T · · Systems ·

Magyar Telekom

Minősített e-Szignó® hitelesítésszolgáltatás és Időbélyegzés-szolgáltatás Szolgáltatási Szabályzata

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.8.2.1.13.3.6

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.11.3.13.1.6

Verziószám: **1.71**

Regisztrációs szám: .....

Hatályba lépés dátuma:.....2007.04.10.

T · · Systems ·

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
1.3	2005-09-01	Magyar Telekom névváltásának és következményeinek módosítása
1,4	2005-11-15	Hatósági ellenőrzést követő változások átvezetése
1.5	2005-12-30	Hatósági és külső ellenőrzéseket követő változások átvezetése
1.6	2006-07-20	Nemzeti Hírközlési Hatóság Hivatalának észrevételei szerinti javítások
1.7	2006-12-18	Ket.-es fejlesztésekhez és a 2006. évi Hatósági szemléhez kapcsolódó módosítások
1.71	2007-03-10	Hatósági észrevételek szerint valamint az rfc3647szerint módosított változat

		Aláírás
Módosítást készítette: Kővári Ferenc	vezető termékmenedzser	.....
Ellenőrizte: Springel János	Biztonsági tisztviselő Magyar Telekom Nyrt.	.....
Jóváhagyta: Dr. Petrányi Dóra	Jogi Ágazat Magyar Telekom Nyrt.	.....

T · · Systems ·

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).

Az [1] törvény[1] {ld. 1.8 Hivatkozások} az **elektronikus aláírás**ok alábbi három (biztonsági) szintjét nevezi meg:

- **Elektronikus aláírás**, amely „elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat".
- **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 a dokumentumon tett – **módosítás** érzékelhető.**"**
- **Minősített elektronikus aláírás**, amely „olyan – fokozott biztonságú – elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki."

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

1.1 Áttekintés

1.1.1 A Szabályzat

Ez a szabályzat a **Magyar Telekom Nyrt.** (ebben a dokumentumban: Szolgáltató) **minősített** hitelesítés-szolgáltatói tevékenységével[2] kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazza.

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

[2] ld. [1] törvény 2. § (18)

A Szabályzat célja, hogy összefogja azokat a dokumentumokat és információkat, melyeket a Szolgáltatóval 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, az ÁSZF ([15]), az igényelt tanúsítványfajtára vonatkozó Hitelesítési Rend (nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványtípus esetén a [14], a közigazgatásban alkalmazható, biztonságos aláírás létrehozó eszköz használatát megkövetelő, aláírás célú minősített tanúsítványok esetén a [19] szerinti dokumentumban rögzített [MHR_Ü] illetve [MHR_K] hitelesítési rendek), valamint az aláíróval / előfizetővel megkötött szerződés ([16]) együttesen szabályozzák {ld. **1.8** Hivatkozások}. Amennyiben a Hitelesítési Rendek, az ÁSZF, valamint jelen szabályzat bármely vonatkozásban ellentmondással vagy eltérő kikötéssel élnének, akkor a vonatkozó Hitelesítési Rend előírásai tekintendők irányadónak.

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.

Ezen belül a Szabályzat a következő hitelesítési rendekre illetve tanúsítványfajtákra vonatkozik:

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

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

- **[MHR_Ü] és [MHR_K]:** A közigazgatásban alkalmazható, biztonságos aláírás létrehozó eszköz használatát megkövetelő, aláírás célú minősített tanúsítványok

  Ezek gyakorlatilag a közigazgatási eljárásokban alkalmazható tanúsítványokat jelentik, melyeket a Szolgátlató köztisztviselők részére, illetve a közigazgatás egyéni és üzleti ügyfelei részére bocsát ki. A [19] dokumentum további adatokat tartalmaz ezen tanúsítványokra vonatkozóan.

Fenti tanúsítványfajtákon túl jelen Szabályzat vonatkozik a Magyar Telekom Minősített Időbélyegzés-szolgáltatás Időbélyezési Rendjére [17] is.

A Szabályzat területi hatálya

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

A Szabályzat időbeli hatálya

A Szabályzat határozatlan időre szól a címlapon 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 PKI szereplők**} minden egyes tagjára, természetes, jogi személyiségű illetve jogi személyiséggel nem rendelkező személyekre (szervezetekre) egyaránt kiterjed.

1.1.3 A szolgáltató

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

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

A Szolgáltató (Magyar Telekom Nyrt.) adatai a következők:

Név:	Magyar Telekom Távközlési Nyilvánosan Működő Részvénytársaság
Cégjegyzékszám:	CG 01-10041928
Székhely:	1013 Budapest, Krisztina krt. 55.
Postacím:	1541 Budapest
Telefon:	+36-1-458 7346
Fax:	+36-1-458 7335
Honlap:	www.magyartelekom.hu

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

1.1.4 Szolgáltatások

A Magyar Telekom Nyrt. 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 Magyar Telekom Nyrt. minősített **hitelesítésszolgáltatási tevékenysége** a következő elemekből áll:

a) **elektronikus aláírás** hitelesítésszolgáltatás

- **regisztráció**,
- **tanúsítvány-előállítás**,
- **tanúsítvány-kibocsátás**,
- (tanúsítvány) **visszavonás-kezelés**,
- (tanúsítvány) **visszavonási állapot közzététele**,
- **tanúsítvány megújítás**[3],
- **kulcscsere, tanúsítvány módosítás**[4],
- **viszontazonosítás**[5]

b) **időbélyegzés** szolgáltatás

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

A fenti elemek a következőeket jelentik:

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

b) **Tanúsítvány-előállítás**: 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.

c) **Tanúsítvány-kibocsátás**: A hitelesítés-szolgáltató szétosztja a **tanúsítvány**okat az **aláíró**k között, és közzé teszi az **érintett fel**ek részére is.

[3] Csak közigazgatási tanúsítványok esetén

[4] Csak közigazgatási tanúsítványok esetén

[5] Csak közigazgatási tanúsítványok esetén

d) **Visszavonás-kezelés**: A hitelesítés-szolgáltató fogadja és 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**: A hitelesítés-szolgáltató **tanúsítvány-visszavonás státus információt** szolgáltat az **érintett fel**eknek. Ez a szolgáltatás a rendszeres időközönként frissített **tanúsítvány visszavonási listákon** (CRL) illetve valós idejű tanúsítványállapot információn (OCSP – Online Certificate Status Protocol) alapul.

f) **Tanúsítvány megújítás** (csak közigazgatási tanúsítványok esetében): A hitelesítés-szolgáltató egy lejáró tanúsítványhoz kapcsolódóan úgy bocsát ki egy új tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai (köztük a nyilvános kulcs is) változatlanok.

g) **Kulcscsere, tanúsítvány módosítás,** (csak közigazgatási tanúsítványok esetében): A hitelesítés szolgáltató mind a kulcscserét, mind pedig a tanúsítvány módosítását oly módon nyújtja, hogy gyakorlatilag új tanúsítványt állít ki, az erre vonatkozó szabályok szerint.

h) **Viszontazonosítás** (csak közigazgatási tanúsítványok esetében): A viszontazonosítás során a szolgáltató a közigazgatás ügyfeleinek kiadott tanúsítványok esetén végzi el az aláíró azonosítását, egy közigazgatási szerv kérésére, a [20] dokumentumnak megfelelően.

i) **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, 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.

j) **Biztonságos aláírás-létrehozó eszköz szolgáltatás**: A hitelesítés-szolgáltató **aláírás-létrehozó adat**ot (magánkulcsot) helyez el (pontosabban hoz létre) 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 3647 (Internet X.509 Nyilvános kulcsú infrastruktúra – Hitelesítési Rend és Szolgáltatási Szabályzat keretrendszer)" ajánlás szerint készült, a Magyar Telekom e-Szignó® minősített hitelesítésszolgáltatása keretében kibocsátott tanúsítványoknak illetve a kapcsolódó Hitelesítési Rendnek megfelelve.

A Szabályzat tartalmi vonatkozásokban eleget tesz az [1], [2], [3] és [22] szerinti hazai jogszabályok előírásainak, kapcsolódó rendeleteinek és ajánlásainak, továbbá felhasználja a [7] és [18] műszaki specifikáció, valamint a [12], [19], [20] és [21] ajánlásait {ld. **1.8 Hivatkozások**}.

1.1.6 Tanúsítványfajták

A minősített elektronikus aláírás hitelesítés szolgáltatása keretében Szolgáltató a következő hitelesítési rendekben rögzítettett tanúsítványfajtákat bocsátja ki, az ezekben rögzítetteknek megfelelően.

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

  Ez a tanúsítvány egy végfelhasználói minősített tanúsítvány, melyet BALE eszközön ad ki a Szolgáltató, olyan személyek részére, akik valamely szervezethez tartoznak és ezt a tanúsítványban is jelzik („Minősített Üzleti Tanúsítvány"). A [14] dokumentum további adatokat tartalmaz ezen tanúsítványra vonatkozóan.

- **[MHR_K]:** Közigazgatási, köztisztviselőhöz kapcsolódó, biztonságos aláírás létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend (OID: 0.2.216.1.100.42.101.2.2.1)

  Ez a tanúsítvány is végfelhasználói minősített tanúsítvány, melyet BALE eszközön ad ki a Szolgáltató, de a tanúsítvány alanya egy köztisztviselő („Minősített Köztisztviselői Tanúsítvány"), és mivel a tanúsítvány megfelel a vonatkozó jogszabályoknak és szakmai ajánlásoknak, ezért a közigazgatási eljárásokban is alkalmazható. A [19] dokumentum további adatokat tartalmaz ezen tanúsítványra vonatkozóan.

- **[MHR_Ü]:** Közigazgatási, ügyfélhez kapcsolódó, biztonságos aláírás létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend (OID: 0.2.216.1.100.42.101.1.2.1)

  Ezt a tanúsítványt a Szolgáltató olyan egyéni[6] és üzleti[7] előfizetők részére bocsátja ki, akik a tanúsítványt illetve az elektronikus aláírást a közigazgatási eljárásokban is szeretnék felhasználni. Ez esetben is végfelhasználói minősített tanúsítványokról van szó, melyet BALE eszközön ad ki a Szolgáltató, és mivel a tanúsítvány megfelel a vonatkozó jogszabályoknak és szakmai ajánlásoknak, ezért a közigazgatási eljárásokban is alkalmazható. A [19] dokumentum további adatokat tartalmaz ezen tanúsítványra vonatkozóan.

[6] „Minősített Személyi Tanúsítvány"

[7] „Minősített Üzleti Tanúsítvány". Bár ez a név azonos az [MTT+BALE] tanúsítványfajta nevével, ahol szükséges, jelezve van, melyikről van pontosan szó.

A Szolgáltató által kibocsátott fenti tanúsítványfajták **minősített tanúsítvány**ok, ezért igen erős biztosítékokkal szolgálnak a bennük megnevezett személyek kilétét illetően. Ez esetben ugyanis követelmény az aláíró személyes megjelenése a Regisztrációs Szervezetnél**.** Emellett a Regisztrációs Szervezet az aláíró (és előfizető[8]) adatait a hatósági adatbázisokkal is egyezteti ill. ellenőrzi. Ezen **tanúsítvány**okhoz kapcsolódó aláíró csak természetes személy lehet. Aláíró szervezete (üzleti és köztisztviselői tanúsítványok esetén Előfizető) - természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet is lehet. A szervezet azonosítása – a természetes személy azonosításához hasonlóan – szigorú módszerekkel történik.

A Szolgáltató az egyes tanúsítványok 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:

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

Az előfizető a Szolgáltatóval egyedi limitekben is megállapodhat. Az igénylőnek (**előfizető**, **aláíró**) mérlegelési joga és felelőssége, hogy a **Szolgáltató** szabályzatai alapján meghatározza, milyen tanúsítványt rendel meg illetve fog alkalmazni egy adott célra.

Teszt tanúsítvány

A **teszt tanúsítvány**ok esetében nem feltétel az aláíró személyes regisztrációja, sem pedig adatainak ellenőrzése. 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 gondoskodnak.

Jelen szabályzat a fentiekben ismertetett tanúsítványfajták 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.

[8] Üzleti és köztisztviselői tanúsítványok esetén a Szolgáltató az aláíró szervezetének az adatait is ellenőrzi. Ezen szervezetek az Előfizetők is egyben.

Jelen szabályzathoz kapcsolódó tanúsítványok felhasználásának joghatásairól a minősített hitelesítésszolgáltatására vonatkozó **Általános Szerződési Feltételek** (ÁSzF) című dokumentum előírásai is rendelkeznek, amely megtalálható a Szolgáltató e-Szignó honlapján a http://www.magyartelekom.hu internetcímen.

1.1.7 Biztonságos aláírás-létrehozó eszköz szolgáltatás

A **minősített** hitelesítésszolgáltatás keretében **Szolgáltató** alapvetően **kétféle** biztonságos aláírás-létrehozó eszközt alkalmaz:

- a **saját** biztonságos aláírás-létrehozó eszközét[9], melyet a minősített tanúsítványok aláírására és a magánkulcsainak tárolására használ és
- az **előfizetők** biztonságos aláírás-létrehozó eszközeit[10], 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) helyez el (pontosabban hoz létre) a **biztonságos aláírás-létrehozó eszköz**ön és azt eljuttatja az igénylő (**előfizető**, **aláíró**) számára. Az egyediséget biztosító megszemélyesítési folyamat két részből áll:

- a biztonságos aláírás-létrehozó eszköz **fizikai megszemélyesítése** (a Szolgáltató arculati elemeinek valamint az igénylő / előfizető nevének elhelyezése az eszközön) és
- a biztonságos aláírás-létrehozó eszköz **logikai megszemélyesítése** (tanúsítványok és magánkulcs[11] elhelyezése az eszközön).

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

- a biztonságos aláírás-létrehozó eszköz **beszerzése és előkészítése** a felhasználó számára,
- az aláíró **kulcspár előállításának kiváltása** az aláírás-létrehozó eszközön és
- a biztonságos aláírás-létrehozó eszköz és az aktivizáló kódot tartalmazó zárt boríték (megfelelően biztonságos módon történő) **eljuttatása** a regisztrált aláíróhoz.

[9] Ez egy kriptográfiai hardver modul.

[10] Ezek intelligens kártyák (chipkártyák).

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

1.1.8 Időbélyegzés-szolgáltatás

Az időbélyegzés szolgáltatás keretében Szolgáltató az elektronikusan aláírt elektronikus dokumentumhoz időbélyegzőt kapcsol.

A szolgáltatáshoz kétféle tevékenység köthető:

- **időjel ellátás**, amelyet a Szolgáltató a belső és külső ügyfelei részére egyaránt biztosít azért, hogy azok hitelesített időforráshoz szinkronizálhassák a rendszereiket[12] és
- **maga az időbélyegzés-szolgáltatás**, amelyet a Szolgáltató minősített időbélyegzés-szolgáltatásként (előfizetéses alapon) nyújt a külső ügyfeleinek.

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

A Szolgáltató két hozzáférési módot ajánl az időbélyegzés-szolgáltatáshoz:

- az első általában egyedi – dedikált – hozzáférés, melyen jellemzően a nagy forgalmú ügyfelek részére szolgáltat[13],
- a második az Internet alapú hozzáférés, mellyel a lehető legszélesebb felhasználói körre kiterjeszthető a szolgáltatás.

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

1.2 A dokumentum neve és azonosítója

Jelen szabályzat neve: **A Magyar Telekom Minősített e-Szignó® hitelesítésszolgáltatás és Időbélyegzés-szolgáltatás Szolgáltatási Szabályzata.**

A szabályzat rövid neve: **Magyar Telekom e-Szignó® mHSzSz**, vagy egyszerűen csak mHSZSZ, (ebben a dokumentumban még Szabályzat).

---

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

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

A **Szabályzat** az alábbi adatokkal azonosítható[14]:

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

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

Verziószám: ..... a Szabályzat fedőlapján található

A hatályba lépés dátuma[15]: ..... a Szabályzat fedőlapján található

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

http://www.magyartelekom.hu

1.3 PKI szereplők

A **Szolgáltató** jelen szabályzatban tárgyalt szolgáltatásaihoz tartozó közösség (a továbbiakban: **Közösség**) az alábbiakból áll.

1.3.1 Hitelesítő szervezet

A Szolgáltató – a saját szervezetén belül, az Informatikai Igazgatóság keretében – hitelesítő szervezetet működtet (Hitelesítő Szervezet), melynek feladata a szolgáltatásokhoz kapcsolódó rendszerek üzemeltetése, a minősített tanúsítványok központi előállítása és menedzsmentje (a Regisztrációs Szervezettől kapott kérelmeknek megfelelően, a hitelesítés-szabályozásért felelős szervezet 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 Egységek (amelyeket a Gyökér Hitelesítő Egység vagy – közigazgatási tanúsítványok esetén – a Közigazgatási Gyökér Hitelesítés-Szolgáltató hitelesít).

A Szolgáltató a **végfelhasználói minősített tanúsítványfajták** kibocsátását, továbbá az időbélyegzés szolgáltatását a jelen Szabályzat és más kapcsolódó szabályzatok előírásainak megfelelően végzi (ezen szabályzatokat lásd a http://www.magyartelekom.hu internetoldalakon).

A Gyökér Hitelesítő Egység 2004.10.01. és 2005.10.01.közötti időszakban használt tanúsítványának lenyomata: 691D 25F1 298B 8ECC EF4E FC77 04CE D79F BDCA AE2D

[14] A 3/2005. (III. 18.) IHM rendelet 1. számú mellékletének megfelelően

[15] A *Szabályzat* aktuális verziójára vonatkozik.

