáltató* magán aláíró kulcsának (és annak összes másodpéldányának) megsemmisítésénél,
- a *Gyökér Hitelesítő Egység (*Root CA) által generált CRL fájlokat tartalmazó **adathordozóknak** a *Hitelesítő Szervezet* MasterLDAP szerverére való továbbításánál (Publikáció),
- a *Gyökér Hitelesítő Egység* nyilvános kulcsát tartalmazó **adathordozó** *Hitelesítő Szervezet* MasterLDAP szerverére való továbbításánál,
- *a Szolgáltató* Operational CA (Hitelesítés szolgáltatónál) HSM-jében használt magánkulcsok nyilvános párjait tartalmazó **adathordozók** a *Gyökér Hitelesítő Egység*hez való továbbításánál, illetve az erre, a *Gyökér Hitelesítő Egység* által kibocsátott tanúsítvány visszaszállításánál,
- *a Szolgáltató* TrustedTimeStamp szervereiben (Időbélyegzés szolgáltatás) (HSM-jeiben) használt nyilvános kulcsokat tartalmazó **adathordozók** a *Gyökér Hitelesítő Egység*hez való továbbításánál, illetve az erre, a *Gyökér Hitelesítő Egység* által kibocsátott tanúsítvány visszaszállításánál. (Megj.: a szerverből két példány van, két külön HSM modullal).

A ***Hitelesítő Szervezettel munkaviszonyban*** álló **rendszeradminisztrátorok**:

- telepítik, konfigurálják és karbantartják a *Hitelesítő Szervezet* védett számítógép termében üzemeltetett megbízható rendszereket,

- beállítják a fenti megbízható rendszerek kezdeti hálózati konfigurációját,
- kezelik a *Hitelesítő Szervezet* állományába tartozó rendszeroperátorok vonatkozásában a rendszerhez való hozzáféréseket (account felvétele, jogosultságok beállítása, módosítása, kezdeti jelszó beállítása, a távozó, illetve munkakört váltó rendszeroperátorok hozzáférési jogainak azonnali megszüntetése),
- letöltik és installálják a felügyeletük alatt üzemeltetett operációs rendszerre és adatbázisra kiadott biztonsági javítócsomagokat, ezen keresztül gondoskodnak az informatika biztonsági szint folyamatos megőrzéséről,
- rendszeres időnként ellenőrzik (víruskereső programok futtatásával, az engedélyezett és a ténylegesen telepített szoftverek egybevetésével) a *Hitelesítő Szervezet* védett géptermében üzemeltetett informatikai rendszernek és információinak a sértetlenségét,
- gondoskodnak a rendszeroperátorok által végzett rendszermentések illetve a *Regisztrációs Szervezet* rendszermentés másolatainak biztonságos tárolásáról,
- gondoskodnak a rendszermentésekről készített, elkülönítetten őrzendő másolati példányok *Regisztrációs Szervezethez* történő szállításáról[56] {ld. **5.1.8 *Fizikailag elkülönítetten őrzött mentési példányok***},
- telepítik, konfigurálják és karbantartják a *Regisztrációs Szervezet* géptermében üzemeltetett megbízható rendszert,
- beállítják a fenti megbízható rendszer kezdeti hálózati konfigurációját,
- kezelik a *Regisztrációs Szervezet* állományába tartozó rendszeroperátorok vonatkozásában a rendszerhez való hozzáféréseket (account felvétele, jogosultságok beállítása, módosítása, kezdeti jelszó meghatározása, a távozó, illetve munkakört váltó rendszeroperátorok hozzáférési jogainak azonnali megszüntetése),

[56] a hétfő délelőtti órákban

- letöltik és installálják a felügyeletük alatt üzemeltetett operációs rendszerre és adatbázisra kiadott biztonsági javítócsomagokat, ezen keresztül gondoskodnak az informatika biztonsági szint folyamatos megőrzéséről,
- rendszeres időnként ellenőrzik (víruskereső programok futtatásával, az engedélyezett és a ténylegesen telepített szoftverek egybevetésével) a *Regisztrációs Szervezet* informatikai rendszereinek, információinak a sértetlenségét,
- gondoskodnak a rendszeroperátorok által végzett rendszermentések és archiválások, illetve a *Hitelesítő Szervezet* rendszermentés másolatainak biztonságos tárolásáról,
- gondoskodnak a rendszermentésekről készített, elkülönítetten őrzendő másolati példányok *Hitelesítő Szervezet*hez történő szállításáról[57],
- telepítik, konfigurálják, karbantartják és központilag felügyelik a *Hitelesítő Szervezet* és a *Regisztrációs Szervezet* védett rendszereit (pontosabban a címtár szervert, valamint az on-line regisztrálást végző szervert) védő tűzfalakat és behatolást detektáló rendszereket,
- elvégzik a *Hitelesítő Szervezet* védett számítógép termében üzemeltetett megbízható rendszer hálózati konfigurációjának kezdeti beállítását,
- ellenőrzik (áttekintik és kiértékelik) és karbantartják (archiválják és törlik) az általuk felügyelt tűzfalak, behatolást detektáló rendszerek biztonsági naplóit,
- gondoskodnak a tűzfalakra, behatolást detektáló rendszerekre kiadott biztonsági javítócsomagok letöltéséről, installálásáról, ezen keresztül a biztonsági szint naprakész megőrzéséről,
- regisztrációs szervezet számára account felvétele, jogosultságok beállítása,, kezdeti jelszó meghatározása, a távozó, illetve munkakört váltó regisztrációs tisztviselők és regisztrációs ügyeleti operátorok hozzáférési jogainak azonnali megszüntetése.

[57] a hétfő délelőtti órákban

A ***Hitelesítő Szervezettel munkaviszonyban*** álló **rendszeroperátorok** folyamatosan üzemeltetik a *Hitelesítő Szervezet* védett számítógép termében működő megbízható rendszereket, melynek során:

- tanúsítványokat generál(tat)nak az aláírók számára,
- tanúsítványokat generál(tat)nak a *Regisztrációs Szervezet* számára,
- aláír(attat)ják a visszavonási listákat,
- kulcspárokat generál(tat)nak az aláírók számára,
- ellenőrzik a biztonságos aláírás-létrehozó eszközök készítését {ld. **6.1.2 *Magánkulcs eljuttatása a tulajdonoshoz***},
- aktivizálják a biztonságos aláírás-létrehozó eszközöket aktivizáló PIN kódok generálását, kinyomtatását és borítékolását végrehajtó funkciókat {ld. **6.1.4 *A szolgáltatói nyilvános kulcs közzététele***},
- gondoskodnak a biztonságos aláírás-létrehozó eszközöket aktivizáló, beborítékolt PIN kódok biztonságos tárolásáról (a címzettekhez történő továbbításig) {ld. **6.1.2 *Magánkulcs eljuttatása a tulajdonoshoz***},
- előkészítik a beborítékolt PIN kódok (a biztonságos aláírás-létrehozó eszköztől elkülönített) szétosztását,
- gondoskodnak a biztonságos aláírás-létrehozó eszközök biztonságos tárolásáról (a címzettekhez történő továbbításig) {ld. **6.1.2 *Magánkulcs eljuttatása a tulajdonoshoz***},
- hetente egyszer rendszermentéseket végeznek,
- szükség esetén helyreállításokat hajtanak végre,
- folyamatosan üzemeltetik a regisztrációs szervezet számítógépes munkaállomásait, mentéseket hajtanak végre, szükség esetén helyreállításokat eszközölnek,
- végrehajtatják a regisztrációs szervezettől érkező visszavonási kérelmeket.

A ***Hitelesítő Szervezet állományába*** tartozó **rendszervizsgáló**:

- ellenőrzi (áttekinti) és karbantartja (archiválja és törli) a Hitelesítő Szervezet védett számítógép termében működő megbízható rendszer biztonsági naplóit,
- ellenőrzi (áttekinti) és karbantartja (archiválja és törli) a Regisztrációs Szervezet számítógép termében működő megbízható rendszer biztonsági naplóit,
- szükség esetén az általa készített archívumokban keresést végez.

A ***Regisztrációs Szervezettel munkaviszonyban*** álló, a regisztrációs szervezetnél tevékenykedő **biztonsági tisztviselő(k)** közreműködik(nek) (egy másik, bizalmi munkakört betöltő társuk jelenlétében) az alábbi tevékenységeknél:

- a *Regisztrációs Szervezet* kijelölt munkatársai aláíró és dekódoló kulcsainak kezdeti generálásánál,
- a *Regisztrációs Szervezet* kijelölt munkatársai aláíró és dekódoló kulcsainak kiosztásánál,
- a *Regisztrációs Szervezet* kijelölt munkatársai aláíró és dekódoló kulcsainak megsemmisítésénél,
- a *Regisztrációs Szervezet* kijelölt munkatársai aláíró és dekódoló kulcsaihoz tartozó aktivizáló adatainak generálásánál, az biztonságos aláírás-létrehozó eszköz és a hozzá tartozó megszemélyesítő adatok (PIN) használójának történő átadásánál.

A ***Regisztrációs Szervezettel munkaviszonyban*** álló, a regisztrációs szervezetnél tevékenykedő **regisztrációs tisztviselők** felelősek:

- a regisztrációs tevékenységek előkészítéséért, az aláíró személyes azonosításáért,
- az aláíró és előfizető igényléshez szükséges adatainak és dokumentumainak begyűjtéséért és átvételéért,
- az aláíró és előfizető adatainak ellenőrzéséért (hatósági adatbázisokkal való egyeztetéséért),
- a tanúsítvány kérelem rögzítéséért az informatikai rendszerben és indításáért a hitelesítő szervezet felé,

- a tanúsítvány illetve a biztonságos aláírás létrehozó eszköz átvételéért a hitelesítő szervezettől,
- a tanúsítvány illetve a biztonságos aláírás létrehozó eszköz átadásáért az aláíró vagy a meghatalmazottja részére.

A ***Regisztrációs Szervezettel munkaviszonyban*** álló, a regisztrációs szervezetnél tevékenykedő **regisztrációs ügyeleti operátorok** felelősek:

- folyamatos, 24 órás ügyfélszolgálati tevékenységért és help desk funkcióért,
- a felfüggesztési és visszavonási kérések fogadásáért és a felfüggesztés végrehajtásáért.

