Magyar Telekom fokozott e- Szignó®

nem-minősített hitelesítés szolgáltatás

Standard Személyi Tanúsítvány

Standard Üzleti Tanúsítvány

Fokozott Személyi Tanúsítvány

Fokozott Üzleti Tanúsítvány

Hitelesítési Rend

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.4
Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.5
Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.6
Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.7

Verziószám:.....2.6
Hatályba lépés dátuma: 2009.01.10

Változáskezelés

Verzió-szám	Módosítás dátuma	A változás leírása
1.0	2003.05.01	Első verzió
2.0	2003.09.10	Változtatások: kisebb módosítások
2.1	2006.03.31	A Magyar Telekom név váltásának és következményeinek módosítása
2.2	2008.07.16	2007. évi Hatósági ellenőrzés észrevételei szerinti javítások
2.3	2008.08.10	A Hatóság észrevételei szerinti módosítás (HL-4921-6/2008)
2.4	2008.09.26	A Hatóság észrevételei szerinti módosítás (HL-4921-9/2008)
2.5	2008.10.30	A Hatóság észrevételei szerinti módosítás (HL-4921-11/2008)
2.6	2008.11.13	A hatósági konzultáció szerinti módosítás

Módosítást készítette: Bauer Géza	Új Üzleti Területek és Üzletfejlesztési Üzletág / Alternatív váll.portf.men.ig.	termékmenedzser
Ellenőrizte: Dr. Demény Péter	Új üzleti területek és üzletfejlesztési üzletágat támogató jogi osztály	jogi munkatárs
Jóváhagyta: Dr. Petrányi Dóra	Magyar Telekom Csoport jogi igazgatóság	jogi munkatárs

Tartalom

1. Bevezetés

1.1 Áttekintés

A Hitelesítési Rend egy „szabálygyűjtemény, mely egy tanúsítványfajta felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára".

Jelen hitelesítési rend az [8] szabványa alapján készült, továbbá megfelel a [11] meghatározott szabványnak, és a közzététel előtt a Szolgáltató megvizsgálta a megfelelőségét a kapcsolódó szolgáltatási szabályzattal. A dokumentum tartalmi vonatkozásokban eleget tesz az [1] törvény, és egyéb hazai jogszabályok [3] előírásainak és ajánlásainak, továbbá a hitelesítés szolgáltatásra vonatkozóan felhasználja az [12] specifikációt, valamint a „Nyilvános kulcs es attribútum tanúsítvány keretrendszer"című ajánlást [7]. A szabályokra vonatkozó követelményeit jelen dokumentum Hitelesítési Rend formájában határozza meg. A jelen dokumentumnak megfelelően kibocsátott tanúsítványok tartalmazzák jelen Hitelesítési Rend azonosítóját, amelyet az érintett felek arra használhatnak, hogy meghatározzák a tanúsítványok alkalmazhatóságát és megbízhatóságát egy adott alkalmazás tekintetében.

Jelen dokumentum az alábbi tanúsítványfajtákat határozza meg:

- Standard Személyi Tanúsítvány
- Standard Üzleti Tanúsítvány
- Fokozott Személyi Tanúsítvány
- Fokozott Üzleti Tanúsítvány

A fenti tanúsítványfajtákkal tett fokozott biztonságú aláírásokra az alábbiak teljesülnek:

- alkalmas az aláíró azonosítására,
- egyedülállóan az aláíróhoz köthető,
- olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak,
- a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető.

1.2 Azonosítás, tanúsítványfajták

A jelen dokumentum az alábbi hitelesítési rendeket definiálja:

- Standard Személyi Tanúsítvány hitelesítési rendjébe tartozó tanúsítványok kibocsátására vonatkozó hitelesítési rend. OID: 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.4
- Standard Üzleti Tanúsítvány hitelesítési rendjébe tartozó tanúsítványok kibocsátására vonatkozó hitelesítési rend. OID: 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.6
- Fokozott Személyi Tanúsítvány hitelesítési rendjébe tartozó tanúsítványok kibocsátására vonatkozó hitelesítési rend. OID: 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.5

- Fokozott Üzleti Tanúsítvány hitelesítési rendjébe tartozó tanúsítványok kibocsátására vonatkozó hitelesítési rend. OID: 1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.7

Ezen hitelesítési rendek alapján a Szolgáltató olyan elektronikus aláírási termékeket bocsát ki, amelyek az 2001 XXXV. Törvény [1] alapján alkalmasak az aláírások ellenőrzésére.

A Hitelesítési Rend érvényességi körében kibocsátott nem-minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyeknél, ha a jogszabály írásba foglalást ír elő, akkor e követelménynek eleget tesz az elektronikusan aláírt elektronikus dokumentumba foglalás is, ha az elektronikusan aláírt dokumentumot fokozott biztonsági szintű elektronikus aláírással írják alá.

1.2.1 Tanúsítványfajták

1.2.1.1 Standard Személyi Tanúsítvány

Ez a tanúsítványfajta a Magyar Telekom – mint hitelesítés-szolgáltató – által nem-minősített kibocsátott tanúsítvány. Ajánlott fokozott biztonságú aláíráshoz, illetve ezen alapuló Aláíró azonosításhoz, átlagos értékű, illetve rövid időre biztonságot követelő szerződésekhez, kereskedelmi tranzakciókhoz, alkalmazásokhoz - elektronikus levelezés, intranet, extranet, on-line vásárlás stb. esetében.

További információért lásd a szolgáltatási szabályzat 4.1.1és 4.1.2 pontjait.

1.2.1 .2 Standard Üzleti Tanúsítvány

Ez a tanúsítványfajta a Magyar Telekom – mint hitelesítés-szolgáltató – által kibocsátott nem-minősített tanúsítvány. Ajánlott fokozott biztonságú aláíráshoz, illetve ezen alapuló Aláíró azonosításhoz, átlagos értékű, illetve rövid időre biztonságot követelő szerződésekhez, kereskedelmi tranzakciókhoz, alkalmazásokhoz - elektronikus levelezés, intranet, extranet, on-line vásárlás stb. esetében.

További információért lásd a szolgáltatási szabályzat 4.1.3és 4.1.4 pontjait.

1.2.1.3 Fokozott Személyi Tanúsítvány

Ez a tanúsítványfajta a Magyar Telekom – mint hitelesítés-szolgáltató – által kibocsátott nem-minősített tanúsítvány. Ajánlott fokozott biztonságú aláíráshoz, illetve ezen alapuló Aláíró azonosításhoz, magasabb értékű, illetve hosszú időre biztonságot követelő szerződésekhez, kereskedelmi tranzakciókhoz, alkalmazásokhoz - elektronikus levelezés, intranet, extranet, on-line vásárlás stb. esetében.

További információért lásd a szolgáltatási szabályzat 4.1.5 és 4.1.6 pontjait.

1.2.1.4 Fokozott Üzleti Tanúsítvány

Ez a tanúsítványfajta a Magyar Telekom – mint hitelesítés-szolgáltató – által nem-minősített kibocsátott tanúsítvány. Ajánlott fokozott biztonságú aláíráshoz, illetve ezen alapuló Aláíró azonosításhoz, magasabb értékű, illetve hosszú időre biztonságot követelő szerződésekhez, kereskedelmi tranzakciókhoz, alkalmazásokhoz - elektronikus levelezés, intranet, extranet, on-line vásárlás stb. esetében.

További információért lásd a szolgáltatási szabályzat 4.1.7 és 4.1.8 pontjait.

1.3 Közösség és alkalmazhatóság

1.3.1 Hitelesítő szervezet

A Magyar Telekom Nyrt., mint hitelesítés szolgáltatást nyújtó szolgáltató (továbbiakban: Szolgáltató) – saját szervezetén belül – egy hitelesítő szervezetet működtet, (teljes név: Magyar Telekom Fokozott CA nevű hitelesítő központi egység, és ebben a dokumentumban Hitelesítő Szervezet vagy HSz) melynek feladata a tanúsítványok központi előállítása és menedzsmentje (a Regisztrációs Szervezettől {RSz} kapott kérelmeknek megfelelően, a hitelesítés-szabályozásért felelős szervezet által meghatározott eljárások szerint).

1.3.2 Regisztrációs szervezet

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

1.3.3 Végfelhasználók

A hitelesítés-szolgáltató által nyújtott szolgáltatások végfelhasználói az alábbiak:

- előfizetők,
- aláírók és
- érintett felek.

Az aláíró az a természetes személy, aki az aláírást létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult.

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 érintett fél természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet lehet, és a Szolgáltatóval nem áll szerződéses viszonyban.

1.3.4 Alkalmazhatóság

Jelen Hitelesítési Rend érvényességi körében kibocsátott nem minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az írásbeliség jogi követelményeit elektronikus formájú adatok vonatkozásában kielégítik, továbbá:

- a kibocsátott tanúsítványok kizárólag aláírási célra használhatók fel,
- végfelhasználói tanúsítványokhoz tartozó aláírás létrehozó adat tanúsítványok aláírására történő felhasználása, vagy bármilyen egyéb hitelesítés szolgáltatás nyújtásához történő alkalmazása tilos,
- a hitelesítés-szolgáltató a végfelhasználói tanúsítványok felhasználását a tanúsítványban jelzett módon tovább korlátozhatja.

1.4 Kapcsolattartás

Szolgáltató és a regisztrációs szervezet

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

Név	Magyar Telekom Nyrt.
Cégjegyzékszám:	01-10-041928
Székhely:	1013 Budapest, Krisztina krt. 55.
Postacím:	Magyar Telekom e-Szignó Központi Ügyfélszolgálat és Fokozott Regisztrációs Szervezet 1519. Budapest, Pf. 434.
Telefon:	+36 80 204 040
Fax:	+36 1 447 4451
Honlap:	http://www.t-systems.hu/nv/hitelesites_szolgaltatasok
Email cím:	eszigno.fokozott@t-systems.hu

Ügyfélszolgálat:

A Magyar Telekom a Végfelhasználók részére e- Szignó Ügyfélszolgálatot biztosít, mely elérhető a hét minden napján 0-24 óra között, a táblázatban megadott telefonszámon (valamint fax, email és postacímen). A tanúsítvány felfüggesztés és visszavonás lehetőségét a Szolgáltató - 0-24 óra között - levélben, faxon és e-mail elérhetőségeken biztosítja.

1.5 Jelölések, rövidítések és meghatározások

Jelen Hitelesítési Rend az alábbi fogalmakat az alábbi értelemben használja:

- **Aláírás-ellenőrző adat**: Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.
- **Aláírás-létrehozó adat**: Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az Aláíró az elektronikus aláírás létrehozásához használ.
- **Aláírás-létrehozó eszköz**: Szoftver vagy hardver, melynek segítségével az Aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
- **Aláíró:** A tanúsítvány (Subject) mezőjében megadott adatokkal meghatározott természetes személy, aki a tanúsítványban szereplő nyilvános kulcs párját jelentő magánkulcs felett rendelkezik
- **Általános Szerződési Feltételek (ÁSZF):** A Szolgáltató szolgáltatásainak, tanúsítványainak igénybevételéhez szükséges feltételeket, illetve egyéb szerződési feltételeket leíró dokumentum.
- **Common Name (CN):** A tanúsítványban szereplő Aláíró neve vagy az Aláíró által megjelölt álnévből képzett karaktersorozat.

- **Elektronikus aláírás:** Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat..
- **Előfizető:** szolgáltatónál egy vagy több aláíró nevében előfizető entitás, aki közvetlenül vagy közvetve elfogadja szolgáltató kikötéseit és feltételeit
- **Eredeti példány:** Magán- vagy jogi személy azonosító okmány eredeti aláírásokat és pecsétet tartalmazó példánya, vagy ezek hitelesített másolata.
- **Érintett Fél:** Az a személy, aki elektronikus aláírás érvényességének ellenőrzése, illetve hiteles időpont megállapítása céljából a Szolgáltató által kibocsátott tanúsítványhoz fordul
- **Eszközszolgáltatás:** Az a szolgáltatás, melynek során a Szolgáltató a Törvény 6. § (1) bekezdésének c) pontja értelmében meghatározott, elektronikus aláíráshoz kapcsolódó aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatást végez.
- **Felügyelet:** Nemzeti Hírközlési Hatóság, a Hitelesítés-szolgáltatók felügyeleti szerve.
- **Folyamatosan elérhető szolgáltatás:** Az év 365 napján a nap 24 órájában elérhető szolgáltatást jelent a Szolgáltató szabályzataiban meghatározott rendelkezésre állási időkkel.
- **Fokozott biztonságú aláírás**: Elektronikus aláírás, amely megfelel a következő követelményeknek:
    - alkalmas az Aláíró azonosítására és egyedülállóan hozzá köthető,
    - olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak,
    - a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető.
- **Hitelesítési rend:** 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.
- **Igénylő:** a tanúsítvány iránti igényt benyújtó személy (aki a szolgáltatást aláíróként és / vagy előfizetőként kívánja igénybe venni)
- **Közhiteles nyilvántartás**: olyan, hatóság által vezetett nyilvántartás, melynek tartalmát, az abban szereplő adatok valódiságát az ellenkező bizonyításig mindenki köteles elfogadni. Ilyen közhiteles nyilvántartás a cégnyilvántartás, valamint a polgárok személyi és lakcím adatait tartalmazó nyilvántartás.
- (**Kriptográfiai**) **Kulcs**: Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.
- **Lenyomat**: Olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:
    - a képzett lenyomat egyértelműen származtatható az adott elektronikus dokumentumból,
    - a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés,

- a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, amelyre alkalmazva a lenyomatképző eljárás eredményeképp az adott lenyomat keletkezik.