A Szolgáltató névváltását követően (Matáv neve Magyar Telekom-ra változott) a Gyökér Hitelesítő Egység részére új szolgáltatói kulcspár és tanúsítvány került kiállításra és felhasználásra 2005.10.01.-től, melynek lenyomata: d0 a8 8c af 91 3f 40 e8 40 03 71 bf a5 29 88 e5 cd 79 d5 9c

A Gyökér Hitelesítő Egység tanúsítványának kiadásával ill. visszavonásával kapcsolatos tájékoztatást (pl. ujjlenyomat) a Magyar Telekom hivatalos formában a Magyar Hírlapban teszi közzé.

A Hitelesítő Szervezet elérése alapvetően a Regisztrációs Szervezeten keresztül történik. Rendszerüzemeltetéssel kapcsolatos hibák esetén a Hitelesítő Szervezet az eszigno.muszaki@t-systems.hu címen is elérhető.

1.3.2 Regisztrációs szervezet

A Szolgáltató – a saját szervezetén belül – minősített e-Szignó és időbélyegzés **regisztrációs szervezetet** (Regisztrációs Szervezet) 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 interneten és telefonon keresztül, illetve (az ügyfélszolgálaton) személyes közreműködéssel látja el.

A Minősített e-Szignó és Időbélyegzés Regisztrációs Szervezet elérési adatai a következők:

Név:	Magyar Telekom Üzleti Szolgáltatások Üzletág, Termék- és Megoldásmenedzsment szervezet, Megoldásmenedzsment osztály, Helpdesk csoport
Cím:	1122 Budapest Maros u. 19-21.
Telefon:	+36-80-20-44-51
Fax:	+36-1-458-7506
Postacím:	1541 Budapest
Honlap:	http://www.magyartelekom.hu
E-levélcím:	eszigno.minositett@t-systems.hu

A Regisztrációs Szervezet általában munkanapokon **8 és 16 óra között** tart nyitva, de egyes napokon ettől eltérő nyitvatartási időpont is lehetséges.

A szolgáltatással kapcsolatos kérdéseikkel, problémákkal a végfelhasználók a Regisztrációs Szervezethez fordulhatnak szóban vagy írásban (ld. honlapon a „Minősített e-Szignó és Időbélyegzés Ügyfélszolgálat és Regisztrációs Szervezet").

A regisztrációs tisztviselők a fenti cím mellett Szolgáltató további öt telephelyén is elérhetőek (regisztrációs pontok):

- 1013 Budapest, Krisztina krt. 55.
- Szeged, Rókus krt. 2-10.
- Miskolc, Régiposta u. 9.
- Debrecen, Bethlen u. 1.
- Pécs, Rákóczi út 19.

Ezen regisztrációs pontokon az ügyintézés (tanúsítványigényléshez szükséges szerződéses papírok és dokumentumok leadása, igénylő személyes ellenőrzése, hiánypótlás, elkészült tanúsítványok és chipkártyák átvétele, tanúsítvány visszavonásának személyes úton történő kezdeményezése) csak előzetes időpontegyzetetést követően lehetséges, az itt dolgozó regisztrációs tisztviselőkkel, akiket a fenti telefonszámon keresztül lehet elérni.

Az Aláíró személyes megjelenése keretében történő azonosítását nemcsak a Regisztrációs Szervezethez tartozó regisztrációs tisztviselők, hanem Szolgáltató valamennyi értékesítési és értékesítés támogató szervezetének munkatársa elvégezheti[16]. Tanúsítvány kiadást megelőző személyes regisztráció esetén a személyes ellenőrzés mellett a munkatársak átveszik az Aláírótól a tanúsítványigényléshez szükséges szerződéses papírokat és továbbítják a regisztrációs tisztviselőkhöz. Tanúsítványkiadás utáni személyes regisztráció esetén a tanúsítványt is átadják a biztonságos aláírás létrehozó eszközzel együtt az aláírónak. Az értékesítési és támogató munkatársak regisztrációhoz kapcsolódó tevékenysége csak a fentieket foglalja magában; a tö bbi regisztrációhoz kapcsolódó tevékenységet (pl. az adatok egyeztetését a hatósági adatbázisokkal, a tanúsítványigénylés feladását és jóváhagyását) kizárólag a regisztrációs tisztviselők végezthetik.

A visszavonással kapcsolatos regisztrációs és adminisztrációs szolgáltatás folyamatosan – **0 és 24 óra között** – elérhető az alábbi telefon ill. faxszámon:

24 órás ügyelet telefonszáma: +36-80-20-40-40

24 órás ügyelet fax száma: +36-1-447 4451

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

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

[16] Aki az erre vonatkozó oktatáson részt vett

1.3.3 Előfizetők és alanyok. Érintett felek

A Szolgáltató által nyújtott szolgáltatások végfelhasználói az alábbiak lehetnek:

- az előfizető, aki a kibocsátott tanúsítvány és az ehhez tartozó kulcspár tulajdonosa,
- az aláíró (a tanúsítvány Alany mezőjében jelzett személy)[17], 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 meghatározott kötelezettségeket, és aki (eltérő megállapodás hiányában) fizet a szolgáltatásért.

Az **előfizető** illetve **aláíró** szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Szolgáltatói Szerződésben illetve Megrendelőlapban (**SzSz**)[18], Általános Szerződési Feltételekben (**ÁSzF**)[19], a vonatkozó Hitelesítési Rend dokumentumban és a jelen Minősített HitelesítésSzolgáltatási Szabályzatban (**mHSzSz**) foglaltak szerint. A Szolgáltató az aláíróval és előfizetővel elsősorban a Regisztrációs Szervezeten keresztül tart kapcsolatot.

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

Az **érintett fél** a Szolgáltatóval szerződéses viszonyban nem álló harmadik személy, aki az elektronikusan aláírt 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. Az érintett fél tevékenységére vonatkozó ajánlásokat a Szabályzat és az abban megnevezett egyéb szabályzatok tartalmazzák.

Az érintett félre vonatkozó előírásokat a Szabályzat **9.6.4** alfejezete tartalmazza A Szolgáltató az érintett féllel elsősorban a címtáron keresztül tart kapcsolatot. A Szolgáltató szabályzatai semmilyen formában sem korlátozzák az érintett felek körét.

[17] Pl. [MHR_Ü] esetén közigazgatás ügyfele, [MHR_K] esetén közigazgatásban dolgozó köztisztviselő

[18] ld. a [16] dokumentumot

[19] ld. a [15] dokumentumot

Az aláíró és (vagy) az előfizető érdeke annak mérlegelése, hogy **milyen tanúsítványt alkalmaz** egy adott célra. Az érintett félnek 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.

1.3.4 Egyéb szereplők

Egyéb szereplőként meg kell említeni:

- A Magyar Telekom Vezetékes Szolgáltatások Üzletág, HI Hálózatirányítási Központ, Intelligens Hálózati Rendszerek osztályát, mint az időjel ellátó rendszer üzemeltetőjét, aki ezt a tevékenységét a Hitelesítő Szervezet részére végzi
- A szabályozásért felelős szervezetet (ld. 1.5 alfejezetet)
- A Közigazgatási Gyökér Hitelesítés Szolgáltatót, aki a Szolgáltatóval való megállapodás alapján felülhitelesíti azt a hitelesítő egységet, amelyikből Szolgáltató a közigazgatási tanúsítványokat bocsátja ki.
- A Szabályzat szerinti szolgáltatással kapcsolatban illetékes fogyasztóvédelmi felügyelőséget, melynek 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

1.4 Tanúsítvány használat

1.4.1 Megfelelő tanúsítvány használat

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.

A kibocsátott végfelhasználói tanúsítványhoz kapcsolódó magánkulcs az elektronikus dokumentumokkal kapcsolatos **elektronikus aláírások megtételére**, a tanúsítványban található nyilvános kulcs az elektronikus aláírások **ellenőrzésére** használható fel, a vonatkozó Hitelesítési Rendnek megfelelően.

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-, tanúsítány visszavonási lista, és OCSP-profilok**lfejezetek 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.

1.4.2 Tiltott tanúsítvány használat

A tanúsítványfajtának megfelelő korlátozások megtalálhatók a vonatkozó Hitelesítési Rend dokumentumban.

1.5 A Szolgáltatási Szabályzat adminisztrálása

1.5.1 Adminisztrációért felelős szervezet és kapcsolattartó személy

A Szolgáltató – szervezetén belül – olyan szervezeti egységet működtet, amely az elektronikus aláírással kapcsolatos szolgáltatásokhoz elengedhetetlen szabályozási feladatokat látja el, beleértve elsősorban a jelen szabályzat valamint az egyéb nyílvános[20] szabályzatok (ÁSZF, Hitelesítési Rendek, Időbélyegzési Rend) el(ő)készít(tet)ésével, egyeztetésével, kiegészítésével, aktualizálásával, jóváhagyatásával és megjelentetésével kapcsolatos **összes feladatot**.

A szabályozási szervezet adatai, és azon belül a fenti tevékenységgel megbízott termékmenedzser elérési adatai a következők:

Név:	Magyar Telekom Üzleti Szolgáltatások Üzletág, Termék- és Megoldásmenedzsment szervezet
Cím:	1122 Budapest Maros u. 19-21.
Telefon:	+36-1-458-0129
e-Mail:	eszigno.minositett@t-systems.hu
Fax:	+36-1-458-7506
Postacím:	1541 Budapest

A szabályzatokra vonatkozóan a hatósággal (NHH) történő hivatalos kapcsolattartás a Magyar Telekom Szabályozói kapcsolatok és árpolitikai ágazat, Hatóságkapcsolati osztály feladata.

[20] A belső szabályozások kezelésével kapcsolatos felelősök külön belső utásításban vannak rögzítve

1.5.2 A Szolgáltatási Szabályzat elfogadási eljárása

A szabályozási tevékenységgel megbízott termékmenedzser összegyűjti a Szabályzatra (vagy az egyéb nyílvános szabályzatra) vonatkozó észrevételeket illetve változtatási igényeket, majd elkészít(tet)i a módosított szabályzattervezetet, melyet ezt követően elküld egyeztetésre. Az esetleges észrevételekkel kiegészített szabályzatot ellenőrzésre és jóváhagyásra megküldi az érintetteknek. Az ellenőrzések és jóváhagyások tényét az érintettek[21] aláírásukkal igazolják. Ezt követően a termékmenedzser eleget tesz a belső és külső (hatósági és ügyfelek érintő) tájékoztatási kötelezettségeknek, az 1.5.4 alfejezet szerint.

A szabályzatok elrendelése és életbe léptetése a Szolgáltató felső vezetőségének jóváhagyásával, az erre vonatkozó belső utasítás alapján történik.

Jelen szolgáltatási szabályzat [10] szabványnak valamint a kapcsolódó Hitelesítési Rendeknek – [MTT+BALE], [MHR_Ü], [MHR_K] - és Időbélyegzési Rendnek való megfelelőségét közzététel előtt Szolgáltató megvizsgálta. A vizsgálatot külső független szakértő is elvégzi évente rendszeresen végzett auditja során.

Ezen felül a Szabályzat megfelelőségét a vonatkozó törvények, jogszabályok, valamint szakmai előírások tekikntetében a Hatóság is megvizsgálja a szabályzat nyílvántartásba vételét (illetve hatályba lépését) megelőzően.

1.5.3 Szabályzat változtatási eljárások

Egy időszak alatt összegyűlt változási igényeket Szolgáltató kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

Értesítés nélkül, illetve értesítéssel változtatható elemek

A szabályzatok bármely részének (elemének) módosítása esetén az erről szóló értesítés és tájékoztatás a következő alfejezet szerint történik. Nincsenek olyan elemek, melyeket Szolgáltató értesítés nélkül változtatna meg jelen szabályzatában (illetve nyílvános szabályzataiban).

Szabályzati objektum-azonosítót vagy -mutatót változtató módosítások

Jelen szabályzat és a hitelesítésszolgáltatással kapcsolatos egyéb nyílvános szabályzatok módosított változatai mindig új verziószámmal kerülnek nyilvánosságra. A szabályzatok módosítása a szabályzatok objektum-azonosítóját is módosítja.

A verziószám egy tizedes értékkel növekszik (pl. 1.6-ot követi az 1.7-es), az objektum-azonosítónak pedig az utolsó számjegye növekszik egy értékkel. (pl. 1.3.6.1.4.1.17835.7.1.2.8.2.1.13.3.4 –et követi az 1.3.6.1.4.1.17835.7.1.2.8.2.1.13.3.5).

[21] Külön belső utasításban rögzítettek

1.5.4 Közzétételi és tájékoztatási elvek

A szabályzat közzététele é s nyílvántartásba vétele

Szolgáltató nyílvános szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően **30 nappal** közzéteszi internetes honlapján, a http://www.magyartelekom.hu internetoldalakon, ezzel egyidejűleg benyújtja azt a Hatóság részére, nyílvántartásba vétel céljából.

Az új szabályzatervezettel kapcsolatos észrevételeket Szolgáltató a hatályba lépést megelőző **14 napig** fogadja a Regisztrációs Szervezet e-mail címén. Amennyiben érkezett észrevétel és azt a Szolgáltató elfogadja, akkor a szabályzat észrevételekkel módosított változatát (beleértve a hatályba lépés időpontját. a módosítás jellegétől függően, a 30 nap figyelembe vételével) Szolgáltató honlapján ismét közzéteszi mint tervezetet, illetve benyújtja a Hatósághoz.

Amennyiben nem érkezik észrevétel vagy azt a Szolgáltató nem fogadja el, a szabályzatot Szolgáltató mint hatályos dokumentumot helyezi el nyilvános internetes honlapján (és az ügyfélforgalom számára nyitva álló helyiségben), ezzel egyidejűleg a korábbi változatot elhelyezi a „hatályát vesztett szabályzatok" közé.

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 8. fejezetben leírt tanúsítási eljárások ezeket a dokumentumokat is vizsgálják.

1.6 Meghatározások.

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 elektronikusan aláírt elektronikus 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 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, aki az aláírás-létrehozó eszközt birtokolja, és a saját vagy más személy nevében aláírásra jogosult

biztonságos aláírás-létrehozó eszköz	a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény (Eat.) 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz
elektronikus aláírás	Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum
elektronikus dokumentum	elektronikus eszköz útján értelmezhető adategyüttes
elektronikus aláírás ellenőrzése	az elektronikusan aláírt dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával
elektronikus aláírás felhasználása	elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése
elektronikusan történő aláírás	elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz
előfizető	Személyi tanúsítvány esetén maga az Aláíró. Üzleti tanúsítvány illetve köztisztviselő részére kiállított tanúsítvány esetén az a szervezet, akihez Aláíró tartozik
érintett fél	az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el
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 az aláíróhoz 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 a dokumentumon tett – módosítás érzékelhető.
Szolgáltatási szabályzat (hitelesítésszolgáltatási szabályzat)	Az Eat. [1] 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 aktuális állapotára vonatkozó információkat
időbélyeg (időbélyegző)	elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett
időbélyegzés-szolgáltató	olyan szolgáltató, amely az időbélyegzés szolgáltatást végzi
igénylő	a tanúsítvány iránti igényt benyújtó személy (jellemzően aki a szolgáltatást aláíróként és / vagy előfizetőként kívánja igénybe venni)

kriptográfiai kulcs	olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a kriptográfiai transzformáció elvégzéséhez, különösen az elektronikus aláírás előállításához vagy ellenőrzéséhez szükséges
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, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, 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 az igénylő illetve az aláíró személyazonosságát. Egy Hitelesítő Szervezet több ilyen szervezettel is együttműködhet.
tanúsítvány	hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot az Eat. [1] 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	a tanúsítvány átadása az aláírónak, valamint a szolgáltató nyilvántartásában a tanúsítvány elérhetővé tétele az aláíró hozzájárulása esetén
tanúsítvány megújítás	új tanúsítvány biztosítása, melyben az aláíró régi 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
Visszavonási nyilvántartások (tanúsítvány visszavonási nyilvántartás)	nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját
Hitelesítési Rend	olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára
időbélyegzési rend	olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára
végfelhasználó	az aláíró, az előfizető, valamint az elfogadó fél

1.7 Rövidítések és jelölések.

A dokumentumban az alábbi jelölések és rövidítések szerepelnek:

- [MTT+BALE]: Nyilvános körben kibocsátott, biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő, minősített tanúsítványtípus Hitelesítési Rendje,
- [MHR_K]: Közigazgatási, köztisztviselőhöz kapcsolódó, biztonságos aláírás létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend
- [MHR_Ü]: Közigazgatási, ügyfélhez kapcsolódó, biztonságos aláírás létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend
- [ ] jelek között a dokumentumokra történő hivatkozások számai szerepelnek.

1.8 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] 3/2005. (III.18.) IHM 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 140-2 (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 3647 (Internet X.509 Nyilvános kulcsú infrastruktúra – Hitelesítési Rend 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 Hitelesítési Rendje, [MTT+BALE] – Magyar Telekom Nyrt.

[15] Minősített e-Szignó Hitelesítésszolgáltatások - Általános Szerződési Feltételek (ÁSzF)- – Magyar Telekom Nyrt.

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

[17] Magyar Telekom Minősített Időbélyegzés-szolgáltatás Időbélyegzési Rendje – röviden (TSP)

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

[19] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható hitelesítési rendekre. 1. sz. melléklete: Biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rendek 1.0 verzió, [MHR_K] illetve [MHR_Ü]

[20] Az Informatikai és Hírközlési Minisztérium ajánlása a hitelesítés szolgáltatók által végzett viszontazonosítás protokolljának műszaki specifikációjára

[21] RFC 2560 (Internet X.509 Nyilvános kulcsú infrastruktúra – Valós idejű állapot Protokoll - OCSP)

[22] A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. tv. (Ket.)