A ***Szolgáltatóval munkaviszonyban*** álló **adattár-felelősök**:

- tárolják és őrzik a bizalmas minősítésű papíralapú és elektronikus dokumentumokat az *Adattár* helyiségében,
- megfelelő eljárás keretében kiadják az erre jogosultaknak a bizalmas minősítésű anyagokat, illetve visszavételezik azokat,
- napra kész nyilvántartást vezetnek a felelősségük alá tartozó *Adattár*-helyiségben tárolt bizalmas dokumentumokról, egyéb értékekről,
- a bizalmas minősítésű anyagok megsemmisítése (selejtezés esetén).

A bizalmi munkakörök között **személyi átfedések nincsenek**, minden személy csak egy bizalmi munkakört tölt be.

Valamennyi fent megnevezett bizalmi munkakört a munkaköri leírások dokumentálják.

A bizalmi munkakörökbe a biztonsági igazgató nevezi ki *Szolgáltató* munkatársait, a biztonsági alapellenőrzés sikeres befejezése után {ld. **5.3.1 *Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények***}.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Általánosan teljesül a hitelesítő szolgáltató egészére, hogy minden munkatárs csak a saját munkakörének megfelelő funkciókat aktivizálja.

A *Hitelesítő Szervezetnél* az alábbi kettős felügyeletet igénylő **munkafolyamatok** vannak, amelyhez két bizalmi munkakört betöltő személy együttes jelenléte (és előzetes, sikeres hitelesítése) szükséges:

- a *Szolgáltató* első saját kulcsának generálása esetén,
- a *Szolgáltató* későbbi saját kulcsgenerálása esetén,
- a *Szolgáltató* magán aláíró kulcsának biztonsági mentése (klónozása) esetén,
- a *Szolgáltató* magán aláíró kulcsának visszaállítása esetén,
- a *Szolgáltató* magán aláíró kulcsának (és annak összes másodpéldányának) megsemmisítése esetén,
- A *Gyökér Hitelesítő Egység (*Root CA) által generált CRL fájlokat tartalmazó **adathordozók**nak a *Hitelesítő Szervezet* MasterLDAP szerverére való továbbításánál (publikáció),
- *a Szolgáltató* Operational CA (Hitelesítés szolgáltatónál) HSM-jében használt magánkulcsok nyilvános párjait tartalmazó **adathordozók** a *Gyökér Hitelesítő Egység*hez való továbbításánál, illetve az erre, a *Gyökér Hitelesítő Egység* által kibocsátott tanúsítvány visszaszállításánál,
- *a Szolgáltató* TrustedTimeStamp szervereiben (Időbélyegzés szolgáltatás) HSM-jében használt nyilvános kulcsait tartalmazó **adathordozók** a *Gyökér Hitelesítő Egység*hez való továbbításánál, illetve az erre, a *Gyökér Hitelesítő Egység* által kibocsátott tanúsítvány visszaszállításánál. (Megj.: a szerverből két példány van, két külön HSM modullal),
- a *Gyökér Hitelesítő Egység* nyilvános kulcsát tartalmazó **adathordozó** *Hitelesítő Szervezet* MasterLDAP szerverére való továbbításánál,
- a *Regisztrációs Szervezet* kijelölt munkatársai aláíró és dekódoló kulcsainak kezdeti generálásánál,

- a *Regisztrációs Szervezet* kijelölt munkatársai aláíró és dekódoló kulcsainak kiosztásánál,
- a *Regisztrációs Szervezet* kijelölt munkatársai aláíró és dekódoló kulcsainak megsemmisítésénél,
- a *Regisztrációs Szervezet* kijelölt munkatársai aláíró és dekódoló kulcsaihoz tartozó aktivizáló adatainak generálásánál, az biztonságos aláírás-létrehozó eszköz és a hozzá tartozó megszemélyesítő adatok (PIN) használójának történő átadásánál.

5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

A *Hitelesítő Szervezet* valamennyi bizalmi munkakört betöltő munkatársának azonosítása és hitelesítése egy intelligens kártyaolvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával történik. Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

A *Regisztrációs Szervezet* valamennyi bizalmi munkakört betöltő munkatársa azonosítása és hitelesítése egy intelligens kártya olvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával történik. Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

5.3 Személyzetre vonatkozó óvintézkedések

A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a lehetőségekkel való visszaélés kockázatának csökkentése.

Ennek érdekében *Szolgáltató* a személyi biztonsággal már a felvételi szakaszban foglakozik, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését.

Valamennyi bizalmi munkakör esetén a felvételire jelentkezőket biztonsági ellenőrzésnek vetik alá. Minden bizalmi munkakört betöltő alkalmazottnak és külső félnek, akik *Szolgáltató* szolgáltatásaival kapcsolatba kerülnek, titoktartási nyilatkozatot kell aláírni.

Szolgáltató egyúttal biztosítja a valamennyi munkakör betöltéséhez szükséges közös, általános, illetve az egyes munkakörök betöltéséhez szükséges speciális szakmai ismereteket megszerzését, illetve továbbfejlesztését.

Ennek érdekében *Szolgáltató* egy 2 lépcsős (tájékoztatás + továbbképzés) képzési rendszert valósít meg:

- a tájékoztatás valamennyi, a *Szolgáltató* szolgáltatásaival vagy informatikai rendszerével kapcsolatba kerülő munkatárs számára egységes {ld. **5.3.3 *Kiképzési követelmények***},
- a továbbképzés moduláris, és az egyes bizalmi munkakörök szerint eltérő felépítésű tananyag szerint történik, 3 különböző szinten (kezdő, középhaladó, haladó), a személyre szóló éves továbbképzési terveknek megfelelően {ld. **5.3.4 *Továbbképzési gyakoriságok és követelmények***}.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A *Hitelesítő Szervezet,* és a *Regisztrációs Szervezet* minden bizalmi munkakörére jelölt személyének (emberi megbízhatóságuk és szakmai alkalmasságuk ellenőrzése céljából) egy kezdeti ellenőrzésen (biztonsági alapellenőrzésen) kell keresztülmennie.

A biztonsági alapellenőrzés során az ellenőrzést végző szakemberek, az életrajzban megadott adatokat (életrajzi elemek, referenciák, szakmai előmenetel, stb.) ellenőrzik. Ennek során:

- a képzettségre vonatkozó adatokat egybevetik a jelölt által benyújtandó bizonyítványokkal, diplomákkal,
- a gyakorlati tapasztalatra vonatkozó állításokat személyes referenciákon keresztül, publikációkra alapozva, illetve egyéb úton igazolják.

A *biztonsági tisztviselők* bizalmi munkakörére jelöltek esetén büntetlen előélet igazolása (hatósági erkölcsi bizonyítvány beszerzése és bemutatása) is szükséges.

Az egyes bizalmi munkakörök betöltéséhez szükséges képzettség és gyakorlat a következő.

biztonsági tisztviselő:

- szakirányú felsőfokú végzettség, valamint
- legalább három év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat.

rendszer (vagy központi) adminisztrátor, rendszervizsgáló, rendszeroperátor, regisztrációs tisztviselő:

- középfokú szakirányú végzettség, valamint
- legalább öt év, hasonló munkakörben szerzett szakmai gyakorlat.

regisztrációs ügyeleti operátor:

- középfokú szakképesítés, valamint
- szakirányú képzés.

adattár-felelős:

- középiskolai végzettség,
- titkos ügyirat kezelői tanfolyami végzettség,
- legalább két év, hasonló munkakörben szerzett szakmai gyakorlat.

Az informatika biztonsággal kapcsolatos valamennyi bizalmi munkakört[58] betöltő munkatársra nézve egy személyes **továbbképzési terv** készül, melyet évente áttekintenek (egyúttal az időközben elvégzett továbbképzési, oktatási anyagokkal kiegészítenek), illetve az adott munkakörhöz tartozó szakmai ismeretek megújulása, változása függvényében aktualizálnak.

5.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások

Valamennyi bizalmi munkakört betöltő munkatársnak a biztonsági alapellenőrzésen túl {ld. **5.2.1** ***Bizalmi munkakörök***} időszakos biztonsági ellenőrzéseken kell átesniük.

[58] Ez a meghatározás az *adattár-felelős* munkakör kivételével az összes többi munkakörre vonatkozik

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a “elfogadhatatlanul nagy biztonsági kockázat” minősítést kapja[59].

Az időszakos biztonsági ellenőrzésre rendszeres időnként kerül sor:

- a biztonsági tisztviselők esetében **3 évente**,
- egyéb bizalmi munkakörök esetében **5 évente**.

Az ellenőrzés során vizsgálják a munkatárs erkölcsi bizonyítványát és olyan körülményeket, melyek kockázati tényezőt jelentenek. E mellett figyelembe veszik a közvetlen vezetők véleményét is.

5.3.3 Kiképzési követelmények

A *Hitelesítő Szervezet* valamint a *Regisztrációs Szervezet* területén dolgozó valamennyi munkatárs felvételét követően, a saját munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt.

Valamennyi munkakörbe való végleges kinevezésnek feltétele az alapkiképzésen való részvétel, s az ezt követő írásos teszten legalább “megfelelő” eredmény elérése.

Egyesített tematika keretében minden munkatárs egy egységes informatika biztonsági alapkiképzésben is részesül. Ennek az (egynapos, intenzív) képzési formának a fő célja az egész hitelesítésszolgáltatásra vonatkozó szervezet biztonságpolitika megismerése, megértése, az ezen alapuló aktuális eljárások és követelmények megismerése és a későbbi helyes alkalmazása érdekében.

Rendszeroperátori munkakörben kinevezett (véglegesített) munkatárs a kinevezést követő **2 hétig** megfelelő gyakorlattal rendelkező kollégával közösen van beosztva (nem lehetséges, hogy a két egyszerre szolgálatban lévő rendszeroperátor mindegyike az adott munkahelyen kezdő).

[59] A már bizalmi munkakört betöltő munkatársaktól való, biztonsági okokból történő megválást az alkalmazható legdiszkrétebb módon hajtják végre.

