1124. Budapest, Stromfeld Aurél út 9.
Tel.: +361 567 8912
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

# Szolgáltatási Szabályzat

Fokozott biztonságú elektronikus aláíráshoz kapcsolódó
hitelesítés-szolgáltatásokhoz és nem-minősített időbélyegzés szolgáltatáshoz

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.24206.4.22.1.4
Verziószám: 1.4
Jóváhagyta: Németh Viktor Péter
Jóváhagyás dátuma: 2015.01.28.
Hatályba lépés dátuma: 2015.03.01.

Digitálisan aláírta: Németh Viktor Péter
Dátum: 2015.01.29 14:16:47 +01'00'

**Változáskövetés**

| Verzió | A változás leírása | Hatálybalépés | Készítette |
|---|---|---|---|
| 1.0 | Első változat | 2011.05.10. | Németh Ágnes Krisztina<br>Németh Viktor Péter |
| 1.1 | Módosítás a NMHH észrevételeinek megfelelően | 2011.07.10. | Németh Ágnes Krisztina<br>Németh Viktor Péter |
| 1.2 | Technikai paraméter változások az NMHH észrevételeinek megfelelően | 2011.07.10. | Németh Ágnes Krisztina<br>Németh Viktor Péter |
| 1.3 | Módosítások a 2013. évi NMHH felügyeleti eljárás határozata alapján.<br><br>Felfüggesztési ügyelet (korábban: Visszavonási ügyelet) megnevezése és telefonszáma módosult.<br><br>A tanúsítvány profilok kiegészítésre kerültek. | 2013.10.10. | Németh Ágnes Krisztina<br>Németh Viktor Péter |
| 1.4 | Aktualizálás | 2015.03.01. | Németh Ágnes Krisztina<br>Németh Viktor Péter |

**Tartalomjegyzék**

# 1. Általános információ

Jelen dokumentum a Digitoll Informatikai és Szolgáltató Kft (továbbiakban: Szolgáltató) fokozott biztonságú (nem minősített) hitelesítés és időbélyegzés szolgáltatására vonatkozó Szolgáltatási Szabályzata (továbbiakban: Szabályzat). E dokumentum a Szolgáltató szolgáltatásaira vonatkozó eljárási és működési szabályokat tartalmazza, és ajánlásokat fogalmaz meg a szolgáltatások segítségével létrehozott elektronikus aláírások és időbélyegzők ellenőrzésében Érintett felek számára.

A Szolgáltató szolgáltatásait a vele szerződéses viszonyban álló ügyfelek részére (továbbiakban: Előfizető) biztosítja.

A Szolgáltató felügyeleti szerve a Nemzeti Média- és Hírközlési Hatóság (továbbiakban: NMHH).

A Szolgáltató fokozott biztonságú - nem minősített - szolgáltatóként való nyilvántartásba vétele 2011.08.05.-én megtörtént.

Jelen Szabályzat az IETF RFC 3647 ajánlás alapján készült, tartalmában és felépítésében követi annak előírásait.

## 1.1. Szolgáltató adatai

| | |
|---|---|
| Név: | Digitoll Informatikai és Szolgáltató Kft. |
| Cégjegyzék szám: | 01-09-861809 |
| Székhely: | 1124 Budapest, Stromfeld Aurél út 9. |
| Ügyfélszolgálati iroda: | 1124 Budapest, Stromfeld Aurél út 9. |
| Nyitva tarás: | Munkanapokon 8:30 – 16:00 óra között |
| Telefonszám: | (+36-1) 567 8900 |
| Felfüggesztési ügyelet (0-24): | (+36-1) 567 8888 |
| Email cím: | ugyfelszolgalat@digitoll.co.hu<br>digitoll@digitoll.co.hu |
| Internet cím: | http://www.digitoll.co.hu<br>http://ds.digitoll.co.hu |

A Szolgáltató önkéntes akkreditációs rendszer keretében nem lett tanúsítva.

## 1.2. Szolgáltatások

A Szolgáltató az alábbi szolgáltatásokat (továbbiakban: Szolgáltatás) illetve tevékenységeket nyújthatja, illetve végezheti az Előfizetői részére, jelen Szabályzat keretein belül:

- Fokozott biztonságú (nem minősített) elektronikus aláírás hitelesítés szolgáltatás;
- Aláíró adattal és aláíró eszközzel kapcsolatos szolgáltatások, együttes nevén eszköz-szolgáltatás;
- Fokozott biztonságú időbélyegzés szolgáltatás:
  - időbélyeg igénylés feldolgozása,
  - időbélyeg előállítása,
  - időbélyeg kibocsátása.

### *1.2.1. Fokozott biztonságú (nem minősített) elektronikus aláírás hitelesítés szolgáltatás*

Az elektronikus aláírás hitelesítés szolgáltatás keretében az alábbi szolgáltatásokat tartalmazza (a megnevezett szolgáltatások együtt értelmezendőek):

- Regisztráció, személyazonosság megállapítása,
- Tanúsítvány igénylés feldolgozása,
- Tanúsítvány kibocsátás,
- Tanúsítvány-menedzselés:
  - Tanúsítvány kibocsátás,
  - Tanúsítvány felfüggesztés és visszavonás kezelés,
  - Tanúsítvány megújítás,
  - Tanúsítvány közzététel.

#### *1.2.1.1. Tanúsítványfajták*

A Szolgáltató a fokozott biztonságú (nem-minősített) hitelesítés szolgáltatás keretében többféle tanúsítványfajtát bocsát ki, mely különbözhet felhasználási körben, alkalmazásban és felelősségvállalásban is.

A tanúsítvány fajtája jelölve van a kibocsájtott tanúsítványon és a Szolgáltatási szerződésben.

A tanúsítvány profilok megtalálhatóak a jelen szabályzat és a kapcsolódó Hitelesítési Rendjének idevonatkozó pontjában.

A fokozott biztonságú (nem minősített) tanúsítványok igen erős biztosítékokkal szolgálnak a bennük megnevezett személyek kilétét illetően, mivel ez esetben az igénylő személyes megjelenése a regisztrációs egységnél követelmény. A Szolgáltató a fokozott biztonságú (nem minősített) tanúsítványokat fokozott biztonságú elektronikus aláíráshoz valamint ezen alapuló Aláíró azonosításhoz bocsátja ki, magasabb értékű, illetve hosszú időre biztonságot követelő szerződések, kereskedelmi tranzakciók, alkalmazások (elektronikus levelezés, intranet, extranet, on-line vásárlás stb.) esetében.

A pénzügyi felelősségvállalás mértékét a Szolgáltatási szerződés tartalmazza.

### *1.2.2. Aláírás-létrehozó eszközszolgáltatás*

A Szolgáltató a fokozott biztonságú (nem-minősített) hitelesítés szolgáltatása keretében alapvetően a következő eszköz – szolgáltatásokat nyújtja (melyeket az előző pontban megnevezett szolgáltatásoktól külön és avval együtt is igénybe lehet venni):

- Kulcsgenerálás, és elhelyezés az aláírás-létrehozó eszközön: a Szolgáltató generál egy aláírás-létrehozó adatot, melyet a kulcspárhoz tartozó tanúsítvánnyal együtt elhelyez az eszközön. Az eszköz lehet chipkártya, vagy USB token (továbbiakban: Eszköz).
- Kulcsmenedzsment: az aláírás-létrehozó adatok védelmének megoldása tikosítással és többlépcsős védelmi rendszerrel.
- Tanúsítvány elhelyezése az aláírás-létrehozó eszközön: A Szolgáltató az Előfizető és/vagy Aláíró aláírás-létrehozó adatához bocsát ki tanúsítványt, melyet elhelyez az Előfizető és/vagy Aláíró aláírás-létrehozó eszközén.

Az eszköz-szolgáltatás során a Szolgáltató:

- az igénylés szerint előkészíti az Eszközt az Előfizető és/vagy Aláíró részére, melynek során elhelyezi rajta az elektronikus aláírás alkalmazást és a tanúsítványt, beállítja a biztonságos működéshez szükséges kulcsokat, és előállítja az aktiváláshoz szükséges adatokat (továbbiakban: PIN kód), melyet biztonságosan és elzárva tárol.
- az elkészült Eszközt és a biztonságosan tárolt PIN kódot átadja az Előfizetőnek és/vagy Aláírónak.
- az aláírás-létrehozó adat az Előfizető közreműködésével jön léte, a PIN kód megadásával.

# 2. Bevezetés

## 2.1. Áttekintés

### *2.1.1. A Szabályzat célja, használhatósága, leírása*

Jelen Szabályzat célja, hogy a Szolgáltatóval kapcsolatba kerülő felek, a Szolgáltató által nyújtott Szolgáltatásokról, azok működéséről, feltételeiről teljes áttekintést kapjanak, mely elősegíti a Szolgáltató működésének és az általa nyújtott Szolgáltatások gyakorlati hátterének megismerését.

A Szabályzat összefoglalóan tartalmazza mindazon szabályokat, információkat, melyek a Szolgáltató hitelesítés-szolgáltatás keretein belül kibocsátott tanúsítványokkal és egyéb kapcsolódó szolgáltatásokkal kapcsolatosak, és melyeket a Szolgáltatóval kapcsolatba kerülő felhasználóknak és érintett feleknek érdemes tudni. Biztosítja a Szolgáltató működésének átláthatóságát, és lehetővé teszi a felhasználók számára, hogy megállapítsák, hogy a Szolgáltató működése, illetve adott Szolgáltatás mennyiben felel meg elvárásaiknak, igényeiknek. A Szabályzat megismerésével és értelmezésével, a tanúsítvány felhasználói egyértelműen meg kell tudják állapítani a tanúsítvány kezelésének módját, az általa garantált biztonság és garancia mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat.

Az igénybe vehető Szolgáltatásokkal kapcsolatos előírásokat tartalmazhat jelen Szabályzaton kívül, a mindenkori Általános Szerződési Feltételek (továbbiakban: ÁSzF), a Hitelesítési Rend, az Időbélyegzési rend, a Szolgáltatási szerződés (továbbiakban: Szerződés), vagy bármilyen írásos szabályzat illetve megállapodás a Szolgáltató és az igénybevevő között, illetve egyéb, a Szolgáltatótól független dokumentum vagy szabályzat is.

### *2.1.2. A Szabályzat hatálya*

#### *2.1.2.1. Tárgyi hatálya*

A Szabályzat tárgyi hatálya az 1.2. fejezetben ismertetett Szolgáltatások nyújtására és igénybevételére, illetve e Szolgáltatásokkal kapcsolatos tárgyi eszközökre terjed ki.

#### *2.1.2.2. Időbeli hatálya*

A Szabályzat időbeli hatálya jelen dokumentum hatályba lépésének dátumától kezdődik és annak módosításáig, vagy visszavonásáig, illetve a Szolgáltatások beszüntetéséig érvényes. Jelen szabályzatot verziószám alapján lehet azonosítani. A verziószám és a hatálybalépés dátuma jelen dokumentum címlapján olvasható. Változtatás esetén új verziószámos dokumentum jön létre.

#### *2.1.2.3. Személyi hatálya*

A Szolgáltató a Szolgáltatásokat a vele előfizetői szerződéses viszonyban álló Előfizetők részére szolgáltatja. A Szabályzat személyi hatálya a Szolgáltató PKI közösségének minden tagjára (jogi vagy nem jogi személyiségekre is), a felhasználó közösségre (Aláíró, Ellenőrző fél) és az Előfizetőre egyaránt kiterjed.

## 2.2. Dokumentum név és azonosító

Jelen Szabályzat hivatalos elnevezése: Digitoll Informatikai és Szolgáltató Kft. Fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatás és nem-minősített időbélyegzés szolgáltatás Szolgáltatási Szabályzata.

Jelen a Szabályzatot az egyedi objektum-azonosító (Object Identifier - OID) azonosítja, ami megfelel az ISO (International Organization for Standardization) és ITU (International Telecommunication Union) szabványoknak és ajánlásoknak. Az OID és a Szabályzat egyéb paraméterei jelen Szabályzat fedőlapján olvashatóak.

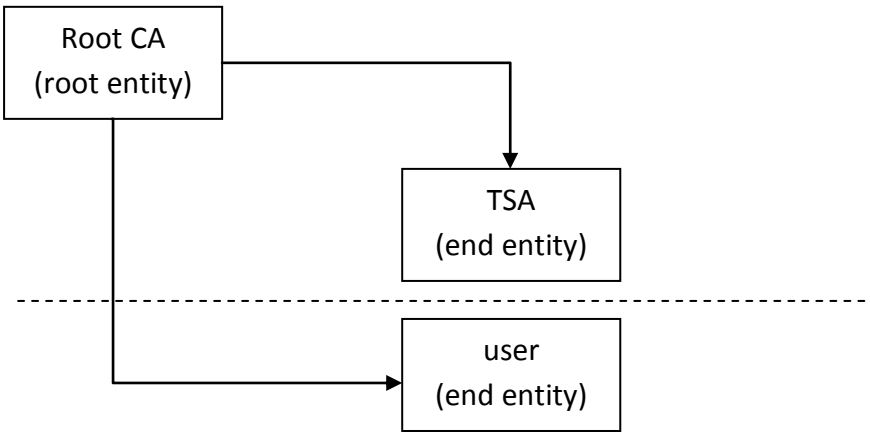
A Szabályzat, és ahhoz elválaszthatatlanul kapcsolódó mindenkori ÁSzF, Hitelesítési Rend és Időbélyegzési Rend elérhető a Szolgáltató ügyfélszolgálati irodájában, vagy elektronikusan a http:/ds.digitoll.co.hu/ internetes címen.

## 2.3. PKI résztvevők

A Szolgáltató Szolgáltatásaihoz tartozó közösség, a Szolgáltatóból, a végfelhasználókból (Előfizetők, Aláírók) és az Érintett felekből áll.

## 2.4. Hitelesítő egység - CA (Certification Authority)

A Szolgáltató, saját egységén belül Hitelesítő egységet működtet, melynek fő feladata a Regisztrációs egységhez benyújtott kérelmek, a Szolgáltató saját szabályozásának és a Magyar jogszabályoknak megfelelően a tanúsítványok - előre definiált profilok alapján - előállítása, kibocsátása, menedzselése (visszavonás, felfüggesztés), azok közzététele. Szintén ez az egység végzi és felügyeli az időbélyegzés szolgáltatást, a kulcsgenerálást, a kulcstároló eszközök menedzselését, és a Szolgáltató szabályzatainak kialakítását, publikálását, valamint a visszavonási listák (CRL) kiadását és publikálását.




A rendszer a gyökérelemből (Root CA), illetve az alátartozó időbélyegzőből (TSA) áll. A gyökérelem bocsátja ki a felhasználói végtanúsítványokat (user), illetve visszavonási adatokat (CRL). A gyökérelem és az időbélyegző a hitelesítés-szolgáltatói oldal, a végfelhasználói tanúsítványok felhasználói oldal részét képezik.

A gyökérelem lenyomata:

- SHA-1:
  E3 : E5 : AE : F8 : 59 : 9A : 07 : AB : 55 : 0A : 19 : 85 :
  31 : CF : BB : 3A : 36 : EA : 95 : FD
- SHA-256:
  76 : 5B : 27 : 1C : 5E : 01 : 9C : 01 : 5B : 7A : D3 : E8 :
  F6 : 10 : 30 : E8 : E5 : 11 : 25 : FF : 28 : 6E : 3D : 68 :
  C1 : 54 : F0 : CF : 81 : AF : AC : 7D

Az időbélyegző lenyomata:

- SHA-1:
  5D : 50 : 67 : 33 : 04 : 26 : 60 : AA : DB : 2E : CD : 96 :
  3F : 81 : 06 : 39 : AC : FB : DA : 9B
- SHA-256:
  AB : DD : 3C : 62 : BB : 84 : 70 : D2 : 22 : 81 : 12 : 1C :
  A1 : A8 : 5D : A5 : A7 : 24 : BB : A8 : B7 : C2 : 6C : CA :
  5A : 00 : F0 : 02 : 27 : 92 : 2A : E7

## 2.5. Regisztrációs egységek- RA (Registration Authority)

A Szolgáltató, saját szervezetén belül Regisztrációs egységet működtet, melynek feladata az ügyfélkezelés, mely a kezdeti regisztrációból és tanúsítványokkal kapcsolatos egyéb feladatok elvégzéséből és az ügyfelekkel való kommunikációból áll.

Ezek a feladatok részletezve:

- Regisztrációs tevékenységek, kezdeti regisztráció:
  - Tanúsítványigénylések fogadása, feldolgozása és elbírálása,
  - Az Előfizető és az Aláíró azonosítása (okmányok alapján),
  - Az Előfizető és az Aláíró adatainak ellenőrzése,
  - Szerződéskötés,
  - Adatok átadása a Hitelesítő egységnek.

- Tanúsítványokkal kapcsolatos feladatok:
  - Az aláírás létrehozó adat és az aláírás ellenőrző adat generálásának felügyelete és annak elhelyezése az biztonságos (tanúsított) aláírást-létrehozó eszközön (továbbiakban: ALE),
  - A CA-tól lekért tanúsítvány elhelyezése az ALE-n,
  - A kész tanúsítvány, aláíró-eszközök átadása az Előfizetőnek és/vagy Aláírónak,
  - Az aláírás létrehozó adat aktiválása,
  - Az előfizetői kérelmek, módosítások fogadása, feldolgozása és elbírálása,
  - Tanúsítványokkal kapcsolatos műveletek (felfüggesztés, visszavonás, visszaállítás csere) elvégzése, dokumentálása,
  - Tanúsítvány-állapotszolgáltatáshoz és Időbélyeg szolgáltatáshoz kapcsolódó adminisztrációs tevékenység,
  - Egyéb adminisztráció, dokumentálás,
  - Kapcsolattartás, panaszkezelés.

A Regisztrációs egység regisztrációs tevékenységet végezhet:

- A Szolgáltató ügyfélszolgálati irodájában,

- Külön díjazás ellenében és előre egyeztetett időpontban az ügyfél által megjelölt helyszínen.

A Szolgáltató egyéb szervezetekkel szerződést köthet külső Regisztrációs helyek kialakítására, melyeknek önálló működési szabályzata van, melyet a Szolgáltató elfogad. A külső Regisztrációs egység szabályzatának tartalmilag és felelősségvállalás szempontjából is összhangban kell lennie a Szolgáltató szabályzataival, valamint meg kell felelnie a vonatkozó magyar jogszabályi feltételeknek.

## 2.6. Végfelhasználók

A Szolgáltató által nyújtott Szolgáltatások végfelhasználói a következőek lehetnek:

- Az Előfizető, aki Szerződést köt a Szolgáltatóval, az általa nyújtott szolgáltatásokra. Az Előfizető határozza meg a Szolgáltatásokat igénybe vevő Aláírók körét, és megfizeti az igénybe vett Szolgáltatások díjait. A kibocsátott tanúsítvány és az ahhoz tartozó kulcspár tulajdonosa. Az Előfizető lehet természetes illetve jogi személy, vagy jogi személyiség nélküli szervezet.

- Az Aláíró, aki a kibocsátott tanúsítványhoz tartozó kulcspár teljes jogú, kizárólagos használója. Az aláíró csak természetes személy lehet.