- **Magánkulcs védelme:** Mindazon tevékenységek összessége, melyek célja a magánkulcs megfelelő védelme, a magánkulcs teljes élettartama során annak generálásától, annak megsemmisítéséig, a hozzá tartozó tanúsítvány státuszától függetlenül.
- **Munkatárs:** A természetes személyek azon köre, amelyeket egy adott szervezet saját magához tartozóként ismer el.
- **Object Identifier (OID):** objektumok azonosítására használt számsor.
- **Publikus (Nyilvános) Kulcsú Infrastruktúra:** A tanúsítványok kibocsátásában és kezelésében, valamint az időbélyegzésben részt vevő technikai eszközök, egységek, ezen tevékenységeket hivatalosan felügyelő és meghatározó intézmények, a felhasználók által alkalmazott kriptográfiai eszközök és tevékenységek összessége.
- **Regisztrációs Egység:** Az ügyfelek adatait összegyűjtő, ellenőrző, tanúsítvány kibocsátási, felfüggesztési, visszavonási kérelmeket összeállító és a Hitelesítő Egységhez továbbító egység.
- **Személyi tanúsítvány:** Természetes személyek számára kibocsátott tanúsítvány, melyekbe foglalt nyilvános kulcs magán párja kizárólag elektronikus aláírás előállítására használható.
- **Subject Name (SN):** Az aláíró vezetékneve.
- **Szolgáltatási Szabályzat**: A [1] Törvény 2. § (20) alapján a Szolgáltató hitelesítési tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum.
- **Szolgáltatási szerződés:** Elsődlegesen az ÁSZF és a Szolgáltatási Szabályzat elfogadását jelző, aláírt dokumentum.
- **Szolgáltató:** Magyar Telekom Nyrt., amely a tanúsítvány-szolgáltatást, és az eszközszolgáltatást nyújtja.
- **Tanúsítvány**: A Szolgáltató által kibocsátott elektronikus igazolás, amely az aláírás-ellenőrző adatot a tanúsítványban meghatározott entitáshoz kapcsolja.
- **Tanúsítvány-szolgáltatás**: azon eljárás, melynek során a Szolgáltató a Szolgáltatási Szabályzatokban meghatározott eljárásban új vagy megújított, aláíró vagy egyéb célú tanúsítványt bocsát ki a felhasználó részére. A tanúsítvány-szolgáltatáshoz kapcsolódóan a Szolgáltató tanúsítványállapot-szolgáltatást is nyújt, melynek keretében fogadja a tanúsítvány-visszavonási- és felfüggesztési kérelmeket és a Szolgáltatási Szabályzatokban meghatározott időközönként Tanúsítvány Visszavonási Listát bocsát ki.
- **Tanúsítványfajta**: Jelen Szabályzat négy megjelenési formáját ismeri: a személyi és az üzleti (munkatársi), és ezeken belül standard illetve fokozott.
- **Tanúsítványállapot-nyilvántartás**: A legközelebb kibocsátásra kerülő Tanúsítvány Visszavonási Lista tartalmához kapcsolt on-line lekérdezhető információk.
- **Tanúsítványtár:** A végfelhasználói és szolgáltatói tanúsítványok, felfüggesztett, visszavont tanúsítványadatok, Szolgáltatói Szabályzatok publikálásáért, tárolásáért felelős alegység.
- **Tanúsítvány Visszavonási Lista (CRL – Certificate Revocation List)**: Valamely okból visszavont, azaz érvénytelenített, illetve felfüggesztett, azaz ideiglenesen érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a Szolgáltató bocsát ki.

- **Üzleti előfizető:** Az jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amely a munkatársi tanúsítvány aláírójával együttesen szerepel a tanúsítványban és aki az aláírót saját magához tartozónak ismeri el.
- **Üzleti tanúsítvány:** Olyan személyes tanúsítvány, amelyben, az abban szereplő természetes személyt az üzleti előfizető (cég, társaság, alapítvány stb) saját magához tartozónak ismeri el.
- **Végfelhasználó:** Szerződéses partner, aki a Szolgáltató által kibocsátott végfelhasználói tanúsítvánnyal rendelkezik.
- **Végfelhasználói tanúsítvány:** A Szolgáltató által kibocsátott olyan tanúsítvány, amelyet az aláíró kizárólag elektronikus aláírás előállítására használhat, de más tanúsítvány hitelesítésére nem.

1.6 Hivatkozások

[1] 2001. évi XXXV. Törvény az elektronikus aláírásról /Eat.

[2] CEN 14167-1 munkacsoport egyezmény: „Biztonsági követelmények elektronikus aláírásokkal kapcsolatos tanúsítványokat kezelő rendszerek megbízható rendszereire”

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

[4] ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1. 2. és 3. rész)

[5] CEN 14167-2 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató aláíró műveleteit megvalósító kriptográfiai modulra” (CMCSO-PP, HSM-PP)

[6] CEN 14167-3 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató kulcs előállítási szolgáltatásait megvalósító kriptográfiai modulra” (CMCKG-PP, HSM-PP)

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

[8] RFC 3647 (korábban RFC 2527) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer

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

[10] A hitelesítés-szolgáltatás területén alkalmazható kriptográfiai algoritmusokról és paraméterekről szóló NHH határozat mindenkor hatályos változata (e szabályzat hatályba lépésekor: HL-21917-12/2008)

[11] ETSI TS 102 280: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons (v1.1.1; 2004-03).

[12] ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

2. Közzétételre és címtárra vonatkozó szabályok

2.1Közzététel és címtár

2.1.1 Hitelesítés-szolgáltatói információ közzététele

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

Kikötések és feltételek közzététele:

A hitelesítés-szolgáltató az aláírók/előfizetők és az érintett felek rendelkezésére bocsátja a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, köztük az alábbiakat:

- az alkalmazott Hitelesítési Rend dokumentumot, beleértve egy egyértelmű nyilatkozatot arra vonatkozóan, hogy a Hitelesítési Rend a nyilvánosság részére kibocsátott tanúsítványokra vonatkozik;
- a tanúsítványok használatára vonatkozó bárminemű korlátozást;
- az előfizető kötelezettségeit a 9.1.4.2 alfejezetben meghatározottaknak megfelelően;
- a tanúsítvány ellenőrzésének mikéntjére vonatkozó információt, beleértve a tanúsítvány visszavonási állapot ellenőrzésére vonatkozó követelményeket, oly módon, hogy az érintett fél "ésszerű módon hagyatkozhasson" a tanúsítványra (lásd 9.1.5)
- a felelősségvállalásra vonatkozó bármilyen korlátozást, beleértve azokat az okokat/használatokat, melyek esetén a hitelesítés-szolgáltató elfogadja, illetve visszautasítja a felelősség vállalását;
- információt arról az időtartamról, amíg a regisztrációs információt megőrzik;
- információt arról az időtartamról, amíg a hitelesítés-szolgáltató eseménynaplóját (lásd 5.4.3) megőrzik;
- információt reklamációkról és viták rendezésére vonatkozó eljárásokról (lásd 9.4.3);
- információt az alkalmazandó jogról(lásd 9.4.1); és

A hitelesítés-szolgáltató elérhetővé teszi a fenti pontokban meghatározott információkat Internetes honlapján keresztül, közérthetően megfogalmazva, elektronikusan továbbítható formában.

Tanúsítványok nyilvánosságra hozatala:

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

- az előállítás után a teljes és pontos tanúsítvány rendelkezésre áll azon aláíró számára, akinek a tanúsítvány kibocsátásra került;
- a tanúsítványok csak azokban az esetekben érhetők el más számára, ha az előfizető és az aláíró előzetesen hozzájárul a nyilvánosságra hozatalukhoz;
- a hitelesítés-szolgáltató az érintett felek rendelkezésére bocsátja a tanúsítvány használatával kapcsolatos kikötéseket és feltételeket;
- egy adott tanúsítvánnyal kapcsolatban a vonatkozó kikötések és feltételek könnyen azonosíthatók.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala:

A hitelesítés-szolgáltató gondoskodik arról, hogy hiteles és érvényes tanúsítvány visszavonási és felfüggesztési kérelmek esetén a tanúsítványok időben visszavonásra, illetve felfüggesztésre kerüljenek, egyúttal ezen információ nyilvánosságra kerüljön. Részletesebben:

A hitelesítés-szolgáltató szolgáltatási szabályzat 4.4.3 és a 4.4.7-es alfejezeteiben dokumentálja a tanúsítványok visszavonásának és felfüggesztésének eljárásait, beleértve az alábbiakat:

- a visszavonási állapot információk nyilvánosságra hozatalánál használt mechanizmusok,
- a legnagyobb késedelem a visszavonási és felfüggesztési kérelem fogadása, és az összes érintett fél rendelkezésére álló információk állapotának megváltozása között.

Továbbá biztosítja, hogy a tanúsítvány visszavonási listákra teljesüljenek az alábbiak:

- minden egyes visszavonási lista tartalmazza a következő visszavonási lista kibocsátási időpontját,
- új visszavonási lista közzétehető a következő visszavonási lista kibocsátására megadott időpont előtt is,
- a visszavonási listát a hitelesítő szervezet a hitelesítés-szolgáltató nevében elektronikusan aláírja.

2.1.2 A közzététel gyakorisága

Kikötések és feltételek közzétételi gyakorisága

A Szabályzattal kapcsolatos új verziók közzététele a {Lásd Szabályzat 8. Leírás adminisztráció fejezet} fejezetben ismertetett eljárásoknak megfelelően történik.

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 kibocsátást követően (gyakorlatilag azonnal) lehetővé teszi az aláíró számára a végfelhasználói tanúsítványok letöltését a szolgáltató honlapjáról.
- A Szolgáltató a végfelhasználói tanúsítványokat a Címtárban az előállítást követően 24 órán belül teszi közzé.

2.1.3 Hozzáférés ellenőrzések

- A Szolgáltató által közzétett kikötések és feltételek, rendkívüli információk, tanúsítványok és állapot információk nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közzététel sajátosságainak megfelelően. A tanúsítványok az előfizető / aláíró hozzájárulásával lehetnek nyilvánosan elérhetőek.
- A hitelesítés-szolgáltató a nyilvánosságnak bocsát ki tanúsítványt, ezért a tanúsítványok, valamint a tanúsítványok használatára vonatkozó kikötések és feltételek nyilvánosak, szabványos felületen bárki által elérhetők;
- A visszavonásra és felfüggesztésre_vonatkozó kérelmeket hitelesíteni kell, a hitelesítés-szolgáltató feldolgozás előtt ellenőrzi, hogy hiteles forrásból származnak-e. A nem írásban tett visszavonási kérelmeket, írásban hivatalos aláírással ellátva is meg kell erősíteni, levélben vagy faxon.
- A hitelesítés-szolgáltató a nyilvánosságnak bocsát ki tanúsítványt, ezért a visszavonási állapotokat tartalmazó tanúsítvány visszavonási listák nyilvánosak, szabványos felületen bárki által elérhetők.

2.1.4 Címtárak

- A hitelesítés-szolgáltató a tanúsítványokat, valamint a tanúsítvány visszavonási listákat címtárán, a tanúsítványok használatára vonatkozó kikötéseket és feltételeket honlapján teszi hozzáférhetővé.
- A honlap, ill. címtár elérhetőségét, valamint az általa biztosított szabványos felületeket és támogatott lekérdezési műveleteket a szolgáltatási szabályzat 2. fejezete határozza meg.
- a szolgáltatási szabályzatban meghatározott mértékben, de minimum 99,5%-os rendelkezésre állással biztosítsa a visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás elérhetőségét minden érdekelt fél számára; ennek során az egyes leállások ideje nem haladhatják meg a 3 órát.

2.2 Bizalmasság

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

- a fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól. A jogszabályoknak való megfelelés, valamint az alapvető üzleti tevékenységek támogatása érdekében szükség van bizonyos bejegyzések biztonságos megőrzésére is. (lásd 5.4 és 5.5 fejezetek);
- gondoskodik az adatvédelmi törvényeknek való megfelelésről;

- megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen kezelése ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen;
- nyilvántartásba veszi az előfizetővel és az aláíróval aláírt megállapodást, beleértve az alábbiakat:
  - hozzájárulás a szolgáltatások során felhasznált információk hitelesítés-szolgáltató által történő nyilvántartásba vételéhez
  - a hitelesítés-szolgáltató szolgáltatásainak leállítása esetén hozzájárulás a nyilvántartásba vett információ harmadik félhez történő továbbításához a vonatkozó szabályzat megkövetelt feltételei szerint,
  - hogy az előfizető vagy aláíró hozzájárul-e a tanúsítványa nyilvánosságra hozatalához.

Gondoskodik az aláíróra és az előfizetőre vonatkozó információ bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk[1] hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja és védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az előfizetővel/aláíróval folytatott, illetve a hitelesítő szervezet – regisztrációs szervezet – címtár rendszerkomponensek közötti adatcsere során is.

2.2.1 Bizalmasan kezelendő információ típusok

A hitelesítés-szolgáltató bizalmas információként kezeli az előfizető és az aláíró minden adatát, kivéve azokat, amelyeket a 2.2.2 alfejezet tárgyal.

A hitelesítés-szolgáltató a birtokába jutott bizalmas információt a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvénynek megfelelően kezeli, s csak a 2.2.3-2.2.7 alfejezetekben említett esetekben és személyek/szervezetek részére fedi fel őket.

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

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

2.2.2 Nem bizalmasnak tekintett információ típusok

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

2.2.3 Tanúsítvány visszavonására/felfüggesztésére vonatkozó információ felfedése

A hitelesítés-szolgáltató az általa kibocsátott tanúsítványok visszavonását és felfüggesztését tanúsítvány-visszavonási listákban teszi közzé.

[1] vagy nevükben az előfizető

2.2.4 Információszolgáltatás hatósági szervek részére

A hitelesítés-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 feltárhat jogszabályban meghatározott bizalmas felhasználói információkat az [1] törvény 11.§ (2) bekezdése szerint.

A hitelesítés-szolgáltató rögzíti az 2.2.4 pontbeli adatátadás tényét, de arról nem tájékoztatja sem az előfizetőt, sem az aláírót.

2.2.5 Információszolgáltatás polgári eljárás keretében

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

A hitelesítés-szolgáltató rögzíti az előző pontban részletezett adatátadás tényét, és arról tájékoztatja az előfizetőt és az aláírót.

2.2.6 A tulajdonos kérésére történő felfedés

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

2.2.7 Egyéb információ közzétételt eredményező körülmények

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

2.3 Szellemi tulajdonjogok

A hitelesítés-szolgáltató által kibocsátott végfelhasználói tanúsítvány és az ennek megfelelő kulcspár tulajdonosa az előfizető, teljes jogú kizárólagos használója pedig az aláíró, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

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

A visszavonási információ a hitelesítés-szolgáltató tulajdonát képezi.

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

A tanúsítványban szereplő megkülönböztető név használatára a megnevezett aláíró jogosult.

Az aláíró egyedi azonosítójában szereplő bármilyen védjegy, szervezeti- és személynév, egyéb adat az előfizető vagy aláíró tulajdonát képezheti.

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

A tanúsítványban szereplő hitelesítő azonosító a hitelesítés-szolgáltató tulajdonát képezi.