[23] A Nemzeti Hírközlési Hatóság Hivatalának az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok és paramétereik meghatározása tárgyában hozott HL-20336-9/2005 számú határozata

2. Közzétételre és tárolásra vonatkozó felelősségek

2.1 Adatbázisok

Adatbázisok alatt elsősorban a tanúsítványtárat, valamint a visszavonási információkat tartalmazó adatbázist lehet érteni (együttesen: címtár). Ezen kívül meg kell még említeni a Szolgáltató honlapját is, ahova a szolgáltatásokra vonatkozó kikötéseket, feltételeket, szabályzatokat; valamint a rendkívüli információkat is közzéteszik. A Szolgáltató címtára egy X.500-as címtárkiszolgáló 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.[22]

2.2 A tanúsítványokra és időbélyegekre vonatkozó információk közzététele

Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait – és ezek részeként a tanúsítványokra és időbélyegzésre vonatkozó információkat - elektronikus formában (MS-Word és / vagy Adobe Acrobat formátumokban) hozza nyilvánosságra az internetes honlapjának oldalain.

Elérhetőség: http://www.magyartelekom.hu.

A dokumentumok korábban érvényben lévő változatai is megtalálhatóak itt az aktuális verziók mellett. A dokumentumok nyomtatott változatai semmilyen formában sem tekinthetők 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 5.8 fejezetet

[22] ld. [3] 17. §

- 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. (ld. 1.3.1.)
- 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 aláírónak átadja a biztonságos aláírás-létrehozó eszközön,
- az érintett felek részére közzéteszi a nyilvános Címtárban.

A tanúsítványok visszavonásának és felfüggesztésének nyilvánosságra hozatala

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

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

A Szolgáltató az általa kibocsátott **végfelhasználói tanúsítvány**okkal kapcsolatos állapot-információkat a Címtárban hozza nyilvánosságra.

Az állapot-információk közlésének módszereit illetően lásd még a **4.9 Tanúsítvány visszavonás és felfüggesztés** alfejezetet.

2.3 A közzététel gyakorisága

Kikötések és feltételek közzétételi gyakorisága

A Szabályzattal kapcsolatos új verziók közzététele az 1.5 alfejezetben ismertetett eljárásoknak megfelelően történik.

A Szolgáltató szükség szerinti gyakorisággal bocsátja ki az egyéb szabályzatait és szerződéses feltételeit, illetve az újabb változatokat.

Rendkívüli információk közzétételi gyakorisága

A Szolgáltató a rendkívüli információkat 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 az üzemszerű használatot megelőző 10 munkanapon belül teszi közzé.
- Az általa működtetett Felhasználói Hitelesítő Egység(ek) tanúsítványa a Címtárban 24 órán belül, internetes honlapján pedig 5 munkanapon belül megjelenik.
- A Szolgáltató a végfelhasználói tanúsítványokat a Címtárban (a tanúsítvány tárban) az előállítást követően 24 órán belül teszi közzé, illetve az aláíróval egyeztetett időpontbanm átadja számára, biztonságos aláírás létrehozó eszközön

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

Szolgáltató az általa működtetett hitelesítő egységek és aláírók / előfizetők tanúsítványával kapcsolatos állapot-információkat a {**4.9.7 „A tanúsítvány-visszavonási lista kibocsátási gyakorisága**"} alfejezetben tárgyalt gyakorisággal teszi közzé.

2.4 Az adatbázisok elérésének szabályozása

A Szolgáltató által közzétett kikötések és feltételek, a rendkívüli események, a tanúsítványok és állapot információk nyilvános információk. Olvasás illetve lekérdezés céljából bárki korlátozás nélkül elérheti ezeket az információkat, a közzététel sajátosságainak megfelelően, Interneten keresztül.

A Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató különböző védelmi mechanizmusokat működtet az információk jogosulatlan módosításának.

3. Azonosítás és hitelesítés

3.1 Megnevezési konvenciók

3.1.1 Név típusok

Szolgáltató által kiállított végfelhasználói tanúsítványok tulajdonos**azonosító mezői** (Alany) a [12] szerinti egyedi név formátum előírásainak felelnek meg, Aláíróra vonatkozóan a „subjectAltname" mezőben szereplő elektronikus levelezési cím struktúrája pedig az RFC 822 elvárásainak felel meg.

Az [MTT+BALE] Hitelesítési Rendben meghatározott végfelhasználói tanúsítvány tulajdonosának **azonosító**ja (az „**Alany**" mező tartalma) a következő módon épül fel:

Jelölés	Jelentés	Adat / Kitöltési szabály
CN	az *aláíró* családi- és keresztneve.[23] (*Common name*[24])	A személyazonosító okmányban szereplő adat.
O	az előfizető szervezet hivatalos neve (*Organization*[25])	A szervezet alapító okirata szerint. Gazdasági társaság esetében a cégbejegyzésben szereplő név (rövid alakban) és a szervezet típusa. Ez a szervezet az előfizető is egyben.
OU	az *aláíró* szervezeti egységének neve az *előfizető* szervezetben (*Organizational unit*[26])	A Megrendelőlapnak megfelelően. Opcionális adat
C	az *előfizető* szervezet székhelye szerinti ország (*Country*[27]).	A szervezet alapító okirata szerint. Gazdasági társaság esetében a cégkivonat szerint.
L	az *előfizető* szervezet székhelye szerinti város (*Locality)*	A szervezet alapító okirata szerint. Gazdasági társaság esetében a cégkivonat szerint
STREET	az *előfizető* szervezet székhelye szerinti közterület neve és házszám (*Street)*	A szervezet alapító okirata szerint. Gazdasági társaság esetében a cégkivonat szerint
PostalCode	az *előfizető* szervezet székhelye szerinti	A szervezet alapító okirata szerint.

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

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

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

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

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

	helység irányítószáma (*PostalCode)*	Gazdasági társaság esetében a cégkivonat szerint
E-mail	az *aláíró* e-levél címe az *előfizető* szervezeten belül (*E-mail*)	A Megrendelőlapnak megfelelően.
Serial Number	egyedi azonosító (*Sorozatszám*)	A szervezet adószáma : az aláírót azonosító okmány száma:opcionálisan aláíró egyéb azonosítója
Title	az *aláíró* szervezeti pozíciója (Title)	Ez egy opcionális adat, Megrendelőlapnak megfelelő

Az [MHR_K] Hitelesítési Rendben meghatározott, azaz közigazgatást képviselő ügyintézőhöz tartozó minősített aláíró tanúsítványok tulajdonosának **azonosító**ja (az „**Alany**" mező tartalma) a következő módon épül fel:

Jelölés	Jelentés	Adat / Kitöltési szabály
SN *(Surname)*	az *aláíró* vezetékneve	A common name mező azon része, mely az ügyintéző vezetéknevének tekintendő, UTF-8 kódolással
Title *(Title)*	az *aláíró* szervezeten belüli pozíciója	Megrendelőlapnak megfelelően Opcionális adat és kizárólag tájékoztató információ az ügyintéző esetleges beosztásáról
L (*Locality)*	A közigazgatási szerv székhelye (ha ez nem értelmezhető, akkor a telephelye) szerinti város	A szervezet alapító okirata vagy egyéb hivatalos irata* szerint.
STREET (Street)	A közigazgatási szerv székhelye (ha ez nem értelmezhető, akkor a telephelye) szerinti közterület neve és házszám	A szervezet alapító okirata vagy egyéb hivatalos irata* szerint.
PostalCode (PostalCode)	A közigazgatási szerv székhelye (ha ez nem értelmezhető, akkor a telephelye) szerinti helység irányítószáma	A szervezet alapító okirata vagy egyéb hivatalos irata* szerint.
Serial Number (Sorszám)	Sorszám	A betű szerint azonos common name mezőtartalommal rendelkező köztisztviselők megkülönböztetésére szolgáló egyedi sorszám, melyet a Magyar Telekom mint szolgáltató a kövtkezőképpen generál: a szervezet adószáma: az *aláírót* azonosító okmány száma: opcionálisan aláíró egyéb azonosítója
CN (*Common*	az *aláíró* neve (vezetéknév + keresztnév).	Az ügyintéző neve, mely betű szerint azonos a regisztráció alapjául szolgáló

name)		személyazonosító okmányban foglalt névvel, szóköz elválasztójel(eke)t és az UTF8 kódolást használva.
OU (*Organizational unit)*	Osztály / részleg Az *aláíró* közigazgatási szerven belüli szervezeti egységét jelöli	A Megrendelőlapnak megfelelően. Opcionális adat.
O (Organization)	A közigazgatási szerv neve, amelyikhez *aláíró* tartozik	A szervezet alapító okirata vagy egyéb hivatalos irata* szerint. Ez a szervezet az előfizető is egyben.
C (*Country).*	HU	

* Az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét és székhelyének (vagy ahol ez nem értelmezhető, telephelyének) címét is tartalmazó meghatalmazás

Az [MHR_Ü] Hitelesítési Rendben meghatározott, azaz közigazgatás ügyfeléhez tartozó minősített aláíró tanúsítványok tulajdonosának **azonosító**ja (az „Alany" mező tartalma) a következő módon épül fel:

Jelölés	Jelentés	Adat / Kitöltési szabály
SN *(Surname)*	az *aláíró* vezetékneve	A common name mező azon része, mely az ügyfél vezetéknevének tekintendő UTF-8 kódolással
Title *(Title)*	Minősített Személyi Tanúsítvány esetén nem kerül kitöltésre Minősített Üzleti Tanúsítvány esetén az *aláíró* szervezeten belüli poziciója	Megrendelőlapnak illetve Szolgáltatási Szerződésnek megfelelően Opcionális adat, kizárólag tájékoztató információ az aláíró szervezetén belüli beosztásáról
L (*Locality)*	Minősített Személyi Tanúsítvány esetén *aláíró* állandó lakhelyének település neve Minősített Üzleti Tanúsítvány esetén *aláíró* szervezetének székhelye szerinti település neve	Minősített Személyi Tanúsítvány esetén aláíró lakcímet igazoló okmánya szerint. Minősített Üzleti Tanúsítvány esetén a szervezet alapító okirata szerint. Gazdasági társaság esetében a cégkivonat szerint
STREET (Street)	Minősített Személyi Tanúsítvány esetén *aláíró* állandó lakhelye szerinti közterület neve és házszáma Minősített Üzleti Tanúsítvány esetén *aláíró* szervezetének székhelye szerinti közterület neve és házszáma	Minősített Személyi Tanúsítvány esetén aláíró lakcímet igazoló okmánya szerint. Minősített Üzleti Tanúsítvány esetén a szervezet alapító okirata szerint. Gazdasági társaság esetében a cégkivonat szerint
PostalCode(PostalCode)	Minősített Személyi Tanúsítvány esetén *aláíró* állandó lakhelyének irányítószáma	Minősített Személyi Tanúsítvány esetén aláíró lakcímet igazoló okmánya szerint.

	Minősített Üzleti Tanúsítvány esetén *aláíró* szervezetének székhelye szerinti irányítószám	Minősített Üzleti Tanúsítvány esetén a szervezet alapító okirata szerint. Gazdasági társaság esetében a cégkivonat szerint
Serial Number *(*Sorszám*)*	Sorszám	A betű szerint azonos common name mezőtartalommal rendelkező ügyfelek megkülönböztetésére szolgáló egyedi sorszám, melyet a Magyar Telekom mint szolgáltató a következőképpen generál. Minősített Személyi Tanúsítvány esetén: az *aláírót* azonosító okmány száma : opcionálisan aláíró egyéb azonosítója Minősített Üzleti Tanúsítvány esetén: szervezet adószáma : az *aláírót* azonosító okmány száma : opcionálisan *aláíró* egyéb azonosítója
CN (*Common name)*	az *aláíró* neve (vezetéknév+keresztnév).	Az ügyfél (természetes személy) neve, mely betű szerint azonos a regisztráció alapjául szolgáló személyazonosító okmányban foglalt névvel, szóköz elválasztójel(eke)t és az UTF8 kódolást használva.
OU (*Organizational unit)*	Minősített Személyi Tanúsítvány esetén ez a mező nem kerül kitöltésre. Minősített Üzleti Tanúsítvány esetében ez a mező abban az esetben kerül kitöltésre, ha az ügyfél tanúsítványában jelezni kívánja a szervezeten belüli azon szervezeti egységének a nevét, amelyikhez tartozik	A Megrendelőlapnak megfelelően Opcionális adat
O (*Organizatio*n)	Minősített Személyi Tanúsítvány esetén ez a mező nem kerül kitöltésre. Minősített Üzleti Tanúsítvány esetében a mező kötelezően kitöltendő annak a szervezetnek a nevével, amelyikhez aláíró tartozik.	A név formátuma a szervezet alapító okirata szerint. Gazdasági társaság esetében a cégbejegyzésben szereplő név (rövid alakban) és a szervezet típusa. Ez a szervezet az előfizető is egyben.
C (*Country).*	HU	

Tájékoztatásul megadjuk az MTT+BALE], az [MHR_Ü] és [MHR_K] Hitelesítési Rendekben meghatározott tanúsítványok „Alany” mezőjének egyes almezőiben használt kódolásokat is:

- UTF8String kódolás (SN, Title, L, STREET, CN, OU, O mezők esetében)
- PrintableString kódolás (SerialNumber, C mezők)

3.1.2 Igény a nevek értelmezhetőségére

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

- Az azonosítónak értelmezhetőnek kell lenni.
- Álnév használata csak az [MTT+BALE] Hitelesítési Rendben meghatározott tanúsítványfajtánál 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.
- Az Aláíró nevének felvétele illetve a tanúsítványban (a Subject / CN, SN mezőkben) történő megjelentetése során Szolgáltató a regisztráció alapjául szolgáló személyazonosság igazolására alkalmas hatósági igazolványban szereplő - betű szerint azonos - írásmódot követi, UTF-8 kódolással.
- Nem magyar állampolgárok esetében az [MTT+BALE] Hitelesítési Rendben meghatározott tanúsítványfajtánál Szolgáltató az útlevélben szereplő írásmódot (ékezetmentes formában) követi.

3.1.3 Álnevek használata

Álnév használata csak az [MTT+BALE] Hitelesítési Rendben meghatározott tanúsítványfajtánál megengedett (ld. még az előző alfejezetet), az [MHR_Ü] és [MHR_K] Hitelesítési Rendekben meghatározott – azaz közigazgatási - tanúsítványok esetében nem.

3.1.4 A különböző elnevezési formák értelmezési szabályai

A tulajdonos-azonosító a következő módon értelmezendő:

- Üzleti és köztisztviselői tanúsítványok esetén a tanúsítvány felhasználója – azaz az aláíró a „Common Name” mező szerinti természetes személy, aki az „Organization” mező szerinti szervezethez tartozik valamilyen minőségben vagy beosztásban, és amely szervezet az Előfizető is egyben. 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 [MTT+BALE] Hitelesítési Rendben meghatározott üzleti tanúsítvány esetén az aláíró e-levél címe (az előfizető szervezettel összefüggésben) az „Email” mezőben található (közigazgatási tanúsítvány esetén az aláíró e-levél címe a SubjectAltname mezőben található).

- Személyi tanúsítvány esetén a tanúsítvány felhasználója – azaz az **aláíró** a „Common Name” mező szerinti természetes személy, aki egyéni előfizetőként igényli illetve használja a tanúsítványt, azaz a tanúsítványában nem kívánja jelezni valamely céghez vagy szervezethez történő tartozását. Az aláíró állandó lakhelye a „Country” mező szerinti ország „Locality” mező szerinti városában található. Az aláíró egyéni e-levél címe a SubjectAltname mezőben található.

A **tulajdonos-azonosító mező**nek az a célja, hogy a tanúsítványhoz tartozó aláírót egyértelműen azonosítani lehessen, valamint - üzleti és köztisztviselői tanúsítvány esetén az, hogy az előfizető szervezet - akihez aláíró tartozik - a Közösség számára egyértelműen azonosítható legyen. Az aláíró az előfizető szervezetén belüli jogosultságainak meghatározása a tanúsítványnak nem célja, ezért erre vonatkozóan információt nem tartalmaz.

Üzleti és köztisztviselői tanúsítványok esetén 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, kivéve a Titulus mezőben opcionálisan jelzett adatot.

Az azonosítók értelmezése érdekében az érintett feleknek a jelen szolgáltatási szabályzatban leírtak alapján kell eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az érintett félnek segítségre lenne szüksége, akkor a Szolgáltatóval 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.

3.1.5 A nevek egyedisége

A **tulajdonos-azonosító** a **Szolgáltató** címtárában egyedi. Erről elsődlegesen a SerialNumber mező adattartalma, továbbá – [MTT+BALE] tanúsítvány esetén az **aláíró** e-levél címének azonosítóban való szerepeltetése gondoskodik. Ez utóbbi esetében 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 „SerialNumber” mező tartalmát egy sorszámmal egészíti ki.

3.1.6 Márkanevek elismerése, azonosításuk és szerepük

A Szolgáltató a szolgáltatása során a „**Magyar Telekom e-Szignó**®” védjegyet alkalmazza. A védjegy a **Magyar Telekom Nyrt.** tulajdona.

A Szolgáltató az előfizető / aláíró által 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 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, Szolgáltatónak jogában áll visszavonni a kérdéses tanúsítványt.

3.2 Kezdeti regisztrálás. A személyazonosság megállapítása

3.2.1 A magánkulcs birtoklásának igazolása

A Szolgáltató saját szervezetén 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.