- Aláírás ellenőrző: Az Érintett fél, aki lehet természetes illetve jogi személy, vagy jogi személyiség nélküli szervezet. Nem áll szerződéses viszonyban a Szolgáltatóval, csak befogadja a hitelesített adatokat. A Szolgáltatónál ellenőrizheti a kapott aláírás, tanúsítvány és időbélyeg érvényességét. A Szolgáltatóval elsősorban a Szolgáltató által karbantartott nyilvántartásokon keresztül érintkezik.

## 2.7. Egyéb egységek

Olyan harmadik feleknek, melyek nem előfizetők, vagy nem része a PKI-nak, szintén van hozzáférésük PKI-val kapcsolatos adathoz. A harmadik feleknek hozzáférésüknek kell, hogy legyen a visszavonási információkhoz (CRL), hogy ellenőrizni tudják az aláírást.

## 2.8. Tanúsítvány használat, alkalmazási lehetőségek

A hitelesítés-szolgáltatás és jelen Szabályzat keretében a Szolgáltató által kibocsátott nem minősített tanúsítványok, generált kulcspárok, és az időbélyegzés szolgáltatás keretein belül

kibocsátott időbélyegekre és a további szolgáltatásokra a következő alpontokban leírt alkalmazhatósági szabályok érvényesek. Az esetleges egyéb alkalmazási lehetőségeket illetve korlátokat a Szerződés is tartalmazhatja.

### *2.8.1. Engedélyezett alkalmazási lehetőségek*

A Szolgáltató általa kibocsátott tanúsítványokhoz tartozó magánkulcsok elektronikus aláírás létrehozására, a hozzá tartozó nyilvános kulcsok, a tanúsítvány, a tanúsítvány visszavonási listák (továbbiakban: CRL), az időbélyegek (vagy időpecsét) a létrehozott elektronikus aláírás ellenőrzésére használhatóak fel. Az időbélyegek további feladata, hogy hitelesítsen egy adott dokumentumot vagy állományt abban a pillanatban, amikor az időpecsételés történt.

A Szolgáltató a részére kibocsátott tanúsítvánnyal hitelesíti az általa kibocsátott tanúsítványokat és azzal készíti el az időbélyegeket.

A Szolgáltató által kibocsátott authentikációs tanúsítványok kizárólag hitelesítésre, a titkosító tanúsítványok pedig titkosításra alkalmazhatóak.

A kibocsátott tanúsítványok minden olyan informatikai alkalmazásban használhatóak, amelyek támogatják a PKI technológián alapuló aláírási funkciókat.

További engedélyezett alkalmazási lehetőségeket jelen Szabályzat, a Hitelesítési Rend, a Szerződés, az ÁSzF és a vonatkozó rendeletek tartalmazhatnak.

### *2.8.2. Korlátozott illetve tiltott alkalmazási lehetőségek*

A tanúsítványt csak az arra jogosult használhatja, és olyan céllal, amivel a tanúsítványt létrehozták. Ez a cél rögzítve van a tanúsítványban is és a Szerződésben is.

A Szolgáltató a Szerződésben leírtaknak megfelelően korlátozhatja az általa kibocsátott tanúsítványok felhasználhatóságát területi, pénzügyi és egyéb vonatkozásban. A korlátozások mértékét a Szolgáltató és hatályos jogszabályok határozzák meg.

Az Előfizető az Aláíróra vonatkozó egyéb korlátozásokat is megadhat, melyet az Előfizetői Szerződésben rögzíteni kell.

A kibocsátott tanúsítványok használatára vonatkozó bármely korlátozás megszegése tilos. A Szolgáltató nem vállal felelősséget a kibocsátott tanúsítvány illetve a hozzá kapcsolódó magán és nyilvános kulcs kibocsátási céltól eltérő felhasználásért.

A kibocsátott tanúsítványokat tilos felhasználni más nyilvános kulcsú tanúsítvány aláírására illetve bármely hitelesítés-szolgáltatás nyújtásához.

További korlátozott, illetve tiltott alkalmazási lehetőségeket jelen Szabályzat, a Hitelesítési Rend, a Szerződés, az ÁSzF és a vonatkozó rendeletek tartalmazhatnak.

## 2.9. Szabályzat adminisztráció

### *2.9.1. Szervezeti dokumentum adminisztráció*

Szervezet:

- Név: Digitoll Informatikai és Szolgáltató Kft.
  - Cím: 1124. Budapest, Stromfeld Aurél út 9.
  - Telefon: 06 1 567 8900
  - E-mail: digitoll@digitoll.co.hu
  - Web: www.digitoll.co.hu, ds.digitoll.co.hu

### *2.9.2. Kapcsolattartó személyek*

Általános információ:

- Név: Németh Ágnes
  - Telefon: 06 1 567 8900
  - E-mail: info@digitoll.co.hu

Technikai támogatás

- Név: Németh Viktor
  - Telefon: 06 1 567 8900
  - E-mail: support@digitoll.co.hu

### *2.9.3. Fogyasztóvédelem*

A Szabályzat szerinti Szolgáltatásokkal kapcsolatban illetékes fogyasztóvédelmi hatóság adatait a következő táblázat tartalmazza:

| | |
|---|---|
| Név: | Budapest Főváros Kormányhivatal<br>Fogyasztóvédelmi Felügyelőség |
| Cím: | 1052 Budapest, Városház u. 7. |
| Postai cím: | 1364 Budapest, Pf. 144. |

| | |
|---|---|
| Telefonszám: | (+36-1) 450 2598 |
| Email cím: | fogyved_kmf_budapest@nfh.hu |
| Internet cím: | http://www.nfh.hu |

#### *2.9.4. Felügyeleti szerv*

| | |
|---|---|
| Név: | Nemzeti Média- és Hírközlési Hatóság<br>E-szolgáltatás-felügyeleti Osztály |
| Cím: | 1088 Budapest, Reviczky utca 5. |
| Postacím: | 1433 Budapest, Pf. 198 |
| Telefonszám: | (+36-1) 429 8600 |
| Internet cím: | http://www.nmhh.hu |

## 2.10. Meghatározások és rövidítések

- Meghatározások és fogalmak a 2001. évi XXXV. törvény az elektronikus aláírásról (továbbiakban: EAT) törvény értelmezésében:

**Aláírás-létrehozó adat:** olyan egyedi adat, melyet az aláíró az elektronikus aláírás létrehozásához használ.
**Aláírás-ellenőrző adat:** olyan egyedi adat, melyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.
**Aláírás-létrehozó eszköz (ALE):** olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
**Aláíró:** az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult.
**Álneves Tanúsítvány:** Akkor nevezünk egy tanúsítványt álneves tanúsítványnak, ha a tanúsítványban nem a tanúsítványhoz tartozó felhasználó (aláíró) valódi - személyazonosításra alkalmas igazolványában szereplő - neve szerepel, hanem valamely más szöveg.
**Biztonságos aláírás-létrehozó eszköz (BALE):** az EAT 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.
**Elektronikus aláírás:** elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
**Elektronikus aláírás ellenőrzése:** az elektronikusan aláírt elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával.

**Elektronikus aláírás felhasználása:** elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése.
**Elektronikus aláírás hitelesítés-szolgáltató:** az EAT 6. § (2) bekezdése szerinti tevékenységet végző személy (szervezet).
**Elektronikusan történő aláírás:** elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz.
**Elektronikus aláírási termék:** olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevő, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, valamint elektronikus aláírások, illetőleg időbélyegző készítéséhez vagy ellenőrzéséhez használható.
**Elektronikus dokumentum:** elektronikus eszköz útján értelmezhető adat együttes.
**Előfizető:** A hitelesítés-szolgáltatónál egy vagy több aláíró nevében előfizető természetes, vagy jogi személy, vagy jogi személyiség nélküli szervezet.
**Érvényességi lánc:** az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú elektronikus aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítvány az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt.
**Fokozott biztonságú elektronikus aláírás:** elektronikus aláírás, amely alkalmas az aláíró azonosítására, egyedülállóan az aláíróhoz köthető, olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak, és a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető.
**Hatóság:** Az elektronikus aláírással kapcsolatos szolgáltatásokat nyújtó szolgáltatókat felügyelő hatóság, a Nemzeti Média- és Hírközlési Hatóság (NMHH).
**Időbélyegző:** elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett.
**Hitelesítési Rend:** olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
**Időbélyegzési Rend:** olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
**Igénybe vevő:** elektronikus aláírással kapcsolatos szolgáltatást igénybe vevő természetes személy, jogi személy vagy jogi személyiség nélküli szervezet.

**Kompromittálódás:** az Aláíró magánkulcsa kompromittálódik, ha elveszik illetve ha véletlenül vagy szándékosan nyilvánosságra kerül.
**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.
**Kriptográfiai kulcs**: Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításhoz és dekódoláshoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.
**Kulcspár**: Az elektronikus aláírás létrehozásához és ellenőrzéséhez létrehozott egyedi aszimmetrikus kriptográfiai jelsorozat pár, mely áll egy publikus (nyilvános) és agy privát (magán) kulcsból.
**Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI):** Olyan szabványrendszer, mely meghatároz különböző biztonsági szolgáltatások körét, amelyek a kétkulcsos aszimmetrikus titkosítást és szabványos tanúsítványok használatát teszi lehetővé. Célja az adatvédelem, hitelesítés, bizalmasság, letagadhatatlanság és rendelkezésre állás megteremtése.
**Szolgáltatási szabályzat:** az EAT 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.
**Szolgáltató:** elektronikus aláírással kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet.
**Tanúsítvány:** a hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot az EAT 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági jelleget.
**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.

- Rövidítések:

| | |
|---|---|
| ANSI | The American National Standards Institute (Amerikai Nemzeti Szabványügyi Intézet) |
| CA | Certification Authority (Hitelesítő egység) |
| CC | Common Criteria (Közös szempontrendszer) |
| CP | Certificate Policy (Hitelesítési Rend) |
| CPS | Certification Practice Statement (Hitelesítés Szolgáltatási Szabályzat) |
| CRL | Certificate Revocation List (Tanúsítvány visszavonási lista) |
| DC | Domain Controller (Tartományvezérlő) |
| EAL | Evaluation Assurance Level (Értékelési Garancia szint) |
| HSM | Hardware Security Module (Hardveres Biztonsági Egység) |
| HwSCDev | Hardware Signature-Creation Device (Aláírás-létrehozó eszköz) |
| IETF | Internet Engineering Task Force |
| LRA | Local Registration Authority (Helyi regisztrációs egység) |
| PIN | Personal Identification Number (Személyi azonosító szám) |
| PKCS | Public-Key Cryptography Standard (Nyilvános kulcsú kriptográfiai szabvány) |
| PKI | Public Key Infrastructure (Publikus Kulcsú Infrastruktúra) |
| RA | Registration Authority (Regisztrációs egység) |
| RFC | Request For Comment (IETF ajánlások) |
| SSCD | Secure Signature-Creation Device (Biztonságos aláírás-létrehozó eszköz) |
| SSL | Secure Sockets Layer |
| SwSCDev | Software Signature-Creation Device (Szoftveres aláírás-létrehozó eszköz) |
| UPN | Universal Principal Name |

# 3. Közzététel, nyilvánosságra hozatal, tanúsítványtár

## 3.1. A szolgáltatói információ közzététele

### *3.1.1. Szabályzatok, kikötések és feltételek közzététele*

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában (PDF) teszi közzé az internetes honlapján (http://ds.digitoll.co.hu/). Ugyanitt elérhetőek a dokumentumok esetleges korábban érvényben lévő változatai is.

A dokumentumok internetes oldalról nyomtatott változatai semmilyen formában sem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a Szolgáltatás biztonságát nem veszélyezteti.

#### *3.1.2. Rendkívüli információk közzététele*

A Szolgáltató a rendkívüli információkat késlekedés nélkül közzéteszi internetes oldalán, a jogszabályi előírásoknak megfelelően, illetve akkor, amikor arra szükség van.

Rendkívüli információnak számít:

- Tájékoztatás új szolgáltatás vagy szolgáltatás-csoport indításáról.
- Tájékoztatás a Szolgáltatás szüneteléséről (Eat 9. § 8.), tervezett beszüntetéséről.
- Tájékoztatás a Szolgáltató magánkulcsának kompromittálódásáról, tanúsítványának felfüggesztéséről, visszavonásáról.
- Tájékoztatás a Szolgáltató tevékenységének befejezéséről.
- Tájékoztatás rendkívüli üzemeltetési helyzetről, körülményről, mely akadályozza a Szolgáltató rendes üzemmenetének folytatását.

Egyes rendkívüli információk esetén, a Szolgáltató írásban (elektronikusan vagy postai úton) is tájékoztathatja a Végfelhasználókat.

A szolgáltatói gyökértanúsítvány állapotváltozásával (visszavonásával), szolgáltatás befejezésével kapcsolatban a Szolgáltató hirdetésként közzéteszi az állapotváltozás tényét, illetve az érintett tanúsítvány adatait (lenyomatát) országos terjesztésű napilapban.

### 3.2. A tanúsítvány állapot információk közzététele

#### *3.2.1. A tanúsítványtár*

A Szolgáltató a végfelhasználók számára tanúsítványtárat üzemeltet, mely internetes oldalán elérhető. Szolgáltató itt teszi közzé a visszavonási listákat és a tájékozató jellegű Nyilvános tanúsítványtárat.

A Szolgáltató a Tanúsítványtárat rendszeres időközönként szükség szerint frissíti.

#### *3.2.1.1. Nyilvános tanúsítványtár*

A Szolgáltató által kibocsátott tanúsítványok és azok állapota elérhető a Nyilvános tanúsítványtárban is, a Szolgáltató internetes oldalán (ds.digitoll.co.hu). A Szolgáltató csak az Előfizető előzetes hozzájárulásával teszi közzé a tanúsítványt.

A Nyilvános tanúsítványtárban tárolt információk tájékoztató jellegűek, a mindenkori érvényes tanúsítványállapotokat a visszavonási listák tartalmazzák.

A Nyilvános tanúsítványtár helye:
http://ds.digitoll.co.hu/tanusitvanytar.php?m=4

#### *3.2.1.2. Tanúsítvány visszavonási lista (CRL)*

Szolgáltató a tanúsítványok érvényességének ellenőrzésére tanúsítvány visszavonási listát (továbbiakban CRL) bocsát ki. A CRL tartalmazza a Szolgáltató által visszavont és felfüggesztett tanúsítványokat.

A visszavonási lista kibocsátása Szolgáltató zárt tanúsítványtárából történik. A CRL-ek kibocsátása között eltelt idő legfeljebb 24 óra. A CRL akkor is kibocsátásra kerül, ha a legutóbbi kibocsátás óta nem történt tanúsítvány visszavonás vagy felfüggesztés. A visszavonási lista mindig tartalmazza a következő lista kibocsátásnak idejét, vagy a kibocsátott CRL érvényességi idejét, de Szolgáltató ennél korábban is kibocsáthat új listát. Felfüggesztés, visszaállítás és visszavonás esetén a Szolgáltató soron kívül új CRL-t bocsát ki. Új CRL kibocsátásakor a régebbi érvényessége megszűnik.

A tanúsítvány visszavonási listák helye:
http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl

A Szolgáltató Nyilvános tanúsítványtára és a visszavonási listája, legalább 99%-os rendelkezésre állással elérhetők, egyúttal az eseti szolgáltatás kiesések nem haladják meg a 24 órás időtartamot.

## 3.3. Adattárak

A Szolgáltató web-alapú felületen hozzáférést biztosít a Végfelhasználók számára a visszavonási adatokhoz (CRL), tanúsítvány információkhoz (Nyilvános tanúsítványtár), és a Szolgáltató publikus dokumentumaihoz (többek között: ÁSzF, Hitelesítési Rend, Időbélyegzési Rend, jelen Szabályzat).

A Szolgáltató dokumentumainak elérhetősége:
http://ds.digitoll.co.hu/dok.php?m=5

Hitelesítési Rend a tanúsítványban:
http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf

Visszavonási lista publikus helye:
http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl

## 3.4. A közzététel gyakorisága

### *3.4.1. Szabályzatok, kikötések és feltételek közzétételi gyakorisága*

A Szabályzattal kapcsolatos új verziók közzététele jelen Szabályzat 3.1.1. pontjában van ismertetve. A Szolgáltató szükség szerint bocsátja ki szerződéses feltételeit és szabályzatait, illetve azok újabb változatait.

### *3.4.2. Rendkívüli információk közzétételi gyakorisága*

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

### *3.4.3. Tanúsítványokkal kapcsolatos információk közzétételének gyakorisága*

A Szolgáltató az egyes tanúsítványok nyilvános közzététele kapcsán a következő gyakorlatot követi:

- a végfelhasználói tanúsítványokat a Nyilvános tanúsítványtárában az előállítást követően tíz munkanapon belül teszi közzé, amennyiben a tanúsítványt tulajdonló Előfizető és Aláíró ehhez előzetesen írásban hozzájárult.
- A visszavont, felfüggesztett tanúsítványokat a Szolgáltató a CRL-ben teszi közzé a visszavonást követően, rendszeres gyakorisággal, amikor erre szükség van.

A lehetséges esetek a következőek:

- lejárt a tanúsítvány,
- jogos felfüggesztési kérelem esetén,
- a tanúsítvány visszavonása esetén,
- felfüggesztés esetén.

### 3.5. Adattárak hozzáférési szabályzása

A Szolgáltató által közzétett kikötések és feltételek, rendkívüli információk, tanúsítványok és állapot információk nyilvános információk a web alapú felületeken harmadik – külső felek – felé is elérhetőek, így megtekintés céljából letölthetőek hitelesítés szüksége nélkül.

A tanúsítványok adatainak nyilvános közzététele csak az Előfizető és az Aláíró előzetes írásos hozzájárulásával lehetséges.

A Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató többféle védelmi mechanizmussal védi az információkat jogosulatlan módosítások ellen.

## 4. Azonosítás és hitelesítés

### 4.1. Névtípusok

A tanúsítvány “subject” (alany) mezője a következő névelemeket tartalmazza (a megadott sorrendben):

- emailAddress (E)

Az “emailAddress” formátuma megfelel az IETF RFC 2822 szabványnak. Ezt a névelemet a “subjectAltName” kiterjesztés is tartalmazhatja.

- commonName (CN)

A “commonName” típusa szabadszöveges mező.

Aláíró tanúsítványok esetében ez a névelem abban az esetben tartalmazhat álnevet, ha az igényelt tanúsítvány típusa álneves aláíró tanúsítvány, és a tanúsítványban levő title (T) mezőben külön fel van tüntetve, hogy a tanúsítvány álneves tanúsítvány. Álneves tanúsítvány esetében a CN mező az álnéven felül egyéb, a tanúsítvány álneves típusára utaló karaktereket tartalmazhat. Minden más aláíró tanúsítvány esetében kizárólag a személyazonosításra használt okmányban szereplő név alapján kerülhet kitöltésre.

Nem aláíró tanúsítvány esetében (például, de nem kizárólagosan: titkosító, vagy authentikációs tanúsítványok) a végfelhasználó által választott név szerepeltethető a CN névelemen belül, ha a jelen szabályzat egyéb rendelkezései (nevek egyedisége, márkanevek és védjegyek) alapján a névválasztás megfelelő.

- title (T)

A “title” típusa szabadszöveges mező. Kitöltése álneves tanúsítvány profil esetében kötelező, tartalma a tanúsítvány álneves típusára vonatkozó megjelölés kell legyen.