3. Azonosítás és hitelesítés

3.1 Kezdeti regisztrálás

A hitelesítés-szolgáltató a kezdeti regisztrálás során:

- gondoskodik arról, hogy az aláíró és az előfizető tanúsítvány kérelmei pontosak, hitelesek és teljesek legyenek;
- az összes nem-minősített tanúsítványfajta esetében megfelelő, hiteles források (közhiteles adatbázisok) igazolásán alapulva megvizsgálja az aláírók és előfizetők azonosságára vonatkozó bizonyítékokat, valamint nevük és a hozzá kapcsolódó adatok pontosságát;
- a nevek regisztrációjának szabályai valamennyi tanúsítványfajtára vonatkoznak.

3.1.1 Név típusok

A tanúsítvány azonosító mezői („Subject" és „Issuer") az X.500 egyedi névformátum előírásainak felelnek meg. A „Subject" és „Issuer" mezőre vonatkozó további szabályok:

- a tanúsítványban az adatok speciális és vezérlő karakterek nélkül szerepelnek,
- a nevek egyes egységeit szóköz választja el,
- a „Title" mező opcionálisan tartalmazhatja az aláíró beosztását, az Aláíró Szervezeten belüli pozícióját tartalmazza,
- a tanúsítvány kiállító (Issuer) „CN" mezőjében a kibocsátó hitelesítő központi egységének neve szerepel,
- a tanúsítványban a karakterek ékezetmentesen szerepelnek,
- munkatársi tanúsítványokban az „Organization" mező kitöltése csak Üzleti Tanúsítvány esetén kötelező. A mező annak a Szervezetnek a nevét tartalmazza, amelyikhez az Aláíró tartozik. A név formátuma: gazdasági társaság esetén a cégbejegyzésben szereplő rövid név, nem gazdasági társaság esetén a Szervezet hivatalos okirata szerint (pl. alapító okirat), (Személyi Tanúsítvány esetén nem kerül kitöltésre)
- az „Organization-unit" mezőben pedig szerepelhet az Igénylő által a Tanúsítványigénylő űrlapon megadott információ, amely jellemzően Üzleti Tanúsítvány esetén kerül kitöltésre, és az Aláíró Szervezeten (pl. cégen) belüli részlegét vagy szervezeti egységét tartalmazza. (Személyi Tanúsítvány esetén nem kerül kitöltésre)
- a „Locality" mezőben feltüntethető Személyi Tanúsítvány esetén Aláíró állandó lakhelyének helységnevét, Üzleti Tanúsítvány esetén a Szervezet székhelyének helységnevét.
- az aláíró lakóhelyének, székhelyének ország megjelölésénél esetén a Szolgáltató a kétkarakteres országkódot (Magyarország esetén „HU") alkalmazza.

Lásd a szolgáltatási szabályzat 7.1.1 pontjában.

3.1.2 Igény a nevek értelmezhetőségére

A tulajdonos azonosítóra ("Aláíró" mezőre)a következő szabályok érvényesek:

- Az azonosítónak értelmezhetőnek kell lenni.
- A tanúsítványban szereplő személynevet a bemutatott személyazonosító okmányban szereplő, de azt ékezet mentesen feltüntető írásmóddal kell kitölteni,
- Az azonosítók értelmezése érdekében Érintett Feleknek a jelen Szabályzatban leírtak figyelembevételével ajánlott eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett Félnek segítségre van szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot. A Szolgáltató az aláíró, illetve az előfizető egyéb adatairól többlettájékoztatást – a tanúsítványban feltüntetett adatok értelmezését segítő információn kívül – csak az erre vonatkozó felhatalmazás alapján ad ki.

Lásd a szolgáltatási szabályzat 3.1.1 pontjában.

3.1.3 A nevek egyedisége

Az aláíró hitelesítés-szolgáltató tanúsítványtárában egyedi névvel rendelkezik. A hitelesítés-szolgáltató gondoskodik arról, hogy teljes élettartama alatt a tanúsítványban általa használt megkülönböztetett nevet sohasem fogja egy másik egyedhez rendelni.

3.1.4 Eljárások a nevekre vonatkozó vitás kérdések megoldására

A beérkező tanúsítvány kérelmek elbírálási sorrendje alapján történik az Igénylők egyedi azonosítójának kiosztása. A tanúsítványigénylőnek bizonyítani kell a jogát egy adott név használatára. A Szolgáltató fenntartja magának a jogot az igényelt nevek kiosztásának visszautasítására. Ha a kérelmezett azonosító már korábban kiosztásra került, a Szolgáltató az egyediséget szolgáló eljárásait követve eltérő azonosítót oszt ki.

Lásd a szolgáltatási szabályzat 3.1.4 pontját.

3.1.4 Márkanevek elismerése, hitelesítése és szerepe

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 védjegye és márkaneve (i) feltüntetését a tanúsítványban. A tanúsítványkérelemmel és elfogadással az ügyfél kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik személy jogait.

3.1.6 A magánkulcs birtoklásának bizonyítási módszere

A Szolgáltató a szolgáltatás nyújtásához alkalmazott kulcsokon kívül kulcsokat nem generál, azokat az igénylők a végfelhasználói interfész segítségével saját környezetükben állítják elő. Az aláírás-létrehozó

eszközök aktivizáló adatainak kezelése az aláíró felelőssége. A tanúsítvány kérelem eljárása biztosítja, hogy az alany a tanúsításra bemutatott nyilvános kulcsnak megfelelő magánkulcsot birtokolja. Ez gyakorlatban azt eredményezi, hogy a tanúsítvány igénylője nem éri el egy olyan nyilvános kulcs hitelesítését, amelynek a magánkulcs párjával nem rendelkezik.

3.1.7 Személyazonosság hitelesítése

A hitelesítés-szolgáltató jogosult az aláíró személyazonosító igazolványa, útlevele, gépjárművezetői engedélye vagy egyéb, személyazonosításra alkalmas okmánya alapján személyazonosságát megállapítani.

A hitelesítés-szolgáltató adategyeztetést végez az aláíró személyazonosságának ellenőrzése céljából közhiteles nyilvántartásokkal.

Lásd a szolgáltatási szabályzat 3.1.8 pontját.

3.1.8 Szervezeti azonosság hitelesítése

Nem-minősített szervezeti tanúsítvány igénylése esetén a képviselt szervezet neve is feltüntetésre kerül a végfelhasználói tanúsítványokban. Ezekben az esetekben a Szolgáltató a tanúsítványokat kizárólag a képviselt szervezet hozzájárulásával bocsátja ki. Szervezeti tanúsítvány igénylése esetén az igénylőnek minden esetben igazolnia kell, hogy jogosult a szervezet nevében eljárni a tanúsítványigénylés folyamán.

A hitelesítés-szolgáltató adategyeztetést végez - az aláíró személyazonosságának és a szervezet okmányainak érvényességének és hitelességének ellenőrzése céljából - közhiteles nyilvántartásokkal.

Lásd a szolgáltatási szabályzat 3.1.7 pontját.

3.2 Érvényes tanúsítvány megújítása

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

A tanúsítvány megújítása akkor lehetséges, ha:

- Aláíró rendelkezik a lejáró tanúsítványával és a hozzá tartozó magánkulccsal
- a Tanúsítvány érvényességi ideje még nem járt le,
- a Tanúsítvány nem szerepel a Tanúsítvány visszavonási listán, mint visszavont vagy felfüggesztett Tanúsítvány,
- az első regisztráció alkalmával rögzített összes - az Aláíróra és Előfizetőre vonatkozó - adat még érvényes (azok is melyek a Tanúsítványban nem, csak Szolgáltató belső nyilvántartásában szerepelnek),
- a Tanúsítványhoz tartozó magánkulcs nem kompromittálódott.

Lásd a szolgáltatási szabályzat 4.4.16 fejezetét.

3.3 Érvénytelen tanúsítvány megújítása

A Szolgáltató nem teszi lehetővé érvénytelen tanúsítványok megújítását.

3.4 Visszavonási és felfüggesztési kérelem

A hitelesítés-szolgáltató lehetővé teszi érvényes tanúsítvány visszavonásának és felfüggesztésének személyes megjelenést nem igénylő megvalósítását a szolgáltatási szabályzat 4.4 alfejezetében meghatározott módon és feltételekkel.

A hitelesítés-szolgáltató gondoskodik arról, hogy az a) pontban meghatározott, egy már korábban nála nyilvántartásba vett aláírótól származó tanúsítvány visszavonási vagy felfüggesztési kérelem teljes, pontos és kellőképpen hiteles legyen.

Ennek érdekében a hitelesítés-szolgáltató dokumentálja a tanúsítványok visszavonásának, felfüggesztésének eljárásait, beleértve az alábbiakat:

- ki adhat be és milyen formában visszavonási, felfüggesztési kérelmeket,
- mik a visszavonási kérelmek megerősítésére vonatkozó esetleges követelmények,
- milyen okból vonható vissza és milyen okból függeszthető fel egy tanúsítvány,
- mi a felfüggesztett állapot maximális időtartama.

4. A tanúsítvány életciklusra vonatkozó követelmények

4.1 Tanúsítvány igénylés

A hitelesítés-szolgáltató nyilvántartásba vesz minden, az előfizető/aláíró azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat és az előfizetővel/aláíróval aláírt megállapodást. A tanúsítványkérelem benyújtását megelőzően, az előfizető/aláíró tanúsítványigényt kell benyújtania a Szolgáltató felé, amely a Szolgáltató honlapján is történhet.

A tanúsítványigénylésben az előfizető/aláíró megadja az a tanúsítványba kerülő adatok körét, az igényelt tanúsítvány fajtáját és felhatalmazza a Szolgáltatót az adatok kezelésére.

4.2 Tanúsítvány kibocsátás

A végfelhasználói tanúsítványok kibocsátása tanúsítványigénylési folyamat végén kerül sor, amely az előfizető/aláíró által megadott és a Szolgáltató rendelkezésére álló adatok alapján történik. A hitelesítés-szolgáltató köteles biztonságosan fenntartani az általa kibocsátott tanúsítványok hitelességét.

Ez vonatkozik a következőkre:

- a tanúsítvány kibocsátás eljárása biztonságosan kapcsolódjon a megfelelő regisztrációhoz,
- előállítása után pontos és hiánytalan tanúsítvány álljon rendelkezésére azon előfizető/aláíró számára, akinek a tanúsítvány kibocsátásra került,
- a hitelesítés-szolgáltató csak akkor bocsátja ki a tanúsítványt, amikor a hozzá tartozó magánkulcs már az előfizető/aláíró birtokában van.

Lásd a szolgáltatási szabályzat 4.1.9 és 4.2 pontjait.

4.3 Tanúsítvány elfogadás

A Tanúsítvány letöltésekor 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. Amennyiben rendellenességről Szolgáltató nem kap bejelentést a kiadástól számított két héten belül, a tanúsítvány elfogadottnak tekintendő.

A tanúsítvány elfogadásával együtt az aláíró elfogadja, hogy:

- ismeri, érti és elfogadja jelen és kapcsolódó szabályzatokat,
- a tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályoknak és törvényi előírásoknak megfelelően használja,
- minden adat, amit a Szolgáltatónak a tanúsítvány kiadásának céljából átadott, a valóságnak megfelel, és azok átadása önkéntes volt,

- a tanúsítványban szereplő minden adat a tudomásával és egyetértésével került a tanúsítványba,
- a tanúsítvány érvényességét befolyásoló tényekről, valamint az igénylés során megadott személyes és szervezeti adatok megváltozása esetén haladéktalanul értesíti a Szolgáltatót,
- tisztában van azzal, hogy a magánkulcs védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége, s ezzel kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
- jogosulatlan személy nem férhet hozzá magánkulcsához,
- ismeri az elektronikus aláírás megfelelő használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,
- amennyiben az aláíró beleegyezett a tanúsítvány nyilvánosságra hozatalába, felhatalmazza a Szolgáltatót a tanúsítvány közzétételével, és saját vagy más nyilvános tanúsítványgyűjtő helyeken történő elhelyezésével.

4.4 Tanúsítvány felfüggesztés és visszavonás

A hitelesítés-szolgáltató kötelessége, hogy hiteles és érvényes tanúsítvány visszavonási, illetve felfüggesztési kérelmek esetén a tanúsítványok a szolgáltatási szabályzatban meghatározott időn belül a visszavonási listán szerepeljenek. A felfüggesztett tanúsítvány mindaddig, míg felfüggesztett állapotban van, ugyanúgy érvénytelenként kezelendő, mint a visszavont. A tanúsítvány visszavonása a tanúsítvány állapotát végérvényesen érvénytelenre állítja.

Felelősségi szabályok a visszavont/visszavonandó Tanúsítvány elfogadásából eredendő károkra:

- a visszavonási/felfüggesztési igény Szolgáltatóhoz történő megérkezéséig az Aláíró felelős a felmerülő károkért,
- a visszavonási/felfüggesztési igény megérkezésétől az érvénytelen állapot címtárban való megjelenésig a Szolgáltató felelős a felmerülő károkért,
- az érvénytelen állapot címtárban való megjelenése után az Érintett fél felelős a felmerülő károkért.

Lásd a szolgáltatási szabályzat 4.4 pontját.

4.4.1 A visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásához a következő körülmények vezetnek.

Aláíró és előfizető kezdeményezése alapján az alábbi esetekben:

- az Aláíró magánkulcsának kompromittálódása,
- az aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása,
- az 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,
- a Hatóság jogerős és végrehajtható határozata,
- jogszabály rendelkezik így.
- különleges esetek (pl.: szolgáltatói névcsere).

4.4.2 Kik kérelmezhetik a visszavonást?

Végfelhasználói tanúsítvány visszavonását az **aláíró**, **előfizető**, **Szolgáltató**, vagy egy hatóság is kezdeményezheti.