3.2.2 Szervezet azonosságának hitelesítése

Az üzleti és köztisztviselői tanúsítványok esetében – azaz amikor az Aláíró a tanúsítványában jelezni kívánja egy adott szervezethez való tartozását is - a Szolgáltató által kibocsátott tanúsítványokban szerepel az előfizető szervezet neve, és opcionálisan szerepelhet az előfizető szervezet egy megnevezett szervezeti egységének neve is.

Az igénylőnek (előfizető, aláíró) ehhez adatokat és bizonyítékokat 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 **Megrendelőlap**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. Köztisztviselői tanúsítvány igénylése esetén szükség van az adott közigazgatási szerv által kiállított és közokiratba foglalt[28], a közigazgatási szerv nevét és székhelyének (vagy ahol ez nem értelmezhető, telephelyének) címét, valamint iktatószámot tartalmazó meghatalmazást arra, hogy az Aláíró a hivatal képviseletében a szolgáltatónál előforduló ügyekben eljárhat, és amely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti.

A regisztrációhoz szükséges iratokról részletes tájékoztatás található az **1. melléklet**ben.

Szolgáltató regisztrációs tisztviselője az előfizető adatait, valamint a bemutatott iratok és okmányok érvényességét és hitelességét a 2001. évi XXXV. tőrvény 12. § (2) bekezdés b) pontja szerinti hatósági adatbázisban 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 alap esetben 15 munkanap (de külön megállapodás esetén ez módosulhat).

Aláírónak (mint természetes személynek) külön is azonosítani kell magát a 3.2.3 pont szerint.

[28] A közokiratba foglalás és az iktatószám csak akkor kötelező, ha a köztisztviselő személyes regisztrációja – kérésére – nem a saját munkahelyén, hanem a Szolgáltató telephelyén történik

3.2.3 Egyén azonosságának hitelesítése és viszontazonosítás

A Szolgáltató a tanúsítványban megnevezésre kerülő természetes **személy** (Aláíró) személyes megjelenését és azonosítását követeli meg a tanúsítvány kiadás feltételeként. Ez történhet a Szolgáltató regisztrációs szervezeténél, vagy – külön díj ellenében – a személy által megjelölt külső helyszínen (mobil regisztráció), előzetes időpontegyeztetést követően. 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[29], születésének dátumát és helyét, valamint az anyja nevét.

A személyazonosításra alkalmas hatósági igazolványban (okmányban) szereplő fénykép alapján az igénylőnek egyértelműen felismerhetőnek kell lennie, és a benne szereplő aláírásnak meg kell egyezni a tanúsítványigénylő űrlapon igénylő által tett aláírással.

A **bemutatott okmányoknak** eredetinek, valódinak és érvényesnek kell lenniük. A Szolgáltató ezt hagyományos módszerekkel, valamint a 2001. évi XXXV. tőrvény 12. § 2) bekezdés a) pontja szerinti személyi adat- és lakcímnyilvántartással, az úti-okmány nyilvántartással vagy a gépjárművezetői nyilvántartással történő adategyeztetéssel ellenőrzi, elektronikus úton. Ennek keretében ellenőrzésre kerül Aláíró elektronikus képmása is.

A Szolgáltató a bemutatott dokumentumokról fénymásolatot készít.

Amennyiben az igénylő nem járul hozzá a személyi azonosító okmányáról fénymásolat készítéséhez, akkor az alábbi eljárásnak kell alávetnie magát. Az igénylőnek fel kell vennie a kapcsolatot a Szolgáltató Regisztrációs Szervezetével, és meg kell jelennie Szolgáltató azon telephelyén, amelyet a regisztrációs tisztviselő kijelöl számára, azaz, ahol a személyes ellenőrzéssel együtt adatainak a hatósági adatbázisban történő egyeztetése is megtehető. Ezen eljárás esetén a regisztrációs tisztviselő 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.
- Igénylő nem járul hozzá a személyazonosító okmány fénymásolásához, és nem hajlandó az ilyen esetekben szükséges eljárásnak alávetnie magát.

[29] 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 alap esetben 15 munkanap (de külön megállapodás esetén ez módosulhat).

A Szolgáltató nem fogad el elektronikus dokumentumot az egyéni azonosság hitelesítésére a kezdeti regisztráció során.

Viszontazonosítás

Közigazgatás ügyfele részére Szolgáltató által kiadott tanúsítvány esetében az ügyintéző hatóság kérésére Szolgáltató viszontazonosítást végez az ügyfél azonosságának megállapítása céljából, a [20] dokumentumnak megfelelően.

A viszontazonosítási kéréseket Szolgáltató a következő címen fogadja:

http://viszontazonositas.magyartelekom.hu

A viszontazonosítási kéréseket és válaszokat Szolgáltató a [20] dokumentumban rögzített protokoll szerint kezeli. A viszontazonosítási kérések hitelességének (az ügyintéző hatóság elektronikus aláírásának) ellenőrzése kapcsán Szolgáltató csak olyan kéréseket fogad el, melyek esetén a kérést aláíró ügyintéző hatóság tanúsítványa megfelel a [18] dokumentumban 3. 6 vagy 7. sorszámmal jelzett tanúsítványra vonatkozó követelményeknek (a tanúsítvány tulajdonosa a köigazgatás szervere, vagy a közigazgatásban eljáró személy). A megfelelőséget Szolgáltató a tanúsítvány OID-je alapján ellenőrzi. Hiteles viszontazonosítási kérés esetén a választ Szolgáltató haladéktalanul megküldi.

3.2.4 Nem ellenőrzött előfizetői információk

Szolgáltató az Aláíró illetve előfizető számlázási címét, az email címét illetve a titulusát csak a szerződés alapján ellenőrzi (de nem végez ellenőrzést pl. az e-mail cím létezésére vonatkozóan).

3.2.5 Jogok, felhatalmazások ellenőrzése

Az üzleti és köztisztviselői tanúsítványok esetében – azaz amikor az Aláíró a tanúsítványában jelezni kívánja egy adott szervezethez való tartozását is – a regisztrációhoz be kell mutatni a Szolgáltatási Szerződéshez kapcsolódó Megrendelőlapot illetve a 3.2.2. pontban jelzett dokumentumokat, mivel Szolgáltató ezen adatok alapján ellenőrzi, hogy Aláíró milyen jogokat és felhatalmazásokat kapott a szervezetétől.

3.2.6 Az együttműködési képességekre vonatkozó követelmények

Szolgáltató nem alkalmaz együttműködési képességekre vonatkozó egyedi követelményeket.

3.3 Azonosítás és hitelesítés kulcs megújítás kérelem esetén

3.3.1 Azonosítás és hitelesítés szokásos kulcs megújítás esetén

A közigazgatási tanúsítványok esetében Szolgáltató az érvényes tanúsítványok megújítását lehetővé teszi. Az igénylőnek (azaz a lejáró tanúsítványban szereplő Aláírónak) a Szolgáltató honlapján található űrlap kitöltésével írásban kell nyilatkoznia arról, hogy az adatai változatlanok. Ebben az esetben Szolgáltató regisztrációs szervezete az adatokat ellenőrzés nélkül elfogadja. Ha az előfizetőre vagy az Aláíróra vonatkozó adatok megváltoztak, a megváltozott adatokat a regisztrációs szervezet az új tanúsítvány kibocsátására irányadó eljárás szerint ellenőrzi (további részletek a 4.6 alfejezetben).

Az [MTT+BALE] tanúsítványfajta megújítását Szolgáltató nem teszi lehetővé. Ezen tanúsítványok esetében a tanúsítvány lejárta után az aláírónak új tanúsítványt kell igényelnie a kezdeti regisztráció módszerével.

3.3.2 Azonosítás és hitelesítés visszavonást követő kulcs megújítás esetén

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 a kezdeti regiszráció módszerével.

3.4 Azonosítás és hitelesítés tanúsítvány visszavonási kérelem esetén

Szolgáltató tanúsítvány visszavonási és felfüggesztési szolgáltatásokat egyaránt nyújt. Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait a **4.9** Tanúsítvány v**isszavonás és felfüggesztés** alfejezet tárgyalja.

4. A tanúsítvány életciklusra vonatkozó követelmények

4.1 Tanúsítvány-kérelem (tanúsítvány igénylés)

4.1.1 Ki nyújthat be tanúsítvány kérelmet

Üzleti és köztisztviselői tanúsítványok esetében – azaz amikor az Aláíró a tanúsítványában jelezni kívánja egy adott szervezethez való tartozását is – a tanúsítványigénylést benyújthatja a (leendő) Aláíró személyesen, vagy a szervezete (előfizető).[30] Személyi tanúsítvány esetén az igénylést a tanúsítvány leendő tulajdonosa (Aláíró) nyújthatja be személyesen.

4.1.2 A tanúsítványigénylés folyamata és a résztvevők felelőssége

Új végfelhasználói tanúsítvány igénylési eljárásának lépései a következők:

a) Az igénylő tájékozódik a Szolgáltató által kibocsátott tanúsítványfajtákról és azok igénylésének folyamatáról Szolgáltató internetes honlapján, vagy telefonon keresztül a Regisztrációs Szervezetnél, vagy Szolgáltató valamelyik üzleti értékesítési szervezeténél

b) Személyi tanúsítványra vonatkozó igényt telefonon keresztül kell bejelenteni;[31] ezt követően az igénylőt Szolgáltató regisztrációs tisztviselője visszahívja, és egyeztetik a megrendelés folyamatát, valamint a regisztrácó körülményeit (hely, időpont, szükséges iratok stb.). Üzleti és köztisztviselői tanúsítvány iránti kérelmet az igénylő a Megrendelőlap kitöltésével és aláírásával, valamint annak a Szolgáltató illetékes értékesítési szervezetéhez és/vagy a Regisztrációs Szervezethez történő eljuttatásával teheti meg.

c) A Szolgáltató regisztrációs tisztviselője elvégzi a leendő Aláíró személyes ellenőrzését, mely történhet a Szolgáltató telephelyén, vagy – külön díj ellenében - külső helyszíni regisztráció útján (mobil regisztráció). Az igénylő a regisztráció során a Szolgáltatóval és annak regisztrációs tisztviselőjével köteles együttműködni,

d) Szolgáltató a jelen Szabályzat 3. és 4. pontokban foglaltaknak megfelelően ellenőrzi az űrlapon szereplő előfizetői és aláírói adatokat illetve a személyes és szervezeti identitásokat,

e) Szolgáltató elfogadja a tanúsítvány megrendelést, rögzíti az adatokat az informatikai rendszerében, létrehozza az aláírás ellenőrző és létrehozó adatot a Biztonságos aláírás

[30] Aláíró személyes megjelenés keretében történő ellenőrzésére (a Szolgáltató által) akkor is szükség van, ha a tanúsítványigényt az előfizető (szervezet) nyújtja be.

[31] Ez megtehető nemcsak a minősített Regisztrációs Szervezetnél, hanem a Fokozott e-Szignó Regisztrácisó Szervezetnél is

létrehozó eszközön, előállítja és kibocsátja a Tanúsítványt és elhelyezi a Biztonságos aláírás létrehozó eszközön.

f) Szolgáltató átadja a Biztonságos aláírás létrehozó eszközt az Aláírónak vagy Aláíró által meghatalmazott személynek.

Amennyiben nem közigazgatási, köztisztviselőhöz kapcsolódó tanúsítványról van szó, az igénylő külön kérése esetén a fenti folyamat annyiban módosulhat, hogy a c) pont szerinti személyes ellenőrzés az f) pontban leírt átadáskor történik meg. Ez esetben az eszközt kizárólag az Aláíró veheti át személyesen, és az átvétel során kell hitelesen igazolnia a személyazonosságát a regisztrációs tisztviselő számára. Ennek hiányában az eszköz nem kerül átadásra, és a tanúsítványt a Szolgáltató visszavonja.

Amennyiben az igényelő kéri, a szolgáltatás nyilvános dokumentumainak helyszíni tanulmányozására is lehetősége van, valamint szóban történő tájékoztatást is kaphat a szolgáltatással kapcsolatban.

A Szolgáltatási Szerződés és Megrendelőlap valamint a Szolgáltató szabályzatai és termékismertetői megtalálhatók a Szolgáltató honlapján is, így előzetesen is áttekinthetők és kitölthetők.

A személy- és szervezeti azonosság, valamint a szervezethez tartozás megállapítása a 3.2.3 és 3.2.2 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 3.1.5 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-kérelem feldolgozása

4.2.1 Az azonosítási és hitelesítési funkciók megvalósítása

A regisztrációs tisztviselő összeveti a Szolgáltatási szerződésen és Megrendelőlapon szereplő előfizetői adatokat a regisztrációhoz bekért dokumentumokkal, majd adategyeztetést végez elektronikus úton a 3.2.3 pontban illetve (gazdasági társaságok esetén) a 3.2.2. pontban megjelölt hatósági adatbázisokkal.

Amennyiben az adatok ellenőrzése megtörtént de azok nem bizonyultak érvényesnek (igaznak) vagy a kérelem jóváhagyásához további információkra vagy hiánypótlásra van szükség, erről a eegisztrációs tisztviselő értesíti az Aláírót és / vagy az előfizetőt. Amennyiben a hiánypótlás megtörtént vagy a kérelem jóváhagyásához szükséges információk beérkeztek, az adatokat a regisztrációs tisztviselő az előzőekhez hasonlóan ellenőrzi.

4.2.2 A tanúsítványkérelem jóváhagyása vagy visszautasítása

Amennyiben az adatok ellenőrzése megtörtént és azok érvényesnek (igaznak) bizonyultak, a regisztrációs tisztviselő rögzíti az adatokat az erre a célra szolgáló rendszerben (RAIF[32]), amely összeállítja a tanúsítványigénylés elektronikus formátumát, amit végül a tisztviselő elektronikus aláírásával hitelesítve továbbít a Hitelesítő Szervezet rendszerébe.

Amennyiben Szolgáltató az igényelt tanúsítványkérelmet visszautasítja (ld még 3.2.2 illetve ,3.2.3 pontokat) akkor a kérelmezőnek a regisztrációs tisztviselő értesítést küld, a visszautasítás okának megjelölésével.

4.2.3 A tanúsítványkérelem feldolgozásának időtartama

A tanúsítványkérelemtől a tanúsítvány kiadásáig vállalt időtartamot a Szolgáltató ÁSZF-jének 5.4 pontja tartalmazza.

[32] Registration Authority Interface

4.3 Tanúsítvány-kibocsátás

4.3.1 A hitelesítés-szolgáltató tevékenysége a tanúsítvány-kibocsátás során

Végfelhasználói tanúsítványok kibocsátására a tanúsítvány-kérelem feldolgozását követően kerül sor. A regisztrációs tisztviselő által feladott elektronikus igény hitelességét a Hitelesítő Szervezet kártyamegszemélyesítő rendszere ellenőrzi. Hiteles igény esetén megtörténik az egyedi név képzése, a kulcspár előállítása a BALE chipkártyán, majd az aláírt tanúsítvány-kérelem eljut a Hitelesítő Szervezet tanúsítványkiadó egységébe. A hitelesítő egység aláírja a tanúsítványt saját magánkulcsával és a tanúsítvány rákerül a chipkártyára. Ezzel együtt megtörténik a kártya megszemélyesítése, az aktivizáló kód generálása, valamint a kódot tartalmazó zárt boríték előállítása is. A fent leírt folyamatot Hitelesítő Szervezet munkatársa (rendszerüzemeltető) felügyeli. Ezt követően a tanúsítvány 24 órán belül kerül közzétételre a nyilvános címtárban.

4.3.2 Az előfizető értesítése a tanúsítvány kibocsátásról

Az elkészült tanúsítványról Szolgáltató regisztrációs tisztviselője értesíti az aláírót és/vagy előfizetőt, majd egyezteteti a szerződéses dokumentumok őket illető példányainak, továbbá a magánkulcsot és tanúsítványt tartalmazó biztonságos aláírás-létrehozó eszköz átadás átvételének körülményeit.(helyszín, időpont). .

4.4 Tanúsítvány-elfogadás

Az előzetesen egyeztetett időpontban az aláíró (vagy meghatalmazottja) személyesen veheti át a szerződéses dokumentumokat, valamint a tanúsítványt és magánkulcsot tartalmazó biztonságos aláírás-létrehozó eszközt (az ennek aktivizáló adatát tartalmazó zárt borítékkal együtt) a regisztrációs tisztviselőtől. Az átvételről feljegyzés készül, melyet Szolgáltató megőriz a jogszabályokban előírt időtartamig.

A magánkulcs használatba vétele előtt az aláírónak 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.

4.5 Kulcspár és tanúsítvány használat

4.5.1 Az alany magánkulcs- és tanúsítvány használata

Aláíró magánkulcsát és tanúsítványát kizárólag aláírásra használhatja fel, a Szolgáltatói Szerződésben,valamint jelen Szabályzatban rögzített korlátozásokkal. Aláírónak az adott helyzetben

általában elvárható gondosságot kell tanúsítania annak érdekében, hogy megelőzze magánkulcsának illetéktelen felhasználását (így például védenie kell a biztonságos aláírás létrehozó eszközét, figyelnie kell arra, hogy az aktivizáló kódja ne tudódjon ki, az eszköz illetve a kód ne jusson illetéktelenek birtokába, kompromittálódás esetén visszavonást kell kérnie). Tanúsítvány elfogadás előtt illetve lejárat után Aláíró nem használhatja fel a magánkulcsát.