- localityName (L)

A “localityName” lista előre definiált nyilvános adminisztratív szabályokon alapszik.

- organizationalUnitName 1 (OU1)

Az “organizationalUnitName 1” típusa szabadszöveges mező.

- organizationalUnitName 2 (OU2)

Az “organizationalUnitName 2” típusa szabadszöveges mező.

- organizationName (O)

Az “organizationName” típusa szabadszöveges mező.

- countryName (C)

A “countryName” egy előre definiált érték (HU).

Az azonosítók értelmezése érdekében az Érintett felek a Szolgáltató nyilvános szabályzataiban leírtak alapján kell eljárniuk. Ha az Érintett félnek bármely, a tanúsítványban foglaltak értelmezésével kapcsolatban segítségre van szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot. A Szolgáltató az Előfizető vagy Aláíró adatairól többlettájékoztatást, erre vonatkozó felhatalmazás hiányában nem ad, csak a tanúsítványban feltüntetett adatok értelmezését segítő információt szolgáltatja.

#### *4.1.1. Márkanevek, védjegyek elismerése, hitelesítése*

A Szolgáltató által kibocsátott tanúsítványok mezőiben előfordulhatnak márkanevek, védjegyek. Ezek jogos használatát a Szolgáltató lehetőségei szerint ellenőrizheti, de nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában, illetve nem vállalja a felelősséget a név jogtalan használata miatt. A Szolgáltató ezért nem garantálja az Előfizető számára a márkaneve és/vagy védjegye feltüntetését a tanúsítványban. Az Előfizető részéről egy védjegy vagy márkanév megszerzése nem tekintendő olyan eseménynek, mely alapján a tanúsítvány megújítását kell kezdeményeznie.

### *4.1.2. Álnevek használata*

Az EAT 9§ (4) szerint a szolgáltatások igénylője jogosult kérni, hogy a tanúsítványba álnév kerüljön. Így Szolgáltató elérhetővé teszi az álnevek használatát az alábbi feltételek szerint:

- Az álneves tanúsítványok azonosítási, igénylési és kibocsátási folyamata, felfüggesztése és visszavonása megegyezik jelen szabályzat 4. és 5. pontjában leírtakkal.
- Az álneves tanúsítványokra Szolgáltató külön tanúsítvány profillal rendelkezik. Az álneves tanúsítványokban a CN mező az álnevet tartalmazza, a T mező a tanúsítvány álneves típusára vonatkozó megjelölést. Szolgáltató a CN mezőben az álnév feltüntetése mellett külön karakterekkel is jelölheti a tanúsítvány álneves mivoltát.
- Álnév kizárólag a tanúsítványban használható, Szolgáltató az igénylésben és a Szerződésben az igénylő valódi megnevezését használja és feltünteti az álnevet.
- Mivel az álneves tanúsítványban bármilyen név szerepelhet – akár más természetes vagy jogi személy neve is – így Szolgáltató a név jogos használatáért nem felelős, nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában, illetve nem vállalja a felelősséget a név jogtalan használata miatt. Ezen okok miatt Szolgáltató megtagadhatja az álnév használatát, ha az sérti a jó ízlést, a szemérmet és az etnikai hovatartozást.
- az álnevek egyediségének garantálása megegyezik Szolgáltató jelen szabályzat idevonatkozó pontjában leírtakkal.

Álnevet használó Aláíró esetén Szolgáltató csak az Aláíró, illetve a képviselt személy vagy szervezet beleegyezésével adhatja át a hatóságoknak vagy bármely más harmadik személynek az Aláíró valódi azonosságára vonatkozó adatokat. Kivétel ez alól, ha az adatokat nyomozó hatóságok kérik (jelen szabályzat 10.6. pont), mert ebben az esetben az adatok átadásáról Szolgáltató nem értesítheti az Aláírót.

Elektronikus aláírás tanúsítványa kibocsátható olyan céllal is, hogy az az aláírót más személy (szervezet) képviseletében történő aláírásra jogosítsa fel. Ebben az esetben a hitelesítés-szolgáltatás igénybe vevőjére vonatkozó szabályokat a képviselőre kell alkalmazni. Ebben az esetben álnév csak a képviselt hozzájárulása esetén tüntethető fel.

### *4.1.3. Nevek egyedisége*

A Szolgáltató az általa kibocsátott tanúsítványok esetében a tanúsítványok alanyait egyértelműen megkülönbözteti a tanúsítványban rögzített összes személyes adataik (név, lakóhely ország, lakóhely város, e-mail cím, illetve a Szolgáltató által esetlegesen generált sorszám) segítségével.

## 4.2. Kezdeti azonosítás

A tanúsítvány igénylése kizárólag írásban történik a Szolgáltató által biztosított online űrlap kitöltésével. Az igényléseket a Szolgáltató elbírálja és ezt követi a regisztrációs folyamat. A regisztrációs folyamat részeként szükséges lehet, hogy az igénylő megjelenjen a Regisztrációs hatóság előtt, melynek helyét és idejét az igénylő a Szolgáltató ügyfélszolgálatával telefonon, vagy írásban egyezteti. A személyes megjelenés történhet az Szolgáltató ügyfélszolgálati irodájában, vagy külön egyeztetés és megállapodás alapján, külső helyszínen.

### *4.2.1. Igénylő személy személyazonosságának hitelesítése*

Személyi tanúsítvány esetén az Előfizető és az Aláíró maga az igénylő természetes személy.

A tanúsítványban megnevezésre kerülő személy személyes megjelenését a fokozott biztonságú aláíró tanúsítványok illetve authentikációs tanúsítványok kiadása esetén követeli meg a Szolgáltató.

Az igénylő személy személyazonosságáról a Szolgáltató Regisztrációs egysége egy bemutatott érvényes, személyazonosításra alkalmas okmánya (külföldi állampolgárok esetén útlevél) és érvényes lakcímkártyája alapján győződik meg. A bemutatott okmányoknak tartalmaznia kell az igénylő személy:

- nevét,
- állandó lakcímét,
- születésének dátumát és helyét,
- anyja nevét.

Ez alapján a Szolgáltató a következő okmányokat fogadja el:

- személyi igazolvány,
- jogosítvány,
- útlevél,
- lakcímkártya (az előzőekben felsorolt okmányok közül az egyikkel együtt bemutatva).

Személyes megjelenés esetén a bemutatott okmány fényképe alapján az igénylő személynek egyértelműen felismerhetőnek kell lennie, s a benne szereplő aláírásnak meg kell egyezni a Szerződésen az igénylő személy által tett aláírással.

A bemutatott okmányoknak és dokumentumoknak, minden kétséget kizáróan eredetinek, valódinak és érvényesnek kell lenniük. A Szolgáltató az összes nem-minősített tanúsítványfajta kiadása esetén az Előfizető adatait, valamint a bemutatott iratok és

okmányok érvényességét és hitelességét EAT 12. § (2) bekezdése szerint közhiteles adatbázisban ellenőrzi.

Külföldi állampolgár esetén a Szolgáltató addig nem állítja ki részére a tanúsítványt, amíg a külföldön kiállított okmányt vagy a külföldi személy személyazonosságát megfelelő biztonsággal nem ellenőrizte.

Az Előfizető aláírásával igazolja, hogy az általa bemutatott okmányok hitelesek, érvényesek és a megadott adatok a valóságnak megfelelőek.

A Szolgáltató a tanúsítvány kibocsátását visszautasítja, amennyiben:

- az átadott adatok és dokumentumok hiányosak,
- az igénylő személy nem képes a személyazonosságát, hitelt érdemlően bizonyítani,
- a bemutatott okmányok, dokumentumok nem érvényesek,
- az igénylő személy személyazonossága minden kétséget kizáróan nem állapítható meg, a közhiteles adatbázisokkal végzett adategyeztetés során kétely merül fel a fentiekkel kapcsolatban,
- az igénylő személy megtagadja az adatszolgáltatást.

A fenti esetek előfordulásakor a Szolgáltató hiánypótlásra szólíthatja fel az igénylő személyt. Amennyiben a Szolgáltató által megadott határidőn belül, az igénylő Személy a felhívásban szereplő adatokat, okmányokat és dokumentumokat nem pótolja, illetve nem helyesbíti, a Szolgáltató ebben az esetben is visszautasíthatja a tanúsítvány kiállítását és kibocsátását.

#### *4.2.1. Szervezet azonosságának hitelesítése*

Szervezeti tanúsítvány esetén az Előfizető az igénylő Szervezet, és a tanúsítványokat a Szervezet képviseletében eljáró Aláíró vagy Aláírók részére állítja ki.

A Szervezeti tanúsítvány felhasználási körét az igénylő Szervezet határozza meg, de a Szolgáltató csak a Szervezet működési körében alkalmazott tanúsítványokra és a Szolgáltatási Szabályzatban illetve a Szerződésben meghatározott alkalmazási esetekre vállal jogi és pénzügyi felelősséget. Ezekben az esetekben a Szolgáltató a tanúsítványt kizárólag az igénylő Szervezet meghatalmazásával bocsátja ki, és annak hozzájárulásával menedzseli (felfüggesztés, visszavonás).

A regisztráció során az Előfizetőnek és Aláíróknak adatokat és bizonyítékokat kell nyújtaniuk a következőkről:

- a szervezet teljes és rövid neve, székhelye,
- a szervezet hivatalos azonosító adatai,
- a szervezeten belüli szervezeti egység neve, ha kérik ennek feltüntetését a tanúsítványban,
- igazolás arra vonatkozóan, hogy a szervezet valóban létező szervezet (cégbírósági bejegyzését igazoló okirat),
- a lehetséges Aláírók adatai és a szervezetben betöltött szerepük,
- ha a szervezet nevében meghatalmazott jár el, igazolás arra vonatkozóan, hogy a szervezet nevében a Szerződést aláíró személy jogosult-e az aláírás megtételére,
- ha a szervezet nevében aláírásra jogosult személy jár el, a regisztrációhoz csatolni kell az aláírásra jogosult személy aláírási címpéldányát vagy más azzal egyenértékű hivatalos dokumentumot, mely a szervezet aláírásra jogosult vezetőinek nevét és aláírását tartalmazza.
- amennyiben a szervezet közigazgatási szerv, a közigazgatási szervet képviselő természetes személynek a regisztrációhoz rendelkeznie kell, az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a Szervezet képviseletében a Szolgáltatónál előforduló ügyekben eljárjon.

A Szolgáltató az Előfizetők valamint Aláírók adatait, valamint a bemutatott iratok és okmányok érvényességét és hitelességét EAT 12. § (2) bekezdése szerint közhiteles adatbázisban ellenőrzi.

Az Aláírók azonosságának hitelesítési eljárása megegyezik a személy azonosságának hitelesítése pontjában leírtakkal. A Szervezet meghatalmazottjának jelen kell lenni az Aláírók regisztrációjánál és igazolnia kell az Aláírók a Szervezethez főződő kapcsolatát.

A Szolgáltató a tanúsítvány kibocsátását visszautasítja, amennyiben:

- az átadott adatok és dokumentumok hiányosak,
- a meghatalmazott illetve Aláíró személyek az igénylő Szervezethez tartozása nem egyértelmű, vagy nem bizonyított,
- nem egyértelmű a Szervezet képviseletében eljáró személy felhatalmazása a tanúsítvány kibocsátásához,
- a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel,

- az igénylő Szervezet azonossága minden kétséget kizáróan nem állapítható meg, a közhiteles adatbázisokkal végzett adategyeztetés során kétely merül fel a fentiekkel kapcsolatban.

A fenti esetek előfordulásakor a Szolgáltató hiánypótlásra szólíthatja fel az igénylő Szervezetet vagy meghatalmazottját. Amennyiben a Szolgáltató által megadott határidőn belül (ÁSzF), a Szervezet a felhívásban szereplő adatokat és dokumentumokat nem pótolja, illetve nem helyesbíti, a Szolgáltató ebben az esetben is visszautasíthatja a tanúsítvány kiállítását és kibocsátását.

Az igénylő Szervezet, mint Előfizető felelősséget vállal a Szerződésben megnevezett Aláírói által tanúsítványokkal végzett műveletekért, vállalja a tanúsítványok kibocsátásával, fenntartásával kapcsolatos és minden egyéb járulékos költséget. Az igénylő Szervezet, mint Előfizető és a hozzá tartozó Aláírók a Szolgáltató szabályzataiban részletesen tárgyalt kötelezettségeket, felelősségeket és jogokat ismeri, és elfogadja azokat.

#### *4.2.2. A magánkulcs birtokba adása*

Az eljárás a következő módon történhet:

- A tanúsítvány a Szolgáltató által biztosított intelligens kártyán vagy USB tokenen kerül kibocsátásra,
- A Szolgáltató nem biztosít a tanúsítványhoz intelligens kártyát vagy USB tokent (kizárólag meghatározott tanúsítvány típusok esetében elérhető, pl.: webszerver-tanúsítvány).

## 4.3. Azonosítás és hitelesítés az új kulcs kérésnél

Tanúsítvány kulcscseréjét a Szolgáltató nem támogatja. Amennyiben kulcscsere válna szükségessé, abban az esetben új tanúsítvány-igénylést kell beadni, az ott meghatározott személyazonosítási szabályok szerint eljárva.

## 4.4. Azonosítás és hitelesítés tanúsítványmegújítás esetén

Tanúsítványmegújítás akkor történik, amikor az Előfizető illetve az Aláíró a már meg lévő tanúsítványa helyett újat igényel. Ha a meglévő tanúsítványt a Szolgáltató állította ki, és így az Előfizető illetve Aláíró átesett a Szolgáltató kezdeti regisztrációs folyamatán (jelen Szabályzat ide vonatkozó pontja szerint), és semmilyen adat nem változott azóta, akkor az Előfizetőnek illetve az Aláírónak az új igénylés mellett, írásban nyilatkoznia kell arról, hogy az új tanúsítványba kerülő adatok helyesek, nem változtak. A nyilatkozatot az Előfizetőnek

illetve az Aláírónak, aláírásával kell igazolnia és el kell juttatnia a Szolgáltatóhoz. Ezt megteheti elektronikusan (érvényes és hiteles elektronikus aláírással, e-mail), személyesen, illetve postán. Ha a Szolgáltató jóváhagyja az igénylést az Előfizető egy előre egyeztetett időpontban egy egyszerűsített azonosítási folyamatot követően átveheti az új tanúsítványát. Az egyszerű azonosítási folyamat a kezdeti regisztrációkor megadott azonosító okmány alapján az Előfizető személyének azonosításából áll.

Ha adatváltozás történik, illetve a tanúsítvány már legalább 2 hónapja lejárt (és ez alatt az idő alatt nem érkezett kérvény a megújításra), az új tanúsítvány kiadásához a kezdeti regisztrációs folyamat megismétlése szükséges.

Szervezeti tanúsítvány esetén az Szervezet képviseletében eljáró meghatalmazottnak új meghatalmazást kell felmutatnia. Minden tanúsítványmegújítás egy új tanúsítvány kibocsátását jelenti, és új Szerződéskötést igényel.

Szervezeti tanúsítvány megújítása esetén, ha a változás az Aláírók személyében történik, úgy az új Aláíróknak részt kell venniük jelen Szabályzat ide vonatkozó pontjában megfogalmazott kezdeti regisztrációs eljáráson.

A Szolgáltató minden egyes tanúsítványmegújítás esetén igényelheti a jelen Szabályzat 4.2 pontjában megfogalmazott kezdeti azonosítási folyamatot és ismételt egyeztetést végezhet a közhiteles adatbázisokkal, és ha bármilyen problémát észlel az ide vonatkozó pontban megfogalmazott eljárást követi.

### 4.5. Azonosítás és hitelesítés a visszavonási és felfüggesztési kérelemhez

Felfüggesztési és/vagy visszavonási kérelmekhez kapcsolódó azonosítási és hitelesítési vonatkozásokat jelen Szabályzat idevonatkozó pontja tárgyalja.

## 5. A tanúsítvány életciklus működési követelményei

### 5.1. A tanúsítvány kérelem létrehozása

#### *5.1.1. Az igénylés feltétele*

A tanúsítványigénylés és szerződéskötés elengedhetetlen feltételei, hogy az igénylőnek hozzáférése legyen az Internethez és rendelkezzen e-mail címmel. A Szolgáltató az esetek többségében elektronikusan kommunikál a meglévő és leendő ügyfeleivel.

### *5.1.2. A tanúsítványigénylés és feldolgozás folyamata*

A tanúsítvány igényléséhez szükséges a Szolgáltató internetes oldalán levő tanúsítványigénylési űrlap pontos kitöltése és elküldése a Szolgáltató részére.

A tanúsítványigénylés eljárás részletes folyamata a következő:

- Az Igénylő fél tájékozódik a Szolgáltató által kibocsátásra kerülő tanúsítványfajtákról és az igénylés feltételeiről, majd kiválasztja a neki megfelelőt. A választáshoz igényelhet segítséget a Szolgáltató ügyfélszolgálati irodájától telefonon, vagy írásban.
- Az Igénylő a Szolgáltató internetes oldalán található elektronikus tanúsítványigénylő űrlap kitöltésével kérelmezi a kiválasztott tanúsítvány kibocsátását. Az igénylőlapon megadott adatok fognak szerepelni a tanúsítványban. Az igénylőlap kitöltése online történik, elküldése a Szolgáltató részére a kitöltés és nyilatkozattétel után történik.
- Az Igénylő az igénylés elküldése után kap egy elektronikus levelet ahol meg kell erősítenie a kérelmét és ezzel együtt a Szolgáltató le tudja ellenőrizni a megadott e-mail cím valódiságát.
- Szervezeti tanúsítvány igénylése esetén, az Aláírók számát előre meg kell adni, és az igénylésen Aláírók adatait pontosan fel kell tüntetni.
- Szervezeti tanúsítvány igénylése esetén, ha a szerződéskötéssel és az igényléssel kapcsolatos műveletek elvégzését az Igénylő (Szervezet) megbízott képviselő látja el, akkor a személyes találkozó alkalmával - a Szolgáltatási Szabályzat idevonatkozó pontjában megfogalmazottakon kívül - a megbízott képviselőnek magával kell hoznia a Szolgáltató internetes oldaláról letölthető Meghatalmazási nyomtatvány - elektronikusan kitöltött és cégszerűen aláírt - kettő darab példányát. A Szolgáltató csak a megfelelően kitöltött és aláírt Meghatalmazási nyomtatványt fogadja el.
- Az igénylési folyamat történhet személyesen, a Szolgáltató ügyfélszolgálati irodájában, vagy előre egyeztetett időpontban külső helyszínen is. A Szolgáltató ebben az esetben is ellenőrzi a megadott e-mail címek helyességét.

Az Igénylő - Szervezeti tanúsítvány esetében az igénylő Szervezet -, mint Előfizető és az általa megnevezett Aláíró is, aki részére igényelve lett a tanúsítvány - az igénylés elküldésével nyilatkozik a következőkről:

- A Szolgáltató Szolgáltatásaira vonatkozó szabályzatait elolvasta, a benne foglaltakat megismerte és elfogadja.
- Büntetőjogi felelőssége tudatában kijelenti, hogy a megadott adatai helyesek, és a valóságnak megfelelnek.
- A választott Szolgáltatásokkal kapcsolatos díjak megfizetését vállalja.
- Tudomásul veszi, hogy a Szolgáltató, a szerződéskötés keretében a megadott személyes és szervezeti adatait a jogszabályi kötelezettségeknek megfelelően:

- közhiteles adatbázissal egyeztesse, és nyilvántartsa
- a tanúsítvány gondozása céljából nyilvántartsa,
- a tanúsítványt nyilvánosságra hozza,
- a hatóságoknak, kormányzati, illetve bírósági illetékeseknek, mint harmadik félnek kiadhatja.