4.4.3 Visszavonási kérelemre vonatkozó eljárás

A Tanúsítvány visszavonási kérelmét az Aláírónak telefonon, levélben vagy faxon van lehetősége bejelentenie az e-Szignó Központi Ügyfélszolgálat és Fokozott Regisztrációs Szervezeténél (a Szervezet elérhetősége a Szolgáltatási Szabályzat 1.4-es pontjában). A visszavonási kérelemre vonatkozó eljárás elindításához az Aláírónak az azonosításhoz szüksége lesz visszavonási jelszóra (amennyiben ezt Aláíró elfelejtette, személyes adatai alapján kerül azonosításra). Az Aláíró szóbeli visszavonási kérelme esetén - Standard biztonsági szintű tanúsítvány esetében– a tanúsítvány visszavonása kérelem beérkezésétől számított 3 órán belül megtörténik, az 1.4 pontban részletezett feltételek szerint. Amennyiben az Aláíró szóbeli visszavonási kérelme Fokozott biztonsági szintű tanúsítványra vonatkozik, a tanúsítvány először felfüggesztésre kerül, a visszavonáshoz az Aláírónak írásban (faxon vagy postai úton) kell megerősítenie visszavonási kérelmét. Az így felfüggesztett Tanúsítvány akkor kerül visszavonásra, amikor Aláíró írásos

kérelme a központi regisztrációs szervezethez beérkezett, vagy a felfüggesztéstől számított 5 munkanap letelt. Ezt követően a Tanúsítvány visszavonásáról a Szolgáltató a lehető leghamarabb intézkedik.

Üzleti Tanúsítvány esetén Előfizető részéről a Szolgáltatási Szerződésben megadott képviselő (k) (jellemzően Aláíró felettese) is kezdeményezheti a visszavonást, a visszavonási kérelmet írásban (faxon vagy postai úton) szükséges, hogy benyújtsa az e- Szignó Központi Ügyfélszolgálat és Fokozott Regisztrációs Szervezeténél.

A visszavonási kérelem benyújtható:

- telefonon, a Magyar Telekom e- Szignó Központi Ügyfélszolgálat és Fokozott Regisztrációs Szervezetén,
- a fent nevezett szervezetnek küldött levélben, illetve faxon.

A visszavonási kérelemnek a következő adatokat kell tartalmaznia:

- a tanúsítvány sorozatszáma, referencia száma, fajtája,
- az Aláíró neve, email címe,
- a visszavonást kérő megnevezése
- a visszavonást kérő beosztása (Üzleti Tanúsítvány esetén),
- a visszavonási jelszó (telefonos visszavonás esetén),
- a visszavonás oka.

Helyes és hiteles kérelem esetén a Szolgáltató további mérlegelés nélkül intézkedik a tanúsítvány visszavonása érdekében: a visszavonást a központi regisztrációs szervezet a kérelem beérkezésétől számított 3 órán belül végrehajtja, az 1.4 pontban részletezett feltételek szerint.

További információért lásd a szolgáltatási szabályzat 4.4.3 pontját.

4.4.4 A felfüggesztés körülményei

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

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

Szolgáltató kezdeményezése alapján az alábbi esetekben:

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

Egyéb visszavonáshoz vezető körülmények:

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

4.4.5 Kik kérelmezhetik a felfüggesztést?

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

4.4.6 Felfüggesztési kérelemre vonatkozó eljárás

A felfüggesztési kérelem a visszavonási kérelemhez hasonlóan nyújtható be Szolgáltatóhoz.

4.4.7 A felfüggesztés időtartama

Tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, vagy míg a kezdeményező annak visszaállítását nem kéri, de legfeljebb 5 munkanapig.

Ezt követően a Tanúsítvány visszavonásáról a Szolgáltatónak a lehető leghamarabb intézkednie kell.

Felfüggesztés megszüntetése:

Amennyiben a felfüggesztést az Aláíró vagy az Előfizető kérelmezte, úgy kérelmezheti a tanúsítvány újbóli érvénybe helyezését is. Aláíró kérelmét telefonon keresztül nyújthatja be; azonosítása jelszava alapján történik; ezt követően – Standard Tanúsítvány esetében Szolgáltató megszünteti a felfüggesztést. Fokozott biztonsági szintű tanúsítvány esetében írásban (faxon) kell az ilyen irányú kérelmet benyújtani a Regisztrációs Szervezethez. Ezt követően a tanúsítvány újbóli érvényesre állításáról a Szolgáltatónak lehető leghamarabb intézkednie kell.

Előfizető részéről a felfüggesztés megszüntetését a kijelölt kapcsolattartónak „standard" és „fokozott" szint esetén is faxon kell benyújtania.

4.5 Rendelkezésre állási feltételek (SLA)

A Szolgáltató minden tőle elvárhatót megtesz azért, hogy a Hitelesítő Központ egysége (Fokozott CA) és annak Interneten keresztül elérhető felülete (e- Szignó honlap) folyamatos működését biztosítsa, és a Szolgáltatási Szabályzatban vállalt Rendelkezésre Állási Feltételeket betartsa.

4.5.1 Hitelesítő Központ egység hálózati rendelkezésre állása

A Hitelesítő Központ egység hálózat havi rendelkezésre állása 90,0 %.

4.5.2 A Fokozott CA szolgáltatásainak rendelkezésre állása

A Fokozott CA heti 7 napon, napi 24 órában elérhető Interneten keresztül, szolgáltatásainak rendelkezésre állása vonatkozásában az alábbi feltételek érvényesek:

- **Tanúsítványigénylés befogadás és feldolgozás, tanúsítvány kibocsátás rendelkezésre állása**

A tanúsítványigénylés befogadás és feldolgozás, tanúsítvány kibocsátás havi rendelkezésre állása 90,0 %.

- **A Tanúsítvány Tár Szolgáltatás rendelkezésre állása**

A Publikus Tanúsítvány Tár Szolgáltatás (kibocsátott tanúsítványokat tartalmazó nyilvántartás) havi rendelkezésre állása 90,0 %.

- **A Tanúsítvány felfüggesztési/visszavonási nyilvántartás rendelkezésre állása**

A Tanúsítvány felfüggesztési/visszavonási nyilvántartás havi rendelkezésre állása 99,5 %. A felfüggesztés / visszavonás kezelési szolgáltatások rendelkezésre állása 99,5% a nyitvatartási időkre vonatkozóan, melyeket az 1.4 fejezet tartalmaz.

5. Elhelyezési, irányítási és működtetetési rendszabályok

A biztonsági óvintézkedésekről általában

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

Ezen belül:

- a hitelesítés-szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározása érdekében,
- a hitelesítés-szolgáltató felelősséget vállal minden elektronikus aláírással kapcsolatos szolgáltatásért még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki,
- a hitelesítés-szolgáltató vezetősége (mely felelős a hitelesítés-szolgáltató informatikai biztonság politikájának meghatározásáért, és e politika által érintett valamennyi alkalmazott részére történő közzétételért) az információ biztonságára vonatkozó útmutatót hagyott jóvá és adott ki,
- a hitelesítés-szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a hitelesítés-szolgáltató vezetősége hagyja jóvá,
- a hitelesítés-szolgáltató (rendszerbiztonsági szabályzatában) dokumentálta, majd megvalósította és folyamatosan fenntartja a hitelesítési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait,
- a hitelesítés-szolgáltató gondoskodik az informatika biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez, illetve egységhez lettek kiadva.

A hitelesítés-szolgáltató biztonsági műveleteiért a végső felelősség a hitelesítés-szolgáltatót terheli.
Ezen biztonsági műveletek közé az alábbiak tartoznak:

- üzemeltetési eljárások és felelősségek,
- biztonsági rendszerek tervezése és elfogadása,
- káros szoftver elleni védelem,
- erőforrás gazdálkodás,
- hálózat menedzselés,
- a biztonsági napló aktív felügyelete, eseményelemzések és nyomkövetések,
- adathordozó eszköz kezelése és biztonsága,
- adat és szoftver csere.

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

Az értékek osztályozása és kezelése

A hitelesítés-szolgáltató gondoskodik arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek. A hitelesítés-szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit osztályokba sorolja és minősíti, az elvégzett kockázat elemzéssel összhangban.

5.1 Fizikai óvintézkedések

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

5.1.1 A telephely elhelyezése és szerkezeti felépítése

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

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

Tanúsítvány előállítással, aláírók eszközzel való ellátásával, visszavonás kezeléssel kapcsolatosan a hitelesítés-szolgáltató egy egyértelműen meghatározott biztonsági körlet létrehozásával fizikai védelmet biztosít az alábbi szolgáltatások számára:

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

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

A hitelesítés-szolgáltató:

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

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

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

5.1.2 Fizikai hozzáférés

A hitelesítés szolgáltató:

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

szolgáltatásokkal kapcsolatos eszközökhöz történő fizikai hozzáférést megfelelően felhatalmazott egyénekre korlátozza.

A hitelesítés szolgáltató:

- tanúsítvány előállítás,
- az aláírók eszközzel való ellátása,

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

5.1.3 Áramellátás, légkondicionálás

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

5.1.4 Beázás és elárasztódás veszélyeztetettsége

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

5.1.5 Tűzmegelőzés és tűzvédelem

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

5.1.6 Adathordozók tárolása

A hitelesítés-szolgáltató az adathordozó eszközöket biztonságosan kezeli a sérülés, eltulajdonítás és jogosulatlan hozzáférés elleni védelem érdekében[2].

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

[2] A személyzet minden irányítói felelősséggel rendelkező tagja felelős a tanúsítványfajta és a vele kapcsolatos gyakorlatok tervezéséért, valamint a szolgáltatási szabályzatban dokumentáltaknak megfelelő, hatékony megvalósításáért.

5.1.7 Selejt kezelése, megsemmisítése

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

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

A Hitelesítő Szervezet biztonság-kritikus szolgáltatásaira vonatkozó adatok mentési példányait a biztonsági körletben elhelyezett tűzbiztos, kódzáras szekrényben, míg a másodpéldányait és az archivált adatokat a Magyar Telekom Katasztrófa Adattárában tárolják.

5.2 Eljárásbeli óvintézkedések

A hitelesítés-szolgáltató gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. A hitelesítés-szolgáltató személyzete olyan adminisztratív és kezelési eljárásokat és folyamatokat végez, amely szinkronban van a hitelesítés-szolgáltató rendszerbiztonsági szabályzatának eljárásaival.

5.2.1 Bizalmi munkakörök

Hitelesítés-szolgáltató a következő bizalmi munkaköröket határozza meg:

- Biztonsági tisztviselő,
- Rendszeradminisztrátor,
- Regisztrációs felelős (illetve regisztrációs tisztviselő),
- Regisztrációs ügyeleti operátor,
- Rendszeroperátor,
- Rendszervizsgáló.
- Informatikai rendszerért általánosan felelős vezető

Bizalmi munkakörökkel kapcsolatos részletes leírást a szolgáltatási szabályzat 5.3.1 pontja tartalmazza.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Általánosan teljesül a hitelesítő szolgáltató egészére, hogy minden munkatárs csak a saját munkakörének megfelelő funkciókat aktivizálja. Szolgáltató vonatkozó belső szabályzata meghatározza az egyes feladatokhoz szükséges személyzeti létszámokat.

Lásd a szolgáltatási szabályzat 5.3.2 pontját.

5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

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

5.3 Személyzetre vonatkozó óvintézkedések

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

A hitelesítés-szolgáltató kellő számú, az elektronikus aláírással kapcsolatos szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet alkalmaz.

A hitelesítés-szolgáltató ügyvezetői, vezető beosztású munkatársainak és felelős munkaköröket betöltő munkatársainak függetlennek kell lenniük minden olyan kereskedelmi, pénzügyi és egyéb hatástól, ami hátrányosan befolyásolhatja a hitelesítő szolgáltató által nyújtott szolgáltatások iránti bizalmat.

A hitelesítés-szolgáltató (ideiglenes és állandó) munkatársai a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaleírásokkal rendelkeznek.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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

A vezető személyzet tapasztalattal rendelkezik az elektronikus aláírási technológia terén, ismeri a biztonsági felelősséggel tartozó munkatársakra vonatkozó biztonsági eljárásokat, valamint gyakorlattal rendelkezik az informatika biztonság és a kockázat elemzés területein.

5.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások

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

5.3.3 Kiképzési követelmények

A hitelesítés-szolgáltató személyzete rendelkezik a kínált szolgáltatásokhoz szükséges szakértői tudással, tapasztalattal és minősítésekkel. Lásd a szolgáltatási szabályzat 5.2.1 pontját.

5.3.4 Továbbképzési gyakoriságok és követelmények

A személyes továbbképzési tervet az illetékes HR Partner osztály bevonásával a közvetlen vezető évente áttekinti, értékeli és (az érintett munkatárs beleegyezésével) aktualizálja.

Lásd a szolgáltatási szabályzat 5.2.2 pontjának előírásai szerint.

5.3.5 A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentáció tartalmazza az 5. pontban említett rendszerbiztonsági szabályzatot.

5.4 A biztonsági naplózás folyamatai

A hitelesítés-szolgáltató szolgáltatási szabályzata határozza meg (a 5.4.1–5.4.8 pontok szempontrendszere alapján), hogy a biztonságos környezet fenntartása érdekében a hitelesítés-szolgáltató milyen eseménynaplózó és ellenőrző rendszereket valósít meg.

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

- a hitelesítés-szolgáltató a környezetére, kulcs- és tanúsítvány gondozására vonatkozó események pontos időpontját is rögzíti[3].
- a hitelesítés-szolgáltató biztosítja személyzete felelősségre vonhatóságát tevékenységéért, többek között az eseménynapló megőrzésén és védelmén keresztül (lásd 5.4.1, 5.4.4 és 5.4.5 fejezetek).

5.4.1 A tárolt események típusai

A hitelesítés-szolgáltató által naplózott és tárolt események a következő folyamatokat érinti:

- a regisztráció,
- tanúsítvány életciklusa,
- kulcsok életciklusa,
- hibaesemények.

Lásd a szolgáltatási szabályzat 5.4.1 pontját.

5.4.2 A napló állomány feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása napi rendszerességgel megtörténik.

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

Lásd a szolgáltatási szabályzat 5.4.2 pontját.

5.4.3 A napló állomány megőrzési időtartama

A naplóállományokat 90 napig tárolja a Szolgáltató a keletkezésük helyén, utána írható médiára kerülnek rögzítésre és az [1] 9. § (7) bekezdésben meghatározott ideig a Szolgáltató megőrzi.

Lásd a szolgáltatási szabályzat 5.4.3 pontját.

5.4.4 A napló állomány védelme

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

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

5.4.5 A napló állomány mentési folyamatai

A naplóállományok napi rendszerességgel (az átvizsgálást megelőzően) mentésre kerülnek egyszer írható médiára aláírt formában. 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.

Lásd a szolgáltatási szabályzat 5.4.6 pontját.

5.4.7 Az eseményeket kiváltó aláírók értesítése

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

5.4.8 Sebezhetőség felmérése

A napi rendszerességgel végzett feldolgozáson túl Szolgáltató szakemberei havonta áttekintik a rendkívüli eseményeket és ezek alapján elemzéseket végeznek a szolgáltatás sebezhetősége szempontjából.