5.3.4 Továbbképzési gyakoriságok és követelmények

Minden bizalmi munkakört betöltő munkatárs esetében egy személyre szóló éves továbbképzési terv készül. (Ez tartalmazza az arra az évre beütemezett szervezett belső továbbképzéseket, illetve külső tanfolyamokon, egyéb továbbtanulási formákban való ismeretszerzést.) A személyes továbbképzési tervet a humánpolitikai részleg bevonásával, a közvetlen vezető évente áttekinti, értékeli és (az érintett munkatárs beleegyezésével) aktualizálja.

Abban az esetben, amikor a hitelesítésszolgáltatásban jelentős változás következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.

Kisebb változások bekövetkezése előtt a munkatársak írásos tájékoztatást kapnak a változásokról.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között nem valósul meg.

5.3.6 A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs esetén, a munkakörbe kinevezéskor a foglalkoztatási dokumentumok részeként

- írásos tájékoztatást kapott jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról,
- munkaköri leírást kapott, mely tartalmazta az őt érintő biztonsági feladatokat,
- titoktartási nyilatkozatot írt alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is megfogalmazódtak.

Mindezek tartalmazzák azokat a munkajogi vagy büntető következményeket, melyek a különböző fegyelem- munkaköri kötelezettség- illetve törvénysértést szankcionálják.

Amennyiben egy munkatárs (gondatlanságból fakadóan vagy szándékosan) megsérti a fenti szabályokat, ellene büntető intézkedéseket hoznak (melyek az elkövetés módjától és következményétől függően a jutalom megvonástól fegyelmi eljárás indításán és kártérítésen át, egészen a hatósági feljelentésig terjedhet).

5.3.7 A szerződéses alkalmazottakra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak vele (vagy a *Regisztrációs Szervezet*tel) munkaviszonyban álló személyt alkalmaz.

Szolgáltató az egyéb feladatok ellátására, alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket (külső munkavállalókat és ideiglenes alkalmazottakat egyaránt) csak az “ellenőrzött beszállítók” listájáról választ. Az ellenőrzött beszállítókkal a *Hitelesítő Szervezet* előzetesen írásos megállapodást köt, melyben vállalta *Szolgáltató* **biztonságpolitikájának** elfogadását.

Valamennyi szerződő fél – még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismerendő üzleti/vállalati titkokat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is.

A külső munkavállalók és ideiglenes alkalmazottak szakmai kiképzésben, továbbképzésben nem részesülnek, erre nem kötelezettek[60].

5.3.8 A személyzet számára biztosított dokumentációk

Minden bizalmi munkakört betöltő munkatárs, írásban megkapja a következő dokumentumokat:

[60] A külső munkavállalókat eleve úgy választják meg, hogy az adott munkafeladathoz minden szakmai ismerettel és gyakorlattal rendelkezzenek. Az ideiglenes alkalmazottak olyan jellegű munkát végeznek, melyhez nincs szükség ki- és továbbképzésre.

- a **kinevezés**i eljárás, illetve az alapkiképzés során:
  - *Szolgáltató* szervezeti biztonságpolitikája,
  - aláírt titoktartási nyilatkozat,
  - egyéni munkaköri leírás,
- a tervezett és rendkívüli **továbbképzés**ek alkalmával:
  - az adott oktatási formához tartozó oktatási segédanyagok
- egyéb esetekben:
  - személyes továbbképzési terv (évenkénti aktualizálása után),
  - a munkavégzést érintő kisebb változások leírása (a változások előtt),
  - módosított biztonsági politika (a bekövetkező változások előtt).

A szervezeti biztonságpolitikában bekövetkező változásokról írásos értesítők formájában mindenki tájékoztatást kap {ld. **5.3.4** ***Továbbképzési gyakoriságok és követelmények***} az említett továbbképzés előtt.

6. Műszaki biztonsági óvintézkedések

A *Szolgáltató*, biztonságtechnikailag értékelt és minősített termékekből álló, megbízható informatikai rendszert használ szolgáltatásai nyújtásához.

A rendszert szállító és kivitelező vállalkozók a hitelesítésszolgáltatás kiépítésében jelentős tapasztalatokkal rendelkeztek, nemzetközileg elismert technológiát alkalmaztak, és kulcsrakész beruházást valósítottak meg.

A rendszer kialakításánál a fejlesztők törekedtek a moduláris felépítésre és a későbbi fejleszthetőségre. A rendszer tervezésénél alapvető szempontként kezelték *Szolgáltató* által támasztott igényeket. A rendszer fejlesztése keretében több informatikai cég működött együtt.

A rendszer kialakításához a Matáv Rt. biztosította:

- a fizikai környezetet,
- a szükséges hálózat kialakítását és a hálózatbiztonsági eszközöket,
- a hardver erőforrásokat (a HSM modulok kivételével),
- az etalon időforrás szolgáltatásához – mely a Matáv NTP-n elérhető - a fizikai és az IP alapú kapcsolatot,
- a mentési és archiválási környezetet,
- az LDAP rendszer kialakítását C=HU ROOT SUFFIX beállításáig.

6.1 Kulcspár előállítás és telepítés

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

6.1.1 Kulcspár előállítás

A ***Gyökér hitelesítő*** kulcspárját saját maga generálja, a saját HSM moduljában. A generált magánkulcsok teljes életciklusuk alatt a kriptográfiai hardverekben maradnak, megsemmisítésükig azt sehová nem kell továbbítani.

A ***Hitelesítő Szervezet*** az alábbi **kulcspárokat** használja:

- Végfelhasználói minősített tanúsítványokat és visszavonási listákat (CRL) aláíró kulcs,
- *Regisztrációs Szervezet* (RA) tanúsítványait aláíró kulcs,
- *Időbélyeget* aláíró kulcs.

A ***Hitelesítő Szervezet*** valamennyi kulcspárját saját maga generálja, HSM modulokban. A generált magánkulcsok teljes életciklusuk alatt a kriptográfiai hardverekben maradnak, megsemmisítésükig azt sehová nem kell továbbítani. Így az **Operational CA** kulcspárjai a saját HSM moduljában keletkeznek, és ugyanígy a **TrustedTimeStamp** szerverek (kettő van) kulcspárjai a saját HSM moduljaikban keletkeznek.

A ***Regisztrációs Szervezet*** az alábbi **kulcspárokat** használja:

- *regisztrációs alkalmazás* operátori aláíró kulcs

A **regisztrációs alkalmazás operátori** kulcsot a CardPerso környezetben a Certificate Manager EE interfész alkalmazásával kell elkészíteni. A kártyán On-board generálódik a kulcs. A tanúsítványt közvetlenül a központi adminisztrátor adhatja ki a Certificate Manager Agent interfész segítségével. A kártyán tárolt kulcsokat a kártyához hozzáférő személy használhatja.

A **CardPerso operátori** titkosító kulcsot (az RA aláíró kulcsot) a CardPerso környezetben a Certificate Manager EE interfész alkalmazásával kell elkészíteni. A kulcs a kártyán **On-board** generálódik. A tanúsítványt közvetlenül a központi adminisztrátor adhatja ki a Certificate Manager Agent interfész segítségével. A kártyán tárolt kulcsokat a kártyához hozzáférő személy használhatja.

Az ***aláírók*** az alábbi **kulcspárt** használják:

- *végfelhasználói minősített* aláíró kulcs.

Ezt a kulcspárt a CardPerso rendszerrel generálják a *Hitelesítő Szervezetnél.* Ennek során a *Regisztrációs Szervezet* által **biztonságos csatornán** küldött regisztrációs adatokat importálja az adatbázisába. A megszemélyesítés során az inputfájlt feldolgozza, és ennek során az alábbi tevékenységeket is elvégzi:

- **generálja** a kártya hozzáféréshez az első PIN-t (transzport PIN);
- **előállíttatja** a kulcspárt a kártyán, majd az igénylői adatokkal kiegészített nyilvános kulcsra tanúsítvány-kérést állit elő;
- **elküldi** a tanúsítvány-kérést az Operational CA-nak, valamint a visszavonási jelszóként is alkalmazott első PIN-el;
- **felírja** a kártyára az Operational CA által aláírt és visszaküldött tanúsítványt.

A minősített aláíró kulcs tehát közvetlenül az intelligens kártyán jön létre, arról másolat nem készül. Ezt követően a magánkulcs teljes életciklusa alatt csak a biztonságos aláírás-létrehozó eszközön (intelligens kártya) marad.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

Mivel a *Hitelesítő Szervezet* valamennyi HSM modulban készülő kulcspárja helyben generálódik {ld. **6.1.1 *Kulcspár előállítás***}, így azokat nem kell sehová továbbítani.

A *Hitelesítő Szervezet* CardPerso operátori kulcspárja a CardPerso környezetben (a Certificate Manager EE interfész alkalmazásával) intelligens kártyán (On-board) generálódik. A CardPerso operátori kártyát (kulcsokat) a biztonsági tisztviselő engedélye alapján a tulajdonos személyesen veheti át a hozzáférési kódokkal együtt.

A *Regisztrációs Szervezet* **Regisztrációs tisztviselőjének kulcspárja** a CardPerso környezetben (a Certificate Manager EE interfész alkalmazásával) intelligens kártyán (On-board) generálódik. A Regisztrációs-Alkalmazás operátori kártyát (kulcsokat) a Matáv Mobil RA csoport vezetőjének kérésére a biztonsági tisztviselő utasítására a tulajdonos személyesen veheti át a hozzáférési kódokkal együtt a *Regisztrációs Szervezet*nél.

Az *aláírók* aláíró magánkulcsát - a védett tárolást és felhasználást biztosító biztonságos aláírás-létrehozó eszközzel együtt - a *Regisztrációs Szervezet*nél **személyesen megjelenő** *aláíró*knak adják át a biztonságos aláírás-létrehozó eszközt aktivizáló PIN kódot tartalmazó zárt borítékkal együtt.

6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A *Hitelesítő Szervezet* valamennyi nyilvános kulcsáról a *Gyökér Hitelesítő Egység* készít tanúsítványt. A nyilvános kulcsokat védetten tartalmazó floppy-t **két biztonsági tisztviselő** személyesen viszi a *Gyökér Hitelesítő Egységhez.*

A *Regisztrációs Szervezet* valamennyi nyilvános kulcsáról a *Hitelesítő Szervezet* készít tanúsítványt. A tanúsítvány igényléshez a Certificate Manager EE interfészt alkalmazzák. A tanúsítványt közvetlen a központi adminisztrátor adhatja ki a Certificate Manager Agent interfész segítségével. A folyamat zárt rendszerű, az igénylés a kulcsgenerálás és hitelesítés, valamint a magánkulcs hordozón történő elhelyezése „egy időben” történik, bizalmi munkakört betöltő személyek jelenlétében és engedélyével.