4.5.2 Az érintett felek nyilvános kulcs- és tanúsítványhasználata

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

- Az érintett fél csak olyan célokra és olyan alkalmazásokkal fogadhat el nyilvános kulcsokat, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat" és „kiterjesztett kulcshasználat" mezőinek tartalmával.
- Mielőtt egy tanúsítványba foglalt nyilvános kulcsot felhasználna, az érintett félnek ellenőriznie kell a tanúsítvány érvényességét, valamint azt, hogy a tanúsítvány nincs felfüggesztve, illetve visszavonva az érvényes visszavonási állapot információ alapján (a 4.9 fejezetnek megfelelően),
- Amennyiben ésszerű módon egy tanúsítványra kíván hagyatkozni, az érintett félnek figyelembe kell vennie a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban és a tanúsítványt kibocsátó szolgáltató szabályzatokban szerepel.

A tanúsítványra vonatkozó ellenőrzéseket érintett félnek ajánlott elvégeznie a **teljes tanúsítási láncra** vonatkozóan. Ha a tanúsítvány vagy a tanúsítási lánc tanúsítványainak valamely adata érvénytelenségére utal, illetve ha az adott kontextusban nem elfogadható, akkor a tranzakciót és a tanúsítvány elfogadását az érintett félnek vissza kell utasítania.

4.6 Tanúsítvány megújítás

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.

A közigazgatási tanúsítványok esetében Szolgáltató az érvényes tanúsítványok megújítását lehetővé teszi. Tanúsítvány megújítás esetén Szolgáltató egy lejáró tanúsítványhoz kapcsolódóan úgy bocsát ki egy új (megújított) tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai (köztük a nyilvános kulcs is) változatlanok.

Tanúsítvány megújítást a lejáró tanúsítvány alanya (Aláíró) kell kezdeményezze a Szolgáltató honlapján, elektronikus úton, a tanúsítvány lejáratát megelőzően legalább 10 munkanappal. A megújításhoz a Szolgáltató honlapján található űrlap kitöltésével és az űrlap elektronikus úton történő aláírásával írásban kell nyilatkoznia arról, hogy az adatai változatlanok, majd az így aláírt űrlapot el kell küldenie a Szolgáltató regisztrációs szervezetének e-mailben.

Ez alapján Szolgáltató regisztrációs szervezete az Aláíró adatait ellenőrzés nélkül elfogadja. Ellenőrzi viszont azt, hogy a tanúsítvány nem járt-e le és nincs-e visszavonva. Amennyiben a szolgáltatásra vonatkozó feltételek megváltoztak, Szolgáltató regisztrációs szervezete tájékoztatja az előfizetőt, és erről - valamint a feltételek elfogadásáról - írásos feljegyzést készít. Ha az előfizetőre vagy az alanyra vonatkozó adatok megváltoztak, azt ugyanezen feljegyzésben kell rögzíteni. Ez esetben a megváltozott adatokat a regisztrációs szervezet az új tanúsítvány kibocsátására irányadó eljárás szerint ellenőrzi. Amennyiben minden szükséges ellenőrzés megtörtént, Szolgáltató kibocsátja az új (megújított) tanúsítványt, és közzéteszi azt a publikus címtárában.

A kibocsátásról Szolgáltató e-mailben értesíti az Aláírót, aki a tanúsítványt rátölti a lejáró tanúsítványt is tartalmazó chipkártyájára. Letöltéskor az új tanúsítvány felülírja a régit, és mivel a megújított tanúsítvány érvényességi idejének kezdő időpontja megegyezik a régi tanúsítvány lejárati dátumával, előfordulhat, hogy néhány napig még nem érvényes a megújított tanústvány, ílletve a hozzá kapcsolódó aláírás sem. Ezt a használat során javasolt figyelembe venni[33].

Megújított tanúsítvány elfogadása az első használatba vétellel, azaz az első elektronikusan történő aláírással valósul meg.

Az [MTT+BALE] Hitelesítési Rendben meghatározott tanusítványok megújítását Szolgáltató nem teszi lehetővé.

4.7 Kulcscsere

A hitelesítés szolgáltató a kulcscserét oly módon teszi lehetővé, hogy gyakorlatilag új tanúsítványt állít ki, az erre vonatkozó eljárás (4.1 – 4.4) szabályai szerint.

4.8 Tanúsítványmódosítás

A hitelesítés szolgáltató a tanúsítvány módosítás oly módon teszi lehetővé, hogy gyakorlatilag új tanúsítványt állít ki, az erre vonatkozó eljárások (4.1 – 4.4) szabályai szerint.

4.9 Tanúsítvány visszavonás és felfüggesztés

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.

[33] Megjegyezzük, hogy ha Aláíró a megújított tanúsítványt túl hamar töltötte le a kártyára és ezáltal felülírta a régi tanúsítványát, a helyzetet megoldhatja oly módon, hogy a Szolgáltató tanúsítvány tárából kikeresi a régi - még érvényes tanúsítványát, és rátölti a kártyára; majd a lejárat előtt közvetlenül ismét rátölti a megújított tanúsítványát az eszközre.

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[34]:

- a visszavonási/felfüggesztési kérelem Szolgáltatóhoz történő megérkezéséig az aláíró és előfizető felelős a felmerülő károkért az Általános Szerződési Feltételeknek (**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.

4.9.1 A visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásához a következő körülmények vezetnek.

Aláíró és előfizető 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,
- 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.

Tanúsítvány megújítás esetén nincs szükség a régi (lejáró) tanúsítvány idő előtti visszavonására, ugyanis a megújított tanúsítvány érvényességének kezdeti időpontja megegyezik a régi tanúsítvány lejárati időpontjával.

Egyéb visszavonáshoz vezető körülmények:

- az Aláíró halála, az előfizető halála vagy megszűnése,

[34] ld. [1] törvény 14. § (4)

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

Különleges esetnek minősült a Szolgáltató 2005.-ös névváltása kapcsán a végfelhasználói tanúsítványok cseréje. Ennek keretében az aláírók ill. előfizetők előzetes megkeresése és tájékoztatása alapján a Szolgáltató által visszavonásra került az összes (Matáv néven) kibocsátott és 2005.10.01-én érvényes minősített tanúsítvány, és helyettük – ingyenesen - új minősített tanúsítvány kerül(t) kibocsátásra a szokásos 1 éves érvényességi időtartammal, melyben az aláíró / előfizető adatai nem változnak, de a „Kibocsátó" már Magyar Telekom néven szerepel.

4.9.2 Kik kérelmezhetik a visszavonást?

Végfelhasználói tanúsítvány visszavonását az **aláíró**, **előfizető**, **Szolgáltató**, vagy egy hatóság is kezdeményezheti.[35] Az **aláíró**nak, **előfizető**nek és **Szolgáltató**nak kötelessége a **4.9.1** {**A visszavonás körülményei**} alfejezetben feltűntetett esetekben a visszavonás azonnali kezdeményezése, illetve végrehajtása.

4.9.3 Visszavonási kérelemre vonatkozó eljárás

Visszavonást illetve felfüggesztést telefonon, személyesen illetve írásban lehet kezdeményezni, az alábbiak szerint.

Tanúsítvány felfüggesztése telefonos kezdeményezés alapján

A tanúsítvány visszavonási kérelmét aláírónak telefonon kell bejelentenie a 24 órás ügyeleti regisztrációs operátorokhoz, a 06 80 20 40 40 telefonszámon. A bejelentéskor meg kell adnia nevét, a tanúsítványban levő e-mail címét, a visszavonási jelszavát (transfer-PIN) és amennyiben emlékszik – a tanúsítvány sorozatszámát, végül pedig egy telefonszámot, amelyen vissza lehet hívni.

Az első két adat alapján az ügyeleti operátor azonosítja a tanúsítványt, a visszavonási jelszó alapján pedig azonosítja az aláírót egyszersmind a kód segítségével **felfüggeszti** a tanúsítványt, mely ezt követően automatikusan megjelenik egy soron kívül generálódó CRL-ben. A telefonos bejelentés és a CRL kibocsátása között maximum két óra telhet el.

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

Fontos tudni, hogy a visszavonási jelszó alapján az operátor csak felfüggeszti a tanúsítvány; a visszavonáshoz az aláíró írásos (vagy személyes) megerősítése szükséges, melyet három napon belül el kell juttatnia a regisztrációs szervezet részére. A felfüggesztett tanúsítvány csak akkor kerül visszavonásra, amikor aláíró írásos kérelme a regisztrációs szervezethez beérkezett, vagy az aláíró személyesen megjelent a regisztrációs szervezetnél. Amennyiben 3 napon belül nem érkezik meg a megerősítés, a Hitelesítő Szervezet visszavonja a tanúsítványt.

Amennyiben az aláíró nem emlékszik a visszavonási jelszavára, vagy rossz jelszót ad meg, a tanúsítványt az ügyeleti operátor nem tudja felfüggeszteni. Ilyenkor az ügyeleti operátor telefonon értesíti aláírót a felfüggesztés sikertelenségéről.

Tanúsítvány visszavonása személyes megjelenés alapján

Aláíró (vagy a szervezet törvényes képviselője) személyesen is kezdeményezheti a visszavonást (vagy a felfüggesztést). Ehhez személyes megjelenés szükséges a regisztrációs szervezet telephelyén (ld. 1.4 fejezetet) a regisztrációs tisztviselőnél.

A személyazonosságot a kérvényezőnek érvényes személyazonosító okmánnyal kell igazolnia. Szervezet törvényes képviselőjének a szükséges céges igazolásokat is be kell mutassa. Ezek alapján a regisztrációs tisztviselő ellenőrzi a kérvényező jogosultságát. Amennyiben a kérvényező jogosultsága nem nyer igazolást, a regisztrációs tisztviselő megtagadja a tanúsítvány visszavonását.

Jogos igénylés esetén a regisztrációs tisztviselő értesítése alapján a hitelesítő szervezet munkatársa visszavonja a tanúsítványt, mely ezt követően automatikusan megjelenik egy soron kívül generálódó CRL-ben. A személyes megjelenés és a CRL kibocsátása között maximum két óra telhet el.

Tanúsítvány Visszavonása / felfüggesztése írásos kezdeményezés alapján

Üzleti tanúsítvány esetén a tanúsítvány visszavonását / felfüggesztését az aláíró (vagy Szervezet törvényes képviselője) írásban is kezdeményezheti, az e-Szignó honlapon található erre a célra szolgáló formanyomtatvány kitöltésével és a Regisztrációs Szervezethez történő eljuttatásával (posta, fax).

Faxon beérkezett kérelem esetén csak felfüggesztésre kerül sor, a végleges visszavonáshoz szükség van az írásos megerősítés beérkezésére is.

A visszavonási kérelemnek a következő adatokat kell tartalmaznia:

- A Tanúsítvány sorozatszáma, típusa,
- Aláíró neve, email címe,
- a visszavonást kérő megnevezése
- a visszavonást kérő beosztása
- 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.

Jogos igénylés esetén a regisztrációs tisztviselő értesítése alapján a hitelesítő szervezet munkatársa visszavonja a tanúsítványt, mely ezt követően automatikusan megjelenik egy soron kívül generálódó CRL-ben. Az írásos kérelem regisztrációs tisztviselőhöz történő beérkezése és a CRL kibocsátása között maximum két óra telhet el.

4.9.4 Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási kérelmet azonnal be kell nyújtani az ezért felelős személynek, amikor valamelyik visszavonáshoz vezető körülményről {ld. **4.9.1 A visszavonás körülményei**} értesül.

4.9.5 A visszavonási idő maximális hossza

A visszavonási idő maximális hossza a 4.9.3. pontnak megfelelően két óra.

4.9.6 Az érintett felek kötelezettsége a visszavonási információk ellenőrzésére

A visszavonási információk ellenőrzése a visszavonási lista ellenőrzésével illetve a valós idejű tanúsítvány állapot információk ellenőrzésével tehető meg.

A visszavonási lista ellenőrzése az érintett felek részére javasolt a tanúsítványok elfogadását megelőzően. A tanúsítványhoz tartozó visszavonási lista elérhetősége bele van foglalva a tanúsítványba. Amennyiben az érintett felek kellő gondossággal kívánnak eljárni, akkor a lista ellenőrzésének arra kell vonatkoznia, hogy a kérdéses tanúsítványt a lista tartalmazza-e, a lista hiteles és sértetlen, s a kérdéses tranzakció szempontjából időben releváns-e.

Szolgáltatót nem terheli felelősség a visszavonási listában közzétett tanúsítványok elfogadásából keletkező esetleges károkért.

A valós idejű tanúsítvány állapot információk ellenőrzésének követelményeit a 4.9.10 pont tartalmazza.

4.9.7 A visszavonási lista kibocsátási gyakorisága

A visszavonási lista kibocsátása Szolgáltató Címtárából történik. A kibocsátások legfeljebb 24 óránként automaikusan követik egymást, de egy végfelhasználói tanúsítvány visszavonását vagy felfüggesztését követően azonnal új visszavonási lista kerül kibocsátásra. A visszavonási lista mindig tartalmazza a következő lista kibocsátásnak idejét, de Szolgáltató ennél korábban is kibocsáthat új listát.

Szolgáltató gyökér hitelesítő egysége havonta egyszer bocsát ki visszavonási listát.

Visszavonási lista kibocsátására különleges esetekben is sor kerülhet. Ilyen esetnek minősül(t) a Szolgáltató 2005. évi névváltásából adódó tanúsítványok cseréje során a tanúsítványok visszavonása, valamint az ehhez kapcsolódó - hosszú lejáratú - visszavonási lista kibocsátása.

A visszavonási listában a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok az újbóli érvényesítés hatására kikerülnek a listából. A visszavont / felfüggesztett tanúsítványokat Szolgáltató törölheti a listából, a tanúsítvány lejártát követően.

4.9.8 Visszavonási lista előállítása és közzététele közötti idő maximális hossza

Végfelhasználói tanúsítványokra vonatkozó visszavonási lista előállítása és közzététele közötti legfeljebb 1 óra telhet el.

4.9.9 Valós idejű tanúsítvány állapot ellenőrzés elérhetősége

Szolgáltató valós idejű visszavonási állapot-szolgáltatást is nyújt Aláíró ill. az érintett felek részére, az erre vonatkozó követelményeknek megfelelően ([21][36]). A szolgáltatás nyilvánosan elérhető a következő helyen:

http://ocsp.magyartelekom.hu/ocsp

A szolgáltatásért külön díjat nem kell fizetni. A szolgáltatáshoz az Aláírónak vagy az érintett félnek olyan alkalmazással kell rendelkeznie, mely támogatja a valós idejű tanúsítvány állapot lekérdezést.

4.9.10 Valós idejű tanúsítvány állapot ellenőrzési követelmények

Szolgáltató valós idejű visszavonási állapot-szolgáltatást az erre vonatkozó műszaki követelményeknek megfelelő protokoll (OCSP - Online Certificate Status Protokoll) szerint nyújtja.

Az OCSP válaszokat aláíró tanúsítvány profiljának Kibocsátó azonosítóját és Tulajdonos azonosítóját a 7.3 pont tartalmazza. Az OCSP szolgáltatás által kiadott elektronikusan aláírt válaszokat az elfogadó félnek ellenőriznie kell az elektornikus aláírás ellenőrzésére vonatkozó követelményeknek megfelelően (a válasz illetve az aláírás sértetlen-e, az aláírás a 7.3 pont szerinti tanúsítványon alapul-e, valamint a tanúsítvány érvényes-e, a. 4.9.6 pontnak megfelelően). Az érvénytelennek bizonyult OCSP válaszokat elfogadni nem szabad, ez esetben elfogadó félnek a visszavonási listára kell támaszkodnia.

[36] RFC 2560 - Internet X.509 Nyilvános kulcsú infrastruktúra – Valós idejű tanúsítvány állapot protokoll – OCSP

4.9.11 A visszavonási hirdetmények egyéb elérhető formái

A visszavonási hirdetmények csak Szolgáltató címtárán illetve a valós idejű tanúsítvány állapot lekérdezés fejezetben megadott címen keresztül érhetők el.

4.9.12 Kulcs kompromittálódásra vonatkozó speciális követelmények

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

4.9.13 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.

A felfüggesztéshez vezető egyéb körülmények:

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

4.9.14 Kik kérelmezhetik a felfüggesztést?

A felfüggesztést ugyanazok kérelmezhetik, akik a visszavonást {ld. **4.9.2 Kik kérelmezhetik a visszavonást?**}

4.9.15 Felfüggesztési kérelemre vonatkozó eljárás

A felfüggesztési kérelem a visszavonási kérelemhez hasonlóan nyújtható be szolgáltatóhoz. Telefonon történő kezdeményezés esetén 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.

4.9.16 A felfüggesztés időtartama

Szolgáltató általi kezdeményezés esetén a 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.

4.10 Tanúsítvány állapot szolgáltatások

Szolgáltató a visszavont tanúsítványok listáját valamint a valós idejű tanúsítvány állapot ellenőrzés elérhetőségét az általa kibocsátott tanúsítványokban meghatározott URL-en elérhetővé teszi (ld. 7.1.2 pontot is).

Szolgáltató biztosítja a tanúsítványtár, valamint az általa kibocsátott tanúsítványok használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét, 99,9%-os rendelkezésre állás mellett, ahol az eseti szolgáltatás-kiesések nem haladhatják meg a 3 órát. Emellett Szolgáltató biztosítja a visszavonási nyilvántartások és a visszavonás kezelési szolgáltatás legalább 99,9%-os rendelkezésre állását, ahol az eseti szolgáltatás-kiesések nem haladhatják meg a 3 órát.