Lásd a szolgáltatási szabályzat 5.4.8 pontját.

5.5 Adatok archiválása

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

5.5.1 A tárolt események típusai

A hitelesítés-szolgáltató gondoskodik arról, hogy rögzítésre kerüljön az összes regisztrációs információ. A tanúsítványokra vonatkozó valamennyi naplóbejegyzés archiválásra kerül.

Azon eseményeket, melyek a fent említett naplóbejegyzéseken túl kerülnek archiválásra (a biztonságos környezet fenntartásának és utólagos ellenőrizhetősége és bizonyíthatósága céljából), a hitelesítés-szolgáltató szolgáltatási szabályzat 5.4.1 pontjában határozza meg.

5.5.2 Az archívum megőrzési időtartama

A hitelesítés-szolgáltató a szolgáltatási szabályzat 5.4.1 pontjában megnevezett nyilvántartásokat megőrzi a tanúsítvány érvényességének lejártától számított tíz évig, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig.

A hitelesítés-szolgáltató az 5.4.1 pontban meghatározott adatokon kívüli napló adatokat (lásd Szolgáltatási Szabályzat 5.4.1. pont) a keletkezésüktől számított tíz évig megőrzi.

A hitelesítés-szolgáltató Hitelesítési Rend dokumentumait és szolgáltatási szabályzatait hatályon kívül helyezésüktől számított tíz évig megőrzi.

5.5.3 Az archívum védelme

A hitelesítés-szolgáltató fenntartja a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét.

A hitelesítés-szolgáltató a tanúsítványokra vonatkozó naplóadatokat teljes körűen és a bizalmasságot garantáló módon archiválja a szolgáltatási szabályzat 5.5.3 pontjában leírt üzleti gyakorlatnak megfelelően.

A hitelesítés-szolgáltató a bejegyzéseket megvédi az elveszéstől, tönkretételtől és hamisítástól.

A hitelesítés-szolgáltató megfelelő műszaki és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen feldolgozása ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen.

5.5.4 Az archívum mentési folyamatai

Az archívum mentési folyamatát a hitelesítés-szolgáltató szolgáltatási szabályzat 5.5.4 pontjában határozza meg.

5.5.5 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[4].

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

5.5.6 Archív információ hozzáférését és ellenőrzését végző eljárások

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

Az aláíró, és az adatvédelmi követelmények korlátozásain belül az előfizető hozzáférhet az aláíróra vonatkozó regisztrációs és egyéb információhoz.

5.6 Helyreállítás rendkívüli üzemi helyzetek esetén

A hitelesítés-szolgáltató a rendkívüli üzemeltetési helyzetek esetére olyan eljárásokat dolgozott ki, amely lehető teszi a megbízható üzemmenet mielőbbi helyreállítását.

A hitelesítés-szolgáltató gondoskodik arról, hogy rendkívüli üzemeltetési helyzet bekövetkezése esetén, beleértve a saját magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, a visszavonási nyilvántartások megbízható helyreállítása maradéktalanul megtörténjen.

Rendkívüli üzemeltetési helyzet bekövetkezése esetén a hitelesítés-szolgáltató haladéktalanul értesíti a Felügyelet, valamint a szolgáltatást igénybe vevő mindazon személyeket, akiket a rendkívüli üzemeltetési helyzet érint.

5.6.1 Sérült számítási erőforrások, szoftverek és/vagy adatok

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

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

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

5.6.2 A szolgáltatói egység nyilvános kulcsának visszavonása

Egy szolgáltatói kulcs visszavonása esetén a hitelesítés-szolgáltató vállalja, hogy a visszavonásról tájékoztatja az összes aláírót/előfizetőt és érintett felet, és jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes (ek).

A hitelesítés-szolgáltató a szolgáltatói kulcs visszavonását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint a végfelhasználók számára új nyilvános kulcsot biztosít új tanúsítvány kiadásával.

5.6.3 Egy szolgáltatói egység kulcsának kompromittálódása

Egy szolgáltatói kulcs kompromittálódása esetén a hitelesítés-szolgáltató vállalja, hogy a kompromittálódásról tájékoztatja az összes aláírót/előfizetőt és érintett felet, és jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes(ek).

A hitelesítés-szolgáltató a szolgáltatói kulcs kompromittálódását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint a végfelhasználók számára új nyilvános kulcsot biztosít új tanúsítvány kiadásával.

5.6.4 Működési képesség természeti vagy más katasztrófát követően

Természeti vagy más katasztrófát követően a hitelesítés-szolgáltató életbe lépteti az üzlet folytonossági terve (illetve katasztrófa utáni helyreállítási terve) által előírt eljárásokat annak érdekében, hogy az üzemeltetés helyreálljon a szolgáltatási szabályzat 5.6.4 alfejezetében megjelölt időn belül.

Katasztrófát követően a hitelesítés-szolgáltató ésszerű lépéseket tesz a katasztrófa ismételt bekövetkezésének megakadályozására.

5.7 A hitelesítés szolgáltatás leállítása

A Szolgáltató a szolgáltatás tervezett megszűntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Hatóságot[5]. 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 és az aláírás-létrehozó adat elhelyezése aláírás létrehozó eszközön szolgáltatásokat.

Lásd a szolgáltatási szabályzat 5.7 alfejezetét.

[5] ld. [1] törvény 16. § (1)

6. Műszaki biztonsági óvintézkedések

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

6.1 Kulcspár előállítás és telepítés

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

6.1.1 Kulcspár előállítás

A hitelesítés-szolgáltató saját kulcspár előállítása

A hitelesítés-szolgáltatónál történő kulcselőállítást fizikailag védett környezetben (lásd 5.1), bizalmi munkakört betöltő személyzet (lásd 5.2.1) végzi, legalább kettős ellenőrzés[6] mellett. A kulcselőállítás funkció végrehajtására felhatalmazott személyzet körét a hitelesítés-szolgáltató szolgáltatási szabályzatának még megfelelve, a lehető legkisebbre korlátozza.

A hitelesítés-szolgáltató a kulcselőállítást olyan biztonságos kriptográfiai modulban hajtja végre, amely tanúsítvánnyal igazoltan megfelel az alábbi követelményeknek:

- a modul garantálja a kulcsok bizalmasságát és sértetlenségét azok teljes életciklusa során,
- a modul képes felhasználói azonosítására és hitelesítésére,
- a modul a felhasználó és annak szerepköre alapján azokra a szolgáltatásokra korlátozza a hozzáférést, amelyek az adott felhasználó adott szerepköréhez vannak rendelve,
- a modul képes egy teszt sorozat lefuttatására, mely ellenőrzi működése helyességét, és hiba észlelése esetén egy biztonságos állapotba lép,
- a modul észleli a fizikai módosítási kísérleteket, s ilyenkor egy biztonságos állapotba lép,
- a modul naplóbejegyzéseket készít minden biztonság-kritikus változtatásról,
- amennyiben a modul támogatja a kulcsok mentését és visszaállítását[7], megvédi a mentési adatok bizalmasságát és sértetlenségét, s legalább kettős ellenőrzést követel meg mind a mentés, mind a visszaállítás műveleténél
- amely szerepel a Felügyelet elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között.

A hitelesítés-szolgáltató a kulcs előállítását olyan algoritmussal valósítja meg, melyet a Felügyelet erre vonatkozó határozatban a célra alkalmasnak jelöl meg.

A hitelesítés-szolgáltató által más felek számára előállított kulcspár előállítás

A hitelesítés-szolgáltató által saját szervezeti egységei /címtár, regisztrációs szervezetek/ számára előállított kulcsokat biztonságos módon, olyan algoritmussal állítja elő, melyet a Felügyelet erre vonatkozó határozata a célra megfelelőnek és alkalmasnak jelöl meg.

A hitelesítés-szolgáltató az aláírók számára nem generál magánkulcsokat. Az aláírás-létrehozó eszköz elkészítését (logikai és fizikai megszemélyesítését) a hitelesítés-szolgáltató ellenőrzi.

[6] Két személy együttes jelenlétével
[7] ez csak egy opcionális elvárás

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

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

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

6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

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

6.1.4 A szolgáltatói nyilvános kulcs közzététele

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

6.1.5 Kulcs méretek

A hitelesítés-szolgáltató saját kulcsának méretére vonatkozóan a hitelesítés-szolgáltató aláíró kulcsára olyan kulcshosszúságot és algoritmust választ, melyet a Felügyelet erre vonatkozó határozata a célra alkalmasnak jelöl meg.

A hitelesítés-szolgáltató által más felek számára előállított kulcsok méretére vonatkozóan a hitelesítés-szolgáltató által más felek (regisztrációs szervezetek) számára generált kulcsok olyan hosszúságúak és olyan algoritmushoz tartozók, melyet a Felügyelet erre vonatkozó határozata a célra alkalmasnak jelöl meg.

6.1.6 A nyilvános kulcs paramétereinek előállítása

A hitelesítés-szolgáltató a nyilvános kulcs paramétereinek előállítása során /beleértve az ehhez szükséges véletlen szám generálást is/ olyan szabványos megoldást használ, melyet a Felügyelet erre vonatkozó határozata a célra alkalmasnak jelöl meg.

6.1.7 A paraméterek megfelelőségének ellenőrzése

A hitelesítés-szolgáltató ellenőrzi valamennyi kulcspár előállítása során a paraméterek minőségét.[8]

6.1.8 Hardver/szoftver kulcselőállítás

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

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

A hitelesítés-szolgáltató saját kulcsainak használati célja az alábbiak egyike lehet:

- tanúsítvány aláírás,
- visszavonási lista aláírás,
- titkosítás.

Az aláírók által használt végfelhasználói aláíró kulcsok használati célja kizárólag aláírás (nonrepudiation, digital signature) lehet[9].

6.2 A magánkulcsok védelme

A hitelesítés-szolgáltató gondoskodik valamennyi általa (saját maga, a regisztrációs szervezetek) előállított magánkulcs titkosságáról és sértetlenségéről. A hitelesítés-szolgáltató ugyanazt az aláíró magánkulcsot használ tanúsítvány aláírásra, és tanúsítvány visszavonási lista aláírásra, egyúttal e kulcsot semmilyen más célra nem használja. A hitelesítés-szolgáltató a tanúsítványokat, illetve a tanúsítvány visszavonási listákat aláíró magánkulcsát fizikailag biztonságos helyszínen használja.

6.2.1 Kriptográfiai modulra vonatkozó szabványok

Hitelesítő szervezet

A hitelesítés-szolgáltató a tanúsítványokat és tanúsítvány visszavonási listákat aláíró magánkulcsát olyan biztonságos kriptográfiai modulban állítja elő, amely tanúsítvánnyal igazoltan megfelel a 6.1.1 alatt felsorolt követelményeknek, s amely szerepel a Felügyelet elektronikus aláírással kapcsolatos nyilvántartásában, a tanúsított elektronikus aláírási termékek között. A tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelményrendszer szerint, azzal egyenértékű értékeli szinten végezték.

A Hitelesítő Szervezet tanúsítványokat és tanúsítvány visszavonási listákat aláíró magánkulcsát olyan biztonságos kriptográfiai modulban tárolja és használja, amely tanúsítvánnyal igazoltan megfelel a 6.1.1 alatt felsorolt követelményeknek, s amely szerepel a Felügyelet elektronikus aláírással kapcsolatos

[8] A szolgáltatási szabályzatban ismertetett módon.
[9] Ez a tanúsítványfajta kizárólag elektronikus aláírásra használható kulcsokkal, tanúsítványokkal foglalkozik. A titkosításra, illetve azonosításra is használható kulcsokkal hitelesítés-szolgáltató egy másik tanúsítványfajtája foglalkozik.

nyilvántartásában, a tanúsított elektronikus aláírási termékek között. A tanúsítást a CEN CMCSO-PP [5] vagy más, alkalmas követelményrendszer szerint, azzal egyenértékű értékeli szinten végezték.

Aláírók

A hitelesítés-szolgáltató aláírók számára nem generál magánkulcsokat az aláíró magánkulcsa a nyilvános kulccsal együtt a tanúsítvány igénylésekor, az aláíró által felügyelt környezetben generálódik.

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

Hitelesítő szervezet

A hitelesítő szervezet magán aláíró kulcsait csak bizalmi munkakört betöltő személyzet állíthatja vissza, legalább kettős ellenőrzés mellett, fizikailag biztonságos környezetben (lásd 5.1.2).

Aláírók

Az aláírók magán aláíró kulcsa a szolgáltatónál nem kerül mentésre, így a szolgáltató általi visszaállítása nem lehetséges.

6.2.3 Magánkulcs letétbe helyezése

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

6.2.4 Magánkulcs mentése

Hitelesítő szervezet

A hitelesítő szervezet magán aláíró kulcsát csak bizalmi munkakört betöltő személyzet másolhatja le (mentésre csak a kulcs helyreállításához szükséges titokrészek kerülnek), illetve tárolhatja le, legalább kettős ellenőrzés mellett, fizikailag biztonságos környezetben (lásd az 5.1.2 pontot).

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

Aláírók

Az aláíróknak előállított magánkulcsok hitelesítés-szolgáltató általi mentése nem lehetséges.

6.2.5 Magánkulcs archiválása

A hitelesítés-szolgáltató magánkulcsot nem archivál.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

Hitelesítő szervezet

A hitelesítő szervezet magánkulcsait az ezeket felhasználó kriptográfiai hardver modul állítja elő, így ezeket nem kell külön a modulba juttatni.

Arra az időre, amíg a fenti kulcsok a kriptográfiai hardver modult elhagyják (átmenetileg, mentési célból, a mentés célját szolgáló tartalék kriptográfiai hardver modulra való áttöltés során, lásd 6.2.4) a hitelesítő szervezet kódolja magánkulcsait, olyan algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs vagy kulcsrészlet teljes hátralévő életciklusában.

A hitelesítő szervezet kriptográfiai hardver modulja kikapcsolt állapotban a magánkulcsokat kódolva tárolja, olyan algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs teljes hátralévő életciklusában.

Aláírók

A hitelesítés-szolgáltató aláírók számára nem generál magánkulcsokat, az aláíró magánkulcsa a nyilvános kulccsal együtt a tanúsítvány igénylésekor, az aláíró által felügyelt környezetben generálódik.

6.2.7 A magánkulcs aktivizálásának módja

Hitelesítő szervezet

A hitelesítő szervezet (tanúsítványokat és tanúsítvány visszavonási listákat aláíró) magánkulcsa aktivizálását az erre felhatalmazott felhasználó birtokláson és tudáson alapuló kombinált hitelesítési eljárással aktivizálhatja.