A sikeresen regisztrált *aláírók* valamennyi nyilvános kulcsáról a *Hitelesítő Szervezet* készít tanúsítványt. A CardPerso rendszer által elküldött tanúsítvány-kérést az Operational CA írja alá, és küldi vissza a CardPerso rendszernek, ahol a tanúsítvány is az intelligens kártyára íródik.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

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

A szolgáltatói nyilvános kulcsot tartalmazó tanúsítvány ellenőrzéséhez szükséges (gyökér) nyilvános kulcs közzététel az alábbi módon valósul meg:

- A *Hitelesítő Szervezet* minden hitelesítő egysége a *Gyökér Hitelesítő Egység*től **adathordozón** kapja meg a nyilvános kulcsot, melyet két biztonsági tisztviselő személyesen hoz el,

- Az aláírók a hitelesítő szervezet által feltöltött biztonságos aláírás-létrehozó eszközön (intelligens kártyán) kapják meg a (gyökér) nyilvános kulcsot a regisztrációs tisztviselőtől.

A *Gyökér Hitelesítő Egység* nyilvános kulcsa megszerezhető, illetve ellenőrizhető közvetlenül is, mivel a *Gyökér Hitelesítő Egység* hirdetésben is közzéteszi saját (önhitelesített) nyilvános kulcsát egy országos terjesztésű napilapban.{ld. **2.6.1**}.

6.1.5 Kulcs méretek

a *Gyökér Hitelesítő-Egység* aláíró kulcsának mérete:..... 2048 bit

a *Hitelesítő Szervezet* aláíró kulcsainak mérete: .... 2048 bit

az *Időbélyegző központ* aláíró kulcsának mérete: .. 2048 bit

a *Regisztrációs Szervezet* aláíró kulcsainak mérete:2048 bit

a *végfelhasználói* aláíró kulcsoknak mérete: ..... 1024 bit

6.1.6 A nyilvános kulcs paraméterek előállítása

A *Hitelesítő Szervezet* és a *Regisztrációs Szervezet* digitális aláírásra az **RSA algoritmus**t használja.

Az RSA algoritmussal van aláírva a rendszer által kibocsátott **minden tanúsítvány**, és ezt az algoritmust használják a rendszeren belül is a letagadhatatlanság (tranzakciók aláírása, *Regisztrációs Szervezet* által archivált adatok aláírása stb.) biztosítására.

A *végfelhasználók* számára kibocsátott tanúsítványok aláíró algoritmusa is az **RSA**.

6.1.7 A paraméterek megfelelőségének ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

- a paraméterekhez felhasznált véletlenszám generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),
- a paraméterekre vonatkozó feltételek, összefüggések teljesülésének ellenőrzése.

A **véletlenszám generálás** megfelelőségének ellenőrzése:

- A rendszerben használt valamennyi kriptográfiai hardver modul képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül. A modulokat az ezzel megbízott bizalmi munkakört betöltő munkatársak rendszeres időközönként tesztelik.
- A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám generálásukat.

A **paraméterekre** vonatkozó feltételek, összefüggések teljesülésének ellenőrzése:

- A rendszerben használt valamennyi kriptográfiai hardver modul a kulcsgenerálás során generált paraméterekre ellenőrzi, hogy azok a rájuk vonatkozó korlátok közé esnek-e, illetve teljesülnek-e az egymás közötti, kötelező összefüggések.

6.1.8 Hardver/szoftver kulcselőállítás

A *Hitelesítő Szervezet* kulcsainak generálása egy nCipher nShield F3 PCI **hardver** eszközzel történik amely FIPS 140-1 szabvány szerint 3. szinten bevizsgált HSM.

A *Regisztrációs Szervezet* kulcsainak előállítása **On-board hardver** generálással történik a Certificate Manager EE és Certificate Manager Agent interface-ek igénybevételével.

Az *aláírók* aláíró kulcspárjainak generálása a CardPerso rendszerben **On-board hardver** generálással történik (tehát az intelligens kártyán).

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

A “kulcs használati” mezők lehetséges (egyúttal kötelezően kitöltendő) értékei az alábbiak:

Hitelesítő szervezet

Kulcs megnevezése	A “kulcs használati” mező értéke	Kritikus / Nem kritikus
végfelhasználói minősített tanúsítványokat és a visszavonási listákat (CRL) aláíró kulcs	***keyCertSign és CRLSign***	**K**
az időbélyegző központ aláíró kulcsai	***NonRepudiation***	**K**
	az „Extended Key Usage” mezőbe: ***timeStamping***	**K**
a *Regisztrációs Szervezet* tanúsítványait aláíró kulcs	***keyCertSign***	**K**

Regisztrációs szervezet

Kulcs megnevezése	"kulcs használati" mező értéke	Kritikus / Nem kritikus
tranzakciókat aláíró kulcs	*nonRepudiation*	K

Aláírók

Kulcs megnevezése	"kulcs használati" mező értéke	Kritikus / Nem kritikus
végfelhasználói minősített aláíró kulcs	***nonRepudiation és digitalSignature***	**K**

6.2 A magánkulcsok védelme

A *Szolgáltató* gondoskodik valamennyi általa (saját maga, *Regisztrációs Szervezet*, illetve *aláíró*k számára) előállított magánkulcs titkosságáról és sértetlenségéről.

A *Szolgáltató* ugyanazt az aláíró magánkulcsot használja a végfelhasználói minősített tanúsítványok és a tanúsítvány visszavonási listák aláírásra.

A *Szolgáltató* a végfelhasználói minősített tanúsítványokat és a tanúsítvány visszavonási listákat aláíró magánkulcsát fizikailag biztonságos helyszínen használja.

6.2.1 Kriptográfiai modulra vonatkozó szabványok

A *Szolgáltató* valamennyi szervezeti egysége (*Hitelesítő Szervezet*, *Regisztrációs Szervezet, Gyökér Hitelesítő Egység*) a kriptográfiai kulcsok gondozását külön hardver modulban valósítja meg.

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

A *Szolgáltató*nál (a *Hitelesítő Szervezetben*) alkalmazzák az “n-ből m” ellenőrzést a magánkulcsokkal kapcsolatos kulcsgondozási funkciók aktivizálásánál.

6.2.3 Magánkulcs letétbe helyezése

*Szolgáltató*nál **magánkulcsot** nem lehet letétbe helyeztetni.

6.2.4 Magánkulcs mentése

A *Szolgáltató*nál a következő magánkulcsok kerülnek mentésre (illetve duplikálásra, klónozásra):

- a *Hitelesítő Szervezet* aláíró magánkulcsai

A magánkulcsok tárolására egy FIPS 140-1 szabvány szerint hármas szinten bevizsgált HSM (nCipher nShield F3 PCI) szolgál. A modulban tárolt kulcsokhoz való hozzáféréshez egy három kártyából álló kártya szett egyikével történő azonosítás szükséges. A **kulcsmentés intelligens (Smart) kártyára** történik, melynek védelme fokozott biztonsági intézkedésekkel van megoldva.

6.2.5 Magánkulcs archiválása

A *Szolgáltató*nál **magánkulcsokat** nem archiválnak.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

A *Hitelesítő Szervezet* magánkulcsait az nCipher nShield F3 PCI kriptográfiai hardver modulja **maga generálja**, és a magánkulcs semmilyen körülmények között nem hagyja el a modult. /Következésképpen soha nem kell kívülről bejuttatni azt./

A *Regisztrációs Szervezet* kulcspárjait a *Hitelesítő Szervezet* CardPerso rendszer segítségével intelligens kártyákon **On-board** generálja. Ezt követően a magánkulcsok teljes életciklusuk során nem hagyják el az intelligens kártyát. /Következésképpen másként nem kell kívülről bejuttatni azokat./

A *végfelhasználói* aláíró kulcspárjait a *Hitelesítő Szervezet,* CardPerso rendszere segítségével intelligens kártyákon **On-board** generálja. Ezt követően a magánkulcsok teljes életciklusuk során nem hagyják el az intelligens kártyát. /Következésképpen másként nem kell kívülről bejuttatni azokat./

6.2.7 A magánkulcs aktivizálásának módja

Hitelesítő szervezet

A HSM kriptográfiai hardver modulok magánkulcsa csak aktív állapotban használható.

Az aktív állapotba kerüléshez a rendszeroperátornak meg kell adnia azonosító és hitelesítő adatait, melyet az általa birtokolt un. Operator Card Set segítségével tehet meg.

Az így aktivált magánkulcs mindaddig használható, amíg a modul aktív állapotban marad.

A rendszeroperátor által használt intelligens kártyák (CardPerso operator card set) magánkulcsai csak aktív állapotban használhatók.

Az aktív állapotba kerüléshez a rendszeroperátornak az alábbiakat kell végrehajtania:

- be kell helyezni az intelligens kártyát az olvasó egységbe,
- ki kell váltania (az alkalmazáson keresztül) egy “login” parancsot,
- kérésre meg kell adnia hitelesítő adatát (PIN).

Az így aktivált magánkulcsok mindaddig használhatók, amíg az intelligens kártya az olvasóban marad

Regisztrációs szervezet

A rendszeroperátor által használt intelligens kártyák magánkulcsai csak aktív állapotban használhatók.

Az aktív állapotba kerüléshez a rendszeroperátornak az alábbiakat kell végrehajtania:

- be kell helyezni az intelligens kártyát az olvasó egységbe,
- ki kell váltania (az alkalmazáson keresztül) egy “login” parancsot,
- kérésre meg kell adnia hitelesítő adatát (PIN).

Az így aktivált magánkulcsok mindaddig használhatók, amíg az intelligens kártya az olvasóban marad

6.2.8 A magánkulcs aktív állapotának megszüntetési módja

Hitelesítő szervezet

A nCipher nShield HSM kriptográfiai hardver modul magánkulcsa akkor dezaktivizálódik, ha a modul (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

- a felhasználó dezaktivizálja a kulcsot,
- a kripto modul áramellátása megszakad (kikapcsolás vagy tápellátási probléma),
- a kripto modul hibaállapotba kerül.