A Szolgáltató a hozzá beérkezett tanúsítványigényléseket nyilvántartásba veszi és feldolgozza. A feldolgozás részeként ellenőrzi, hogy a választott tanúsítványhoz minden adat rendelkezésére áll-e, illetve ellenőrzi azokat. Ha megfelelőnek találja, időpontot egyeztet az Igénylővel. A személyes találkozó alkalmával történik meg a Szerződés létrejötte a Szolgáltató – vagy megbízott alkalmazottja - és az Igénylő - vagy megbízottja - együttes aláírásával. Az Igénylő a továbbiakban már Előfizetőnek minősül. A tanúsítvány elkészítésére a tanúsítványigénylés során, az igénylésben megadott, a Szerződésben megerősített, a tanúsítvány fajtájától függően ellenőrzött, illetve az igénylés során érvényesnek elismert adatok alapján kerül sor. A tanúsítványigénylés feltételeinek teljesülése esetén a Szolgáltató feldolgozza azt.

Ha a beérkező adatokat a Szolgáltató hiányosnak, vagy valótlannak találja, felhívást küldhet az Igénylőnek hiánypótlásra, pontosításra. Az Igénylő köteles a felhívásnak a felhívásban meghatározott időn belül eleget tenni, vagy késedelmét írásban indokolni. Amennyiben ezt nem teszi meg, a Szolgáltató semmisnek veheti az igénylést. A Szolgáltató, megfelelő indoklással visszautasíthatja az igénylést.

Egyes Szolgáltatásokhoz szükséges az Igénylőnek a személyes megjelenése azonosítás céljából. Az eljárás részletei jelen Szabályzat idevonatkozó pontjában vannak rögzítve.

Ha a Szolgáltató az igénylést visszautasítja, vagy ha a Szerződés megkötésének megtagadása történik, illetve bármely más ok miatt a felek között a Szerződés nem jön létre, az Igénylő személyes adatait a Szolgáltató 5 napon belül megsemmisíti.

A Szolgáltató a tanúsítványigénylések feldolgozását beérkezési sorrendben kezdi meg. A feldolgozás ideje függ az Előfizető által igényelt Szolgáltatásoktól.

Jelen folyamatoktól külön írásos megállapodás keretében, a jogszabályi és törvényi előírásokat betartva el lehet térni, amennyiben az eltérő tanúsítványigénylési folyamat nem befolyásolja a tanúsítvány kibocsátási folyamat biztonságosságát.

Jelen folyamatokat a Szolgáltató Regisztrációs egysége végzi.

#### *5.1.3. A tanúsítványigénylés elfogadásának feltételei*

A Szolgáltató csak akkor fogadja el a tanúsítványkérelmet, ha a következő feltételek teljesülnek:

- Az igénylő benyújtotta a kérelmét a Szolgáltatónak.
- A természetes személy (akinek nevében az igénylő eljár) azonos a kérelemben szereplő alannyal,
- Szervezeti tanúsítvány esetén a leendő Aláíró hozzájárult a kibocsátáshoz,
- A kérelemben szereplő adatok ellenőrizhetők és pontosak.

## 5.2. A tanúsítványkérelem feldolgozása

A tanúsítványkérelem feldolgozási folyamata:

- Az ügyfélszolgálat (RA) ellenőrzi a regisztrációs információkat. Ezután dönt az regisztráció elfogadásáról vagy visszautasításáról.
- Elfogadás esetén az ügyfélszolgálat kitölti a kiadási űrlapot elektronikus formában.

A tanúsítványkérelem létrehozásának folyamata:

- Az ügyfélszolgálat és az RA operátorok hagyhatják jóvá a tanúsítvány kérelmeket.
- Az ügyfélszolgálat (RA) terjeszti elő a tanúsítványkérelmet, amelyhez szükség van a felhasználói adatokra.
- Az elfogadási folyamat egy web alapú interfészen keresztül történik (HTTPS protokollon). Az interfész egy RA modulhoz kapcsolódik, ahol az operátornak a titkos kulcsával (token) kell aláírni a kérelmet.

## 5.3. A tanúsítvány kibocsátása

A tanúsítvány kibocsátás folyamata:

- A Regisztrációs egység, a tanúsítványigénylés feldolgozását követően, ha a személy- és szervezetazonosítás megtörtént, egyezteti a Szerződésben foglalt adatokat a személy- és szervezetazonosítás során ellenőrzött adatokkal. Ha nem történik személyes megjelenés, a Regisztrációs egység akkor is ellenőrzi a megadott adatokat. Ezután dönt a regisztráció elfogadásáról vagy visszautasításáról.
- Elfogadás esetén az Regisztrációs egység kitölti a kiadási űrlapot elektronikus formában és megküldi az adatokat a Hitelesítő egységnek.

- Az adatok kiegészítésre és megerősítésre (pl.: CRL-ek) kerülnek. Csak az érvényes kérelmek kerülnek az adatbázisba.
- A regisztrációs információk mentésre kerülnek az RA regisztrációs adatbázisába. A tanúsítványok státusz információi el vannak tárolva az adatbázis tábláiban.
- A kulcspár szerver oldalon generálódik.
- A CA operátor érvényesíti a tanúsítvány kérelmeket a CA interfészét használva.
- A CA operátor manuálisan indítja el a tanúsítványok kiadását minden kérésre.
- A kibocsátott tanúsítványok az adatbázisba mentődnek.
- A titkos kulcsot (PKCS#12 állományokat és kapcsolódó jelszavakat) egy különválasztott CA hálózaton levő adatbázisba kell archiválni.
- Ezt követően a Hitelesítő egység kiállítja az igényelt tanúsítványt, majd visszaküldi a Regisztrációs egységnek.
- A Regisztrációs egység az eszközre helyezett Tanúsítványt és kulcsot átadja az Előfizetőnek illetve Aláírónak.
- A Szolgáltató a kibocsátást követően közzéteszi a tanúsítványt a Nyilvános tanúsítványtárában, ha az Előfizető ehhez előzetesen írásban hozzájárult.

Aláíró tanúsítvány kibocsátható olyan céllal is, hogy az Aláírót más személy (szervezet) képviseletében történő aláírásra jogosítsa fel. Ebben az esetben a hitelesítés-szolgáltatás igénybe vevőjére vonatkozó szabályokat a képviselőre kell alkalmazni. A tanúsítvány akkor bocsátható ki, ha a képviseleti jogosultságot igazolják. A képviseleti jogosultság meglétét Szolgáltató ellenőrzi és a kibocsátásról a képviselt személyt (szervezetet) haladéktalanul tájékoztatja.

## 5.4. A tanúsítvány elfogadása

A tanúsítványok és a kulcsok adathordozókon vannak tárolva. A CA tanúsítványok, felfüggesztési és visszavonási információk (nyilvános adatok) elérhetőek még nyilvános, web alapú könyvtárakban.

A tanúsítvány elfogadás az Aláíró részéről kétféleképpen történhet:

- online letöltéssel (online igazolás),
- személyes megjelenés alkalmával biztonságos (tanúsított) aláírás-létrehozó eszközön (ALE) való átvétel (személyes igazolás).

Az Aláíró a tanúsítvány használatba vétele előtt köteles igazolni a tanúsítvány átvételét, és a tanúsítvány adatainak helyességét. Ha az Aláíró rendellenességet talál, a magánkulcsot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonása érdekében. Amennyiben rendellenességről Szolgáltató nem kap bejelentést a kiadástól számított 1

munkanapon belül, a tanúsítvány elfogadottnak tekintendő és az ebből eredő minden kár és kockázat az Aláírót terheli.

Ha az igényelt tanúsítványfajta megköveteli a személyes megjelenést, akkor annak átadása is kizárólag személyesen történhet meg tanúsított ALE-n, a személyazonosság igazolását követően. Ekkor az Aláíró megkapja az használathoz szükséges kódokat (PIN) egy lezárt borítékban, melyet átvételkor ellenőriznie kell. Az Előfizető és/vagy Aláíró az átvételt követően köteles aláírni a Szerződés idevonatkozó mellékletét az Eszköz és Tanúsítvány átadás-átvételi nyilatkozatot.

A Szolgáltató a tanúsítvány kibocsátásáról és elfogadásáról értesíti az Aláírót és/vagy Előfizetőt az általa megadott e-mail címen.

## 5.5. Kulcspár és tanúsítvány használat

Az előre megadott tanúsítvány-profilok tartalmaznak előfeltételeket a keyUsage és extKeyUsage kiegészítőkhöz. Bővebb információkat a Hitelesítési Rend ide vonatkozó pontja tartalmaz.

### *5.5.1. Az Aláíróra és az Érintett félre vonatkozó általános szabályok, ajánlások*

A kulcspár és a tanúsítvány használata során a következő pontokat kell betartani:

- Az aláíró tanúsítványokat kizárólag fokozott biztonságú elektronikus aláírás létrehozására szabad használni.
- Az Aláíró a tanúsítványát kizárólag a tanúsítványban szereplő kulcshasználatnak megfelelően használhatja. A használat során be kell tartani az 2.8. fejezetben leírt korlátokat.
- Titkosításra és hitelesítésre csak az arra alkalmas tanúsítványokat lehet felhasználni.
- Csak érvényes és fel nem függesztett tanúsítvány használható fel.
- Az Aláíró az aláírás-létrehozó adatot kizárólag az aláírás létrehozására használhatja, betartva a Szerződésben jelzett esetleges egyéb korlátozásokat is.
- Az Aláírónak gondoskodnia kell arról, hogy az aláírás-létrehozó adata ne kompromittálódjon. Ha esetleg ez mégis megtörténik, akkor arról a lehetőségei szerint azonnal tájékoztassa a Szolgáltatót és ne alkalmazza azt.

Annak érdekében, hogy az Érintett fél megalapozottan hagyatkozhasson a tanúsítvánnyal hitelesített kriptográfiai kulcspár használatával működő alkalmazásra, ajánlott a kulcspár megfelelő használatát és a hozzá tartozó tanúsítványt az adott helyzetben tőle általában elvárható gondossággal ellenőriznie. Az Érintett fél csak abban az esetben fogadjon el

nyilvános kulcsokat, ha azokat a tanúsítványban rögzített módon alkalmazták illetve csak abban az esetben fogadja el a kulcsokhoz tartózó tanúsítványokat, ha azok érvényesek és nincsenek felfüggesztett vagy visszavont állapotban. Elektronikus aláírás ellenőrzése esetén, ha az ellenőrzendő elektronikus aláírás, a hozzá kapcsolódó tanúsítvány vagy a tanúsítványlánc bármely adata a művelet érvénytelenségére utal, illetve ha az adott alkalmazásban nem elfogadható, akkor az elektronikus aláírást és a tanúsítvány elfogadását az Érintett félnek célszerű elutasítania.

Nem érvényes elektronikus aláírás elfogadásból eredő minden kár és kockázat az Érintett felet terheli.

### *5.5.2. Elektronikus aláírás készítése*

Az elektronikusan aláírt adat, üzenet, levél vagy bármely dokumentum előállításának folyamatáért elsősorban az Aláíró a felelős. Az Aláíró birtokolja a magánkulcsot, ismeri az aláírandó adat, üzenet, levél vagy bármely dokumentum tartalmát, dönt az aláírási szándékról és üzemelteti az aláírást elvégző technikai eszközt. Így ha nem tartja be az alkalmazásra vonatkozó előírásokat (jelen Szabályzat, Hitelesítési Rend, Szerződés, törvényi és jogszabályi előírások) úgy az ebből származó kárért ő felel.

### *5.5.3. Magánkulcs birtoklása*

A magánkulcsot az Aláíró birtokolja. Az elektronikus aláírás csak akkor biztonságos, ha a magánkulcs az Aláírón kívül más számára nem hozzáférhető. A kulcsot jelszóval kódoltan és hardvervédelemmel kell ellátni. A kulcs elvesztéséből, véletlen vagy szándékos nyilvánosságra hozatalából eredő károkért az Aláíró felelős. A kulcs kompromittálódását a Szolgáltatónál be kell jelenteni.

### *5.5.4. Az elektronikus aláírás ellenőrzése*

Az elektronikus aláírás elfogadása előtt ellenőrizni kell azt, az alábbiak szerint:

- A tanúsítvány és az aláírás összetartozik.
- Szervezeti tanúsítvány esetén az Aláíró jogosult-e a tanúsítvány használatára.
- A tanúsítvány érvényes volt (érvényességi idő nem telt le, nincs felfüggesztve, visszavonva) az aláírás pillanatában, illetve időbélyeg hiányában az elfogadáskor.

- A tanúsítvány alkalmazása megfelel a tanúsítványban rögzített alkalmazási lehetőségeknek.
- A kibocsátó szervezet tanúsítványa illetve kulcsa érvényes.

## 5.6. Tanúsítvány csere

A tanúsítvány cserét (új tanúsítvány kibocsátása régi kulccsal) Szolgáltató nem támogatja.

## 5.7. Tanúsítvány megújítás

A tanúsítvány megújítás azt a folyamatot jelenti, amikor egy már a regisztrációs folyamaton átesett Előfizetőnek és/vagy Aláírónak a már érvényes Szerződése keretében korábbi tanúsítványa helyett másik tanúsítványt kell kibocsátani. A tanúsítvány megújítás illetve csere minden esetben új tanúsítvány kibocsátását jelenti.

Tanúsítvány megújítás a következő esetekben lehet szükséges meglévő érvényes tanúsítvány esetén:

- a tanúsítvány (és magánkulcs) le fog járni,
- a magánkulcs kompromittálódott,
- a regisztrációs folyamat alatt rögzített adatokban változás történt.

A tanúsítvány megújítására a következő szabályok vonatkoznak:

- A tanúsítvány megújítását az Előfizető kezdeményezheti.
- A Szolgáltató minden esetben megkövetelheti a személyes megjelenést és azonosítást.
- Abban az esetben, ha az Előfizető és/vagy Aláíró korábbi tanúsítványa még érvényes, de szükség van a tanúsítvány megújítására, megfelelő egyeztetések után a korábbi tanúsítványt vissza kell vonni.
- Az adatváltozás esetén a régi tanúsítványt vissza kell vonni és újat kell kiállítani. Az Előfizetőnek illetve az Aláírónak a kezdeti regisztrációval megegyező módon igazolnia kell magát és a megváltozott adatokat, a Szolgáltató csak a kezdeti regisztrációval megegyező ellenőrzési folyamatokat követően állítja ki az új tanúsítványt. Minden, a Szolgáltatásokat érintő adatváltoztatást haladéktalanul be kell jelenteni a Szolgáltatónak. Ennek elmulasztása esetén a Szolgáltató nem vállal sem jogi, pénzügyi, sem egyéb felelősséget és garanciát.
- Szolgáltató az új tanúsítványt csak új kulcshoz bocsájt ki.
- Az új tanúsítvány kibocsátása előtt a Szolgáltató ellenőrzi, hogy a régi tanúsítvány létezett-e, valamint, hogy az új tanúsítványba kerülő minden új vagy régi adat helyes és érvényes, ismételt egyeztetést végezhet közhiteles adatbázissal.

## 5.8. Tanúsítvány felfüggesztése és visszavonása

A Szolgáltató tanúsítvány visszavonási és felfüggesztési szolgáltatást nyújt. A tanúsítvány visszavonása a tanúsítvány-állapotát végérvényesen érvénytelenre állítja, a felfüggesztett tanúsítvány mindaddig, míg felfüggesztett állapotban van, ugyanúgy érvénytelenként kezelendő, mint a visszavont. Egy tanúsítvány egy alkalommal legfeljebb 5 napig lehet felfüggesztett állapotban, ezen időtartam után állapotát újra érvényesre kell állítani, vagy vissza kell vonni. A visszavont tanúsítványokhoz tartozó magánkulcs használatát azonnal meg kell szüntetni és felfüggesztett tanúsítványokhoz tartozó magánkulcs használatát pedig felfüggeszteni. Ha a tanúsítvány visszavonásra kerül a hozzátartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges.

Jogos visszavonási, illetve felfüggesztési kérelem esetén a kérelem feldolgozását követően a Szolgáltató értesíti az Aláírót illetve az Előfizetőt, és legfeljebb 8 órán belül közzéteszi a visszavont, vagy felfüggesztett tanúsítványt egy soron kívül kibocsátott visszavonási listában.

A visszavont, visszavonandó és felfüggesztett, felfüggesztendő tanúsítvány elfogadásából eredő károkra a következő felelősségi szabályok vonatkoznak:

- A visszavonási/felfüggesztési kérelem Szolgáltatóhoz történő megérkezéséig az Aláíró, illetve az Előfizető a felelős a felmerülő károkért.
- A visszavonási és felfüggesztési kérelem, Szolgáltató általi befogadását követően (megfelelő azonosítás után), a nyilvánosságra hozatalig a Szolgáltató felelős a felmerülő károkért,
- Amennyiben a Szolgáltató már közzétette a tanúsítvány érténytelen visszavonási állapotát, az Érintett Fél felelős a felmerülő károkért.

### *5.8.1. A visszavonás körülményei*

A tanúsítvány visszavonását a következő körülmények tehetik szükségessé:

- Előfizető kezdeményezése alapján:
  - az Előfizető visszavonási kérelme,
  - az Aláíró magánkulcsának kompromittálódása,
  - a tanúsítványban foglalt adatok megváltozása, érvénytelensége,
  - az aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása,
  - az aláírás-létrehozó eszköz hozzáférési adatának kompromittálódása.

- Szolgáltató kezdeményezése alapján:
  - A Szerződés és a Szolgáltató egyéb szabályzatai feltételeinek megszegése Aláíró, illetve Előfizető által,

- az Aláíró és az Előfizető kötelezettségeinek be nem tartása (különösen azonnali felmondás, fizetési késedelem esetén),
- a Szolgáltató tudomására jutott tény a regisztráció során megadott, illetve tanúsítványban szereplő adatok valótlanságáról,
- a tanúsítványban szereplő Szolgáltatói adatok érvénytelensége,
- a Szolgáltató valamely magánkulcsának kompromittálódása,
- a Szerződés megszűnése,
- az Elektronikus aláírás hitelesítés szolgáltatás vagy a Szolgáltató megszűnése,
- Illetve ha a tanúsítvány aláírására használt algoritmus már nem biztonságos, illetve nem alkalmas tanúsítványok aláírására.

Egyéb visszavonáshoz vezető körülmények:

- az Aláíró illetve az Előfizető halála vagy megszűnése,
- az NMHH vagy más hatóság jogerős és végrehajtható határozata,
- jogszabály rendelkezik így,
- különleges esetek (pl.: szolgáltatói névcsere).

Ezek alapján visszavonást kezdeményezhet:

- Előfizető,
- Szolgáltató,
- NMHH vagy más hatóság jogerős és végrehajtható határozat ellenében.