A hitelesítő szervezet egyéb (a hitelesítés-szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsa aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.

Regisztrációs szervezet

A regisztrációs szervezet (az archiválandó regisztrációs adatokat és tranzakciókat aláíró) magánkulcsa aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.

A regisztrációs szervezet egyéb (a hitelesítés-szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsai aktivizálását az erre felhatalmazott felhasználó[10] tudáson alapuló hitelesítési eljárással aktivizálhatja.

Aláírók

Az aláíró magánkulcsa illetéktelen felhasználásának megakadályozása érdekében az aláírás-létrehozó eszközben tárolt magánkulcs használatát az aláíró csak tudáson alapuló hitelesítési eljárással aktivizálhatja.

6.2.8 A magánkulcs aktív állapotának megszüntetési módja

Hitelesítő és regisztrációs szervezet

[10] a rendszerüzemeltető

A magánkulcsok aktív állapotának megszüntetése (deaktiválása) akkor lehetséges, ha a magánkulcsot tároló kriptográfiai hardver modulok szabályos vagy szabálytalan módon kikerülnek az aktivizálást és felhasználást lehetővé tevő állapotból.

Aláírók

A magánkulcsok deaktiválása akkor lehetséges, ha a magánkulcsot tároló aláírás-létrehozó eszköz szabályos vagy szabálytalan módon kikerül az aktivizálást és felhasználást lehetővé tevő állapotból.

6.2.9 A magánkulcs megsemmisítésének módja

Hitelesítő és regisztrációs szervezet és aláíró magánkulcsainak megsemmisítése

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

A hitelesítés-szolgáltató magán aláíró kulcsainak használatát korlátozza oly módon, hogy az összhangban legyen a tanúsítvány előállításához használt lenyomatozó függvényre, aláíró algoritmusra és kulcshosszra vonatkozó (6.1.5. pontban kifejtett) gyakorlatnak.

A hitelesítés-szolgáltató kriptográfiai hardver moduljában tárolt szolgáltatói magán aláíró kulcsokat a hardver modul visszavonásakor megsemmisíti oly módon, hogy a magánkulcsok ne legyenek helyreállíthatók.

A hitelesítés-szolgáltató magán aláíró kulcsainak megsemmisítésekor azok összes másolatát is megsemmisíti oly módon, hogy a magánkulcsok ne legyenek helyreállíthatók.

Az aláíró magánkulcsának megsemmisítése az aláíró felelőssége.

6.3 A kulcspár gondozásának egyéb szempontjai

6.3.1 A nyilvános kulcsok archiválása

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

6.3.2 A nyilvános és magánkulcsok használatának periódusa

Hitelesítő és regisztrációs szervezet

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

Aláírók

Az aláíró magánkulcsának használati periódusa nem haladhatja meg a tanúsítvány érvényességi idejét, ennek betartása viszont kívül esik a hitelesítés-szolgáltató felelősségi körén. Ennek betartása az előfizető

és az aláíró kötelessége (lásd 9.1.4.1 és 9.1.4.2 fejezetek), ellenőrzése pedig az érintett felek részére ajánlott.(lásd 9.1.5 fejezet).

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

A hitelesítés-szolgáltató aláírók számára nem generál magánkulcsokat az aláíró magánkulcsa a nyilvános kulccsal együtt a tanúsítvány igénylésekor, az aláíró által felügyelt környezetben generálódik. Az aláírás-létrehozó eszközök aktivizáló adatainak kezelése az aláíró felelőssége.

6.4.2 Az aktivizáló adatok védelme

A hitelesítés-szolgáltató aláírók számára nem generál magánkulcsokat az aláíró magánkulcsa a nyilvános kulccsal együtt a tanúsítvány igénylésekor, az aláíró által felügyelt környezetben generálódik. Az aláírás-létrehozó eszközök aktivizáló adatainak kezelése az aláíró felelőssége.

6.4.3 Az aktivizáló adatok egyéb szempontjai

A hitelesítés-szolgáltató aláírók számára nem generál magánkulcsokat az aláíró magánkulcsa a nyilvános kulccsal együtt a tanúsítvány igénylésekor, az aláíró által felügyelt környezetben generálódik. Az aláírás-létrehozó eszközök aktivizáló adatainak kezelése az aláíró felelőssége.

6.5 Számítógép biztonsági óvintézkedések

6.5.1 Speciális számítógép biztonsági műszaki követelmények

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

A hitelesítés-szolgáltató védi rendszerei és információi sértetlenségét vírusok, káros és engedély nélküli szoftverek ellen.

A hitelesítés-szolgáltató biztonságosan kezeli adathordozó eszközeit a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.

A hitelesítés-szolgáltató gondoskodik a felhasználói[11] hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.

A hitelesítés-szolgáltató gondoskodik arról, hogy az információhoz és az alkalmazói rendszer funkciókhoz történő hozzáférés, a hozzáférés ellenőrzési szabályzatnak megfelelően korlátozott legyen, és hogy a hitelesítés-szolgáltató rendszere megfelelő számítógép biztonsági ellenőrzéseket nyújtson a hitelesítés-szolgáltató szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében, beleértve a biztonsági, adminisztrátori és üzemeltetési funkció elkülönítését. Különösképpen a rendszer szolgáltatási programok használatát korlátozza és ellenőrzi szigorúan.

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

A hitelesítés-szolgáltató gondoskodik arról, hogy személyzetét sikeresen azonosítsák és hitelesítsék, mielőtt a tanúsítvány gondozásával kapcsolatos kritikus alkalmazásokat használhatnák.

A hitelesítés-szolgáltató eljárásokat dolgoztat ki és hajtat végre valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására.

A hitelesítés-szolgáltató műszaki óvintézkedéseket juttat érvényre, hogy a hitelesítés-szolgáltató belső hálózati tartományai védettek legyenek a harmadik felek számára elérhető külső hálózati tartományoktól.

A hitelesítés-szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.

A hitelesítés-szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni és regisztrálni az erőforrásaihoz való jogosulatlan és/vagy szabálytalan hozzáférési kísérleteket, valamint képes legyen ezekre időben reagálni.

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

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

A hitelesítés-szolgáltató gondoskodik arról, hogy az érzékeny adatokat[12] megvédjék az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.

A hitelesítés-szolgáltató biztosítja a személyzet tevékenységéért való felelősségre vonhatóságát.

6.5.2 Informatikai biztonsági minősítés

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

A hitelesítés-szolgáltató megbízható informatikai rendszereket alkalmaz.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

A hitelesítés-szolgáltató gondoskodik arról, hogy az általa, illetve a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény-meghatározási fázisban figyelembe vegyék, annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

A hitelesítés-szolgáltató konfiguráció kezelési eljárásokat alkalmaz valamennyi működő szoftvere esetében a kibocsátásokra, a módosításokra és a sürgős szoftver javításokra vonatkozóan.

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

6.6.2 Biztonságkezelési óvintézkedések

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

6.6.3 Az életciklusra vonatkozó biztonság osztályozása

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

6.7 Hálózatbiztonsági óvintézkedések

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

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

- az érzékeny adatokat[13] megvédi, amikor azok átvitele (cseréje) nem biztonságos hálózatokon keresztül történik,
- a hitelesítés-szolgáltató biztosítja általános informatikai biztonságát még akkor is, ha a hitelesítés-szolgáltató egyes funkciót más szervezet (pl. a regisztrációs szervezet) valósítja meg.

A regisztrálással kapcsolatosan:

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

A tanúsítvány előállítással és visszavonás kezeléssel kapcsolatosan:

- a hitelesítés-szolgáltató gondoskodik arról, hogy a helyi hálózati komponensek (például routerek) fizikailag biztonságos környezetben legyenek és konfigurációikat időszakonként auditálják,
- a hitelesítés-szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni, regisztrálni az erőforrásaihoz (hálózatról) történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre.

A tanúsítvány kibocsátásával kapcsolatosan:

- A hitelesítés-szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést

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

érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.

A tanúsítvány visszavonás kezeléssel kapcsolatosan:

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

6.8 A kriptográfiai modul ellenőrzése

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

- a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják szállítás közben;
- a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják tárolás közben;
- a hitelesítés-szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktivizálása, mentése és visszaállítása legalább két bizalmi munkakört betöltő alkalmazott együttes jelenlétét kívánja meg (lásd a szolgáltatási szabályzat 5.3.2 fejezetét);
- a tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardver helyesen működik;
- a hitelesítés-szolgáltató kriptográfiai hardverén tárolt hitelesítés-szolgáltatói magán aláíró kulcsokat az eszköz visszavonásakor megsemmisítik.

7. Tanúsítvány és tanúsítvány visszavonási lista profilok

7.1 Tanúsítvány profil

A hitelesítés-szolgáltató által kibocsátott tanúsítványok megfelelnek a [9] szabványban leírt X.509 3-as verziójú tanúsítványoknak.

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

Tanúsítványmező	Tartalom	Megjegyzés
Verzió (Version)	v3	
Szériaszám (SerialNumber)		A Kibocsátó hitelesítő egységen belül egyedi szám, célja az adott Tanúsítvány egyértelmű azonosítása.
Aláírási algoritmus (Signature Algorithm)	SHA-1 RSA	
Kiállító (Issuer)		Kibocsátó (vagy Kiállító) - a tanúsítványt kibocsátó Szolgáltató illetve Hitelesítő központi egységének egyedi azonosítója
CN (Common Name)	Magyar Telekom Fokozott CA	Kibocsátó hitelesítő központi egységének neve
OU (Organizational Unit)	Magyar Telekom Trust Center	Kibocsátó szervezeti egységének (részlegének) neve
O (Organization)	Magyar Telekom	Kibocsátó (Szolgáltató) neve
C (Country)	HU	
Érvényesség kezdete (Validity - notBefore)		A kiadás dátuma és időpontja, egyben a Tanúsítvány érvényességének kezdete.
Érvényesség vége (Validity - notAfter)		A lejárat dátuma és időpontja, egyben a Tanúsítvány érvényességének vége.
Tulajdonos (Subject)		A Tanúsítvány felhasználójának (Aláíró) egyedi azonosítója. Ez a mező illetve ennek almezői jelölik az Aláírót, akinek a kulcsát a Szolgáltató hitelesíti.
CN (CommonName)		*Az Aláíró kereszt- és vezetéknevét tartalmazza (a bemutatott személyazonosító okmányban szereplő, de azt ékezet mentesen feltüntető írásmóddal kell kitölteni). Ellenőrzése a benyújtott dokumentum (jellemzően személyigazolvány másolata) alapján történik, minden esetén adategyeztetéssel (közhiteles adatszolgáltatókkal) Amennyiben az Aláíró igényli, álnévvel is szerepelhet a

		Tanúsítványban; ilyenkor a CN mezőben az álnév szerepel, és az álneves Tanúsítvány jelzése pedig a “Title” mezőben történik.
SN (Surname)		*Aláíró vezetéknevét tartalmazza
2.5.4.5 (SerialNumber)		* ! Kitöltése csak Üzleti Tanúsítvány esetén illetve Fokozott Személyi Tanúsítvány esetén kötelező. Üzleti Tanúsítvány esetén a Szervezet adószámát, Fokozott Személyi Tanúsítvány esetén Aláíró személyazonosító okmányszámát tartalmazza. Ellenőrzése a benyújtott dokumentumok (jellemzően cégkivonat illetve személyazonosító okmány) alapján történik, minden esetben közhiteles adatbázissal történő adategyeztetéssel. Szolgáltató a mezőt egyedi megkülönböztetés céljából használja. Azon tanúsítványtípusok esetén, amelyek kötelezően nem tartalmazzák az adószámot, illetve személyazonosító okmány számát, megkülönböztetés céljából szolgáltató egyedi azonosítót generál.
T (Title)		(Titulus) Az Igénylő által a Tanúsítványigénylő űrlapon megadott információ, jellemzően Üzleti Tanúsítvány esetén kerül kitöltésre, és az Aláíró Szervezeten belüli pozícióját tartalmazza. Ellenőrzése a benyújtott dokumentum (Szervezet által kiadott igazolás) alapján történik. Magánszemély esetén ezen mezőbe az igénylésben megadott információ kerül, ellenőrzés nélkül. Ha Aláíró álnévvel szerepel, akkor ezen mezőnek tartalmaznia kell az erre vonatkozó utalást.
STREET		*! Kitöltése csak Üzleti Tanúsítvány esetén illetve Fokozott Személyi Tanúsítvány esetén kötelező. Üzleti Tanúsítvány esetén a Szervezet székhelyének utca nevét. Fokozott Személyi Tanúsítvány esetén Aláíró állandó lakhelyének utcanevét tartalmazza. Ellenőrzése a benyújtott dokumentumok (jellemzően cégkivonat illetve személyazonosító okmány) alapján történik, minden esetben közhiteles adatbázissal történő adategyeztetéssel.
Locality		* Személyi Tanúsítvány esetén Aláíró állandó lakhelyének helységnevét, Üzleti Tanúsítvány esetén a Szervezet székhelyének helységnevét tartalmazza. Ellenőrzése a fentiek szerint.
Postal Code		* ! Kitöltése csak Üzleti Tanúsítvány esetén illetve Fokozott Személyi Tanúsítvány esetén kötelező.