Az így dezaktivizált magánkulcs mindaddig nem használható, amíg a modul ismét aktív állapotba nem kerül.

Az intelligens kártyák (ALE) (CardPerso operator card set) magánkulcsai akkor dezaktivizálódnak, ha az intelligens kártya (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

- az intelligens kártyát kiveszik az olvasó egységből,
- az intelligens kártya külső (az olvasó felöl kapott) áramellátása megszakad,
- az intelligens kártya hibaállapotba kerül.

Az így dezaktivizált magánkulcsok mindaddig nem használhatók, amíg az intelligens kártya ismét aktív állapotba nem kerül.

Regisztrációs szervezet

Az intelligens kártyák (ALE) magánkulcsai akkor dezaktivizálódnak, ha az intelligens kártya (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

- az intelligens kártyát kiveszik az olvasó egységből,
- az intelligens kártya külső (az olvasó felöl kapott) áramellátása megszakad,
- az intelligens kártya hibaállapotba kerül.

Az így dezaktivizált magánkulcsok mindaddig nem használhatók, amíg az intelligens kártya ismét aktív állapotba nem kerül.

6.2.9 A magánkulcs megsemmisítésének módja

A *Hitelesítő Szervezet* HSM kriptográfiai hardver moduljaiban tárolt magánkulcsok megsemmisítése két biztonsági tisztviselő együttes jelenlétében sikeres hitelesítésük után, a szükséges kulcsmegsemmisítő funkciók kiváltásával történhet.

A *Regisztrációs Szervezet* intelligens (ALE) eszközben tárolt magánkulcsok megsemmisítése két regisztrációs tisztviselő együttes jelenlétében, sikeres hitelesítésük után, a szükséges kulcsmegsemmisítő funkciók kiváltásával történhet.

A magánkulcs megsemmisítés az aláíró felelőssége.

6.3 A kulcspár gondozásának egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

A *Regisztrációs Szervezet* **minden**, a *Szolgáltató* által előállított tanúsítványt archivál az alábbi időszakra:

- nem végfelhasználói tanúsítványok: az érvényesség lejártától számított ..... **10 évig**,
- végfelhasználói tanúsítványok: az érvényesség lejártától számított ..... **10 évig**.

A nyilvános kulcsok archiválásáért a *Hitelesítő Szervezet*ben dolgozó rendszeroperátorok a felelősek .

Az archiválás (az integritásellenőrzést biztosító lenyomatértékekkel együtt) egyszer írható CD-kre történik.

6.3.2 A nyilvános és magánkulcsok használatának periódusa

Hitelesítő Szervezet

A *Hitelesítő Szervezet* aláíró kulcsához tartozó tanúsítvány érvényességi ideje: **10 év**

A *Hitelesítő Szervezet* magán kulcsainak érvényességi ideje: ..... **10 év**

Regisztrációs Szervezet

A *Regisztrációs Szervezet* aláíró kulcsához tartozó tanúsítvány érv. ideje: **1 év**

A Regisztrációs Szervezet aláíró kulcsához tartozó tanúsítványának érvényességének ideje meghosszabbítható.

A Regisztrációs Szervezet magán kulcsának érvényességi ideje: nincs korlátozva.

Az aláírók

Az aláírók aláíró kulcsához tarozó tanúsítvány érvényességi ideje: ..... **1 év**

Az aláírók magán kulcsának érvényességi ideje: ..... **nincs korlátozva.**

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

A *Hitelesítő Szervezet* az általa kibocsátott minden aláírás-létrehozó eszköz aktivizáló adatát (PIN kódjait) a CardPerso rendszerrel állítja elő szabványos generálási módszerrel.

6.4.2 Az aktivizáló adatok védelme

A *Hitelesítő Szervezet* az általa kibocsátott aláírás-létrehozó eszközök aktivizáló adatait (PIN kódjait) műszaki és szervezési intézkedésekkel védi.

6.4.3 Az aktivizáló adatok egyéb szempontjai

A *Hitelesítő Szervezet* által kibocsátott aláírás-létrehozó eszközök aktivizáló adatainak kezelése a kibocsátást követően az aláíró felelőssége.

6.5 Számítógépes biztonsági óvintézkedések

6.5.1 Speciális számítógépes biztonsági műszaki követelmények

A *Hitelesítő Szervezet* olyan megbízható informatikai rendszereket alkalmaz, mely az alábbi termékeken alapul:

Root CA

- Operációs rendszer (Debian Linux 3.0 + X),
- Kernel-verzió: 2.4.25-andrews (grsec security patch),
- Minősített tanúsítvány kibocsátó alkalmazás (iPlanet CMS 4.2 SP2),
- Kriptográfiai hardver modul PCI csatolón (HSM).

Operational CA

- Operációs rendszer (Debian Linux 3.0 + X),

- Kernel-verzió: 2.4.25-andrews (grsec security patch),
- Minősített tanúsítvány kibocsátó alkalmazás (iPlanet CMS 4.2 SP2),
- Kriptográfiai hardver modul PCI csatolón (HSM).

Trusted Time StampServer (kettő darab)

A Trusted Time StampServer Rack Mount

A TSS rendszerbe két darab Trusted Time StampServer SA200n kerül beépítésre. Az SA200n **2048 bites kulcshossz esetén** másodpercenként **50** időpecsét előállítására képes.

- Windows 2000 alapú szerver(ek),
- A szerver modul a host rendszer számára is biztosítja a megbízható időt, és garantálja, hogy 100 milliszekundumon belül marad az UTC időhöz képest,
- A TTS képes digitálisan aláírni az időbélyeget,
- A telepített szerverek a TCP alapú kommunikációt (RFC 3161) támogatják.

CardPerso *(standard PC kártyaolvasókkal, kártyanyomtatóval és PIN borítéknyomtatóval)*

- Operációs rendszer Windows 2000,
- Fejlesztett megszemélyesítő alkalmazás, InterBase adatbázis.

Registration Manager (HSM +SFTP server)

- Operációs rendszer (Debian Linux 3.0 + X),
- Kernel verzió 2.4.25-andrews (grsec security patch),
- Kriptográfiai hardver modulok (HSM),
- Tűzfal (FW). Saját csomagszűrő FW-t (IP Tables) működtet.

LDAP (Master LDAP, Auth.LDAP)

- Operációs rendszer (Debian Linux 3.0 + X),
- Kernel verzió: 2.4.25-andrews (grsec security patch).

Tartaléka az Operational CA gépnek, ennek érdekében a CA telepítéséhez szükséges környeztet is tartalmazza.

(Auth. LDAP, Master LDAP)

Nyilvános LDAP szerviz (HA gép-pár)

- Operációs rendszer [Debian Linux 3.0 + HA (HeartBeat HA szoftver)],
- Kernel verzió 2.4.25-andrews (grsec security patch),
- Tűzfal; Saját csomagszűrő FW-t (IP Tables) működtet.

Tűzfal ALF (HA gép-pár)

- Operációs rendszer (Debian Linux 3.0 + X),
- Kernel verzió 2.4.25-andrews (grsec security patch),
- Saját csomagszűrő FW-t (IP Tables) működtet.

A ***Regisztrációs Szervezet*** olyan megbízható informatikai rendszert alkalmaz, mely az alábbi termékeken alapul:

Registration Agent

- Operációs rendszer Windows XP,
- Fejlesztett RA alkalmazás.

Az **operációs rendszerek** által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a központi adminisztrátori hozzáférések és tevékenységek rögzítése, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása),

- a felhasználói adatok védelme (a **hozzáférés ellenőrzési** szabályok alapjainak érvényre juttatása /rendszer fájlok védelme, a felhasználói adatok csak alkalmazáson keresztüli elérésének biztosítása/, a tárolt adatok sértetlenségének védelme /beleértve a vírusok, káros és engedély nélküli szoftverek elleni védekezés támogatását is/, a maradvány információ védelmének megvalósítása),
- **azonosítás és hitelesítés** (a központi adminisztrátorok azonosítása és hitelesítése, az operációs rendszer által biztosított funkciók elérésének sikeres hitelesítéshez kötése),
- **biztonságkezelés** (a biztonsági szerepkörök kezelése, a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
- **biztonsági funkciók** megbízható **védelme** (alap biztonsági tesztelés végrehajtása, biztonságos állapot megőrzése hiba esetén, a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása, a különböző alkalmazói folyamatok által használt tartományok elkülönítése).

Az **alkalmazások** által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a rendszeroperátori hozzáférések és tevékenységek rögzítése),
- **biztonságos kommunikáció** (a Hitelesítő Szervezet és a regisztrációs szervezet közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása /a kriptográfiai hardver modulok megfelelő funkcióinak aktivizálásával/),
- **felhasználói adatok védelme** (a hozzáférés ellenőrzési szabályok érvényre juttatása /az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják/, a maradvány információ védelmének támogatása),
- **azonosítás és hitelesítés** (a rendszeroperátorok azonosítása, hitelesítése, az alkalmazások által biztosított funkciók elérésének sikeres hitelesítéshez kötése).

A **kriptográfiai hardver modulok** által megvalósított biztonsági funkciók részletesen az N CIPHER nShiel/payShield User Guide /Linux/ dokumentációjában találhatók.

A **tűzfal** által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a hálózati kommunikáció naplózása, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),
- **felhasználói adatok védelme** (az információ áramlás ellenőrzési szabályok érvényre juttatása /szűrés, a tiltott információ áramlás megakadályozása, megfigyelése,)
- **azonosítás és hitelesítés** (központi adminisztrátorok/ azonosítása, hitelesítése, a tűzfal funkciók elérésének sikeres hitelesítéshez kötése),
- **biztonsági funkciók** megbízható **védelme** (az információ áramlás ellenőrzés megkerülhetetlenségének biztosítása).

6.5.2 Informatikai biztonsági minősítés

A *Hitelesítő Szervezet* olyan megbízható informatikai rendszert alkalmaz, mely az alábbi komponenseken alapul:

- operációs rendszer Debian Linux 3.0 + X,
- tanúsítvány kibocsátó alkalmazás (CA),
- saját csomagszűrő FW-t (IP Tables) működtet.