4.11 A tanúsítványelőfizetés vége

A tanúsítvány lejáratakor (amennyiben nem történik megújítás) a szolgáltatásra vonatkozó szerződés automatikusan megszűnik. Amennyiben a szolgáltatásra vonatkozó szerződést Aláíró vagy előfizető fel kívánja mondani a tanúsítvány lejárata előtt, ezt írásban vagy faxon kell bejelenteni a Regisztrációs Szervezet részére.

4.12 Kulcs letétbe helyezése és visszaállítása

Szolgáltató a minősített végfelhasználói tanúsítványokhoz tartozó magánkulcsokat nem őrzi meg, letébe helyezés és visszaállítás szolgáltatást nem nyújt.

Szimmetrikus rejtjelző kulcsokokra vonatkozó rendelkezéseket Szolgáltató nem alkalmaz.

5. Elhelyezési, irányítási és működtetési előírások

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 előírások

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 biztonság növelése érdekében egy falbontás érzékelő riasztó rendszer került telepítésre és beüzemelésre.

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 ipari klíma illetve egy tartalékként létesített 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 biztonság növelése érdekében egy nedvességérzékelő riasztó rendszer került telepítésre és beüzemelésre.

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 Magyar Telekom Nyrt. 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 **A mentési példányok fizikai elkülönítése**}.

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 A mentési példányok fizikai elkülönítése**}.

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 Hulladék megsemmisítése és selejtezés

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 A mentési példányok fizikai elkülönítése

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 Szolgáltató 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 felelős (illetve regisztrációs tisztviselő)
- regisztrációs ügyeleti operátor,
- rendszeroperátor (rendszerüzemeltető):
- rendszervizsgáló.
- szolgáltató informatikai rendszeréért általánosan felelős vezető

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 Egységhez 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 Egységhez 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[37] {ld. 5.1.8 A mentési példányok fizikai elkülönítése} ,
- telepítik, konfigurálják és karbantartják a Regisztrációs Szervezet géptermében üzemeltetett megbízható rendszert,
- beállítják a fenti megbízható rendszer kezdeti hálózati konfigurációját,

[37] Heti rendszerességgel

- 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),
- 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 Szervezethez történő szállításáról[38],
- 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.

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,

[38] Heti rendszerességgel

- aláír(attat)ják a visszavonási listákat,
- kulcspárokat generál(tat)nak az aláírók számára,
- ellenőrzik a biztonságos aláírás-létrehozó eszközök készítését {ld. 6.1.2 pont},
- aktivizálják a biztonságos aláírás-létrehozó eszközöket aktivizáló PIN kódok generálását, kinyomtatását és borítékolását végrehajtó funkciókat {ld. **6.1.4 pont**},
- gondoskodnak a biztonságos aláírás-létrehozó eszközöket aktivizáló, beborítékolt PIN kódok biztonságos tárolásáról (a címzettekhez történő továbbításig) {ld. 6.1.2 pont},
- 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 pont},
- 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 vagy a regisztrációs szervezetnél tevékenykedő **regisztrációs ügyeleti operátorok** felelősek:

- folyamatos, 24 órás ügyfélszolgálati tevékenységért és help desk funkciók fogadásáért,
- 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).

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 pont**}.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Általánosan teljesül a 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 Egységhez 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 Egységhez 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.

Szolgáltató vonatkozó belső szabályzata meghatározza az egyes feladatokhoz szükséges személyzeti létszámokat is.

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.

5.2.4 Egymást kizáró munkakörök

Szolgáltató gyakorlatában a bizalmi munkakörök között **személyi átfedések nincsenek**, minden személy csak egy bizalmi munkakört tölt be, az erre vonatkozó jogszabályi[39] előírásoknak megfelelően.

5.3 Személyzetre vonatkozó előírások

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

Ennek érdekében Szolgáltató külön a személyzetre vonatkozó belső előírással rendelkezik és ezek szerint jár el, így 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:

[39] 3/2005-ös IHM rendelet

- a tájékoztatás valamennyi, a Szolgáltató szolgáltatásaival és az érintett informatikai rendszerével kapcsolatba kerülő munkatárs számára egységes {ld. **5.3.3** pont},
- a továbbképzés moduláris, és az egyes bizalmi munkakörök szerint eltérő felépítésű tananyag szerint történik, a személyre szóló éves továbbképzési terveknek megfelelően {ld. **5.3.4** pont}.

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 bizalmi munkakört betöltő (vagy arra jelölt) személyek és a vezető tisztségviselők esetén büntetlen előélet igazolása (hatósági erkölcsi bizonyítvány beszerzése és bemutatása) is szükséges.

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

- Informatikai rendszerért általánosan felelős vezető:
  - szakirányú felsőfokú végzettség, valamint
  - legalább három év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat.

- biztonsági tisztviselő, rendszer (vagy központi) adminisztrátor, rendszervizsgáló, rendszeroperátor,:
  - középfokú szakirányú végzettség vagy szakképesítés és legalább öt év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat, vagy
  - szakirányú felsőfokú végzettség vagy felsőfokú szakképesítés és legalább három év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat.

- regisztrációs tisztviselő, 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[40] betöltő munkatársra nézve **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 Előélet vizsgálatára és biztonsági háttér ellenőrzésekre vonatkozó eljárások

Valamennyi bizalmi munkakört betöltő munkatárs biztonsági alapellenőrzésen esik túl {ld. 5.3.1}, emellett mindenkinek időszakos biztonsági ellenőrzéseken is át kell esniük.

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a “elfogadhatatlanul nagy biztonsági kockázat” minősítést kapja[41].

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.

---

[40] Ez a meghatározás az *adattár-felelős* és az ügyeleti operátor munkakör kivételével az összes többi munkakörre vonatkozik

[41] Ilyen esetekben Szolgáltató gondoskodik a megfelelő személy kijelöléséről.

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).

5.3.4 Továbbképzési gyakoriságok és követelmények

Minden bizalmi munkakört betöltő munkatárs esetében 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 Szervezettel) 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 nem részesülnek, erre nem kötelezettek[42].

5.3.8 A személyzet számára biztosított dokumentációk

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

- a kinevezési eljárás, illetve az alapkiképzés során:
  - Szolgáltató szervezeti biztonságpolitikája,
  - aláírt titoktartási nyilatkozat,
  - egyéni munkaköri leírás,
- a tervezett és rendkívüli továbbképzések 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),

[42] 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.

- 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.

5.4 Naplózási eljárások

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.

5.4.1 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.

5.4.2 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.

5.4.3 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.[43]

5.4.4 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 mentések védik (ld. 5.4.5 pont). 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.

5.4.5 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 erre vonatkozó belső szabályzatai írják le részletesen.

5.4.6 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.

5.4.7 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 Szolgáltatóval való együttműködés (kivéve ha a Szolgáltatóval nem állnak szerződéses viszonyban).

[43] ld. [1] törvény 9. § (7)

5.4.8 Log-elemzés

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

5.5 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.

5.5.1 Az archivált adatok típusai

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

- a Szolgáltatóhoz 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.

5.5.2 Az archívum megőrzési időtartama

Szolgáltató valamennyi (papíralapú vagy elektronikus) iratot a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított **10 évig**, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrzi.[44]

5.5.3 Az archívum védelme

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

[44] ld. [1] törvény 9. § (7)

A Szolgáltató a hitelesítésszolgáltatás során elektronikus formában tárolt archivált adatállományt minősített aláírással és időbélyegzővel látja el.

5.5.4 Az archívum mentési folyamatai

Az elektronikus másolati példányban létező iratokat (amennyiben keletkeznek ilyenek) egyszer írható médiára rendszeresen mentik.

5.5.5 A rekordok időbélyegzésére vonatkozó követelmények

Lásd az 5.5.3 alfejezetet.

5.5.6 Az archívum gyűjtési rendszere

A regisztráció során keletkezett papíralapú iratokat az Adattárban tárolják és őrzik. Az elektronikus másolatok elektronikus adathordozón, biztonságos formában kerülnek az Adattár archívumába[45].

5.5.7 Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés aláírónak és előfizetőnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 9.4.4, 9.4.5. és 9.4.6 alfejezetek szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és azt naplózza.

5.6 Kulcscsere

Szolgáltató nem alkalmaz egyedi szabályokat erre vonatkozóan; az új kulcs a régivhez hasonló módon kerül kiadásra.

5.7 Kompromittálódást és katasztrófát követő helyreállítás

5.7.1 Váratlan esemény és kompromittálódás kezelési eljárások

Rendkívüli üzemeltetési helyzet bekövetkezése esetén a szolgáltató haladéktalanul értesíti a Hatóságot 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."

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

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.

Kompromittálódás esetén az 5.7.3 alfejezetben írtak kerülnek alkalmazásra.

5.7.2 Meghibásodott 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.

5.7.3 Egy szolgáltatói egység kulcsának kompromitálódása

Szolgáltató katasztrófa elhárítási terve a szolgáltatói magánkulcsok[46] kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik az ez által érintett valamennyi fél értesítéséről, megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet.

A szolgáltatói nyilvános kulcsok visszavonásáról Szolgáltató a **2** fejezetnek megfelelően értesítést tesz közzé.

5.7.4 Működés folyamatosságának biztosítása katasztrófát követően

Szolgáltató **elsődleges működési helyszín**ein kívül másodlagos helyszínekkel is rendelkezik[47]. Természeti vagy más katasztrófát követően, illetve Szolgáltató berendezéseinek olyan mértékű meghibásodását illetően, mely a fentiek szerint nem kezelhető, Szolgáltató a másodlagos helyszínen is képes szolgáltatásainak beindítására.

---

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

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

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.

5.8 Hitelesítésszolgáltató vagy regisztrációs szervezet leállítása

A Szolgáltató a szolgáltatás tervezett megszűntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Hatóságot[48]. 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.

Szolgáltató a tervezett megszűnés előtt legalább **20 nappal** intézkedik a végfelhasználói tanúsítványok visszavonásáról[49]. 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 átadja egy ilyen szolgáltatónak.

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 Hatóságot. A Szolgáltató az aláírókat és az előfizetőket elektronikus levélben, az érintett feleket az internetes honlapon történő közzététel útján tájékoztatja. A Szolgáltató a Gyökér Hitelesítő Egység tanúsítványának visszavonását **5 nappal megelőzően** hirdetményt tesz közzé.

[48] ld. [1] törvény 16. § (1)
[49] ld. [1] törvény 16. § (1)

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.

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 Szolgáltató 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 Magyar Telekom 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 kulcsok,
- Időbélyeget aláíró kulcs (TrustedTimeStamp szerverek kulcsai)

- OCSP válaszokat aláíró kulcs
- Viszontazonosítási válaszokat 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.

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 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 állít 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 az előfizetőhöz

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 biztonsági tisztviselő engedélye alapján a tulajdonos személyesen veheti át a hozzáférési kódokkal együtt a Regisztrációs Szervezetnél.

Az **aláírók** magánkulcsát - a védett tárolást és felhasználást biztosító biztonságos aláírás-létrehozó eszközzel együtt - a **regisztrációs tisztviselők személyesen az aláíró**knak (vagy meghatalmazottjuknak) 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. Fentiek alól kivételt képez a közigazgatási tanúsítványokat kibocsátó hitelesítő egység nyilvános kulcsa, amelynek tanúsítványát a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGYHSZ) állítja ki, az erre vonatkozó hatósági eljárásnak megfelelően.

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 szolgáltatói nyilvános kulcsokat tartalmazó tanúsítványokat a **Címtár**ban, valamint a Szolgáltató honlapján.

Ez vonatkozik a Szolgáltató saját gyökér hitelesítő egységének nyilvános kulcsára illetve tanúsítványára is. A közigazgatási tanúsítványokat kibocsátó hitelesítő egység tanúsítványát aláíró Közigazgatási Gyökér Hitelesítés-szolgáltató nyilvános kulcsának illetve tanúsítványának közzététele a www.kgyhsz.gov.hu oldalon történik, ahol a tanúsítvány lenyomata is megtalálható.

A Szolgáltató saját Gyökér Hitelesítő Egységével kapcsolatos információkat (pl. tájékoztató a visszavonásról, kiadásról, illetve a tanúsítvány lenyomata) egy országos terjesztésű napilapban is közzéteszi.{Id. 1.3.1}.

6.1.5 Kulcs méretek

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

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

az Időbélyegző szerverek 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 és ellenőrzése

A Hitelesítő Szervezet és a Regisztrációs Szervezet digitális aláírásra az RSA algoritmust 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.

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.

6.1.7 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***	**K**

6.2 A Szolgáltatói magánkulcsok védelme és a kriptográfiai modulokkal kapcsolatos előírások

A Szolgáltató gondoskodik valamennyi általa (saját maga, Regisztrációs Szervezet, illetve aláírók 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.

A Hitelesítő Szervezet kulcsainak generálása egy nCipher nShield F3 PCI hardver eszközzel történik amely FIPS 140-2 szabvány[50] szerint 3. szinten bevizsgált HSM. Az eszköz rendelkezik a Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezet (Hunguard Kft.) által erre a célra kiadott kiadott igazolással.

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).

Fentiek során a Nemzeti Hírközlési Hatóság által a [23] dokumentumban jelzett algoritmusokat használata megengedett.

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

A Szolgáltatói magánkulcs visszaállításánál (a Hitelesítő Szervezetben) az ebben részt vevő bizalmi munkakört betöltő személyek alkalmazzák az “n-ből m” ellenőrzést a magánkulcsokkal kapcsolatos kulcsgondozási funkciók aktivizálásánál (ld. még 6.2.4).

[50] Ld. [6] hivatkozás

6.2.3 Magánkulcs letétbe helyezése

Szolgáltatónál **magánkulcsot** nem lehet letétbe helyeztetni.

6.2.4 Magánkulcs mentése

A Szolgáltatónál a következő magánkulcsok nem kerülnek mentésre. A Hitelesítő Szervezet magánkulcsait ugyanis az nCipher nShield F3 PCI kriptográfiai hardver (FIPS 140-2 level3) modulja **maga generálja**, és a magánkulcs semmilyen körülmények között nem hagyja el a modult. Mentésre a kulcs helyreállításához szükséges titokrészek kerülnek. A titokrészek a kulcsgenerálást követően egy 3 kártyából álló kártya szettre, illetve egyes titokrészek a rendszerkörnyezetben kerülnek tárollásra, mentésre, melyek védelme fokozott biztonsági intézkedésekkel van megoldva.

Ha a fenti aláíró magánkulcsok megsemmisülnek, akkor ezeknek helyreállítása a gyártó által biztosított (FIPS 140-2 level3 szinten tanúsított) funkcióval, a titokmegosztás elve alapján történik (3 kártyából bármelyik kettőnek illetve a rendszerkörnyezet mentésének alkalmazásával).

6.2.5 Magánkulcs archiválása

A Szolgáltatónál **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./ Ha a magánkulcsok megsemmisülnek, akkor ezek helyreállítása a 6.2.4 pont szerint történik.

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 Magánkulcs tárolása a kriptográfiai modulba

A szolgáltatói magánkulcsok tárolása külön kriptográfiai modulban történik, a hozzáfáérés-ellenőrzésekkel együtt az előző alfejezeteknek megfelelően.

6.2.8 A magánkulcs aktiválásának 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 az intelligens kártyájának hitelesítő adatát (PIN).

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

6.2.9 A magánkulcs aktív állapotának megszüntetési módja

Hitelesítő szervezet

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

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

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

Az intelligens kártyák (ALE) (CardPerso operator card set) magánkulcsai akkor deaktiválódnak, 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 deaktivált magánkulcsok mindaddig nem használhatók, amíg az intelligens kártya ismét aktív állapotba nem kerül.

Regisztrációs szervezet

Az intelligens kártyák (ALE) magánkulcsai akkor deaktiválódnak, 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 deaktivált magánkulcsok mindaddig nem használhatók, amíg az intelligens kártya ismét aktív állapotba nem kerül.

6.2.10 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.

Aláíró magánkulcsának megsemmisítés az Aláíró felelőssége.

6.2.11 A kriptográfiai modulok értékelése

A 6.2.1 ponttal összhangban az alábbi táblázat tartalmazza a 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 visszaállítás/resetelés/) • 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 illetve a Nemzeti Hírközlési Hatóság által a [23] dokumentumban jelzett algoritmusokat alkalmaznak.
Öntesztek	A modulok képesek öntesztek végrehajtására, annak kimutatására, hogy megfelelően működnek
Értékelési szint	FIPS 140-2 szabvány szerint 3. szinten bevizsgált

6.3 A kulcspár kezelésének egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

A Szolgáltató minden általa 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 Szervezetben dolgozó rendszeroperátorok a felelősek.

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

6.3.2 A tanúsítványok és a kulcspárok 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.

Az **aláíró** részére kibocsátott chipkártyához egy PIN-boríték is átadásra kerül, mely tartalmaz egy PUK kódot valamint egy PIN-kódot. Ez utóbbi egy ötjegyű kód[51], amelynek segítségével a legelső használat előtt az **aláíró** köteles beállítani a végleges PIN-kódot („Aláírói PIN"), mely minimum hatjegyű kód.

A **Hitelesítő Szervezet** által kibocsátott aláírás-létrehozó eszközök aktivizáló adatainak kezelése a kibocsátást követően az aláíró felelőssége. Aláírónak a tőle elvárható gondossággal kell eljárnia az aktivizáló adatainak védelme és használata során.

6.4.3 Az aktivizáló adatok egyéb szempontjai

Az aktivizáló adatok felhasználására vonatkozóan Aláírónak a következőket kell tudni.

A borítékban található ötjegyű PIN-kód (transzport PIN) egyben az Aláíró visszavonási jelszava is, ezért ezt meg kell jegyeznie, mivel egy szüksége lehet rá a tanúsítvány visszavonásánál (ld. 4.9.3).