			Üzleti Tanúsítvány esetén a Szervezet székhelyének irányítószámát, Fokozott Személyi Tanúsítvány esetén Aláíró állandó lakhelyének irányítószámát tartalmazza. Ellenőrzése a fentiek szerint.
OU (Organizational Unit)			Az Igénylő által a Tanúsítványigénylő űrlapon megadott információ, jellemzően Üzleti Tanúsítvány esetén kerül kitöltésre, és az Aláíró Szervezeten (pl. cégen) belüli részlegét vagy szervezeti egységét tartalmazza. Ellenőrzése a benyújtott dokumentum (Szervezet által kiadott igazolás) alapján történik. Személyi Tanúsítvány esetén nem kerül kitöltésre.
O (Organization)			* ! Kitöltése csak Üzleti Tanúsítvány esetén kötelező. Személyi Tanúsítvány esetén nem kerül kitöltésre. Annak a Szervezetnek a nevét tartalmazza, amelyikhez az Aláíró tartozik. A név formátuma: gazdasági társaság esetén a cégbejegyzésben szereplő rövid név, , nem gazdasági társaság esetén a Szervezet hivatalos okirata szerint (pl. alapító okirat). Ellenőrzése a benyújtott dokumentumok (pl. cégkivonat) alapján történik, minden esetben közhiteles adatbázissal történő adategyeztetéssel.
C (Country)		HU	
Nyilvános kulcs (SubjectPublicKeyInfo)			Ez a mező tartalmazza az Aláíró nyilvános kulcsát (legalább 1024 bit), valamint az aláíró algoritmus megjelölését (RSA)
Tulajdonos kulcsazonosítója (Subject key ID)	non critical		Kibocsátó által generált adat, Aláíró (Tulajdonos) kulcs azonosítója
Hitelesítési Rend (Certificate Policies)	non critical		Itt kerül megadásra a Hitelesítési Rend OID-je, a Szolgáltatási Szabályzat elérési helye, és a vonatkozó szöveges információk a névelemek ékezet nélkül megjelenítésével kapcsolatban.
Tulajdonos alternatív neve (SubjectAltName)	non critical	felhasznalonev@domain.hu	(RFC822name) * Az az e-mail cím, amelyet az igénylő a Tanúsítvány-igénylésben megadott, az Aláíró részére a szolgáltatáshoz kapcsolódó értesítőket (pl. Tanúsítvány kibocsátás, megújítás) erre a címre küldi a Szolgáltató.
Kibővített kulcshasználat (ExtKeyUsage)	non critical		Secure Email, clientAuth,
CA kulcsazonosítója (Authority key ID)	non critical		A Szolgáltató által generált adat, a Kibocsátó egység kulcsának ellenőrzésére szolgál

CRL elérési helyei (CRL distribution point	non critical		Itt azokat a helyeket (URL) jelöli meg a Szolgáltató, ahol a Visszavont Tanúsítványok Listája (CRL) elérhető http és ldap protokollon
Kulcshasználat (KeyUsage)	critical	digitalSignature nonRepudiation	A kulcshasználat jelzésére szolgál.
Alapvető típusmegkötések (Basic constrains)	critical		Tulajdonos típusa=Végfelhasználó
Ujjlenyomat-algoritmus		sha1	
Ujjlenyomat			Kibocsátó által generált adat

7.1.1 Verzió szám(ok)

Lásd a 7.1, valamint a szolgáltatási szabályzat 7.1.1 pontját.

7.1.2 Tanúsítvány kiterjesztések

A Szolgáltató által kiadott Hitelesítési Rendben meghatározott nem-minősített tanúsítványok **kiterjesztései** a következők:

Mezőnév	Érték vagy szabály	Kritikus
Hitelesítési Rend Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.6 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=Magyar Telekom Notice Number=1 Notice Text=A tanusitvany ertelmezesehez es elfogadasahoz a Magyar Telekom Fokozott biztonsagu e-Szigno hitelesites szolgaltatas szabalyzatai szerint kell eljarni (Fokozott e-Szigno ASZF, Fokozott e-Szigno HSZSZ, Fokozott Szervezeti Tanusitvany Hitelesitesi Rend), amelyek a kovetkezo web-oldalon erhetok el: http:// www..t-systems.hu/szolgaltatas_feltetelei [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS	Nem

	Qualifier: http:// www.t-systems.hu/szolgaltatas_feltetelei	
Alapvető megkötések Basic Constraints	Tulajdonos típusa=Végfelhasználó	Igen
Kulcshasználat Key Usage	NonRepudiation , digitalSignature	Igen
Kibővített kulcshasználat Extended Key Usage	Client Authentication, Secure Email	Nem
CRL szétosztási pont CRL Distribution Points	[1] CRL elérési helye URL=http://eszigno.t-systems.magyartelekom.hu/download_crl?issuer=Magyar%20Telekom%20Fokozott%20CA [2] CRL elérési helye URL=ldap://trustcenter-fca.magyartelekom.hu:389/cn=Magyar%20Telekom%20Fokozott%20CA,c=HU?certificateRevocationList?base?objectClass=certificationAuthority	Nem

Lásd a 7.1, valamint a szolgáltatási szabályzat 7.1.2 pontját.

7.1.3 Algoritmus objektumazonosítók

Lásd a 7.1, valamint a szolgáltatási szabályzat 7.1.3 pontját.

7.1.4 Elnevezési formák

Szolgáltató a tanúsítvány kibocsátó azonosító és az aláíró-azonosító esetében az egyedi X.500 név formátumot alkalmazza. Lásd a 7.1 fejezetet.

7.1.5 Elnevezésre vonatkozó korlátozások

Szolgáltató ilyen korlátozást nem alkalmaz.

7.1.6 Tanúsítványfajta objektumazonosító

Lásd a 7.1, valamint a szolgáltatási szabályzat 7.1.6 pontját.

7.1.7 A „tanúsítványfajta korlátozás" kiterjesztés használata

Szolgáltató ezt a kiterjesztést nem használja.

7.1.8 Szabályzat minősítő szintaxis és szemantika

Lásd a 7.1, valamint a szolgáltatási szabályzat 7.1.8 pontját.

7.1.9 A kritikus tanúsítványfajta kiterjesztés feldolgozása

Lásd a 7.1, valamint a szolgáltatási szabályzat 7.1.9 pontját.

7.2 Tanúsítvány visszavonási lista profil

A hitelesítő-szolgáltató által kibocsátott tanúsítvány visszavonási listák megfelelnek a [7] ajánlásának.

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

Szolgáltató által kibocsátott visszavonási listák alap mezői a következők:

Mezőnév	Érték vagy szabály
Verzió *Version*	A tanúsítvány visszavonási lista a [4] ajánlás 2. verziójának felel meg {ld. 7.2.1}.
Algoritmus azonosító *Signature Algorithm Identifier*	Ez a szám *Szolgáltató* visszavonási listát hitelesítő elektronikus aláírásának algoritmus azonosítója: SHA-1 RSA (OID=1.2.840.113549.1.1.5).

Aláírás *Signature*	*Szolgáltató* visszavonási listát hitelesítő elektronikus aláírása a [8] 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. UTC szerinti érték a [8] szerinti kódolással.
Következő kibocsátás *Next Update*	A következő visszavonási lista kibocsátásának ideje {ld. Szolg. szabályzat **4.4.9**}. UTC szerinti érték a [8] szerinti kódolással.
Visszavont tanúsítványok *Revoked Certificates*	A visszavont tanúsítványok listája a tanúsítvány sorozatszámával és a visszavonás idejével.

7.2.1 Verzió szám(ok)

Lásd a 7.2 fejezetet, valamint a szolgáltatási szabályzat 7.2.1 pontját.

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

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

Mezőnév	Érték vagy szabály	Kritikus
Visszavonás oka *Reason Code*	.....[14]	Nem
Érvénytelenség ideje *Invalidity Date*	.....[15]	Nem
Útmutató *Hold Instruction*	.....[16]	Nem

Szolgáltató a kiterjesztéseket nem köteles kitölteni.
Szolgáltató által kitöltött visszavonási lista kiterjesztések a következők:

Mezőnév	Érték vagy szabály	Kritikus
CRL sorozatszám *CRL number*	.....[17]	Nem

[14] Ebbe a mezőbe a visszavonás oka kerül.
[15] Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerül.
[16] Ebbe a mezőbe a felfüggesztett tanúsítvány kezelése kerül.
[17] Ebbe a mezőbe a visszavonási listák egyesével növekvő sorozatszámai kerülnek.

Lásd a 7.2 fejezetet, valamint a szolgáltatási szabályzat 7.2.2 pontját.

8. Leírás adminisztráció

A hitelesítés-szolgáltató rendelkezik egy olyan szolgáltatási szabályzattal, mely a jelen dokumentumban leírt valamennyi állításra tartalmazza a megvalósítás gyakorlatát és eljárását. A hitelesítés-szolgáltató szolgáltatási szabályzata meghatározza a hitelesítés-szolgáltató szolgáltatásait támogató valamennyi külső szervezetre vonatkozó kötelezettségeket is, beleértve az alkalmazandó szabályzatokat is.

8.1 Leírás változtatási eljárások

A hitelesítés-szolgáltató egy felülvizsgálati folyamattal gondozza jelen Hitelesítési Rendet és a hozzá tartozó szolgáltatási szabályzatot.

A hitelesítés-szolgáltató időben értesítést tesz közzé a jelen Hitelesítési Rendben, illetve az ehhez tartozó szolgáltatási szabályzatában tervezett változtatásokról, majd a (8.3 fejezet szerinti történő) jóváhagyást követően az átdolgozott Hitelesítési Rendet (vagy szolgáltatási szabályzatot) - a 8.2 fejezetben előírtak szerint - haladéktalanul hozzáférhetővé teszi.

8.2 Közzétételi és tájékoztatási elvek

A hitelesítés-szolgáltató a szolgáltatási szabályzatát a szolgáltatási tevékenység megkezdésével nyilvánosságra hozza, és azt az ügyfélforgalom számára nyitva álló helyiségben, valamint az interneten elérhetővé teszi.

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

8.3 Hitelesítési rend jóváhagyási eljárások

Jelen hitelesítési rendjére vonatkozóan:

- jelen hitelesítési rend tartalmilag megfelel a hitelesítési renddel szemben támasztott minimális követelményeknek,
- jelen hitelesítési rend formailag megfelel a [8] szabványnak,
- a hitelesítés-szolgáltató jóváhagyás előtt megvizsgálja a hitelesítési rend (fenti két pontban meghatározott) követelményeknek való megfelelőségét,
- a hitelesítési rend jóváhagyására a hitelesítés-szolgáltató részéről legalább középszintű vezető szükséges, elrendelése felsővezetői utasítással történik.

- a Hitelesítési Rend ezt követően benyújtásra kerül a Felügyelet részére, amely ezt nyilvántartásba veszi. A szabályzat megfelelőségét a hitelesítés-szolgáltatóra vonatkozólag, a Felügyelet jogosult vizsgálni[18] ellenőrzési eljárása során.

A szolgáltatási szabályzatra vonatkozóan:

- A jelen Hitelesítési Rendhez tartozó szolgáltatási szabályzat tartalmilag és formailag is megfelel e Hitelesítési Rendnek[19].
- A hitelesítés-szolgáltató jóváhagyás előtt megvizsgálja a szolgáltatási szabályzatot a Hitelesítési Rendnek való megfelelőség szempontjából.
- A szolgáltatási szabályzat jóváhagyására a hitelesítés-szolgáltató részéről legalább középszintű vezető szükséges, elrendelése felsővezetői utasítással történik
- A szolgáltatási szabályzat ezt követően benyújtásra kerül a Felügyelet részére, amely ezt nyilvántartásba veszi. A szabályzat megfelelőségét a hitelesítés-szolgáltatóra vonatkozólag, a Felügyelet jogosult vizsgálni[20] ellenőrzési eljárása során.

[18] értékeli: nyilvántartásba veszi vagy módosíttatja.
[19] A tartalmi és formai megfelelés azt jelenti, hogy a hitelesítési rend „mit valósít meg a hitelesítés-szolgáltató" típusú állításait a szolgáltatási szabályzat „hogyan valósítja meg ezeket" típusú leírásai ellentmondás mentesen és hasonló szerkezeti felépítéssel részletezik.
[20] értékeli: nyilvántartásba veszi vagy módosíttatja.

9. Kötelezettségek, egyéb üzleti és jogi kérdések

9.1.1 A hitelesítés-szolgáltató nem minősített szolgáltatásaival kapcsolatos általános kötelezettségei

A hitelesítés-szolgáltató (a hitelesítő szervezet, a regisztrációs szervezet(ek) és a címtár együttes tevékenységével) az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat biztosítja: elektronikus aláírás hitelesítés szolgáltatás (a továbbiakban: hitelesítés szolgáltatás), ezen belül:

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

A hitelesítés-szolgáltató gondoskodik a hitelesítés-szolgáltatóra vonatkozó valamennyi, a 3.-8. fejezetekben részletezett állítás teljesüléséről, amennyiben azok az adott tanúsítványfajtára alkalmazhatóak. A hitelesítés-szolgáltató szolgáltatásait hozzáférhetővé teszi minden olyan igénylő számára, akinek tevékenysége kinyilvánított működési területére esik.

A hitelesítés-szolgáltató jogi személy.

A hitelesítés-szolgáltató megfelelően dokumentált megállapodásokkal és szerződéses kapcsolatokkal rendelkezik azon esetekre, amikor a szolgáltatások nyújtása alvállalkozókat, illetve más, harmadik felekkel kötött megegyezéseket érint. A hitelesítés-szolgáltató olyan szabályzatokkal rendelkezik, mely jelen Hitelesítési Rend dokumentumban azonosított valamennyi követelmény kielégítésére szolgáló gyakorlatra és eljárásra vonatkozik.

A hitelesítés-szolgáltató szabályzatai meghatározzák a hitelesítés-szolgáltató szolgáltatásait támogató valamennyi külső szervezetre vonatkozó kötelezettségeket, beleértve az alkalmazandó szabályzatokat és gyakorlatokat is.

A hitelesítés-szolgáltató valamennyi szolgáltatását szabályzataival összhangban nyújtja.

A szabályzatokat a hitelesítés-szolgáltató felsőszintű irányító testülete hagyja jóvá. A szabályzatok megfelelő megvalósításáért a hitelesítés-szolgáltató felső vezetősége felel. A hitelesítés-szolgáltató a szolgáltatási szabályzatát a szolgáltatási tevékenység megkezdésével nyilvánosságra hozza, és azt az ügyfélforgalom számára nyitva álló helyiségben, valamint az interneten elérhetővé teszi.

A hitelesítés-szolgáltató rendszeresen felülvizsgálja szabályzatait, az újra érvényesített szabályzat tartalmazza a szükséges módosításokat. A hitelesítés-szolgáltató időben értesítést tesz közzé a szolgáltatási szabályzatában tervezett változtatásokról és a fenti jóváhagyást követően az átdolgozott szolgáltatási szabályzatát haladéktalanul hozzáférhetővé teszi.

Ha a hitelesítés-szolgáltató ellen felszámolási vagy végelszámolási eljárás indult, haladéktalanul köteles tájékoztatni a Nemzeti Hírközlési Hatóságot (továbbiakban: Felügyelet) e tényről, megnevezve az eljárást lefolytató szervezetet.

9.1.2 A hitelesítő szervezet kötelezettségei

A hitelesítő szervezet biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatást:
elektronikus aláírás hitelesítés szolgáltatáson belül: tanúsítvány előállítás és kibocsátás.