A *Hitelesítő Szervezet* informatikai rendszerében alkalmazott kriptográfiai hardver modulok minősítésére vonatkozóan lásd a {**6.2.1 *Kriptográfiai modulra vonatkozó szabványok***} és {**6.7 *A kriptográfiai modul ellenőrzése***} alfejezeteket.

A *Regisztrációs Szervezet* olyan megbízható informatikai rendszert alkalmaz, mely az alábbi, komponenseken alapul:

- Windows XP,
- fejlesztett RA kliens alkalmazás.

A *Regisztrációs Szervezet* informatikai rendszerében alkalmazott intelligens kártyákra vonatkozóan lásd a {**6.2.1 *Kriptográfiai modulra vonatkozó szabványok***} és {**6.7 *A kriptográfiai modul ellenőrzése***} alfejezeteket.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

Annak érdekében, hogy a *Hitelesítő Szervezet* és a *Regisztrációs Szervezet* valamennyi rendszerfejlesztési projektjében a biztonság követelményeit magas színvonalon biztosítsák, a teljes fejlesztés során (már a tervezési és követelmény-meghatározási fázisban is) figyelembe vegyék a különös követelményeket.

6.6.2 Biztonságkezelési óvintézkedések

A *Hitelesítő Szervezet* és a *Regisztrációs Szervezet* szolgáltatásai nyújtásához olyan termékeket használ, amelyek biztosítják a tanúsítványtípus biztonságkezelésre vonatkozó elvárásait, a helyes konfigurációt megalapozó megfelelő útmutató dokumentációk használatával, valamint a helytelen használat lehetőségének és egyéb sebezhetőségek vizsgálata, útján.

6.6.3 Az életciklusra vonatkozó biztonság osztályozása

A *Hitelesítő Szervezet* és a *Regisztrációs Szervezet* által a szolgáltatások nyújtásához használt termékek, életciklusra vonatkozó biztonsági szempontok figyelembevételével kerültek alkalmazásra.

6.7 Hálózatbiztonsági óvintézkedések

Hitelesítő szervezet

A *Hitelesítő Szervezet* és a *Regisztrációs Szervezet* közötti kommunikáció (belső hálózat) védett a bizalmasság, sértetlenség és letagadhatatlanság elvesztése ellen. A magas szintű védelmet titkosítással és digitális aláírással biztosítják A *Hitelesítő Szervezet* külső kommunikációt nem folytat a végfelhasználókkal.

Regisztrációs szervezet

A *Regisztrációs Szervezet* informatikai rendszer segítségével egyáltalán nem folytat kommunikációt a végfelhasználókkal.

6.8 A kriptográfiai modulok ellenőrzése

Az alábbi táblázat tartalmazza a hitelesítés-szolgáltató által alkalmazott kriptográfiai hardver modulokra nézve, az ezek ellenőrzése, bevizsgálása és értékelése során megállapított legfontosabb tényeket, tulajdonságokat:

Kriptográfiai modul	HSM nChiper/nShield
A modul fizikai konfigurációja	• Önálló modul
Szolgáltatások	• kriptográfiai műveletek (kódolás, dekódolás, üzenet sértetlenség, digitális aláírás generálás, digitális aláírás ellenőrzés) • kulcsmenedzsment (kulcs generálás, védett kulcstárolás, kulcs klónozás, „n-ből m” aktivizálás, kulcs nullázás,) • kriptográfiai menedzsment funkciók (naplózási paraméterek bevitele és beállítása, alarm kezelés és “resetel”-és) • felhasználó által választható ön-tesztek végrehajtása (kriptográfiai algoritmus tesztek, szoftver/förmver tesztek, a kritikus funkciók tesztjei, statisztikus véletlenszám generátor teszt) • "státusz kijelzés" (a következőket jelzik ki: aktív szerepkör, a modul kriptográfiai státusza /nullázott, beavatkozás következményeként fellépő, betöltött, inicializált/, hiba kód (ha a modul hiba állapotban van)
Az operációs rendszer biztonsága	A modulok nem nyújtanak olyan eszközt, amelynek segítségével egy operátor a modul hatáskörébe nem tartozó szoftvereket / förmvereket tölthet be és hajthat végre. Ezért ez a kérdéskör jelen modulokra nem releváns.
Kriptográfiai kulcskezelés	A modulok védik a tárolt titkos és magánkulcsokat a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben. A modulok védik a tárolt nyilvános kulcsokat a jogosulatlan módosítással és kicseréléssel szemben. A kulcsgenerálás és a kulcs megsemmisítésének módszere szabványos és biztonságos
Kriptográfiai algoritmusok	A modulok FIPS által jóváhagyott algoritmusokat alkalmaznak.

Öntesztek	A modulok képesek öntesztek végrehajtására, annak kimutatására, hogy megfelelően működnek
Értékelési szint	FIPS 140-1 szabvány szerint 3. szinten bevizsgált

7. Tanúsítvány-, CRL- és időbélyeg-profilok

7.1 Tanúsítványprofil

Szolgáltató által kibocsátott **végfelhasználói tanúsítvány**ok alap mezői a következők:

Mezőnév	Érték vagy szabály
Verzió *Version*	A tanúsítvány a [12] ajánlás 3. verziójának felel meg {ld. **9 *Hivatkozások***}. Ebbe a mezőbe az „**x.509v3**” adat kerül a tanúsítványokon.
Sorozatszám *Serial Number*	A tanúsítványok sorozatszáma **12 karakter** hosszúságú egyedi szám, amelyet a *Hitelesítő Szervezet* ad ki.
Algoritmus azonosító *Signature Algorithm Identifier*	Ez a szám a *Szolgáltató* **tanúsítványokat hitelesítő elektronikus aláírás**ának algoritmusát azonosítja {ld. **7.1.3**}.
Aláírás *Signature*	A *Szolgáltató* tanúsítványt hitelesítő **elektronikus aláírása**, amelyet a [9] szerint generál és kódol.
Kibocsátó *Issuer*	A tanúsítványt kibocsátó *Hitelesítő Szervezet* egyedi azonosítója {ld.**3.1.1** és **7.1.4**}.
Érvényesség *Valid From & Valid To*	A tanúsítvány érvényességének kezdete és vége {ld. **4.7**}, amely UCT szerinti érték a [9] szerinti kódolással.
Aláíró (tulajdonos) **azonosító** *Subject*	Az *aláíró* (tulajdonos) egyedi neve {ld. **3.1.1** és **7.1.4**}.
Aláíró nyilvános kulcsának algoritmus-azonosítója *Subject Public Key Algorithm Identifier*	Ebbe a mezőbe az aláírói nyilvános kulcs algoritmusának azonosítója kerül {ld. **7.1.3**}.
Aláíró nyilvános kulcsa *Subject Public Key Value*	Az aláíró nyilvános kulcsa.
Kibocsátó egyedi azonosító *Issuer Unique Identifier*	A *Szolgáltató* nem tölti ki.
Aláíró egyedi azonosító *Subject Unique Identifier*	A *Szolgáltató* nem tölti ki.

7.1.1 Verzió szám(ok)

Szolgáltató a [12] ajánlás 3. verziójának megfelelő szolgáltatói és végfelhasználói tanúsítványokat bocsát ki.

7.1.2 Tanúsítvány-kiterjesztések

Szolgáltató által kibocsátott végfelhasználói tanúsítványok kiterjesztései a következők[61]:

Mezőnév	Érték vagy szabály	Kritikus
Tanúsítványtípusok *Certificate Policies*	Policy Identifier=1.3.6.1.4.1.17835.7.1.2.8.2.1.12.2.1.1 Policy Qualifier=http://www.eszigno.matav.hu User Notice="A tanúsítvány elfogadása előtt ismerje meg a Tanúsítványtípus Szabályzat és a minősített HSZSZ előírásait a http://www.eszigno.matav.hu internetoldalakon"{ld. **7.1.6**}	Nem
Alapvető megkötések *Basic Constraints*	Subject Type=End Entity Path Length Constraint=None	Nem
Kulcshasználat *Key Usage*	NonRepudiation	Igen
CRL szétosztási pont *CRL Distribution Points*	A ldap://cimtar.matav.hu/ internetcímen. Továbbá: URL=ldap://trustcenter.matav.hu:389/CN=Matav%20Minositett%20CA,C=HU Class=CertificationAuthority	Nem
Megfelelőség *QC Compliance* OID**: .....**	A Szolgáltató kijelenti, hogy ez a tanúsítvány - a 2001. évi XXXV. törvény és végrehajtási rendeletei alapján - minősített tanúsítvány.	Nem
Tranzakciós limit *Transaction limit* OID:	10.000.000 HUF 100.000.000 HUF 500.000.000 HUF (megállapodás alapján)	Nem
Adatmegőrzési idő *Retention time of data* OID: **.....**	A Szolgáltató kijelenti, hogy a jelen tanúsítványhoz kapcsolódó dokumentációt a 2001 évi XXXV. törvény alapján, a tanúsítvány lejártát követő **10 évig**, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus	Nem

[61] A minősített végfelhasználói tanúsítványra vonatkozó 2/2002 MeHvm irányelvnek és az ETSI szabványnak megfelelően.

	dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi.	
Megjegyzés *Netscape Comment*	Figyelem! Ez a Matáv által BALE-eszközön kibocsátott minősített üzleti tanúsítvány, amelyre a Szolgáltató szabályzata vagy egyedi megállapodás szerinti értékhatárig vállal felelősséget. További információk a www.eszigno.matav.hu weboldalon..	

Valamennyi fenti kiterjesztés kitöltésre kerül.

7.1.3 A tanúsítványok algoritmus objektum-azonosítója

Szolgáltató a tanúsítványok aláírásakor az **Sha-1** *RSA algoritmus*t (1024 bit) használja. A **végfelhasználói tanúsítványok** lenyomatképző **algoritmusazonosítója**: OID=1.2.840.113549.1.1.5 a [9] szerint.

7.1.4 Elnevezési formák

Szolgáltató a **tanúsítvány kibocsátó azonosító** és az **aláíró-azonosító** esetében az egyedi X.500 név formátumot alkalmazza, a **3.1.1** alfejezet szerint.

7.1.5 Elnevezésre vonatkozó korlátozások

A *Szolgáltató* által kibocsátott **tanúsítványok** nem tartalmazhatnak álnevet.