### *5.8.2. Visszavonás kérelemre vonatkozó eljárás*

Végfelhasználói tanúsítvány visszavonását kezdeményezheti az Előfizető, a Szolgáltató, vagy egy hatóság. Az Előfizetőnek és Szolgáltatónak kötelessége az 5.8.1 pontban feltűntetett esetekben a visszavonás azonnali kezdeményezése, illetve végrehajtása.

A tanúsítvány visszavonása - az Előfizető által - történhet személyesen, vagy írásban (papíron, vagy elektronikusan érvényes és hiteles elektronikus aláírással ellátva). A Szolgáltató a visszavonási kérelmeket kizárólag nyitvatartási időben fogadja. Nyitvatartási időn kívül, tanúsítvány felfüggesztési kérelmet lehet benyújtani, jelen Szabályzat 5.8.3.-5.8.4. pontjaiban leírtak szerint.

A visszavonási kérelmeket a Szolgáltató folyamatosan fogadja és haladéktalanul megkezdi azok feldolgozását. A kérelmet kézhezvételtől számítva a Szolgáltató egy munkanapon belül, soron kívül dolgozza fel. A feldolgozás részeként a Szolgáltató Regisztrációs egysége ellenőrzi a visszavonási kérelemben szereplő adatokat, ellenőrzi a kérelmező személyazonosságát. Ha az adatok helytelenek, a kérelmező kiléte vagy a visszavonásra való jogosultság nem

állapítható meg, akkor a Szolgáltató a tanúsítvány visszavonást megtagadja. Valóságnak megfelelő és hiteles kérelem esetén a Szolgáltató további mérlegelés nélkül visszavonja a tanúsítványt. Amint a visszavonási kérelem feldolgozásra került, a Szolgáltató értesíti erről az Aláírót illetve az Előfizetőt, és legfeljebb 8 órán belül közzéteszi a visszavont tanúsítványt egy soron kívül kibocsátott visszavonási listában, és megváltoztatja a tanúsítvány státuszát a tanúsítványtárban.

A visszavonási kérelemnek legalább a következő adatokat kell tartalmaznia:

- a visszavonást igénylő megnevezése, elérhetősége (telefon, e-mail),
- a visszavonást igénylő kapcsolata a tanúsítvány birtokosával, vagyis az Aláíróval,
- az Aláíró megnevezése, elérhetősége (telefon, e-mail),
- a tanúsítvány sorszáma vagy egyedi neve,
- a tanúsítvány típusa és kibocsátási dátuma,
- a visszavonás oka.

- Szervezeti tanúsítvány esetén az Előfizető részéről a meghatalmazással rendelkező képviselő (aki azonosítva lett a Szerződés megkötésekor) kezdeményezheti a visszavonást. A visszavonási kérelem mellé a következő dokumentumokat kell csatolnia az Előfizető meghatalmazottjának:
  - aláírási címpéldányt,
  - a Szervezet cégkivonatát,
  - a meghatalmazással rendelkező képviselő személyes adatait tartalmazó okirat,
  - a meghatalmazással rendelkező képviselő meghatalmazását.

A tanúsítvány a visszavonási folyamat végéig felfüggesztett állapotban van, a visszaélések ellen. Ezeket a tanúsítványokat már nem lehet visszaállítani.

Amennyiben egy tanúsítvány visszavonásra került, azt nem lehet újra használatba venni. A tanúsítvány visszavonásával a Szolgáltató és az Előfizető között létrejött Szerződés megszűnik.

### *5.8.3. A felfüggesztés körülményei*

A tanúsítvány érvényességének felfüggesztését a következő körülmények tehetik szükségessé:

- Aláíró és Előfizető kezdeményezése alapján:
  - az Aláíró illetve az Előfizető felfüggesztési kérelme.

- Szolgáltató kezdeményezése alapján:
  - megalapozottan feltételezhető, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak,
  - megalapozottan feltételezhető, hogy az aláírás-létrehozó adat nem az aláíró kizárólagos birtokában van,
  - fennálló gyanú a regisztráció során megadott, illetve tanúsítványban szereplő adatok érvénytelenségéről,
  - fennálló gyanú a Szolgáltató valamely magánkulcsának kompromittálódása,
  - az Előfizető nem teljesíti a Szerződésben vállalt kötelességeit (Pl.: díj nem fizetés).

Egyéb felfüggesztéshez vezető körülmények:
- az NMHH vagy más hatóság jogerős és végrehajtható határozata,
- jogszabály rendelkezik így.

Ezek alapján a felfüggesztést kezdeményezhet:
- Előfizető,
- Aláíró,
- Szolgáltató,
- NMHH vagy más hatóság jogerős és végrehajtható határozat ellenében.

Szolgáltató a visszavonási kérelmeket ideiglenesen kielégítheti felfüggesztéssel is, amennyiben a bejelentett körülmények kivizsgálását szükségesnek tartja.

A Szolgáltató a tanúsítvány kiállításának díját nem téríti vissza.

### *5.8.4. Felfüggesztési kérelemre vonatkozó eljárás*

A tanúsítvány felfüggesztése - az Előfizető és/vagy Aláíró által - történhet személyesen, írásban (papíron vagy elektronikusan érvényes és hiteles elektronikus aláírással ellátva) vagy telefonon. A Szolgáltató az írásos felfüggesztési kérelmeket (személyesen, vagy levélben érkezett) kizárólag nyitvatartási időben fogadja. Szolgáltató a telefonos felfüggesztési kérelmeket a hét minden napján, a nap 24 órájában, kizárólag az 1.1 pontban megadott Visszavonási ügyeleti számon fogadja.

A felfüggesztési kérelmet a visszavonási kérelemmel megegyező módon dolgozza fel Szolgáltató.

A tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 5 munkanapig. Kivételtét képez ez alól a Szolgáltató általi technikai felfüggesztés időtartalma, mely legfeljebb 30 naptári nap. A felfüggesztett állapot kezdő időpontja a felfüggesztési kérelem elfogadásától számítandó. Ha ez idő alatt a felfüggesztéshez vezető körülmények gyanúja cáfolatot nem nyer, Szolgáltató a tanúsítványt visszavonja. Ha ez idő alatt a felfüggesztéshez vezető körülmények gyanúja cáfolatot nyer, Szolgáltató a tanúsítványt visszaállítja. Amint a felfüggesztési kérelem feldolgozásra került, a Szolgáltató értesíti erről az Aláírót illetve az Előfizetőt, és legfeljebb 8 órán belül közzéteszi a felfüggesztett tanúsítványt egy soron kívül kibocsátott visszavonási listában.

Felfüggesztett tanúsítvánnyal hitelesített elektronikus aláírás érvénytelennek tekintendő. Érvénytelen elektronikus aláírásnak nincs joghatása.

A felfüggesztett állapotról a Szolgáltató mindig értesíti az Aláírót illetve az Előfizetőt. A tanúsítvány felfüggesztés állapota megjelenik a visszavonási listában is.

A Szolgáltató a tanúsítvány kiállításának díját nem téríti vissza.

#### *5.8.4.1. Felfüggesztés telefonon*

A Szolgáltató a sürgős visszavonási - felfüggesztési kérelmekre való tekintettel (kompromittálódás, eltulajdonítás, stb.) 7*24 órás telefonos ügyeletet tart fenn, kizárólag a Szolgáltató adatainál megnevezett telefonszámon. A telefonbeszélgetés naplózásra és rögzítésre kerül.

Telefonos bejelentés esetén a Szolgáltató csak felfüggeszti a tanúsítványt, a visszavonáshoz az Előfizetőnek írásban (papíron vagy elektronikusan aláírva) kell megerősítenie visszavonási kérelmét. Az így felfüggesztett tanúsítvány akkor kerül visszavonásra, amikor Aláíró illetve az Előfizető írásos kérelme a Regisztrációs egységhez beérkezett, vagy a felfüggesztéstől számított 5 munkanap letelt. Ha az Előfizető és/vagy Aláíró nem erősíti meg a visszavonást, illetve nem kéri a Tanúsítvány visszaállítását, a Szolgáltató az 5 munkanap leteltével visszavonja a Tanúsítványt és erről értesíti az Előfizetőt és/vagy Aláírót. A Szolgáltató a Tanúsítvány díját nem téríti vissza.

A felfüggesztésről a Szolgáltató mindig küld tájékoztatást az Előfizetőnek és/vagy Aláírónak. Így a felfüggesztésből vagy visszavonásból eredő esetleges károkért a Szolgáltató nem vállalja a felelősséget.

Telefonos bejelentés esetén azonosítás céljából a felfüggesztést igénylő Előfizetőnek és/vagy Aláírónak a következő adatokat kell megadnia:

- a kérelmező nevét, jogi státuszát
- kezdeti regisztrációkor megadott felfüggesztési jelszót,
- Előfizető és Aláíró nevét,
- a Tanúsítvány azonosítóját,
- kezdeti regisztrációkor megadott igazolvány számát,
- felfüggesztés okát.

A Szolgáltató minden esetben a kezdeti regisztrációkor megadott egyéb adatokra is rákérdezhet.

Ha a Szolgáltató nem tudja egyértelműen azonosítani a felfüggesztést kérelmezőt vagy a felfüggeszteni kívánt Tanúsítványt, illetve a kérelmező nem adja meg a fenti listában szereplő, kötelező adatok valamelyikét, vagy nem a helyes jelszót adja meg, a Szolgáltató elutasítja a felfüggesztési kérelmet.
Ebben az esetben a Szolgáltató nem fogadja be a felfüggesztési kérelmet, a felelősség az Előfizetőé és/vagy az Aláíróé.

Amint a Szolgáltató a telefonbeszélgetés során sikeresen megállapította a kérelmező felfüggesztési jogosultságát, befogadja a kérelmet és megkezdi annak feldolgozását. Amint a felfüggesztési kérelem feldolgozásra került, a Szolgáltató értesíti erről az Aláírót illetve az Előfizetőt, és legfeljebb 8 órán belül közzéteszi a felfüggesztett tanúsítványt egy soron kívül kibocsátott visszavonási listában.

A felfüggesztés az összes, a kiadott kártyán és/vagy tokenen szereplő tanúsítványra vonatkozik.

### *5.8.5. A tanúsítvány visszaállítása*

A tanúsítvány visszaállítása a felfüggesztett tanúsítvány újbóli érvényesítését jelenti.

Ha az Aláíró illetve az Előfizető kérvényezte a felfüggesztést, a felfüggesztés időtartalma alatt kérvényezhet a visszaállítást is, de a visszaállítás esetleges következményeiért ő felel (kompromittálódás, jogtalan használat, stb.). A visszaállítás kérelem benyújtása történhet személyesen, vagy elektronikus úton (érvényes és hiteles elektronikus aláírással ellátva). A visszaállítási kérvény befogadása csak a megfelelő azonosítást követően történik meg.

A Szolgáltató díjat számol fel a Tanúsítvány visszaállításáért. A díj a Szolgáltató internetes oldalán a mindenkori árlistájában szerepel. Ha az Előfizető a díjat a kiküldött számlán jelzett időpontig nem fizeti meg, a Szolgáltató az ÁSzF-ben foglaltak szerint járhat el.

Ha ugyanarra a tanúsítványra több féltől is érkezik felfüggesztési kérelem, akkor a Szolgáltató csak akkor állítja vissza a tanúsítványt, ha mindegyik felfüggesztő fél kéri a visszaállítást is.

## 5.9. A tanúsítvány előfizetés vége

A Szolgáltató által kibocsátott tanúsítványok érvényességi idejének lejártával megszűnik az adott tanúsítvány előfizetésének ideje is. Tanúsítvány megújításakor a meglévő Szerződés Szolgáltató és Előfizető közös akaratával meghosszabbítható, Szolgáltató erre a célra használt Szerződés-módosítási űrlapjának kitöltésével.

Az előfizetés lemondható a lejárati idő előtt az Aláíró illetve az Előfizető, vagy Szervezeti tanúsítvány esetében a megbízott képviselő által. Ebben az esetben a tanúsítvány visszavonására vonatkozó szabályok az irányadóak, és a tanúsítvány kiállításának díját a Szolgáltató nem téríti vissza. A visszavonással egy időben a Szerződés is megszűnik.

A Szerződést és a tanúsítvány előfizetést indokolt esetben a Szolgáltató is felmondhatja, és a tanúsítványt visszavonhatja. Ezeket az eseteket részletesen az ÁSzF tartalmazza.

Ha az tanúsítvány érvényességének lejártakor az Aláíró illetve az Előfizető a Szolgáltató előírásai szerint nem újítja meg a tanúsítványt, a Szerződés automatikusan megszűnik.

## 5.10. Fokozott biztonságú időbélyegzés szolgáltatás

A Szolgáltató Fokozott biztonságú időbélyegzés szolgáltatást (továbbiakban: időbélyegzés szolgáltatás) jelen szabályzat és a hozzá kapcsolódó Időbélyegzési Rend alapján nyújt. Jelen pontban nem szabályozott kérdésekre a jelen szabályzatban a tanúsítvány-szolgáltatásnál, az ÁSzF-ben, és az Időbélyegzési Rendben leírtakat értelemszerűen kell alkalmazni.

Az időbélyegzés szolgáltatást természetes személy vagy szervezet egyaránt igényelhet. Az igénylés történhet e-mail-ben, levélben, vagy személyesen a Szolgáltató ügyfélszolgálati irodájában, illetve előre egyeztetett külső helyszínen is.

Az igénybevétel történhet:

- a Szolgáltatóval történő eseti megállapodás, vagy
- a Szolgáltató által nyújtott ajánlatok, csomagok elfogadott megrendelése keretében.

A szolgáltatás használatához szerződéskötés szükséges. A Szolgáltató csak írásos igényléseket fogad el. A szerződéskötés menete megegyezik a Szerződés megkötésének menetével.

Az Szolgáltatás igénybevétele authentikációs tanúsítvány alapján történik. Az authentikációs tanúsítvány kiállításához szükséges a személyes megjelenés és a kezdeti regisztráció. A kezdeti azonosítás, a tanúsítványigénylés és kibocsátás folyamatának leírása jelen Szabályzat 4. és 5. pontjában található.

Az időbélyegzés szolgáltatás igénybevétele során az Előfizető egy dokumentum lenyomatát adja meg, amelyre a Szolgáltató aláírt időbélyeget ad vissza.

Az időbélyegzés szolgáltatás rendelkezésre állása 98%, míg az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

A Szolgáltató az Interneten keresztül nyújt időbélyegzés szolgáltatást, publikus szervereinek eléréséhez internetkapcsolat szükséges.

A szolgáltatás a https://pki.digitoll.co.hu/tsa címen érhető el.

# 6. Létesítmény-, menedzsment- és működésellenőrzés

A Szolgáltató rendelkezik belső, nem publikus Informatikai Biztonság Szabályzattal (IBSz). Az itt nem tárgyalt kérdésekben az IBSz-ben leírtak szerint jár el a Szolgáltató.

## 6.1. Fizikai óvintézkedés

Szolgáltató gondoskodik arról, hogy a kellő fizikai biztonsági óvintézkedéseket telephelyein és bérelt helyiségein belül garantálja. A kialakított infrastruktúra biztonságos fizikai környezetben üzemel, mely biztosítja a jogosulatlan fizikai és informatikai hozzáférések és belépések megakadályozását, valamint a folyamatos üzemmenetet, melyet a Szolgáltató meghatározott időközönként, előre meghatározott folyamatként ellenőriz.

Szolgáltató a fizikai rendszerellenőrzésről jegyzőkönyvet vezet.

### *6.1.1. Telephelyek, bérelt helyek elhelyezkedése*

A Szolgáltató védett számítógép teremben, négy egymástól elkülönített, és fizikailag egymástól nagyobb távolságra elhelyezkedő helyen valósítja meg a szolgáltatásokat.

### *6.1.2. Fizikai hozzáférés*

A Szolgáltató által igénybevett helyiségekben gondoskodik a megfelelő fizikai védelemről. Ez telephely illetve bérelt helyiség függvényében állhat:

- riasztórendszerből,
- kamerarendszerből,
- 24 órás őrszolgálatból,
- naplózott, mágneskártyás beléptető rendszerből.

A Szolgáltatás nyújtásához szükséges eszközökhöz csak az arra jogosult és kijelölt biztonsági munkakört betöltő személyek férnek hozzá.

A kommunikáció biztonságos, védett bérelt vonalon történik.

### *6.1.3. Áramellátás, légkondicionálás*

A Szolgáltató az általa igénybe vett helyiségekben gondoskodik a megfelelő és folyamatos áramellátásról (redundáns, szünetmentes tápegység) és hűtéséről (légkondicionáló berendezés).

### *6.1.4. Tűzvédelem*

A Szolgáltató által igénybevett helyiségekben a tűzmegelőzés és tűzvédelem biztosított.

### *6.1.5. Vízvédelem (beázás, elázás)*

A Szolgáltató által igénybevett infrastruktúra beázás és elárasztódás ellen védett. A szervertermek kialakítása biztosítja az elárasztódás veszélyének minimalizálását.

### *6.1.6. Adathordozók tárolása*

Az adathordozók tárolása a Szolgáltató telephelyén biztonsági, korlátozott hozzáférésű páncélszekrényben történik.

A páncélszekrény tartalma meghatározott időközönként ellenőrzésre kerül az arra kijelölt személy által.

#### *6.1.7. Bizalmas minősítésű adatok megsemmisítése, selejtkezelés*

A selejtkezelési szempontból a Szolgáltató megkülönböztet papír alapú és elektronikus alapú bizalmas minősítésű adatokat, melyeket különböző módon semmisít meg, ha azok feleslegessé váltak.

A papír alapú bizalmas minősítésű dokumentumok megsemmisítése aprítógéppel történik.

A bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat először, az arra kijelölt személy törli, majd szétszereli, végül összetöri. Az adathordozókat még tartalmuk törlése után sem használják fel nem bizalmas minősítésű adatok tárolására.

Az egyéb mágneses adathordozókat demagnetizálás után összetörik.

#### *6.1.8. Mentési példányok fizikai elkülönítése*

A bizalmas minősítést kapott adatok, dokumentumok, adathordozók fizikailag elkülönítve korlátozott hozzáférésű páncélszekrényben vannak őrizve. Ezen kívül minden adatot biztonsági mentésként a Szolgáltató elektronikusan is archivál elkülönített rendszeren. Az adatokhoz való hozzáférés korlátozott.

### 6.2. Folyamatellenőrzés

A működési folyamatok Ellenőrző listákban vannak rögzítve.

A rendszer informatikai működésének ellenőrzését, az arra kijelölt személy havi rendszerességgel megteszi a lista vezetésével. A felelős vezető minden hónap elején ellenőrzi a listák vezetését.

A rendszer ellenőrzése havonta egyszer történik Ellenőrzési lista vezetésével, az ellenőrzést az arra kijelölt személy végzi.

Ha a folyamat ellenőrzése közben az ellenőrző személy hibát vagy rendellenességet talál, naplózza és haladéktalanul jelenti a felelős vezetőnek. A felelős vezető elrendeli a hiba javítását. A hibajavítást követően újabb rendszerellenőrzésre kerül sor.

## 6.3. Személyzet ellenőrzése

Szolgáltató kellő számú, szolgáltatások nyújtásához szükséges feladatok jellegének megfelelő tudással rendelkező személyzetet alkalmaz. Az alkalmazottak a feladatok szétválasztása és a meghatalmazás szempontjai szerint meghatározott munkaköri leírásokkal rendelkeznek. A munkaleírások meghatározzák a munkakört és az ahhoz kapcsolatos feladatokat.