A minősített elektronikus aláírás készítésekor az előző alfejezet szerint beállítot minimum hatjegyű Aláírói PIN-kódot kell Aláírónak megadni.

A chipkártyához tartozó felhasználói alkalmazásban szereplő „Global PIN" megegyezik a borítékban található ötjegyű PIN-kóddal. Ezt akkor kell használni, ha a chipkártyára Aláíró nem minősített tanúsítványt szeretne telepíteni, illetve az ehhez kapcsolódó magánkulcsot használni szeretné.

Ha az Aláírói PIN-kód blokkolásra kerül, annak feloldását Aláíró a borítékban található PUK kód felhasználásával teheti meg.

Ha viszont a Global PIN (amely megegyezik a transzport PIN-nel) blokkolódik, akkor a kártyát többet nem lehet felhasználni, azt a Szolgáltató sem tudja feloldani.

[51] A borítékban található ötjegyű PIN kódot „transzport PIN-nek" is nevezik, mivel ezzel ellenőrizhető a szállítás során az esetleges illetéktelen használat.

6.5 Informatikai biztonsági óvintézkedések

6.5.1 Speciális informatikai biztonsági műszaki követelmények

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

Root CA

- Operációs rendszer (Debian GNU/Linux + X),
- Kernel-verzió: folyamatosan frissített stabil verzió,
- Tanúsítvány kibocsátó alkalmazás (iPlanet CMS 4.2 SP2),
- Kriptográfiai hardver modul PCI csatolón (HSM).

Operational CA

- Operációs rendszer (Debian GNU/Linux + X),
- Kernel-verzió: folyamatosan frissített stabil verzió
- 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

Az időbélyegző rendszerbe két darab Trusted Time StampServer SA200n kerül beépítésre. Az SA200n 1024 bites kulcshossz esetén másodpercenként 120, 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 Trusted Time StampServer 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 (visszavonási szolgáltatáshoz +SFTP server)

- Operációs rendszer (Debian GNU/Linux + X),
- Kernel verzió folyamatosan frissített stabil verzió
- Registration Manager (iPlanet CMS 4.2 SP2)

LDAP (Master LDAP, Auth.LDAP)

- Operációs rendszer (Debian GNU/Linux + X),
- Kernel verzió: folyamatosan frissített stabil verzió.

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 GNU/Linux + HA (HeartBeat HA szoftver)],
- Kernel verzió: folyamatosan frissített stabil verzió

Tűzfal ALF (HA gép-pár)

- Operációs rendszer (Debian GNU/Linux + X),
- Kernel verzió: folyamatosan frissített stabil verzió,
- ALF tűzfal szoftver.

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 GNU/Linux + 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 {**6.2.11 A kriptográfiai modul értékelése**} alfejezeteket.

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

- Windows XP,
- fejlesztett RA kliens alkalmazás.

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 tanúsítványok 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 azon informatikai rendszerével, mely a Hitelesítő Szervezet rendszerével kapcsolatos, nem folytat kommunikációt a végfelhasználókkal.

6.8 Időbélyegzés

Szolgáltató időbélyeggel látja el az elektornikus formában tárolt archivált adatállományt (ld. 5.5.3 pont). Emellett Szolgátlató időbélyeget használ a szolgáltatás leállításával kapcsolatos eljárás során, az 5.8 fejezettel összhangban.

Fentieken túl Szolgáltató ügyfeleinek is nyújt időbélyegzés szolgáltatást, az 1.1.8. alfejezetnek megfelelően.

7. Tanúsítvány-, CRL- és OCSP profilok

7.1 Tanúsítványprofilok

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

Mezőnév	Érték vagy szabály
Verzió *Version*	A tanúsítvány a [12] ajánlásban leírt X509 3-as verziójú tanúsítványnak felel meg {ld. **1.8 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.**7.1.4**}.
Érvényesség *Valid From & Valid To*	A tanúsítvány érvényességének kezdete és vége[52], 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] ajánlásban szereplő X509 3. verziónak megfelelő szolgáltatói és végfelhasználói tanúsítványokat bocsát ki.

[52] A két időpont közötti időtartam 1 év

7.1.2 Tanúsítvány-kiterjesztések

A Szolgáltató által kiadott, [MTT+BALE] Hitelesítési Rendben meghatározott minősített tanúsítványok **kiterjesztései** a következők:

Mezőnév	Érték vagy szabály	Kritikus
Tanúsítvány irányelv *Certificate Policies*	Policy Identifier=1.3.6.1.4.1.17835.7.1.2.8.2.1.12.2.1.5 Policy Qualifier=http://www.magyartelekom.hu User Notice="A tanúsítvány elfogadása előtt ismerje meg a Hitelesítési Rend és a minősített HSZSZ előírásait a http://www.magyartelekom.hu internetoldalakon"{Id. **7.1.6**}	Nem
Tulajdonos alternatív neve *SubjectAltName*	Aláíró email címe, a [9] ajánlásnak megfelelően (rfc822Name)	Nem
Alapvető megkötések *Basic Constraints*	Subject Type=End Entity Path Length Constraint=None	Igen
Kulcshasználat *Key Usage*	NonRepudiation	Igen
CRL szétosztási pont *CRL Distribution Points*	[1] CRL elérési helye URL=ldap://trustcenter.magyartelekom.hu:389/cn=Magyar%20Telekom%20Minositett%20CA,c=HU?certificateRevocationList?base?objectClass=certificationAuthority [2] CRL elérési helye URL=http://www.eszigno.t-systems.magyartelekom.hu/download_crl?issuer=Magyar%Telekom%Minositett%CA	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:	0 HUF 10.000.000 HUF 100.000.000 HUF 500.000.000 HUF (megállapodás alapján)	Nem
Adatmegőrzési idő *Retention time of data*	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 dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi.	Nem
QcSSCD nyilatkozat OID:	Szolgáltató kijelenti, hogy a jelen tanúsítványhoz tartozó magánkulcs a 2001. évi XXXV. törvény szerinti biztonságos aláírás létrehozó eszközön (BALE) van tárolva	
Megjegyzés	Figyelem! Ez a Magyar Telekom által BALE-eszközön kibocsátott	

Netscape Comment	minősített üzleti tanúsítvány, amelyre a Szolgáltató szabályzata vagy egyedi megállapodás szerinti értékhatárig vállal felelősséget. További információk a www.magyartelekom.hu weboldalon.	

Az [MHR_K] Hitelesítési Rendben meghatározott, azaz köztisztviselő részére kiadott minősített aláíró tanúsítványokban a Szolgáltató által alkalmazott kiterjesztések (a [18]-nak megfelelően) az alábbiak.

Mezőnév	Érték vagy szabály	Kritikus
CA kulcsazonosítója *Authority keyIdentifier*	A Szolgáltató által generált adat, a [18] ajánlásnak megfelelően	Nem
Tulajdonos kulcsazonosítója *Subject keyIdentifier*	A Szolgáltató által generált adat	Nem
Kulcshasználat *Key Usage*	NonRepudiation	Igen
Tanúsítvány irányelv *Certificate Policies*	[1] Policy Identifier=0.2.216.1.100.42.101.2.2.1 [1.1] policyQualifierID=CPS qualifier=http://eszigno.t-systems.magyartelekom.hu/ismerteto/szolgaltatasfeltetelei.vm [1.2] policyQualifierID=User Notice qualifier=A tanúsítvány tulajdonosa: a közigazgatásban eljáró személy. A tanúsítvány elfogadása előtt ismerje meg az ÁSZF, a Hitelesítési Rend és a minősített HSZSZ előírásait a Magyar Telekom honlapján.	Nem
Tulajdonos alternatív neve *SubjectAltName*	Aláíró email címe, a [18] ajánlásnak megfelelően (rfc822Name)	Nem
Alapvető megkötések *Basic Constraints*	Subject Type=End Entity Path Length Constraint=None	Igen
CRL szétosztási pont *CRL Distribution Points*	[1] CRL elérési helye URL=ldap://trustcenter.magyartelekom.hu:389/cn=Magyar%20Telekom%20Minositett%20KET%20CA,c=HU?certificateRevocationList?base?objectClass=certificationAuthority [2] CRL elérési helye URL=http://www.eszigno.t-systems.magyartelekom.hu/download_crl?issuer=Magyar%20Telekom%20Minositett%20KET%20CA	Nem
Internet Certificate Extensions	[1] Authority Information Access accesMethod 1.3.6.1.5.5.7.48.2 (szolgáltatói tanúsítvány hozzáférés OID) URL=http://eszigno.t-systems.magyartelekom.hu/eszignohitelesitokozpont/szolgaltatoitanusitvanyok.vm [2] Authority Information Access accesMethod 1.3.6.1.5.5.7.48.1 (OCSP szolgáltatás hozzáférés OID)	Nem

	URL=http://ocsp.magyartelekom.hu/ocsp	
Megfelelőség *QC Compliance*	A Szolgáltató kijelenti, hogy ez a tanúsítvány - a 2001. évi XXXV. törvény és végrehajtási rendeletei alapján - minősített tanúsítvány.	Nem
Tranzakciós limit *Transaction limit*	0 HUF 10.000.000 HUF 100.000.000 HUF 500.000.000 HUF (megállapodás alapján)	Nem
Adatmegőrzési idő *Retention time of data*	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 dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi.	Nem
QcSSCD nyilatkozat	Szolgáltató kijelenti, hogy a jelen tanúsítványhoz tartozó magánkulcs a 2001. évi XXXV. törvény szerinti biztonságos aláírás létrehozó eszközön (BALE) van tárolva	Nem

Az [MHR_Ü] Hitelesítési Rendben meghatározott, azaz közigazgatás ügyfele számára kiadott minősített aláíró tanúsítványokban a Szolgáltató által alkalmazott kiterjesztések (a [18]-nak megfelelően) az alábbiak.

Mezőnév	Érték vagy szabály	Kritikus
CA kulcsazonosítója *Authority keyIdentifier*	A Szolgáltató által generált adat, a [18] ajánlásnak megfelelően	Nem
Tulajdonos kulcsazonosítója *Subject keyIdentifier*	A Szolgáltató által generált adat	Nem
Kulcshasználat *Key Usage*	NonRepudiation	Igen
Tanúsítvány irányelv *Certificate Policies*	[1] Policy Identifier=0.2.216.1.100.42.101.1.2.1 [1.1] policyQualifierID=CPS qualifier=http://eszigno.t-systems.magyartelekom.hu/ismerteto/szolgaltatasfeltetelei.vm [1.2] policyQualifierID=User Notice qualifier=A tanúsítvány tulajdonosa: a közigazgatás ügyfele. A tanúsítvány elfogadása előtt ismerje meg az ÁSZF, a Hitelesítési Rend és a minősített HSZSZ előírásait a Magyar Telekom honlapján.	Nem
Tulajdonos alternatív neve *SubjectAltName*	Aláíró email címe, a [18] ajánlásnak megfelelően (rfc822Name)	Nem
Alapvető megkötések *Basic Constraints*	Subject Type=End Entity Path Length Constraint=None	Igen
CRL szétosztási pont *CRL Distribution Points*	[1] CRL elérési helye URL=ldap://trustcenter.magyartelekom.hu:389/cn=Magyar%20Telekom%20Minositett%20KET%20CA,c=HU?certificateRevocationList?base?objectClass=certificationAuthority	Nem

	[2] CRL elérési helye URL=http://www.eszigno.t-systems.magyartelekom.hu/download_crl?issuer=Magyar%20Telekom%20Minositett%20KET%20CA	
Internet Certificate Extensions	[1] Authority Information Access accesMethod 1.3.6.1.5.5.7.48.2 (szolgáltatói tanúsítvány hozzáférés OID) URL=http://eszigno.t-systems.magyartelekom.hu/eszignohitelesitokozpont/szolgaltatoitanusitvanyok.vm [2] Authority Information Access accesMethod 1.3.6.1.5.5.7.48.1 (OCSP szolgáltatás hozzáférés OID) URL=http://ocsp.magyartelekom.hu/ocsp	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:	0 HUF 10.000.000 HUF 100.000.000 HUF 500.000.000 HUF (megállapodás alapján)	Nem
Adatmegőrzési idő *Retention time of data*	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 dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi.	Nem
QcSSCD nyilatkozat OID:	Szolgáltató kijelenti, hogy a jelen tanúsítványhoz tartozó magánkulcs a 2001. évi XXXV. törvény szerinti biztonságos aláírás létrehozó eszközön (BALE) van tárolva	Nem

7.1.3 Az algoritmus objektum-azonosítója

Szolgáltató a tanúsítványok aláírásakor az **Sha-1 RSA algoritmust** (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 az aláíró azonosító (Alany/Subject) esetében illetve jelen alfejezet szerint a kibocsátó-azonosító (Kibocsátó/Issuer) esetében.

Az [MTT+BALE] Hitelesítési Rendben meghatározott végfelhasználói tanúsítványok kibocsátó azonosítója (a „Kibocsátó” mező tartalma) a következő:

Jelölés	Jelentés	Adat
CN	a tanúsítvány kibocsátását végző szervezet neve (*Common name*)	Magyar Telekom Minositett CA
O	a szolgáltató szervezet neve (*Organization*)	Magyar Telekom Rt.
OU	a szolgáltató szervezeti egység neve (*Organizational* unit)	Magyar Telekom Trust Center
C	ország név (*Country*)	HU
L	a szervezet székhelye - városnév (*Locality*)	Budapest

Az [MHR_K] és [MHR_Ü] – azaz közigazgatási - végfelhasználói minősített aláíró tanúsítványok kibocsátó azonosítója (a „Kibocsátó” mező tartalma) a következő:

Jelölés	Jelentés	Adat
CN	a tanúsítvány kibocsátását végző szervezet neve (*Common name*)	Magyar Telekom Minositett KET CA
OU	a szolgáltató szervezeti egység neve (*Organizational* unit)	Magyar Telekom Trust Center
O	a szolgáltató szervezet neve (*Organization*)	Magyar Telekom
L	a szervezet székhelye - városnév (*Locality*)	Budapest
C	ország név (*Country*)	HU

Kibocsátó-azonosító a következő módon értelmezendő: a tanúsítványt a Magyar Telekom e-Szignó® Minősített Hitelesítő Szervezete adta ki.

7.1.5 Elnevezésre vonatkozó korlátozások

Szolgáltató ilyen korlátozást nem alkalmaz.

7.1.6 A Hitelesítési Rend objektum-azonosítója

A Szolgáltató által kibocsátott tanúsítványok a vonatkozó **Hitelesítési Rend** egyedi objektum-azonosítóját tartalmazzák {ld. **7.1.2 Tanúsítvány-kiterjesztések**}.

7.1.7 A „Hitelesítési Rend korlátozás” kiterjesztés használata

Szolgáltató ezt a kiterjesztést nem használja.

7.1.8 Szabályzatminősítő szintaxis és szemantika

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

7.1.9 A kritikus Hitelesítési Rend kiterjesztés feldolgozása

Szolgáltató által alkalmazott Tanúsítvány-irányelv 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] ajánlásban leírt X509 2. verziójú visszavonási listának 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. **4.9.7**}. 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] ajánlásban leírt X509 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*	……..…[53]	Nem
Érvénytelenség ideje *Invalidity Date*	……..[54]	Nem
Útmutató *Hold Instruction*	……..[55]	Nem

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

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

Mezőnév	Érték vagy szabály	Kritikus
CRL sorozatszám *CRL number*	……[56]	Nem

7.3 OCSP- profil

Az OCSP válaszok aláírásához kapcsolódó szolgáltatói tanúsítvány kibocsátó azonosítója (a „Kibocsátó” mező tartalma) a következő.

Jelölés	Jelentés	Adat
CN	a tanúsítvány kibocsátását végző szervezet neve (*Common name*)	Magyar Telekom Root CA
OU	a szolgáltató szervezeti egység neve (*Organizational* unit)	Magyar Telekom Trust Center
O	a szolgáltató szervezet neve (*Organization*)	Magyar Telekom Rt.
L	a szervezet székhelye - városnév (*Locality*)	Budapest
C	ország név (*Country*)	HU

Az OCSP válaszok aláírásához kapcsolódó szolgáltatói tanúsítvány tulajdonosának **azonosító**ja (az „Alany” mező tartalma) a következő módon épül fel:

[53] Ebbe a mezőbe a visszavonás oka kerül.

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

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

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

Jelölés	Jelentés	Adat
CN *(Common name/*	Az OCSP válaszokat aláíró kulcs neve	Magyar Telekom OCSP
OU *(Title)*	Az OCSP válaszokat aláíró kulcs szervezeti egységének neve (*Organizational* unit)	Magyar Telekom Trust Center
O *(*Organizatio*n)*	Az OCSP válaszokat aláíró kulcs szervezetének neve	Magyar Telekom
L (*Locality)*	a szolgáltató szervezet neve (*Organization*)	Budapest
C (*Country).*	HU	

A Kibocsátó és Alany mezőkre Szolgáltató az egyedi X.500 név formátumot alkalmazza.

8. Megfelelőségi audit és egyéb ellenőrzések

8.1 Az ellenőrzések körülményei és gyakorisága

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**[57], 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**.

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 megfelelőségének vizsgálatára először 2004-ben a hatósági nyílvántartásba vételi eljáráshoz kapcsolódóan került sor, ezt követően a vizsgálatok a jogszabályoknak megfelelően éves gyakorisággal történnek, a hatósági ellenőrzésekhez igazodva.[58] Emellett a Szolgáltató rendelkezik folyamatosan ellenőrzött minősígirányítási és információbiztonsági irányítási rendszerrel.