A hitelesítő szervezet közreműködik (a visszavonási listák aláírásával) az alábbi elektronikus aláírással kapcsolatos szolgáltatás biztosításában:
visszavonási állapot közzététele.

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

- az Aláíró által levél formájában vagy az interneten keresztül elküldött elektronikus tanúsítvány-igénylést az operátor rögzíti;
- összeveti az iratok és az elektronikus tanúsítvány-igénylés tartalmát azonosság szempontjából, ellenőrzi a benyújtott dokumentumok érvényességét, meglétét, az adatok azonosságát, érvényességét (szükség esetén hiánypótlást kér az Aláírótól);
- a nem-minősített tanúsítvány aláírására használt magánkulcsát a nem-minősített tanúsítványok, valamint a visszavonási listák aláírására használja fel;
- csak olyan nem-minősített tanúsítványokat állít elő, amelyek megfelelnek a szolgáltatási szabályzatban meghatározott, támogatott tanúsítványfajtáknak;
- gondoskodik arról, hogy a tanúsítványban foglalt „megkülönböztetett név" egyedi legyen a hitelesítés-szolgáltató szolgáltatási körén belül;
- gondoskodik arról, hogy a hitelesítés-szolgáltató teljes szolgáltatási körén belül kibocsátott tanúsítványokhoz tartozó kulcsok mindvégig egyediek maradjanak.

Sikeres regisztráció esetén az LRA operátor jóváhagyja az igénylést, sikertelen regisztráció esetén értesítő e-mailt küld az Aláíró által megadott címre.

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

- ellenőrzi a regisztrációs szervezettől érkező visszavonási lista aláírási kérelmet, s ebben az aláírandó tanúsítvány visszavonási lista sértetlenségét és hitelességét;
- a szolgáltatási szabályzatban meghatározott mértékben, de minimum 99,5%-os havi rendelkezésre állással biztosítja a felfüggesztési/visszavonási nyilvántartások elérhetőségét, a kibocsátott tanúsítványokat tartalmazó nyilvántartást (tanúsítványtár), a tanúsítvány igénylést, befogadást és feldolgozást illetve a tanúsítvány kibocsátást havi 90%-os rendelkezésre állással biztosítja minden érdekelt fél számára; ezek során az egyes leállások ideje nem haladhatják meg a 3 órát.
- feldolgozza a regisztrációs szervezettől érkező hiteles és sértetlen visszavonási lista aláírási kérelmet, melynek során aláírja a tanúsítvány visszavonási listát;
- rendszeresen új tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, naponta egyszer, a szolgáltatási szabályzat 4.4.9 alfejezetében meghatározott frissítési időponthoz igazodóan, mely tartalmazza a következő lista tervezett kibocsátási idejét is;

- rendkívüli esetben[21] új tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, mely tartalmazza a következő lista tervezett kibocsátási idejét is;
- az általa üzemeltetett gyökérhitelesítő egységgel (azaz CA-val), havonta egyszer új tanúsítvány visszavonási listát készít;
- eljuttatja a címtárba a gyökérhitelesítő egység által előállított tanúsítvány visszavonási listát, biztosítva ennek hitelességét és sértetlenségét;
- megválaszolja a regisztrációs szervezettől kapott visszavonási lista aláírási kérelmet, elküldve az aláírt tanúsítvány visszavonási listát, biztosítva a válaszüzenet sértetlenségét és hitelességét.

9.1.3 A regisztrációs szervezet kötelezettségei -

A regisztrációs szervezet biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:
- regisztráció,
- visszavonás kezelés.

A regisztrációs szervezet egyúttal közreműködik az alábbi elektronikus aláírással kapcsolatos szolgáltatások biztosításában:
- tanúsítvány előállítás,
- kibocsátás,
- visszavonás.

A regisztrációs szervezet a regisztráció szolgáltatás keretén belül:

- gondoskodik a tanúsítványt igénylő megfelelő azonosításáról, illetve arról, hogy a tanúsítványt igénylő formanyomtatványok teljesek, pontosak és kellőképpen hitelesek legyenek;
- ellenőrzi a tanúsítványt igénylő aláíró (vagy) előfizető személyazonosságát és azon egyedi jellemzőiket, melyet a nem-minősített tanúsítvány igazol;
- összegyűjti, illetve meghatározza a regisztráció során valamennyi, meghatározott, tanúsítványba kerülő adatot;
- ellenőrzi a tanúsítványt igénylő aláíró által átadott személyazonosító és egyéb igazoló dokumentumok valódiságát, érvényességét, sértetlenségét és hitelességét. A nem minősített tanúsítvány igénylés esetén az adatokat ellenőrzés céljából összeveti a közhiteles nyilvántartások adataival. Összeveti egymással és a valósággal az egyes iratokon szereplő adatokat (így különösen a tanúsítványt személyesen igénylő aláíró fotóját az arcával, aláírását a helyszíni aláírásával).
- írásbeli indoklással visszautasítja a tanúsítvány kiadását, amennyiben a tanúsítványigénylés nem teljes, nem helyes, nem az arra jogosult által történik, vagy egyéb módon nem felel meg az elvárt feltételeknek;
- nyilvántartásba vesz minden, a tanúsítványok kiadásához kapcsolódó valamennyi információt;

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

- megőrzi a nyilvántartásokat a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig;
- bizalmas információként kezeli az előfizető és az aláíró minden adatát, kivéve azokat, amelyeket a 2.2.2 alfejezet tárgyal. A hitelesítés-szolgáltató a birtokába jutott bizalmas információkat a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli, s csak a 2.2.3-2.2.7 alfejezetekben említett esetekben és személyek részére fedi fel őket;
- korlátozás nélkül biztosítja az aláíró számára a rá vonatkozó regisztrációs és egyéb információhoz történő hozzáférést (lásd 2.2.6).

A regisztrációs szervezet a visszavonás kezelés szolgáltatás keretén belül:

- ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét valamint szabályosságát
- a hitelesítési rend 1.4 fejezetében leírt feltételek mellett végrehajtja a hiteles, érvényes és szabályos, tanúsítvány visszavonásra, felfüggesztésre vonatkozó kérelmeket, illetve teljesíti a felfüggesztés megszüntetésére vonatkozó kérelmeket a 4.4.7 fejezetben részletezett feltételek szerint (vagyis a kérelmezett változást átvezeti a tanúsítványtár alapját képező tanúsítvány állapot adatbázisába);
- visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket;
- intézkedik a tanúsítvány visszavonásáról, amennyiben olyan tényről szerez tudomást, ami a tanúsítvány felhasználhatóságának biztonságát fenyegeti (a hitelesítési rend 1.4 fejezetében leírt feltételek figyelembevételével);
- a hitelesítési rend 1.4 fejezetében leírt feltételek – amelyek a felfüggesztésre / visszavonásra vonatkoznak - figyelembevételével, biztosítja a visszavonás kezelési szolgáltatást minden érdekelt fél számára, egyúttal megadja az előre tervezett és rendkívüli leállások leghosszabb időtartamát.

A regisztrációs szervezet a tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:

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

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

- fogadja a hitelesítő szervezettől kapott új tanúsítványokat és a szabályzó szervezettől kapott szabályzatokat, valamint ellenőrzi ezek hitelességét és sértetlenségét;

- elküldi a címtárnak az új tanúsítványokat, biztosítva az ezeket tartalmazó üzenet hitelességét és sértetlenségét.

9.1.4 Az aláíró és az előfizető kötelezettségei

A nem minősített hitelesítés-szolgáltatás bizalmi jellege miatt, a szolgáltató elvárja az előfizető és az aláíró közötti fokozottabb együttműködést. Amennyiben mindkét személy (aláíró és előfizető) is jogosult a Szolgáltatónál eljárni, akkor a szolgáltatást érintő cselekményeikről egymást kötelesek tájékoztatni. A tájékoztatás elmaradásából eredő károkért a Szolgáltató nem felelős.

9.1.4.1 Az aláíró kötelezettségei

A hitelesítés-szolgáltató az aláírókat megállapodáson keresztül az alábbiakra kötelezi:

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

9.1.4.2 Az előfizető kötelezettségei

A hitelesítés-szolgáltató az előfizetőt megállapodáson keresztül az alábbiakra kötelezi:

- pontos és teljes információt nyújtson be a regisztrációs szervezethez jelen Hitelesítési Rend követelményeinek megfelelően, különös tekintettel a regisztrációra;
- teljes gonddal járjon el, hogy megelőzze az aláíró magánkulcsának illetéktelen felhasználását;
- késedelem nélkül értesítse a hitelesítés-szolgáltatót, amennyiben az alábbiak közül bármelyik bekövetkezik a tanúsítványban megadott érvényességi időszak vége előtt:
- az aláíró magánkulcsa elveszett, azt ellopták, esetlegesen kompromittálták,
- az aláíró elvesztette ellenőrzését magánkulcsa felett, aktivizálási adatai (például PIN kód) kompromittálódása, illetve más okokból kifolyólag,
- az előfizető tudomására jutott, hogy a tanúsítvány tartalmában vagy egyéb regisztrációs adatokban pontatlanság van, illetve változás következett be;
- a hitelesítés–szolgáltatás díjait a hatályos szabályzatok és Szolgáltatási Szerződés szerint fizesse meg.

9.1.5 Az érintett félre vonatkozó ajánlások

Az érintett felek számára rendelkezésre bocsátott kikötések és feltételek tartalmaznak egy megjegyzést, miszerint, ha ésszerű módon egy tanúsítványra kívánnak hagyatkozni, az alábbiakat ajánlott tenniük:

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

9.1.6 A címtár kötelezettségei

A címtár a hitelesítő szervezet részeként biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:

- tanúsítvány kibocsátás,
- visszavonási állapot közzététele.

A címtár a kibocsátás szolgáltatás keretén belül:

- közzé teszi a végfelhasználói tanúsítványokat;
- biztosítja a végfelhasználói tanúsítványokat érintő információk folyamatos[22] elérhetőségét.

A címtár a visszavonási állapot közzététele szolgáltatás keretén belül;

- közzé teszi a hiteles és sértetlen új tanúsítvány visszavonási listát;
- biztosítja a legfrissebb tanúsítvány visszavonási lista folyamatos[23] elérhetőségét.

9.2 Felelősség

9.2.1 A hitelesítés-szolgáltató általános felelőssége

- A hitelesítés-szolgáltató felelősséget vállal az általa támogatott Hitelesítési Rend dokumentumban leírt eljárásoknak való megfelelőségért, még abban az esetben is, amikor a hitelesítés-szolgáltató egyes tevékenységeit alvállalkozók végzik[24].
- A hitelesítés-szolgáltató a vele szerződéses jogviszonyban álló felekkel (ilyen az aláíró és az előfizető) szemben a Magyar Köztársaság Polgári Törvénykönyve (Ptk.) szerződésszegésért való felelősség szabályai szerint felelős.
- A hitelesítés-szolgáltató a vele szerződéses jogviszonyban nem álló harmadik féllel (ilyen az érintett fél) szemben a Ptk. szerződésen kívüli károkozásról szóló szabályai (Ptk. 339. §) szerint felelős.

[22] A hét 7 napján, a nap 24 órájában.
[23] A hét 7 napján, a nap 24 órájában.
[24] A hitelesítés-szolgáltató általánosan felelős a hitelesítő szervezet, a regisztrációs szervezet, valamint a címtár kötelezettségeiért, tevékenységeiért.

- A hitelesítés-szolgáltató nem felelős az olyan kárért, mely abból adódott, hogy az érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok szerint járt el, illetve nem úgy járt el, ahogyan az adott helyzetben általában elvárható.
- A hitelesítés-szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helyt állni.
- A hitelesítés-szolgáltató pénzügyi felelősségének korlátozását az ÁSZF 10. fejezete tartalmazza.

9.2.2 A hitelesítő szervezet felelőssége

A hitelesítő szervezet felelős az:
- az általa kibocsátott tanúsítványok hitelességéért,
- a generált kulcspárok megfelelőségéért, a magánkulcs- nyilvános kulcs és tanúsítvány összetartozásáért,
- az aláírás-létrehozó eszközaktivizáló kódjának, és az eszközre töltött kulcsok összetartozásáért,
- általában kötelezettségei betartásáért.

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.

9.2.3 A regisztrációs szervezet felelőssége

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

9.2.4 Az aláíró felelőssége

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

9.2.5 Az előfizető felelőssége

Az előfizető felelős:

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

9.2.6 Az érintett fél felelőssége

Az érintett fél felelős:

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

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

9.3 Pénzügyi felelősség

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

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

9.3.1 A hitelesítés-szolgáltatóval szembeni kártérítés

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

9.3.2 Adminisztratív folyamatok

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

9.4 Értelmezés és érvényesítés

9.4.1 Irányadó jog

A hitelesítés-szolgáltató tevékenységét a következő főbb jogszabályok illetve irányadó dokumentumok szabályozzák[25]:

- 2001. évi XXXV. törvény az elektronikus aláírásról[26].

[25] A főbb jogszabályok szövege elérhető a Hatóság honlapján keresztül, a www.nhh.hu címen.
[26] A törvényt kiegészítő, alább felsorolt alacsonyabb szintű jogszabályok a 2008.06.01.-i állapotot tükrözik.

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.
- 45./2005. (III.11.) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat-és hatásköréről, valamint eljárásainak részletes szabályairól.
- 4/2006. (IV.19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról
- 3/2005. (III.18.) IHM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- 9/2005. (VII.21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
- 7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről.

9.4.2 Érvénytelenség, fennmaradás, megszűnés, értesítések

Érvénytelenség

Amennyiben jelen Hitelesítési Rend valamely pontja érvénytelen lenne, jelen dokumentum egészének és más pontjainak érvényességét nem érinti.

Fennmaradás

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

Megszűnés

Jelen Hitelesítési Rend a Közösség (lásd 1.3) valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A Hitelesítési Rend egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében. A Hitelesítési Rend csak írott és hitelesített formában módosítható, a Felügyelet által vezetett Hitelesítési Rend nyilvántartásban való átvezetés mellett.

Értesítések

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

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

9.4.3 Vitás kérdések megoldására vonatkozó eljárások

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

9.5 Díjak

Szolgáltató aktuális díjai az e-Szignó honlapján találhatóak, mely elérhető a www.t-systems.hu/arak oldalról. A díjak a Tanúsítvány érvényességének időtartama alatt érvényesek, a Tanúsítvány kibocsátásának idején érvényes árlista szerint.