A munkakörökhöz kapcsolódó elvárt azonosítás és hitelesítés a következőek:

- A szolgáltatást ellátó személyek a regisztrációval és tanúsítvány-kezeléssel kapcsolatos alkalmazások használata előtt megfelelő azonosítási és hitelesítési eljáráson esnek át.
- A bizalmas munkakörben dolgozók csak chipkártyás azonosítással végezhetik a munkájukat, mely hatáskörileg, és hozzáférési szint alapján is szabályozva van.

Az személyzet munkáját a felelős vezető ellenőrzi. A szerepkörök elosztását a Bizalmi munkakörök dokumentum tartalmazza.

### *6.3.1. A bizalmi munkakörök*

Általános felelős vezető: A szolgáltatás biztonságáért általánosan felelős személy, aki tanúsítványok előállítását, kibocsátását, felfüggesztését és visszavonását nem végzi. Munkaviszonyban áll a Szolgáltatóval.

Rendszergazda:

- Rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy. Munkaviszonyban áll a Szolgáltatóval.

- Rendszerüzemeltető: Az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy. Munkaviszonyban áll a Szolgáltatóval.

Biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy. Munkaviszonyban áll a Szolgáltatóval.

Regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy. Munkaviszonyban áll a Szolgáltatóval.

Független rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy. Megbízásos viszonyban áll a Szolgáltatóval.

A Szolgáltató biztosítja, hogy a bizalmi munkakörök közül:

- a biztonsági tisztviselő nem töltheti be a független rendszervizsgáló munkakört;
- az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő, illetve a független rendszervizsgáló feladatait.

A kinevezett személyek munkaköri leírása tartalmazza a feladatukat és titoktartási nyilatkozatot írnak alá.

## 6.4. Vizsgálati naplózás folyamatai

A Szolgáltató gondoskodik arról, hogy az általa vagy megbízottja által elvégzett műveletek, illetve a Szolgáltatásokkal kapcsolatos rögzített adatok megőrzésre kerüljenek, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

A naplóbejegyzések többek között a regisztráció, az aláírás-létrehozó és ellenőrző kulcs-pár generálása, az aláírás-létrehozó eszköz megszemélyesítése, a tanúsítvány létrehozása, kibocsátása és kezelése, valamint egyéb szolgáltatói tevékenységek és az esetleges hibaesemények során készülnek. A naplózott adatállománynak tartalmazzák a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

A naplók vezetését a műveleteket végző, azonosított személy végzi, az ellenőrzési feladatokat a felelős vezető látja el.

A naplók hosszú távú archiválása havi rendszerességgel történik. A naplók nyomtatott formában, valamint elektronikus biztonsági mentésként is archiválásra kerülnek. A naplók a velük kapcsolatba hozható tanúsítványok érvényességi idejének lejártától számított tíz évig, vagy a velük kapcsolatban felmerült és a Szolgáltató felé bejelentett jogvita jogerős lezárásáig megőrzésre kerülnek. Az elektronikus adatok tárolása, jelszóval védett mappába történik. A papír alapú adatokat, Ellenőrző listákat, és ezek meglétét igazoló dokumentumokat a felelős vezető lezárásként aláírásával látja el és elzárva tárolja.

## 6.5. Feljegyzések archiválása

A szolgáltatás nyújtása közben létrejött papír alapú dokumentumokat, papír és elektronikus adat formájában (mint biztonsági mentés) is tárolja a Szolgáltató. A Szolgáltató a napló adatokat fokozott biztonságú fizikai környezetben menti el, a mentett állományokat

időbélyeggel ellátott elektronikus aláírással hitelesíti, és védett környezetben tárolja. A naplók olvasása hozzáférési jogosultság szerint korlátozott. A papír alapú adatokat a felelős vezető lezárásként aláírásával látja el és elzárva tárolja. Az intézményi biztonsági dokumentumai szintén ezen eljárás keretében kerülnek mentésre.

Az informatikai rendszerben keletkező napló állományokról (log), adatbázisokról napi egyszeri mentés készül. A lementett fájlokat a szolgáltató külön fizikai eszközön, jelszóval ellátva tárolja. A szerverekről a mentés hetente történik.

A tanúsítvány visszavonási kérelmek pontos naplózásra kerülnek. Ha a kérelem telefonon érkezik, a telefont kezelő személyzet rögzíti a hívás időpontját, a hívó félt, a hívás indokát, függetlenül attól, hogy a hívó félt sikeresen azonosította e vagy sem.

## 6.6. Informatikai biztonság

### *6.6.1. Jelszókezelés*

A Szolgáltató munkatársai és megbízottjai meghatározott azonosítási eljárást követően saját azonosító tokent kapnak, a rendszerhez való hozzáféréshez – jogosultság függvényében - megfelelően generált jelszót kapnak. A jelszavak tárolása fizikailag biztonságos környezetben, ellenőrzötten történik.

### *6.6.2. Vírusirtás*

A Szolgáltató a szolgáltatásban használt számítógépei vírus és kémprogram elleni védelemmel rendelkeznek. Ezek frissítése a „Biztonsági protokollok” pontban foglaltak szerint történik.

### *6.6.3. Tűzfal*

A Szolgáltató a szolgáltatás nyújtásához dedikált tűzfallal rendelkezik, melyen több biztonsági zóna is kialakításra került. A tűzfalszabályok kialakítása szerint külön zónába tartoznak a publikus elérésű szerverek, a nem publikus elérésű szerverek, az egyéb, biztonsági funkciókat megvalósító hardverelemek, és a munkaállomások. A zónák közötti átjárás hálózati port, MAC cím és IP cím alapján szűrve van.

#### *6.6.4. Biztonsági protokollok*

##### *6.6.4.1. Publikus elérés*

A szolgáltatást nyújtását biztosító rendszer a Szolgáltató egyéb informatikai infrastruktúrájától elszigetelve működik. A szolgáltató rendszer kívülről, az internet felhasználásával nem elérhető (kivéve a publikus szervereket).

##### *6.6.4.2. Rendszerfrissítések*

A szükséges operációs rendszer és vírusadatbázis frissítéseket a megfelelő technikai személyzet minden hónap első napján végzi el a munkaállomásokon. A szervereken előzetesen kitűzött tervezett rendszerkarbantartás keretében történik a telepítés.

##### *6.6.4.3. Adathordozók használata*

A szolgáltatás nyújtásához használt munkaállomásokon házirendben (policy) tiltott az USB adattároló eszközök használata, az adatszivárgás megakadályozása érdekében. Ugyancsak tiltott az optikai lemezek írása.

Az adathordozók használata szabály alól kivételt képeznek a rendszer felügyeletét ellátó személyek.

## 6.7. Helyreállítás betörés vagy katasztrófa után

Katasztrófa illetve betörés, rongálás következtében alkalmazandó eljárásokat a „Helyreállítási terv rendkívüli üzemhelyzetek esetén” című dokumentum tartalmazza.

Rendkívüli üzemeltetési helyzet bekövetkezése esetén Szolgáltató haladéktalanul értesíti a vele szerződéses viszonyban lévő ügyfeleit, valamint erre vonatkozó tájékoztatást tesz közzé internetes oldalán. Szolgáltató értesíti az NMHH-t is a rendkívüli üzemeltetési helyzet bekövetkezéséről, annak várható hatásairól és időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, az elhárítás közben esetlegesen felmerült további következményekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről is. A Szolgáltató hivatkozott dokumentumában részletesen szabályozza a különböző sérülések és katasztrófahelyzetek esetén követendő eljárásokat. Jelen Szabályzatban a katasztrófa elhárítási irányelveket foglaljuk össze.

### *6.7.1. Sérült számítási erőforrások, szoftverek és/vagy adatok*

Szolgáltató megnövelt biztonságú eszközökkel rendelkezik, a hardver és/vagy szoftver meghibásodások, illetve az adatvesztés elkerülése érdekében. A Szolgáltatások infrastruktúrájának helyreállíthatóságát Szolgáltató szerződései és saját tartalék eszközei biztosítják. Szolgáltató rendszeres biztonsági mentései és naplózási rendszere segítségével teszi lehetővé az adatok visszaállíthatóságát valamely adattároló eszköz meghibásodásának esetére. Szolgáltató ily módon képes a megelőzően elkészített biztonsági mentései közül a megfelelő működőképes állapotot visszaállítani. Az esetleges hibákról, és a visszaállított állapotokról Szolgáltató jegyzőkönyvet készít.

### *6.7.2. Szolgáltatói egység kulcsának kompromittálódása*

Szolgáltató hivatkozott dokumentumában rendelkezik a szolgáltatói egység magánkulcsának kompromittálódása esetén követendő eljárásokról. A Szolgáltató saját magánkulcsainak kompromittálódása esetén:

- Beszünteti a kompromittálódott kulcs használatát. Visszavonja a kompromittálódott kulcshoz tartozó tanúsítványt.
- Azonnali hatállyal értesíti a Végfelhasználókat jelen Szabályzat 3.1.2. pontja szerint. Az értesítésben jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok és visszavonási állapot információk már nem érvényesek.
- Szükség esetén új tanúsítvánnyal (és hozzá tartozó kulccsal) látja el az Előfizetőket és Aláírókat, a szolgáltatói egységet.
- Kivizsgálja a kompromittálódás körülményeit és megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen.

### *6.7.3. Helyreállítás természeti, vagy egyéb katasztrófát követően*

Szolgáltató a Szolgáltatásokkal kapcsolatos tevékenységeit négy, egymástól fizikailag is nagyobb távolságra elhelyezkedő helyszínen végzi. Szolgáltató kialakított struktúrájára jellemző, hogy:

- rendelkezik elsődleges, és másodlagos helyszínnel is,
- elkülönített biztonsági zónával rendelkezik a kiemelt biztonságú eszközök számára (pl.: HSM),
- ügyfélszolgálati irodája az elsődleges és másodlagos helyszíntől elkülönülő, független egységet képez.

Természeti vagy más katasztrófát követően, illetve Szolgáltató rendszereinek olyan szintű meghibásodásakor, amely az elsődleges rendszeren nem, vagy csak hosszabb kieséssel javítható, Szolgáltató a másodlagos helyszínen is képes szolgáltatásai egy részének beindítására. Ilyen esetekben Szolgáltató az alábbi Szolgáltatások legfeljebb 24 órán belüli elindítását vállalja:

- a tanúsítványtár közzététele,
- a felfüggesztés- és visszavonás-kezelés,
- a visszavonási állapot közzététele.

## 6.8. CA vagy RA leállítás

A Szolgáltató a jogszabályokban előírtaknak megfelelően gondoskodik a szolgáltatásainak megszüntetéséből származó, az Aláírókat, Előfizetőket és az Érintett feleket érintő potenciális zavar minimalizálásáról, továbbá a jogi eljárásokhoz szükséges tanúsítvány nyilvántartások fenntartásáról.

A szolgáltatás megszűnése esetén a Szolgáltató a 2001. évi XXXV. elektronikus aláírás törvény 16. §-a és a 3/2005 IHM rendelet 10. §-a szerint jár el, melyek összefoglalva a következőek:

- A Szolgáltató a szolgáltatásainak befejezése előtt 60 nappal tájékoztatja a Hatóságot (NMHH) az általa kibocsátott érvényes vissza nem vont tanúsítványokban megjelölt Aláíró személyeket, és az Előfizetőket. Az értesítésben megjelöli azt a szolgáltatót, aki az adatok és nyilvántartások kezelését a tevékenység befejezését követően átveszi. Ha ezt nem teszi meg, a Hatóság jelöli ki a szervezetet.
- Szolgáltató a tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést készít. A mentett adatállományokat védi a jogosulatlan módosítástól, illetve biztosítja azt, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá. Biztosítja továbbá, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

A Szolgáltató a bejelentését követően nem bocsát ki új tanúsítványokat.

A Szolgáltató a tevékenységének befejezésre megjelölt időpontot megelőző 20 nappal visszavonja az általa kibocsátott és érvényes tanúsítványokat.
A Szolgáltató a tevékenységének befejezésre megjelölt időpontig eleget tesz a nyilvánosságra hozatali kötelességeinek.

A Szolgáltató megjelöl - egy vele azonos besorolású - szolgáltatót mely átveszi a tanúsítvány visszavonási listákat, a visszavonási állapot nyilvántartásokat (felfüggesztés és visszavonás információkat), a visszavont tanúsítványokkal kapcsolatos minden adatot (naplófájlokat, megőrzési időket), továbbá a visszavont tanúsítványokhoz kapcsolódó személyes adatokat, a nyilvános szabályozási dokumentumokat, valamint az aláírás ellenőrző adatokat. Ezt egy keretszerződés kereteiben teszi meg.

Ha a Szolgáltató ellen felszámolási vagy végelszámolási eljárás indult, haladéktalanul tájékoztatja a Hatóságot e tényről, megnevezve az eljárást lefolytató szervezetet.
A Szolgáltató megszűnését követően megsemmisíti, illetve visszavonja magánkulcsait.
A Szolgáltató megszűnése vagy a szolgáltatási tevékenység abbahagyása esetén a Hatóság törli a hitelesítés-szolgáltatót a nyilvántartásból.

# 7. Műszaki biztonsági ellenőrzés

## 7.1. Kulcspár-generálás és telepítés

A CA-knak számos kérést kell kezelniük:

- végfelhasználói tanúsítvány kiállítás PKCS#10 kérések feltöltése alapján
- végfelhasználói tanúsítvány kiállítás szerveroldalon generált kulcspárok alapján

A CA kulcsa a biztonságos HSM eszközön belül került létrehozásra, a kulcs aktiválásához egyidejűleg egy darab eszköz (chipkártya) és jelszó megadása szükséges. Összesen négy darab chipkártya került létrehozásra, azaz az „n-ből m” jelen esetben „4-ből 1” a hitelesítésnél.

A Szolgáltató által használt kulcspárok az alábbiak:

- a Szolgáltató gyökér hitelesítő egységének kulcsa 4096 bites,
- a Szolgáltató fokozott időbélyegző egységének kulcsa 2048 bites,
- a Szolgáltató operátori kulcsai 2048 bitesek,
- SSL protokollhoz használt kulcsok 2048 bitesek,
- a végfelhasználói tanúsítványokban lévő kulcsok legalább 2048 bitesek.

Az aláíró tanúsítványok aláíró kulcsai közül, melyek biztonságos eszközön generálódnak, és sosem hagyják el a biztonságos környezetet, csak a publikus részt szabad lekérni a PKCS#10 lekérések létrehozásához. Az eredmény egy base64 kódolású tanúsítvány, amely a szerverről PEM vagy DER formátumban tölthető le. A kulcsok a tanúsítványokkal együtt a Szolgáltató által kerülnek feltöltésre az adathordozóra (chipkártya), ez alól az SSL szerver tanúsítványok

képeznek kivételt, ahol PKCS#12 adatként kerülnek átadásra, külön csatornán eljuttatott jelszó segítségével.

A titkosító tanúsítványok titkosító kulcsai a CA szerveren generálódnak, és base64 kódolású tanúsítványként, és különálló kulcsfájlként tárolhatók. Az eredményt a szerverről PKCS#12 fájlként lehet letölteni.

## 7.2. Magánkulcs megsemmisítése

A hitelesítő egység HSM eszközében tárolt magánkulcsok megsemmisítése a Szolgáltató két munkatársának (a rendszergazda és a biztonsági tisztviselő) együttes jelenlétében lehetséges.

A végfelhasználói tanúsítványokban használt magánkulcsok megsemmisítése az Aláíró felelőssége. A Szolgáltató vállalja ügyfélszolgálati irodájában az intelligens kártyán, vagy tokenen lévő magánkulcsok ügyfél előtt történő megsemmisítését.

## 7.3. Alkalmazott eszközök

A Szolgáltató a szolgáltatás nyújtásához (kulcskezelés, tárolás, előállítás) nCipher nShield Connect 500 (nShield F3 500e nC4033E-500N) típusú HSM eszközt használ. Az alkalmazott eszköz förmver verziói: 2.38.4-3 és 2.38.7-3.

A végfelhasználói eszközök kulcspár és tanúsítvány tárolására alkalmas aláírás-létrehozó eszközök, melyek típusa Gemalto ID Classic 300 (korábbi megnevezés: Gemalto TPC IM CC), és CCEAL 4 tanúsítással rendelkeznek. A végfelhasználói eszközök képesek a BALE üzemmódra is, de Szolgáltató jelenleg ALE módban biztosítja az eszközöket.

Szolgáltató által szolgáltatásai során használt elektronikus aláírási termékek az Eat. szerinti megfelelőségi igazolással rendelkeznek.

Szolgáltató által használt algoritmusok megfelelnek a mindenkori törvényeknek, jogszabályoknak és ajánlásoknak. Felhasznált algoritmus SHA256 with RSA, 2048-8192 bites kulcshosszal.

## 7.4. Privát kulcsok védelme és a kriptográfiai modul technikai ellenőrzése

A privát kulcsok egy biztonságos hardveres környezetben (aláíró kulcsok), és szerver adatbázisokban (titkosító kulcsok) tárolódnak.

A kulcsokat tároló adathordozóknak és kriptográfiai moduloknak független biztonsági ellenőrök által készített igazolások közül legalább egy érvényes tanúsítással rendelkeznie kell.

Szolgáltató HSM modulja

- FIPS 140-2 level 3

tanúsítással rendelkezik, mely magyarországi hitelesítő hatóság által felül lett hitelesítve.

A Szolgáltató által az Aláírók részére kiadott végfelhasználói eszközöknek

- Common Criteria EAL4, vagy magasabb tanúsítással kell rendelkezniük.

Amennyiben az Aláíró saját, már meglévő végfelhasználói eszközét kívánja használni, ugyanezeket a tanúsításokat kell tudnia igazolni az eszközzel kapcsolatban.

## 7.5. A kulcspár-kezelés egyéb szempontjai

A publikus kulcsok és a tanúsítványok is archiválva tárolódnak. Ez a rendszeres biztonsági mentési folyamat része.

## 7.6. Aktivációs adatok

Az adathordozókon tárolt, újonnan kiadott tanúsítványokat és kulcsokat jelszó védi. Az adathordozók jelszavát a felhasználó bármikor megváltoztathatja.

## 7.7. Hálózat és számítógép-biztonsági ellenőrzés

Jelen dokumentum ide vonatkozó pontja, illetve belső biztonsági policy szerint történik.

## 7.8. Időbélyegzés

A tanúsítványok és a visszavonási információ (CRL) idő- és dátuminformációkat tartalmaznak. Így az idő és a dátum alá van írva.

# 8. Tanúsítvány-, és CRL-profilok

## 8.1. Tanúsítványprofil

A tanúsítványok profilja az IETF RFC 5280, illetve ETSI TS 102 280 szabványban leírt X509v3-nak felel meg.

| mező/kiterjesztés | tartalom |
|---|---|
| version | kötelező; tanúsítvány változata (v3) |
| serialNumber | kötelező; tanúsítvány sorszáma |
| signature | kötelező; tanúsítvány aláírása<br>(a hatályos törvényi és jogszabályi előírásoknak, illetve a nemzetközi ajánlásoknak megfelelően) |
| issuer | (ld. táblázatok) |
| validity | (ld. táblázatok) |
| subject | (ld. táblázatok) |
| subjectPublicKeyInfo | (ld. táblázatok) |
| extensions | (ld. táblázatok) |

Az alapesettől való eltéréseket az alábbi táblázatok határozzák meg.