A tanúsításhoz és vizsgálatokhoz a Szolgáltató alapvetően külső szervezete(ke)t vesz igénybe {ld. **8.2 Az auditor és szükséges képesítése**}. A Szolgáltató e külső tanúsításokon túl saját belső központi ellenőrzési szervezettel is rendelkezik, mely rendszeresen vizsgálja a korábbi tanúsításoknak való megfelelőséget, és eltérés esetén megteszi a szükséges lépéseket. Ezen felül Szolgáltató informatikai szervezetében saját belső szakértői csoport tevékenykedik, mely a Hitelesítő Szervezet tevékenységét eseti és / vagy tervezett jelleggel megvizsgálja.

[57] Intelligens kártyák (chipkártyák)

[58] ld. [1] 20. §

A Szolgáltató minősített hitelesítés-szolgáltatóként történő önkéntes minősítési (akkreditációs) eljárásban a jelen szabályzat hatályba lépésének időpontjáig nem volt minősítve.

8.2 Az auditor és szükséges képesítése

A kriptográfiai hardver modulok, a saját informatikai rendszerén belül alkalmazott intelligens kártyák és a biztonságos aláírás létrehozó eszközök tanúsítását egy erre feljogosított tanúsító szervezet {ld. [1] törvény[59] 24. §} végezte, melynek kijelölésére a [3] rendelet[60] előírásainak megfelelően került sor. Mindhárom tanúsított elektronikus aláírási terméket a Hatóság nyilvántartásba vette.

A minősített tanúsítványok kezeléshez használt rendszerek és módszerek megfelelőségének vizsgálatára külső, független, a Hatóság által nyilvántartásba vett elektornikus aláírás szakértő által, valamint Szolgáltató erre a célra létrehozott belső központi ellenőrzési szervezetének auditorai által kerül sor.

Emellett a Szolgáltató mind belső, mind pedig külső, független rendszervizsgáló(ka)t is megbíz a minőségirányítási és információbiztonsági rendszerek ellenőrzésére. Ezen szakemberek többéves szakmai gyakorlattal valamint megfelelő végzettséggel és szakképesítéssel rendelkeznek.

Mindezeken felül a Szolgáltatónál a Hatóság is helyszíni szemlét és ellenőrzést tart, évente legalább egyszer.

8.3 Az auditor és az auditált rendszer függetlensége

A Szolgáltatóval kapcsolatban tanúsítást végző szervezetek a Szolgáltatótól függetlenek, és befolyástól mentesen végzik tevékenységüket. A vizsgálatot végző külső, független szervezet nem rendelkezik tulajdonrésszel vagy érdekeltséggel a Szolgáltatót illetően, és Szolgáltató nem tulajdonosa közvetlenül vagy közvetve a vizsgálatot végző szervezetnek. A tanúsító szervezetek díjazása nem függ a tanúsítás során végzett tevékenységük megállapításaitól.

8.4 Az auditálás által lefedett területek

A vizsgálatok által lefedett területek a következők:

- A biztonságos aláírás-létrehozó eszközök tanúsítása, mely az [1] törvény 1. mellékletének való megfelelőség vizsgálatára irányul.
- A kriptográfiai hardver modulok tanúsítása, mely a [2] harmadik részének 1. fejezetében maghatározott követelményeknek való megfelelőség vizsgálatára irányul.

[59] 2001. évi XXXV. törvény az elektronikus aláírásról

[60] 3/2005. IHM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

- A minősített tanúsítványok kezeléséhez használt rendszerek és módszerek tanúsítása (beleértve a dokumentálásra, folyamatokra, fizikai és műszaki biztonságra, az érintett személyzetre, valamint az adatvédelemre) mely a vonatkozó jogszabályok[61] előírásainak, a jelen Szabályzatban rögzített Hitelesítési Rend dokumentumoknak valamint Szolgáltató egyéb szabályzatainak való megfelelőség vizsgálatára irányul.
- Szolgáltató minőségirányítási és információbiztonsági irányítási rendszere, mely a külső és belső szabványok, ajánlások és leírások követelményei végrehajtásának megfelelőségére irányul

8.5 A hiányosságok kezelése

A vizsgálatok vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató az előírt határidőre megszünteti a vizsgálatot végző szervezettől kapott információ és ajánlások alapján.

8.6 Az eredmények közzététele

A Szolgáltató a tanúsítások illetve vizsgálatok végeredményét saját honlapján közzéteszi, amennyiben ezek a pubikus szabályzatait és dokumentumait érintik. Ez nem vonatkozik a tanúsítási eljárás során feltárt, az eljárás végeredményét nem befolyásoló hiányosságokra és részeredményekre.

[61] [1], [3], [22] és kacsolódó rendeletei és vonatkozó ajánlások

9. Egyéb üzleti és jogi kérdések

9.1 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.

Aláírás hitelesítés-szolgáltatáshoz kapcsolódó díjak. A Szolgáltató a vonatkozó szolgáltatási szerződés szerint kibocsátott tanúsítványokért az ÁSZF-ben megjelölt díjelemekből álló díjat számol fel az előfizető felé.

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

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.

Tanúsítvány hozzáférési díjak. A Szolgáltató a közzétett tanúsítványok eléréséért nem számol fel díjat az érintett felek irányában.

Visszavonási és állapot-információ hozzáférési díjak. A Szolgáltató a közzétett visszavonási vagy státus-információ eléréséért nem számol fel díjat az érintett felek irányában.

Egyéb szolgáltatásokra vonatkozó díjak. A Szolgáltató a kibocsátott tanúsítványok visszavonásáért, felfüggesztéséért és újraérvényesítéséért, a viszontazonosításért, és a valós idejű tanúsítvány állapot információ nyújtásáért eljárási díjat nem számol fel.

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** nem összetartozóak a Szolgáltató hibájából fakadóan,
- a kibocsátott biztonságos aláírás-létrehozó eszközön szereplő **adatok**,[62] hibásak a Szolgáltató tevékenysége következtében,

[62] pl. a kártya fizikai megszemélyesítése nem megfelelő

- 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 előfizetőnek kérvényt kell beadnia a Szolgáltató részére írásban a díj visszatérítése céljából a tanúsítvány kibocsátását követő **30 naptári napon belül** a regisztrációt végző Regisztrációs Szervezetnél. 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.

9.2 Anyagi felelősségvállalalás. Bankgarancia, 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..[63]

A Szolgáltató ezen felül, a megbízhatóság biztosítása érdekében teljes körű felelősségbiztosítással is rendelkezik a Lloyds biztosítótársaságnál. A felelősségbiztosítási szerződés kiterjed a Szolgáltató által a szolgáltatások nyújtásával összefüggésben okozott valamennyi kárra. A **biztosítás** egy biztosítási esemény vonatkozásában káreseményenként[64] és 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.

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.[65]

További információkat a 9.8 és 9.9 fejezetek tartalmaznak.

[63] ld. [3] 12-14. §

[64] ld. a [3] 11. § (3)

[65] ld. [3] 11. § (5)

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.

9.3 Az üzleti információk bizalmassága

Szolgáltató az általános alapszabályokon túlmenően nem alkalmaz egyedi szabályt erre vonatkozóan.

9.4 A személyes adatok védelme

A Szolgáltató az előfizető és aláíró adatait a jogszabályoknak megfelelően kezeli. A Szolgáltató társasági szintű adatkezelési szabályzattal rendelkezik, mely a személyes adatok kezelésével kiemelten foglalkozik és amely általánosságban vonatkozik az elektronikus aláírással kapcsolatos szolgáltatásokra is. A szolgáltatásokra vonatkozó speciális adatkezelést jelen szabályzat valamint Szolgáltató belső (nem nyilvános) szabályzatai operatív szinten tárgyalják.

Az előfizető és aláíró a tanúsítvány igénylésével hozzájárul ahhoz, hogy a személyes adatait a Szolgáltató (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A hozzájárulás egyaránt vonatkozik az adatok aláíróval és előfizetővel való megosztására (ha a két fél különbözik), valamint a törvény által meghatározott és nyilvántartásba vett információk harmadik félhez történő továbbítására a Szolgáltató szolgáltatásainak leállítása esetén[66]. A Szolgáltató az előfizetői adatokat kizárólag csak a hitelesítésszolgáltatással összefüggésben használja fel.

Az előfizető illetve aláíró tanúsítványban megjelenő adatai a tanúsítványba foglalva 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.

A Szolgáltató a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi, majd a bizalmasnak számító információkat vissza nem állítható módon megsemmisíti.

[66] ld. [1] 16. § (2)

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. Így például a felhasználói adatok papír alapú eredeti példányát (felhasználói szerződés) és a regisztrációhoz szükséges dokumentumokat, ha ilyenek keletkeznek, az adott megrendelésben részt vevő regisztrációs tisztviselő (vagy az illetékes értékesítési terület illetékes munkatársa) kezeli, másnak át nem adja, imásoktól elzárt módon tárolja, majd a megrendelés lezártával a **Magyar Telekom Informatikai Igazgatóság Katasztrófa Adattárában** (ebben a dokumentumban Adattár) helyezi el végső megőrzésre. Az elektronikus rendszerekben csak azon adatok kerülnek rögzítésre, amelyek a tanúsítvány kiadáshoz, a regisztrációhoz, illetve a viszontazonosításhoz szükségesek; Ezen rendszerekhez kizárólag a regisztrációs szervezet és hitelesítő szervezet munkatársai férhetnek hozzá. A hozzáférések és jogosultságok kezelésére Szolgáltató külön belső szabályzattal rendelkezik (Rendszerszintű Informatikai Biztonsági Szabályzat), melynek alapján a rendszerek megfelelőségét és a jogosultságkezelési szabályok betartását mind belső, mind pedig külső független auditorok és a Hatóság (NHH) ellenőrzik rendszeresen.

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 állás**ról.

9.4.1 Bizalmasan kezelendő információ-típusok

a) A Szolgáltató bizalmas információként kezeli az előfizető és az aláíró minden adatát, kivéve azokat, amelyeket a **9.4.2** 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 **9.4.3** – **9.4.7** 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,
- elektronikus tanúsítványigénylések és szolgáltatási szerződések,
- tranzakciós és napló adatok,
- nem nyilvános szabályzatok,
- minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

9.4.2 Nem bizalmasnak tekintett információ típusok

A **Szolgáltató** nem bizalmas információként kezeli mindazon adatokat, melyet a tanúsítványba belefoglal[67]. Ezek az adatok a Szolgáltatási Szerződésben, illetve Megrendelőlapon egyértelmű jelöléssel szerepelnek.

9.4.3 Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése

A **Szolgáltató** az általa kibocsátott tanúsítványok visszavonását és felfüggesztését a **tanúsítvány-visszavonási listá**ban, illetve OCSP[68] válaszban teszi közzé, a tanúsítvány sorszámának és opcionálisan a visszavonás/felfüggesztés okának a jelölésével. Bővebb információ a **7.** fejezetben található.

9.4.4 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[69] 11.§ (2) bekezdése szerinti körben.

b) A Szolgáltató rögzíti az a) pontbeli adatátadás tényét, de arról nem tájékoztatja sem az előfizetőt, sem az aláírót.

c) A Szolgáltató olyan esetben is szolgáltathat információt, amikor egyéb jogszabály(ok) ezt előírják (pl. viszontazonosítás).

9.4.5 Információszolgáltatás polgári eljárás keretében

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

b) A Szolgáltató rögzíti az a) pontbeli adatátadás tényét, és arról tájékoztatja az előfizetőt és az aláírót.

---

[67] Függetlenül attól, hogy az előfizető hozzájárul-e (az alany nevében) a tanúsítvány nyilvánosságra hozásához.

[68] Ld. [21]

[69] 2001. évi XXXV. törvény az elektronikus aláírásról

9.4.6 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.

9.4.7 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[70] 16. § 2. bekezdése szerint.

9.5 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.

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

9.6 Tevékenységért viselt felelősség és helytállás

A Szolgáltató általános felelőssége:

a) A Szolgáltató felelősséget vállal a Hitelesítési Rend dokumentumban leírt eljárásoknak való megfelelőségért, még abban az esetben is, amikor a Szolgáltató egyes tevékenységeit alvállalkozók végzik[71].

[70] 2001. évi XXXV. törvény az elektronikus aláírásról

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

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.

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. A Szabályzat keretei között végzett szolgáltatói tevékenységekért (beleértve az esetlegesen igénybe vett alvállalkozókét is) a **Magyar Telekom Nyrt. a felelős.**

9.6.1 A hitelesítés-szolgáltató felelőssége és helytállása

a) A Hitelesítő Szervezet **felelős**:

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

9.6.2 A regisztrációs szervezet felelőssége és helytállása

A Regisztrációs Szervezet felelős:

- az aláírók és előfizetők 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.

9.6.3 Az előfizető felelőssége és helytállása

Az előfizető felelős:

- a regisztráció során megadott adatok 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 értesítéséért és teljes körű tájékoztatásáért vitás ügyekben,
- a hitelesítésszolgáltatás díja(i)nak szerződés szerinti kifizetéséért, azaz a számlákon szereplő összegek megjelölt időpontig történő kifizetéséért (eltérő megállapodás hiányában),
- általában a kötelezettségei betartásáért.

9.6.4 Az érintett fél felelőssége

Az érintett fél felelős a jogszabályokban írt kötelezettségek betartásáért és az adott helyzetben általában elvárható magatartás tanúsításáért, különösen az elektronikus aláírás ellenőrzéséért, illetve a tanúsítványok elfogadása során tanúsított körültekintő eljárásért[72].

9.6.5 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,

[72] Pl. az érintett félnek ellenőriznie kell az elektornikus aláíráshoz kapcsolódó tanúsítvány érvényességét, valamint azt, hogy a tanúsítvány nincs felfüggesztve illetve visszavonva az érvényes visszavonási állapot információk alapján (CRL vagy OCSP), a Szabályzat 4.5.2 pontjának megfelelően.

- magánkulcsának és aktivizáló kódjának biztonságáért,
- a biztonságos aláírás-létrehozó eszköz biztonságáért,
- általában a kötelezettségei betartásáért.

9.7 Helytállás érvénytelenségi köre

Szolgáltató nem alkalmaz különleges szabályokat erre vonatkozóan.

9.8 Felelősségi korlátozások

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.

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.

9.9 Kártérítési kötelezettségek

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az előfizetővel / aláíróval megkötött szolgáltatási szerződésekben valamint az előző pontban rögzített korlátozásokkal kártérítést fizet.

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

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.

9.10 Érvényesség

Jelen szabályzat időbeli hatályát az 1.1.2 pont tartalmazza.

A Szabályzat 9 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.

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

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.

9.11 A felek közötti kommunikációra vonatkozó előírások

Az előfizető és aláíró jognyilatkozatait Szolgáltató felé kizárólag írásban, hivatalosan aláírt módon teheti meg. Az előfizető és az aláíró egyéb esetekben a Szolgáltatót írásban, elektronikus levél vagy fax formájában is értesítheti. A Szolgáltató értesítési címei jelen szabályzat 1.4 alfejezetében találhatóak.

9.12 Kiegészítések

Szolgáltató nem alkalmaz különleges szabályokat erre vonatkozóan.

9.13 Vitás kérdések megoldása

A szolgáltatással kapcsolatos bármely vitás kérdés vagy panasz felmerülése esetén a vita jogi útra terelése előtt az aláírónak és az előfizetőnek 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 Szervezetet is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az 1.4 Kapcsolattartás fejezetben rögzített Regisztrációs Szervezetre vonatkozó elérhetőségeken lehet megtenni.

Az eljárás további részleteit az ÁSZF dokumentum 13.§-a tartalmazza.

9.14 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.

9.15 Az érvényben lévő jogszabályoknak való megfelelőség

A legfontosabb jogszabályok felsorolását a vonatkozó Hitelesítési Rend tartalmazza.

10. Melléklet: A regisztrációhoz szükséges adatok

Az alább felsorolt iratokat a Minősített e-Szignó Hitelesítésszolgáltatás keretében igényelt tanúsítványokhoz különböző dokumentumokat kell a regisztráció során a **Regisztrációs tisztviselő** számára átadni ill. eljuttatni.

1. **Üzleti tanúsítvány igényléséhez az alábbi iratok összegyűjtése szükséges:**
   - Amennyiben a szervezet **gazdasági szervezet** 1 hónapnál nem régebbi eredeti cégkivonat (gazdasági szervezetek listája lásd 4. pont),
   - Amennyiben **nem gazdasági szervezet,** az 5. 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 3. pont).
2. **Köztisztviselői tanúsítvány igényléséhez az alábbi iratok összegyűjtése szükséges:**
   - 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,
   - az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét és székhelyének (vagy ahol ez nem értelmezhető, telephelyének) címét, valamint iktatószámot tartalmazó meghatalmazást arra, hogy az Aláíró a hivatal képviseletében a szolgáltatónál előfordulló ügyekben eljárhat, és amely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti. Ezen dokumentum gyakorlatilag a Szolgáltatási Szerződés részét képező Megrendelőlapot jelenti, melyet közokiratba kell foglalni.
   - Minden igénylő **(aláíró) személyazonosságát** garantáló iratainak fénymásolata (lásd 3. pont).

3. **Személyi tanúsítvány igényléséhez szükséges – egyben a személyek azonosságát garantáló - iratok:**

A következő okmányok közül legalább 1 szükséges:

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

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

4. A gazdasági szervezetek tételes fölsorolása, üzleti tanúsítványokhoz:

- 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

5. Egyéb (nem gazdasági) szervezetektől bekérendő iratok

Üzleti tanúsítványok igényléséhez – amennyiben a szervezet nem gazdasági szervezet - az alább felsorolt iratok 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**.	▪ 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).

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).	"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."