7.1.6 Tanúsítványtípus objektum-azonosító

A *Szolgáltató* által kibocsátott tanúsítványok a **minősített végfelhasználói tanúsítványtípus** egyedi objektum-azonosítóját tartalmazzák {ld. **7.1.2** ***Tanúsítvány-kiterjesztések***}.

7.1.7 A „tanúsítványtípus korlátozás” kiterjesztés használata

Szolgáltató ezt a kiterjesztést nem használja.

7.1.8 Szabályzatminősítő szintaxis és szemantika

A *Szolgáltató* által kibocsátott tanúsítványok a szolgáltatási szabályzatának internetcímét, valamint figyelmeztető szöveget tartalmaznak {ld. **7.1.2** ***Tanúsítvány-kiterjesztések***}.

7.1.9 A kritikus tanúsítványtípus kiterjesztés feldolgozása

Szolgáltató által alkalmazott szabályzat-kiterjesztés nem kritikus. Mindazonáltal *Szolgáltató* előírásainak és kikötéseinek figyelmen kívül hagyásáért a végfelhasználók a felelősek.

7.2 Tanúsítvány visszavonási lista (CRL) profil

Szolgáltató által kibocsátott **visszavonási listák** alap mezői a következők:

Mezőnév	Érték vagy szabály
Verzió *Version*	A tanúsítvány visszavonási lista a [12] ajánlás 2. verziójának felel meg {ld. **7.2.1**}.
Algoritmus azonosító *Signature Algorithm Identifier*	Ez a szám *Szolgáltató* **visszavonási listát hitelesítő elektronikus aláírásá**nak algoritmus azonosítója: **SHA-1** (OID=1.2.840.113549.1.1.5).
Aláírás *Signature*	*Szolgáltató* visszavonási listát hitelesítő elektronikus aláírása a [9] szerint generálva és kódolva.
Kibocsátó *Issuer*	A visszavonási listát kibocsátó Hitelesítő Szervezet és egység egyedi azonosítója {ld. **3.1.1** és **7.1.4**}.
Hatályba lépés *Effective Date*	A visszavonási lista hatályba lépésének kezdete. *Szolgáltató* által kibocsátott tanúsítványok esetében ez megegyezik a kibocsátás idejével. UCT szerinti érték a [9] szerinti kódolással.
Következő kibocsátás *Next Update*	A következő visszavonási lista kibocsátásának ideje {ld. **4.4.9**}. UCT szerinti érték a [9] szerinti kódolással.
Visszavont tanúsítványok *Revoked Certificates*	A visszavont tanúsítványok listája a tanúsítvány sorozatszámával és a visszavonás idejével.

7.2.1 Verzió szám(ok)

Szolgáltató a [12] ajánlás 2. verziójának megfelelő **visszavonási listákat** bocsát ki.

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

Szolgáltató által használt **visszavonás bejegyzési kiterjesztések** a következők:

Mezőnév	Érték vagy szabály	Kritikus
Visszavonás oka *Reason Code*	……..…[62]	Nem
Érvénytelenség ideje *Invalidity Date*	……..[63]	Nem
Útmutató *Hold Instruction*	……..[64]	Nem

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

Szolgáltató által kitöltött **visszavonási lista kiterjesztések** a következők:

Mezőnév	Érték vagy szabály	Kritikus
CRL sorozatszám *CRL number*	……[65]	Nem

[62] Ebbe a mezőbe a visszavonás oka kerül.

[63] Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerül.

[64] Ebbe a mezőbe a felfüggesztett tanúsítvány kezelése kerül.

[65] Ebbe a mezőbe a visszavonási listák egyesével növekvő sorozatszámai kerülnek.

8. Leírás-adminisztráció

A Szolgáltató a szolgáltatási tevékenység bejelentése előtt elkészíti hitelesítésszolgáltatási szabályzatát (jelen szabályzatot), amelyet a szolgáltatási tevékenység megkezdésével egyidejűleg nyilvánosságra hoz és az ügyfélforgalom számára nyitva álló helyiségben, valamint interneten elérhetővé tesz.

8.1 Leírás-változtatási eljárások

8.1.1 Szabályzat-változtatási eljárások

Szolgáltató szervezetén belül *Szabályozási Egység* működik, amely a hitelesítésszolgáltatással kapcsolatos szabályzatok létrehozásáért és karbantartásáért felelős. E csoport gyűjti össze a változtatási igényeket, majd elvégzi a módosításokat, továbbá életbe lépteti a változtatásokat, és végül a (belső és külső) tájékoztatási kötelezettségeknek is eleget tesz.

A *Szabályozási Egység* a változtatásokat összegyűjti, majd belső, nem nyilvános munkaváltozatokat hoz létre a megváltoztatott szabályzatokból, melyek a közzététel előtt még belső **felülvizsgálaton** is átesnek. *Szolgáltató* a változásokat kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A hitelesítésszolgáltatással kapcsolatos szabályzatok módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

8.1.2 Értesítés nélkül változtatható elemek

Szolgáltató névcsere, hibás névírás, szám, vagy számítási hiba vagy más hasonló elírás, kontaktadatok változása esetén **fenntartja a jogot** a Szabályzat elemeinek előzetes értesítés és bejelentés nélküli megváltoztatására.

8.1.3 Értesítéssel változtatható elemek

Minden, a **8.1.2.** pont körén kívül eső, - a tanúsítványok biztonsági szintjét, felhasználhatóságát módosító - értesítésre kötelezett változtatás a **8.2** alfejezet szerint történik.

8.1.4 Észrevételek kezelése

A **8.2** alfejezet szerint közzétett új szabályzattal kapcsolatos észrevételeket *Szolgáltató* a hatályba lépést megelőző **14 napig** fogadja a Regisztrációs Szervezet internetcímén. A szabályzat észrevételekkel módosított változatát szolgáltató a hatályba lépést megelőző **7. nap** zárja le és teszi közzé.

8.1.5 Szabályzati objektum-azonosítót vagy -mutatót változtató módosítások

Minden olyan jelentősebb módosítás, melyet a *Szolgáltató* csak az újonnan kibocsátásra kerülő tanúsítványok esetében alkalmaz (a már kibocsátottak esetében nem) a Szabályzat verziószámának fő jegyét és a Szabályzat objektum-azonosítóját is módosítja.

8.2 Közzétételi és tájékoztatási elvek

8.2.1 A szabályzatban nem tárgyalt elemek

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

8.2.2 A szabályzat közzététele

Szolgáltató hitelesítésszolgáltatási szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően **30 nappal** közzéteszi internetes honlapján, a http://www.eszigno.matav.hu internetoldalakon. *Szolgáltató* alkalmanként ezt megelőzően is tájékoztatja a közösséget a tervezett változtatásairól.

8.3 Szolgáltatás szabályzat jóváhagyási eljárások

Jelen szolgáltatási szabályzat [10] szabványnak valamint a ***Nyilvános körben kibocsátott, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő, minősített tanúsítványtípus***nak ***[MTT+BALE]*** való megfelelőségét közzététel előtt *Szolgáltató* megvizsgálta. A vizsgálatot a tanúsítást végző szervezet is elvégzi évente rendszeresen végzett auditja során.

A szabályzat törvényeknek[66] való megfelelőségét a *Hatóság* is megvizsgálta a szabályzat hatályba lépését megelőzően.

Szolgáltató a hitelesítésszolgáltatási szabályzatának a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően **30 nappal** átadja a *Hatóság* részére. *Szolgáltató* alkalmanként ezt megelőzően is konzultál a *Hatósággal* a tervezett változtatásairól.

[66] a 2001. évi XXXV. törvény az elektronikus aláírásról

9. Hivatkozások

A *Szolgáltató* a jelen dokumentumban az alábbi dokumentumokra hivatkozik:

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

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

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

[4] Minősített tanúsítványtípus minták minősített hitelesítés-szolgáltatók számára, v1.0 ---

[5] ISO 3166

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

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

[8] ETSI TS 101 862 Minősített tanúsítvány profil

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

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

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

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

[13] A minősített tanúsítványtípus mintáknak megfelelő szolgáltatási szabályzat minták, v1.0 ---

[14] Nyilvános körben kibocsátott, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő, minősített Tanúsítványtípus Szabályzat, ill. tanúsítványtípus [MTT+BALE] ---Matáv Rt.

[15] Általános Szerződési Feltételek (**ÁSzF**)--- Matáv Rt.

[16] Matáv e-Szignó® Minősített Hitelesítésszolgáltatás Szolgáltatói Szerződése – röviden Szolgáltatói Szerződés (**SzSz**)

10. Jelölések, rövidítések és meghatározások

A dokumentumban az alábbi jelölések és rövidítések szerepelnek:

- [**MTT+BALE**]**:** Nyilvános körben kibocsátott, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő, minősített tanúsítványtípus,
- [ ] jelek között a dokumentumokra történő hivatkozások számai szerepelnek.