### *8.1.1. Természetes személyek tanúsítvány profiljai*

1) Magánszemély fokozott biztonságú tanúsítványa titkosításra, hitelesítésre SSCD/HwSCDev/SwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |
| emailAddress | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az subjectAltName névelemmel) |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| title | opcionális; tanúsítvány tulajdonosának titulusa |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel), vagy Microsoft UPN eleme |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, keyEncipherment, keyAgreement, dataEncipherment) |

| | |
|---|---|
| extKeyUsage | tanúsítvány kibővített kulcshasználata (clientAuth, emailProtection, Microsoft Smartcard Logon) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

2) Magánszemély fokozott biztonságú tanúsítványa letagadhatatlan elektronikus aláírásra SSCD/HwSCDev/SwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |
| emailAddress | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az subjectAltName névelemmel) |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| title | opcionális; tanúsítvány tulajdonosának titulusa |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel) |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

3) Magánszemély fokozott biztonságú álneves tanúsítványa letagadhatatlan elektronikus aláírásra SSCD/HwSCDev/SwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának álneve (esetenként speciális karakterekkel megjelölve az álnév tényét) |
| emailAddress | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az subjectAltName névelemmel) |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |

| | |
|---|---|
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| title | kötelező; a tanúsítvány álneves típusára vonatkozó megjelölés |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel) |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

4) Szervezeti személy fokozott biztonságú tanúsítványa titkosításra hitelesítésre SSCD/HwSCDev/SwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |
| emailAddress | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az subjectAltName névelemmel) |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| title | opcionális; tanúsítvány tulajdonosának titulusa |
| organizationName | tanúsítvány tulajdonosához kapcsolódó szervezet neve |
| organizationalUnitName #1 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| organizationalUnitName #2 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel) , vagy Microsoft UPN eleme |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, keyEncipherment, keyAgreement, dataEncipherment) |
| extKeyUsage | tanúsítvány kibővített kulcshasználata (clientAuth, emailProtection, Microsoft Smartcard Logon) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége |

| | |
|---|---|
| | http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

5) Szervezeti személy fokozott biztonságú tanúsítványa letagadhatatlan elektronikus aláírásra SSCD/HwSCDev/SwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |
| emailAddress | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az subjectAltName névelemmel) |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| title | opcionális; tanúsítvány tulajdonosának titulusa |
| organizationName | tanúsítvány tulajdonosához kapcsolódó szervezet neve |
| organizationalUnitName #1 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| organizationalUnitName #2 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel) |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

6) Szervezeti személy fokozott biztonságú álneves tanúsítványa letagadhatatlan elektronikus aláírásra SSCD/HwSCDev/SwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának álneve (esetenként speciális karakterekkel megjelölve az álnév tényét) |
| emailAddress | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az subjectAltName névelemmel) |

| | |
|---|---|
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| title | kötelező; a tanúsítvány álneves típusára vonatkozó megjelölés |
| organizationName | tanúsítvány tulajdonosához kapcsolódó szervezet neve |
| organizationalUnitName #1 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| organizationalUnitName #2 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel) |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

### *8.1.2. Nem természetes személyek tanúsítvány profiljai*

1) Szervezet fokozott biztonságú tanúsítványa titkosításra, hitelesítésre SSCD/HwSCDev/SwSCDev használatával

| **mező/kiterjesztés** | **tartalom** |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |
| emailAddress | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az subjectAltName névelemmel) |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| organizationName | tanúsítvány tulajdonosához kapcsolódó szervezet neve |
| organizationalUnitName #1 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| organizationalUnitName #2 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel) |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |

| | |
|---|---|
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, keyEncipherment, keyAgreement, dataEncipherment) |
| extKeyUsage | tanúsítvány kibővített kulcshasználata (clientAuth, emailProtection, Microsoft Smartcard Logon) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

2) SSL szerver fokozott biztonságú tanúsítványa SwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| organizationName | tanúsítvány tulajdonosához kapcsolódó szervezet neve |
| organizationalUnitName #1 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| organizationalUnitName #2 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel) |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, keyEncipherment, keyAgreement, dataEncipherment) |
| extKeyUsage | tanúsítvány kibővített kulcshasználata (serverAuth) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

3) Domain Controller szerver fokozott biztonságú tanúsítványa SwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |

| | |
|---|---|
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| organizationName | tanúsítvány tulajdonosához kapcsolódó szervezet neve |
| organizationalUnitName #1 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| organizationalUnitName #2 | tanúsítvány tulajdonosához kapcsolódó szervezeti egység neve |
| subjectAltName | kötelező; tanúsítvány tulajdonosának e-mail címe (megegyezik az emailAddress névelemmel) |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (digitalSignature, keyEncipherment) |
| extKeyUsage | tanúsítvány kibővített kulcshasználata (serverAuth, clientAuth) |
| validity | kötelező; tanúsítvány érvényessége (365 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

### *8.1.3. Szolgáltatók tanúsítvány profiljai*

1) CA tanúsítványa SSCD/HwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (4096 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (CA) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (cRLSign, keyCertSign) |
| validity | kötelező; tanúsítvány érvényessége (5479 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

2) TSA fokozott biztonságú végtanúsítványa SSCD/HwSCDev használatával

| mező/kiterjesztés | tartalom |
|---|---|
| commonName | kötelező; tanúsítvány tulajdonosának neve |
| countryName | kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve |
| localityName | opcionális; tanúsítvány tulajdonosához kapcsolódó település neve |
| subjectPublicKeyInfo | kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit) |
| basicConstraints | kötelező; tanúsítvány típusa (végfelhasználói) |
| keyUsage | kötelező; tanúsítvány kulcshasználata (nonRepudiation) |
| extKeyUsage | tanúsítvány kibővített kulcshasználata (timeStamping) |
| validity | kötelező; tanúsítvány érvényessége (730 nap) |
| cRLDistributionPoints | tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl |
| certificatePolicies | tanúsítványhoz kapcsolódó Hitelesítési rend elérhetősége http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_24206_2_22_1_4.pdf |

## 8.2. CRL-profil

A CRL visszavonási adatok profilja az IETF RFC 5280 szabványban leírt v2 változatnak felel meg.

| mező/kiterjesztés | tartalom |
|---|---|
| version | kötelező; visszavonási adat változata (v2) |
| signature | kötelező; visszavonási adat aláírása<br>(a hatályos törvényi és jogszabályi előírásoknak, illetve a nemzetközi ajánlásoknak megfelelően) |
| issuer | kötelező; visszavonási adat kibocsátója |
| thisUpdate | kötelező; visszavonási adat kibocsátásának dátuma és időpontja |
| nextUpdate | visszavonási adat következő kibocsátásának dátuma és időpontja (thisUpdate + 24 óra) |
| revokedCertificates | kötelező; visszavonási adaton szereplő tanúsítványok sorszáma, a visszavonás dátuma és időpontja, a visszavonás oka |

### 8.3. Időbélyeg profilok

Az időbélyegek profilja az IETF RFC 3161 szabványban leírt v1 változatnak felel meg.

| mező/kiterjesztés | tartalom |
|---|---|
| version | kötelező; időbélyeg változata (v1) |
| policy | kötelező; időbélyegzéshez kapcsolódó Időbélyegzési Rend azonosítója (1.3.6.1.4.1.24206.3.22.1.2) |
| messageImprint | kötelező; időbélyeghez kapcsolódó lenyomatképző algoritmus azonosítója és lenyomat |
| serialNumber | kötelező; időbélyeg sorszáma |
| genTime | kötelező; időbélyeg kibocsátásának dátuma és időpontja |

## 9. Megfelelőségi vizsgálat és egyéb felmérések (audit)

A Szolgáltató rendszerét, folyamatait megfelelő időközönként felül kell vizsgálni. A vizsgálatok során független auditorok ellenőrzik az alábbi elemek megfelelőségét:

- a végfelhasználói tanúsítványok aláírására használt biztonságos eszközöknél: nShield Connect 500 (Part Code: NH2033) netHSM
- az előfizetők számára kibocsátott aláírás-létrehozó eszközöknél (pl. intelligens kártyáknál)
- a végfelhasználói és szolgáltatói tanúsítványok kezelésénél.

### 9.1. Ellenőrzés gyakorisága vagy körülményei

A rendszer és a folyamatok felülvizsgálatát kétévente legalább 1 alkalommal el kell végezni. A felülvizsgálatot végző szervezet független a Szolgáltatótól.

A rendszer ellenőrzése során végre kell hajtani a hitelesítés-szolgáltatás nyújtásához kapcsolódó alapvető funkciókat (pl. tanúsítvány kiadása).

A folyamatok ellenőrzése során meg kell vizsgálni, hogy azok a felügyeleti szerv számára benyújtott, illetve egyéb belső szabályzatok alapján zajlanak.

Az auditorok függetlenségére, illetve a belső szervezeti felépítésre vonatkozólag az alábbi jogi megkötések érvényesek:

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

7. § A szolgáltató köteles biztosítani, hogy a 2. § a) pontja szerinti bizalmi munkakörök közül:
   a) a biztonsági tisztviselő nem töltheti be a független rendszervizsgáló munkakört;
   b) az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő, illetve a független rendszervizsgáló feladatait.

## 9.2. Ellenőr személyazonossága, képesítése

A felülvizsgálatokat külső, független fél végzi el. Az auditorra vonatkozólag léteznek jogi megkötések, amelyeknek megfelel az eljárás:

- 2001. évi XXXV. törvény az elektronikus aláírásról

  24. §
  (1) Aláíró eszközök és egyéb elektronikus aláírási termékek tanúsítására jogosult tanúsító szervezetként a miniszter azokat a természetes személyeket és szervezeteket jelöli ki, amelyek erre vonatkozó kérelmet nyújtanak be, és rendelkeznek az aláíró eszközök és egyéb elektronikus aláírási termékek tanúsításához szükséges szakértelemmel.
  (2) A kijelölt, illetőleg a laboratóriumok, a tanúsító és az ellenőrző szervezetek akkreditálásáról szóló 1995. évi XXIX. törvény szerinti szakmai akkreditáló bizottságok által az (1) bekezdés szerinti tevékenységre akkreditált szervezeteket a Hatóság nyilvántartásba veszi.
  (3) Tanúsító szervezet az aláíró eszközök és az egyéb elektronikus aláírási termékek tanúsítását külső befolyástól mentesen köteles végezni.
  (4) A kijelölést, illetve az akkreditációt vissza kell vonni és a tanúsító szervezeteket törölni kell a nyilvántartásból, ha nem rendelkeznek a szükséges feltételekkel, vagy ha a tanúsító szervezet nem a jogszabályoknak megfelelően végzi tevékenységét. Ha a Hatóság a (2) bekezdés szerinti szervezet tekintetében észleli e jelenségeket, jelzéssel él a kijelölő miniszter, illetőleg a szakmai akkreditáló bizottság felé.
  (5) A nyilvántartásból való törlés nem érinti a tanúsító szervezet által a törlést megelőzően kiadott igazolások érvényességét.

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

A külső felülvizsgálat mellett belső auditor is ki van jelölve, amely ellenőrzése alatt tartja a folyamatokat, észrevételeket tesz, amelyek alapján javító intézkedéseket hajtanak végre.

## 9.3. Ellenőr viszonya a felmért egységhez

A Szolgáltató felülvizsgálatát végző szervezetek függetlenek a Szolgáltatótól, és tevékenységét befolyástól mentesen végzik. A felülvizsgálatot végző szervezetek nem rendelkeznek tulajdonrésszel vagy érdekeltséggel a Szolgáltatóban, és a Szolgáltató nem tulajdonosa közvetlenül vagy közvetve a felülvizsgálatot végző szervezeteknek. A felülvizsgálatot végző szervezetek díjazása nem függ a tanúsítás tett megállapításaitól.

## 9.4. Az ellenőrzés által lefedett témakörök

A felülvizsgálat kiterjed a rendszerre és a folyamatokra egyaránt. A rendszernek képesnek kell lennie az alapvető hitelesítés-szolgáltatói folyamatok végrehajtására. A folyamatoknak meg kell felelnie a szabályzatokban leírtaknak, amelyek a felügyeleti szerv számára benyújtásra kerültek.

A rendszer ellenőrzése során végre kell hajtani az alábbi feladatokat:

- a rendszerek indítása
- a rendszerek leállítása
- a tanúsítványok kiadása
- a tanúsítványok és kulcsok kimentése
- az adathordozón tárolt kulcsok használata
- a tanúsítványok exportálása
- a tanúsítványok visszavonása
- a CRL soron kívüli kiadása

A folyamatok ellenőrzése során meg kell vizsgálni az alábbi dokumentumokat:

- Általános Szerződési Feltételek Fokozott biztonságú, nem minősített, elektronikus aláíráshoz kapcsolódó, valamint időbélyegzés szolgáltatások igénybevételéhez
- Szolgáltatási Szabályzat Fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatásokhoz és nem-minősített időbélyegzés szolgáltatáshoz
- Hitelesítési Rend Fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatásokhoz
- Időbélyegzési Rend Fokozott biztonságú időbélyegzés-szolgáltatásokhoz
- Helyreállítási terv rendkívüli üzemhelyzetek esetén fokozott biztonságú hitelesítés- és időbélyegzés-szolgáltatásokhoz

- Biztonsági mentési és visszaállítási eljárás elektronikus aláírás szolgáltatásokhoz
- Informatikai Biztonsági Szabályzat (IBSz)
- Bizalmi munkakörök
- Hálózati beállítások
- Esetleges eszköz megfelelőségi tanúsítványok

### 9.5. Teendők hiányosságok esetén

A felülvizsgálat eredményéről készített jelentést a független auditorok átadják a Szolgáltató felelős vezetőjének, aki kiértékeli azokat, szükség esetén javító intézkedéseket rendel el.

### 9.6. Az eredmények kommunikálása

A felülvizsgálati eredményekről a Szolgáltató tájékoztatja a felügyeleti szervet, illetve az esetlegesen módosult szabályzatokat publikálja.

## 10. Egyéb üzleti és jogi kérdések

### 10.1. Díjak

A mindenkor érvényes Szolgáltatások díjait a Szolgáltató saját internetes oldalán (http://www.digitoll.co.hu/, és http://ds.digitoll.co.hu/) és ügyfélszolgálati irodájában nyomtatott formában teszi közzé.

A Szolgáltató az árlistát módosíthatja és a módosítást annak a hatályba lépése előtt 30 nappal a honlapján közzéteszi. Az előre kifizetett Szolgáltatások árát a módosítás nem érinti. Az díjak kifizetésével és visszatérítésével kapcsolatos rendelkezéseket a Szerződés és mellékletei – különösen az ÁSzF – tartalmazzák.

A mindenkori árlistától való eltérés kizárólag csak a Szolgáltatóval kötött külön megállapodással, illetve a Szolgáltató által meghirdetett akciókkal lehetséges.

A Szolgáltató Szolgáltatásait csak a vele szerződéses viszonyban levő felek vehetik igénybe.

## 10.2. Jogok, kötelezettségek

### *10.2.1. A Szolgáltató kötelezettségei*

A Szolgáltató (és szervezetei) köteles a saját mindenkori szabályzatainak (ÁSzF, jelen Szabályzat, Hitelesítési rend, Időbélyegzési rend, működési szabályzatok, Szerződés) megfelelően a Szolgáltatásait nyújtani, megfelelve a mindenkor magyar jogrendszernek és törvényeknek.

A Szolgáltató kötelezettséget vállal, hogy minden lehetséges és törvényes eszközzel biztosítja a Szolgáltatások problémamentes működését.

A Szolgáltató köteles az Előfizetőt, az igénylés előtt pontosan tájékoztatni, az ügymenetekről, és elérhetővé tenni a nyilvános szabályzatait.

A Szolgáltató mindenkor az Előfizető által az elektronikus tanúsítvány-igénylésben benyújtott, a Regisztrációs szervezet által jelen Szolgáltatási szabályzatban és Hitelesítési Rendben meghatározott módon ellenőrzött adatok alapján bocsátja ki a tanúsítványt, az adatokon változtatást nem alkalmazhat. Az Előfizető általi – tanúsítványban foglalt adatok változására vonatkozó – bejelentés automatikusan a tanúsítvány visszavonását vonja maga után. A módosított adatokkal kibocsátott tanúsítvány új tanúsítványnak minősül.

A Szolgáltató köteles tájékoztatni az Előfizetőt:

- a Szolgáltatásaira irányadó jogszabályváltozásokról,
- bármely szabályzatainak (ÁSzF, jelen Szabályzat, Hitelesítési rend, Időbélyegzési rend, Szerződés) megváltoztatásáról,
- bármely döntésről, ami érinti az Előfizetőt, vagy annak igénybevett Szolgáltatásait.

A Szolgáltató nyilvántartást vezet minden eseményről, változásról, és az előfizetői adatokról.

A Szolgáltató jogait, kötelezettségeit és felelősségeit az ÁSzF ide vonatkozó pontja is részletezi.

### *10.2.2. A végfelhasználók jogai és kötelezettségei*

Az Előfizető jogosult a Szolgáltatások igénybevételéhez, a szabályzatok és a Szerződés szerint, ha azok igénybevételéhez a Szerződés rendelkezéseinek megfelelő Szolgáltatásokkal kapcsolatos díjakat határidőre a Szolgáltatónak megfizette.

Az Előfizető jogosult a Szerződésben meghatározott tanúsítványok visszavonását, felfüggesztését, visszaállítását kérni.

Az Előfizető jogosult az Aláíró(k) adatait megváltoztatni, és törölni, új Aláíróval bővíteni az Aláíró(k) listáját. Az Előfizetőhöz tartozó Aláírók jogait a jelen Szabályzat tartalmazza.

Az Előfizető jogosult indoklás nélkül betekinteni a róla nyilvántartott adatokba, Szolgáltató ügyfélszolgálati irodájában, nyitvatartási időben.

Az Előfizető és/vagy Aláíró tudomásul veszi, hogy a magán kulcsukkal készített elektronikus aláírás a saját elektronikus aláírásának minősül, és viseli ennek jogkövetkezményeit.

Az Előfizető és/vagy Aláíró köteles a Szolgáltatásokat kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a jelen Szabályzatban és a hozzá kapcsolódó egyéb szabályzatokban foglaltaknak megfelelően használni.

A Szolgáltatás igénybevételéhez az Előfizető és/vagy Aláíró kötelessége, hogy megismerje, elfogadja és betartsa a Szolgáltató szabályzatait (ÁSzF, jelen Szabályzat, Hitelesítési rend, Időbélyegzési Rend, Szerződés).

Az Előfizető köteles a Szerződésben meghatározott díjakat megfizetni a Szolgáltatások igénybevételéhez, a meghatározott határidőn belül. Ha ezt nem teszi, köteles vállalni érte a felelősséget, késedelmi díj fizetésére kötelezhető. Ennek értéke és feltételei a Szerződésben van rögzítve.

Az Előfizető és/vagy Aláíró köteles a valóságnak megfelelő adatokat hiánytalanul szolgáltatni a Szolgáltatónak a Szolgáltatások igénylése és teljesítése során. Amennyiben kiderül, hogy a benyújtott adatok nem felelnek meg a valóságnak, a Szolgáltatónak joga van felülbírálni az Előfizető és/vagy Aláíró Szerződését, felszólíthat javításra, illetve azonnali hatállyal felbonthatja a Szerződést.