A Szolgáltató a dokumentumban szereplő fogalmakat az alábbi értelemben használja:

Fogalom	Meghatározás (magyarázat)
aktivizáló adatok	a kriptográfiai modul működtetéséhez szükséges adatok, melyeket védeni kell (pl. PIN kód, jelmondat vagy manuálisan birtokolt kulcs-részlet)
aláírás-ellenőrző adat (az aláíró nyilvános kulcsa)	olyan egyedi adat, (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ
aláírás-létrehozó adat (az aláíró magánkulcsa)	olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ
aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön	az aláírás-létrehozó eszközök elkészítése és az aláíró részére történő átadása
aláírás-létrehozó eszköz	olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza
aláíró (aláíró fél)	az a természetes személy, akihez az elektronikus aláírás hitelesítés-szolgáltató (hitelesítés-szolgáltató) által közzétett aláírás-ellenőrző adatok jegyzéke szerint az aláírás-ellenőrző adat kapcsolódik
biztonságos aláírás-létrehozó eszköz	a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény (Eat.) 1. számú mellékletében foglalt követelményeknek

	eleget tevő aláírás-létrehozó eszköz

Fogalom	Meghatározás (magyarázat)
elektronikus aláírás	elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum
elektronikus dokumentum	elektronikus eszköz útján értelmezhető adat, mely elektronikus aláírással van ellátva
elektronikus aláírás ellenőrzése	az elektronikus dokumentum tartalmának összevetése aláíráskor, illetve ellenőrzéskor, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, valamint a *tanúsítvány* felhasználásával
elektronikus aláírás felhasználása	elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése
elektronikus irat	olyan elektronikus dokumentum, mely szöveget és más olyan adatot (pl. fejlécet) tartalmaz, amely legfeljebb a szöveg illusztrálására, azonosítására szolgál, továbbbá digitális jeleket is tartalmaz (az olvasó számára közvetlenül nem érzékelhető módon) a szöveggel összefüggő informatikai funkciók megvalósítása érdekében
elektronikus okirat	olyan elektronikus irat, mely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy nyilatkozat kötelezőnek elismerését foglalja magában. Az elektronikus okirat fogalmát az eljárási törvényekben szereplő okirati bizonyítási eszközök virtuális megfelelőjeként hozza létre a Javaslat, azok hagyományos meghatározásával összhangban
elektronikusan történő aláírás	elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz
előfizető	szolgáltatónál egy vagy több aláíró nevében előfizető entitás, aki közvetlenül vagy közvetve elfogadja szolgáltató kikötéseit és feltételeit
érintett fél	az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el
eszköz-szolgáltató	olyan hitelesítés-szolgáltató, amely a hitelesítésszolgáltatás mellett az aláírás-létrehozó adat elhelyezése az aláírás-létrehozó eszközön szolgáltatást is felvállalja

Fogalom	Meghatározás (magyarázat)
fogadó fél (elfogadó fél)	az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el
fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető, olyan eszközökkel hozták létre, melyek kizárólag az aláíró befolyása alatt állnak és a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető. Az ilyen fajta elektronikus aláírást is hitelesítés-szolgáltató tanúsítja, de az aláírás technológiája, biztonsági foka vagy a hitelesítés-szolgáltató körülményei nem valósítják meg a minősített elektronikus aláírás követelményeit
hitelesítésszolgáltatási szabályzat	a 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat
hitelesítés-szolgáltató	személy (szervezet), amely a hitelesítésszolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványokhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány visszavonási listát
időbélyeg (időbélyegző)	elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját, és amely a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető
időbélyegzés-szolgáltató	olyan szolgáltató, amely az időbélyegzés szolgáltatást felvállalja
igénylő	Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki e-szignó minősített hitelesítésszolgáltatást *aláíró*ként vagy *előfizető*ként kíván igénybe venni.
kriptográfiai kulcs	olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és

	visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges

Fogalom	Meghatározás (magyarázat)
kulcsgondozás	a kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, szoros kapcsolatban az alkalmazott biztonsági eljárásmóddal
minősített elektronikus aláírás	olyan – fokozott biztonságú – elektronikus aláírás, amely biztonságos aláírás-létrehozó eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki
nyilvános (publikus) kulcsú infrastruktúra	tanúsítványok létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is
regisztrációs szervezet	szervezet, amely ellenőrzi a tanúsítvány aláírójának személyazonosságát. Egy Hitelesítő Szervezet több ilyen szervezettel is együttműködhet.
tanúsítvány	hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot a 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát
tanúsítvány-előállítás	tanúsítványok létrehozása és a hitelesítés-szolgáltató által történő aláírása (a regisztrációs szolgáltatásra alapozva)
tanúsítvány kibocsátás	egy tanúsítvány rendelkezésre bocsátása az aláíró számára, valamint a tanúsítvány közzététele a hitelesítés-szolgáltató nyilvántartásában
tanúsítvány megújítás	új tanúsítvány biztosítása, melyben az aláíró megváltozott új nyilvános kulcsát és régi adatait a hitelesítés-szolgáltató (új érvényességi időtartamra) érvényes magánkulcsával aláírja
tanúsítvány visszavonási állapot közzététele	Információ nyújtása az elfogadó fél számára a tanúsítványok visszavonásáról. A szolgáltatás lehet valós idejű, vagy az információk előre meghatározott időközönkénti aktualizálásán kell alapulnia.
tanúsítvány visszavonási lista	valamely okból visszavont, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a hitelesítés szolgáltató bocsát ki

Fogalom	Meghatározás (magyarázat)
tanúsítvány visszavonási nyilvántartás	nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját
tanúsítványtípus	szabályok összessége, amely megmutatja adott tanúsítványok alkalmazhatóságát egy bizonyos közösségre, illetve alkalmazások olyan csoportjára, ahol azonosak a biztonsági követelmények
végfelhasználó	az aláíró, az előfizető, valamint az elfogadó fél

1. Melléklet: A regisztrációhoz szükséges adatok

Az alább felsorolt iratokat a *Minősített e-Szignó Hitelesítésszolgáltatás* regisztrációja során a **Regisztrációs tisztviselő** gyűjti össze.

A szolgáltatás **nem lakossági** ügyfeleket (jelen dokumentumban: szervezeteket) szolgál ki. A tanúsítványt a szervezetben található természetes személyek részére adjuk ki (aláírók), mint a szervezet dolgozója/képviselője vagy bármilyen tagja.

Az alábbi iratok összegyűjtése szükséges:

- Amennyiben a szervezet **gazdasági szervezet** 1 hónapnál nem régebbi eredeti cégkivonat (gazdasági szervezetek listája lásd 2. pont),
- Amennyiben **nem gazdasági szervezet** a 3. pontban felsorolt iratok azonosítják a szervezetet,
- A **szervezet vezetőjének aláírási címpéldánya** (eredeti, vagy hiteles másolat),
- Megfelelően (Regisztrációs tisztviselő által vagy az előfizető/aláíró által) kitöltött és minden igénylő (aláíró) és a szervezet vezetője (aláírásra jogosult személy) által **aláírt szolgáltatási szerződés** (eredeti) és annak mellékletei,
- Minden igénylő **(aláíró) személyazonosságát** garantáló iratainak fénymásolata (lásd 1. pont).

1. A <u>személyek</u> azonosságát garantáló iratok:

A következő okmányok közül legalább 1 szükséges:

- 1992. január 1. után kiállított útlevél,
- 1993. július 1. után kiállított személyazonosító igazolvány (személyi),
- 2001. január 1. után kiállított vezetői engedély (jogosítvány).

<u>Megjegyzés</u>: a 2000. január 1. után kiállított személyazonosító igazolvány (kártyás személyi) csak a lakcím-azonosító igazolvánnyal (lakcímkártya) együtt fogadható el.

2. A <u>gazdasági szervezetek</u> tételes fölsorolása:

- Közkereseti társaság (Kkt.)
- Betéti társaság (Bt.)
- Közös vállalat (Kv.)
- Korlátolt felelősségű társaság (Kft.)
- Részvénytársaság (Rt.)
- Egyesülés
- Vállalat
- Egyéb állami gazdálkodó szerv
- Szövetkezet
- Közhasznú társaság (Kht.)
- Vízgazdálkodási társulat
- Erdőbirtokossági társulat
- Külföldiek magyarországi közvetlen kereskedelmi képviselete
- Oktatói munkaközösség
- Külföldi vállalkozás magyarországi fióktelepe
- Végrehajtói iroda

3. Egyéb (nem gazdasági) szervezetektől bekérendő iratok

A személyekre vonatkozóan az 1. pontban feltüntetett személyazonosságot igazoló okiratok az alább felsorolt iratokon felül továbbra is szükségesek.

MRP (Munkavállalói Résztulajdonosi Program szervezete); Egyház; Párt; Nyugdíjpénztár; Egyesület; Sportági országos szakszövetség; Alapítvány; Közalapítvány	▪ **kivonat** a szervezetről a nyilvántartásba vevő bíróságtól, ▪ a képviseletre jogosult személy **aláírási címpéldánya** (eredeti vagy hiteles másolat).
Költségvetési szerv (önkormányzatok, minisztériumok stb.)	▪ **igazolás** az Államháztartási Hivatal által vezetett nyilvántartásból, ▪ a **kinevezésről szóló dokumentum**, ▪ a szerv vezetőjének **aláírási címpéldánya** (eredeti vagy hiteles másolat).
Köztestület (különösen MTA, szakmai és gazdasági kamarák)	▪ a képviseletre jogosult személy **aláírási címpéldánya** (eredeti vagy hiteles másolat), ▪ Ha bírósági nyilvántartásba került, akkor **kivonat** a nyilvántartásból. ▪ Ha nem került bírósági nyilvántartásba, akkor: a **létrehozásáról szóló törvényt tartalmazó**, valamint a képviseletére **jogosult személy kinevezését tartalmazó** *Magyar Közlöny* egy-egy példánya, ▪ a köztestület **alapszabálya**.
Egyéni vállalkozó	▪ az **egyéni vállalkozói igazolvány**
Közoktatási intézmények	▪ **Kivonat** az oktatási intézményt nyilvántartásba vevő szerv nyilvántartásából (költségvetési

	szerv esetén a nyilvántartást vezető szerv, más esetben jegyzőnél vagy főjegyzőnél), ▪ a képviseletre jogosult személy **aláírási címpéldánya** (eredeti vagy hiteles másolat).
Felsőoktatási intézmények ***Megjegyzések***: A felsőoktatási intézmények vezetői: ▪ egyetemek - **rektor** ▪ többkarú főiskola - **főiskolai rektor** ▪ karokra nem tagozódó főiskola – **főigazgató** Az első kategóriát a köztársasági elnök, a másodikat és a harmadikat a miniszterelnök nevezi ki és menti fel, tehát tőlük származik egy **kinevező okirat**. A felsőoktatási törvény I. számú melléklete tartalmazza a Magyarországon jelenleg működő összes felsőoktatási intézmény jegyzékét (ezt a listát a törvény mindig tartalmazza, tehát mindig elegendő megnézni **az éppen hatályos felsőoktatási törvényt**).	▪ **Jogszabály**, ▪ **alapító okirat** (szervezet neve és címe), ▪ a **kinevezésről szóló dokumentum** (a jegyzésre jogosult személy /jjsz/ igazolásához), ▪ a képviseletre jogosult személy **aláírási címpéldánya** (eredeti vagy hiteles másolat). "Ha a szervezet rendelkezik **adószámmal** és az általunk bekért dokumentumok azt nem tartalmazzák, kérjük azt az APEH-től származó, adószámról szóló **értesítéssel** vagy **adószám igazolással** igazolja."