Az Előfizető és/vagy Aláíró köteles minden olyan változást bejelenteni, mely érinti a Szerződést, vagy bármely dolgot, ami a Szolgáltatással kapcsolatos, a bejelentést írásban teszi meg, és vállalja az esetleges átírási költségeket.

Az Érintett fél kötelessége és felelőssége kiterjed a tanúsítványok elfogadása során tanúsított körültekintő eljárásért és általában a kötelezettségei betartásáért. Az Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a

tanúsítvány érvényességének és hatályosságának ellenőrzése során nem az irányadó jogszabályok és a tőle elvárható gondosság szerint járt el.

## 10.3. Anyagi felelősség - Felelősségek

A Szolgáltató a vele szerződéses jogviszonyban álló felekkel szemben az általa okozott, az EAT 15 § (1) bekezdés szerinti károkért vállal felelősséget.

Ennek biztosítása érdekében Szolgáltató felelősségbiztosítással rendelkezik a 3/2005 IHM rendelet 11 § (3) bekezdése szerinti mértékben, jelen Szabályzat 10.3.3 pontja szerint.

A Szolgáltató kizárja felelősségét, ha az Előfizető és/vagy Aláírók nem a nyilvános szabályzatokban, Szerződésben meghatározott módon, vagy jogellenesen járnak el.

### *10.3.1. A Szolgáltató általános felelőssége és felelősségének korlátai*

A Szolgáltató felelősséget vállal a szabályzataiban leírt eljárásoknak való megfelelőségért.

A Szolgáltató a vele szerződéses jogviszonyban álló felekkel (Előfizető, Aláíró) szemben a Ptk. szerződésszegésért való felelősség szabályai szerint felelős és a vele szerződéses jogviszonyban nem álló harmadik féllel (Érintett fél) szemben a Ptk. szerződésen kívüli károkozásról szóló szabályai (Ptk. 519 §) szerint felelős.

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az Előfizetővel és/vagy Aláíróval megkötött Szerződésekben rögzített korlátozásokkal kártérítést fizet.

A Szolgáltató felelős a kötelezettségei megszegéséért.

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy az Előfizető, Aláíró vagy az Érintett Fél a tanúsítványok felhasználása és ellenőrzése során nem a hatályos jogszabályoknak, illetve a Szolgáltató szabályzatainak megfelelően járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató nem felelős az abból adódó károkért, amikor valamely külső, elháríthatatlan esemény miatt a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.

A regisztrációs eljárás részeként a Szolgáltató közhiteles adatbázissal végez adategyeztetést, a tanúsítványok kibocsátását megelőzően. A Szolgáltató nem vállal felelősséget e közhiteles adatbázis által szolgáltatott információk pontatlanságából eredő károkért.

Miután az aláírás-létrehozó adat az Előfizető és/vagy Aláíró(k) birtokába kerül, a Szolgáltató nem vállal semmilyen felelősséget:

- az aláírás-létrehozó eszköz (továbbiakban: ALE), és annak használatához szükséges titkos kódok, jelszavak és maga az aláírás-létrehozó adat védelméért,
- az ALE és az aláírás-létrehozó adat segítségével létrehozott aláírásokért. Kivéve, ha az Előfizető jelzi - a Szolgáltatási szabályzat szerinti módon - az aláírás-létrehozó adat kompromittálódását, vagy kéri a tanúsítvány felfüggesztését, vagy visszavonását. A Szolgáltató akkor felelős, ha a Szabályzatban meghatározott időintervallumon belül nem hagyja jóvá, vagy viszi véghez a visszavonási, vagy felfüggesztési folyamatot.

A Szolgáltató felelőssége az EAT és a kapcsolódó jogszabályok szerint kiadott tanúsítvány hitelességéig terjed, adott pénzügyi és idő intervallumban. Ha az elektronikusan aláírt adaton vagy dokumentumon hitelesített elektronikus aláírás szerepel és az aláírás ellenőrzésének eredményéből más nem következik, vélelmezni kell, hogy a dokumentum tartalma az aláírás óta nem változott.

A Szolgáltatót semmilyen felelősség nem terheli, Szerződésben feltüntetett alkalmazhatósági korlátok be nem tartatása miatt bekövetkezett káreseménnyel kapcsolatban, valamint az Aláírók magánkulcsaival, illetve aláíró eszközeivel kapcsolatos tevékenységeiért, és az Érintett felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért.

A Szolgáltató kötelezettségeit és felelősségeit az ÁSzF ide vonatkozó pontja is részletezi.

### *10.3.2. A Szolgáltató pénzügyi felelőssége*

A Szolgáltató a magyar jogszabályozás és törvények szerint, az Előfizetővel és/vagy Aláíróval szemben a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással vagy időbélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal okozott kárért, ha megszegte kötelességeit.

A Szolgáltató a kártérítés felső határát az EAT 6.§ szerint tanúsítványonként és káreseményenként külön és összességében is korlátozhatja. Az egy alkalommal vállalható legmagasabb kötelezettség értéke a Szolgáltató által kibocsátott tanúsítványoknál a tanúsítványban feltüntetett összeg. Ezen korlátokat meghaladó ügyletekben kibocsátott és

aláírt elektronikus dokumentumokból származó követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.

A Szolgáltató pénzügyi felelősségével kapcsolatos további részleteket az ÁSzF ide vonatkozó pontja tartalmazza.

### *10.3.3. Felelősségbiztosítás*

A Szolgáltató a megbízhatósága biztosítása érdekében felelősségbiztosítással rendelkezik, mely kiterjed a Szolgáltató által a szolgáltatások nyújtásával összefüggésben okozott valamennyi kárra.

A felelősségbiztosítási szerződés egy biztosítási esemény vonatkozásában káreseményenként fokozott biztonságú, nem minősített szolgáltatások esetében a Szerződésben vállalt felelősségvállalási érték legalább háromszorosáig nyújt fedezetet az összes károsultnak okozott károkra.

A felelősségvállalás tanúsítványonkénti mértékét a Szerződés tartalmazza, de az egy alkalommal vállalható legmagasabb kötelezettség értéke 6 000 000 magyar forint.

Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül. A vonatkozó jogszabály szerint, ha a több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

### *10.3.4. A Végfelhasználók felelőssége*

Az Előfizető és Aláíró felelős a Szolgáltató szabályzatai és a Szerződés betartásáért.

Az Előfizető és Aláíró felelős a kezdeti regisztráció keretében megadott adatai valódiságáért, pontosságáért és érvényességéért.

Az Előfizető és/vagy Aláíró felelős az adataiban bekövetkezett változások bejelentéséért.

Az Előfizető felelősséget vállal a Szerződésben megnevezett Aláíró(k), adatainak valósságáért és azok megváltozását követi és tájékoztatja erről a Szolgáltatót is.

A magánkulcs védelme és az aláírás készítése kizárólag az Előfizető és/vagy Aláíró felelőssége, így annak kompromittálódása, vagy jogszerűtlen használata esetén a Szolgáltatót semmilyen felelősség nem terheli.

Az Előfizető felelős a Szerződésben rögzített szolgáltatások díjainak kifizetéséért, azaz a számlákon szereplő összegek megjelölt időpontig történő kifizetéséért. Az ettől való eltérés csak írásos megállapodás keretében történhet.

Az Érintett fél kötelessége és felelőssége kiterjed a tanúsítványok elfogadása során tanúsított körültekintő eljárásért és általában a kötelezettségei betartásáért. Az Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem az irányadó jogszabályok és a tőle elvárható gondosság szerint járt el.

Az Előfizető és/vagy aláíró felelősséget vállal kötelezettségei betartásáért.

Az Előfizető kötelezettségeit és felelősségeit az ÁSzF ide vonatkozó pontja is részletezi.

#### *10.3.5. Szolgáltatóval szembeni kártérítés*

Az Előfizető és/vagy Aláíró kártérítési felelősséggel tartoznak a Szolgáltatónak azokért a veszteségekért és károkért, amelyeket kötelezettségeik, felelősségeik és a rájuk vonatkozó ajánlások be nem tartásával okoznak számára.

A Szolgáltató a vagyoni felelősségre vonhatóság, a Szolgáltató által okozott károkkal kapcsolatos saját felelősség, illetve a Szolgáltatónak okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a napló állományok sértetlenségét és hitelességét, valamint hosszú távon is megőrzi (archiválja) a naplóadatokat.

## 10.4. Üzleti információ titkossága

A Szolgáltató kötelezettséget vállal arra, hogy a Szolgáltatásai során tudomására jutott üzleti titkokat a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvényben foglaltak szerint megőrzi.

## 10.5. Adatkezelés, bizalmasság

A Szolgáltató az Előfizető és Aláíró adatait a jogszabályoknak megfelelően kezeli. Az Előfizető és Aláíró a tanúsítvány igénylésével járul hozzá ahhoz, hogy a személyes adatait a Szolgáltató Adatvédelmi nyilatkozatának megfelelő módon tárolja és kezelje. Az Szolgáltató kibocsátott tanúsítványok és a bennük található személyes adatok nyilvánosságra hozatala csak az Előfizető és/vagy Aláíró előzetes írásos hozzájárulásával történhet meg. A hozzájárulásukat a regisztrációs folyamat részeként tehetik meg. A Szolgáltató az Előfizetői és Aláíró személyes adatait kizárólag csak a szolgáltatásaival összefüggésben használja fel.

### *10.5.1. Adatkezelési szabályok, titoktartási kötelezettség*

Az ÁSzF ide vonatkozó pontja és a Szolgáltató Adatvédelmi nyilatkozata szerint.

### *10.5.2. Adatok nyilvánosságra hozatala*

A tanúsítványba megjelenő adatok nyilvánosságra hozatala és közzététele, jelen Szabályzat ide vonatkozó pontjában van részletezve.

### *10.5.3. Bizalmas jellegű információk*

A Szolgáltató bizalmas információnak tekinti azokat az előfizetői és aláírói adatokat melyek az általa kibocsátott tanúsítványban nem szerepelnek.

A Szolgáltató bizalmasnak nyilvánítja a saját nem nyilvános dokumentumait, vizsgálati és tesztadatait.

### *10.5.4. Nem bizalmas jellegű információk*

A Szolgáltató nem bizalmas információnak tekinti azokat az előfizetői és aláírói adatokat, melyek az Előfizető és Aláíró engedélye alapján nyilvánosként kezelhet.

A Szolgáltató nem bizalmas információnak tekinti a jogszabályok által meghatározott szabályzatokat (jelen Szabályzat, Hitelesítési rend, Időbélyegzési rend), illetve az általa meghatározott egyéb szabályzatokat, nyilatkozatokat, felhasználói segédleteket és a visszavonási listákat (CRL).

A Szolgáltató nem bizalmas jellegű információként kezeli a tanúsítványtárban elhelyezett azon tanúsítványokat, amelyek nyilvánosságra hozatalát az Előfizető engedélyezte.

A Szolgáltató az általa kibocsátott tanúsítványok visszavonását és felfüggesztését a tanúsítvány visszavonási listában teszi közzé, a tanúsítvány adatainak jelölésével.

## 10.6. Személyi adatok bizalmas kezelése

A Szolgáltató kötelezettséget vállal arra, hogy a hitelesítés-szolgáltatás során tudomására jutott személyes adatokat a 2011. évi CXII. törvényben foglaltak szerint megőrzi.

A Szolgáltató a Szerződés keretében a Szolgáltatások nyújtása, illetve igénybevétele során tudomására jutott adatokat, információkat – jogszabályi kötelezettséget, hatósági, kormányzati, illetve bírósági kötelezést nem számítva – harmadik személynek kizárólag az érintett személyek írásbeli beleegyezésével adhatják át.

A Szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése céljából, illetőleg nemzetbiztonsági érdekből az Eat. 11. §-ának (2) bekezdésében meghatározott esetekben és adatokra vonatkozóan a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak díjmentesen adatokat továbbíthat. Az adatátadás tényét rögzíteni kell, az adatátadásról Szolgáltató az aláírót nem tájékoztathatja.

## 10.7. Szellemi tulajdonjogok

A Szolgáltató szabályzatai, szerződéses feltételei, dokumentumai, CRL listái a Szolgáltató tulajdonát képezik.

A Szolgáltató által kibocsátott tanúsítványok és az azoknak megfelelő kulcspárok tulajdonosai az Előfizetők, teljes jogú felhasználója pedig az Aláírók, tekintet nélkül arra a fizikai közegre, amelyek tárolják és védik a kulcsokat. A Szolgáltató a szabályzatokban egyezetett módon kezelheti a tanúsítványokat.

## 10.8. Garanciák jogi nyilatkozatai

A Szolgáltató kötelezettséget vállal, hogy minden lehetséges és törvényes eszközzel biztosítja a Szolgáltatás problémamentes működését, betartva a saját biztonsági és működési szabályzatait.

A Szolgáltató a vele szerződéses jogviszonyban álló felekkel szemben az általa okozott, az EAT 15 § (1) bekezdés szerinti károkért vállal felelősséget.

A Szolgáltató a kárt azt követően téríti meg, miután a kártérítési igény elbírálásához szükséges, valamint a Szolgáltató felelősségét, a kár időpontját és összegét bizonyító valamennyi dokumentum a rendelkezésre áll.

A Szolgáltató kizárja felelősségét, ha az Előfizető vagy Aláírók nem a Szerződésben vagy ahhoz tartozó egyéb szabályzatokban meghatározott módon, vagy jogellenesen járnak el.

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért fizetendő kártérítést (a hatályos jogszabályokkal összhangban) korlátozhatja a vele szerződéses jogviszonyban álló ügyfelekkel szemben. A korlátozás mértéke az Előfizető által választott díjcsomagtól függően eltérő lehet; a korlátozás pontos összegét a Szerződés tartalmazhatja. A kártérítés korlátozása kiterjedhet vagyoni és nem vagyoni kárra, az elmaradt haszonra, költségekre (a veszteségek és károk minden típusára), amely a Szolgáltató hibájából ered. A Szolgáltató kárfelelősségének esetleges korlátozása a Szolgáltatások díjából biztosított kedvezményekre tekintettel, a biztosított kedvezményekhez mérten, azzal arányos módon kerülhet megállapításra. Az élet és testi épségben okozott károkra a felelősség nem terjed ki.

A Szolgáltató kizárja felelősségét, ha az aláírás ellenőrzés lépései a szabályzatokban meghatározott módon bármi okból – beleértve a Szolgáltatónál keletkező előre bejelentett üzemeltetési és menedzselési problémát is – nem hajthatóak végre az aláírás ellenőrzésének időpontjában, és az elektronikus aláírás, illetve az aláírással ellátott dokumentum az aláírás érintett fele által ennek ellenére elfogadásra kerül.

A Szolgáltatót semmilyen felelősség nem terheli, a szerződésben és nyilvános szabályzataiban feltüntetett alkalmazhatósági korlátok be nem tartatása miatt bekövetkezett káresemény miatt.

A Szolgáltató a Szolgáltatás egy részét képező eszközök működéséért és minőségéért nem vállalja a felelősséget, azok garanciája az adott gyártótól függ.

## 10.9. A felelősség korlátai

Az anyagi felelősség mértéke az adott tanúsítvány fajtától függ. Ezt az értéket a Szerződés tartalmazza.

## 10.10. Érvényesség, módosítás

### *10.10.1. A Szabályzat érvényessége*

Jelen Szabályzat visszavonásig, vagy újabb verzió hatályba lépéséig érvényes.

### *10.10.2. Érvénytelenség, fennmaradás*

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

A Szabályzat 10. fejezete érvényben marad a Szabályzat hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, melyet a Szolgáltató a Szabályzat hatálya alatt bocsátott ki.

### *10.10.3. A Szabályzat értelmezése*

A Szabályzat a PKI közösség kötelezettségét, felelősségét és jogát tartalmazza. Kivétel ez alól az Érintett Fél, kinek részére kötelezettséget nem, csak ajánlást és felelősséget fogalmaz meg.

A Szabályzat egyetlen pontja sem értelmezhető a jelen dokumentumban foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében.

Jelen Szabályzat magyarul íródott, és a magyar nyelv szabályai szerint kell értelmezni.

## 10.11. Egyedi értesítések és kommunikáció a résztvevőkkel - Felek közötti kommunikáció

A Szolgáltató az aláírók illetve az Előfizetők részére ügyfélszolgálati tevékenységet nyújt.
Az ügyfélszolgálat elérhetőségét a szolgáltató jelen Szabályzat 1.1. pontjában és internetes oldalán közzéteszi: http://ds.digitoll.co.hu/.

Az ügyfélszolgálati iroda minden munkanap 8:30-16:00 óra között érhető el. A Szolgáltató Visszavonási ügyeletet üzemeltet minden nap 0-24 órában a jelen Szabályzat 1.1. pontjában megadott telefonszámon.

Az Előfizető a reklamáció illetve a hiba bejelentését írásban teheti meg, a Szolgáltató ügyfélszolgálatánál személyesen átadva, postai úton, vagy elektronikus formában elektronikusan aláírva.

A Szolgáltató minden tevékenységével kapcsolatos panaszt, reklamációt és hibabejelentést nyilvántartásba vesz. A nyilvántartásba vett panaszokat a jogi szabályozásnak megfelelően 30 napon belül kivizsgálja és annak eredményéről a bejelentőt tájékoztatja.

A számlareklamációkkal kapcsolatos feltételeket az ÁSzF tartalmazza.

## 10.12. Módosítások

### *10.12.1. A Szabályzat módosítása*

Jelen Szabályzatot a Szolgáltató egyoldalúan módosíthatja. A módosításról a Szabályzat hatályba lépése előtt 30 nappal tájékozatja az Előfizetőit. Kivétel ez alól azon módosítások, melyek a szolgáltatások biztonsági szintjét, felhasználhatóságát nem módosítják (ilyenek tipikusan a helyesírási hibák, formai változtatások, különböző kapcsolatadatok) együttesen kerülnek módosításra és értesítésre. Azok az Előfizetők, akik a módosítást nem fogadják el, jogosultak a hatálybalépést követően 15 napon belül, 15 napos felmondási idővel az Szerződést felmondani. A Szerződés felmondása egyben a kiadott tanúsítvány iránti visszavonási kérelemnek is tekintendő, és a Szolgáltató jogosult a tanúsítványt nyilvántartásából törölni. Ebben az esetben a Szolgáltató az Előfizető által már befizetett díjakat nem köteles visszatéríteni. Az Előfizető vállalja a visszavonással kapcsolatban felmerülő költségeket.

Minden szabályzat egyedi azonosítóval rendelkezik (OID, verziószám).

A Szolgáltató felügyeleti szerve az NMHH minden esetben megvizsgálja a módosított Szabályzat jogszabályi megfelelősségét majd nyilvántartásba veszi. A Szabályzat csak írott és hitelesített formában módosítható, a NMHH által vezetett szabályzat-nyilvántartásban való átvezetés mellett.

Az új verziószámmal ellátott Szabályzat hatálybalépésével egyidejűleg, az azt megelőző Szabályzat hatálya visszavonásra kerül, érvényét veszti.

## 10.13. Rendelkezések a viták rendezéséről

A Szolgáltató és Előfizetői (Felek) kölcsönösen megállapodnak abban, hogy a Szerződésből eredő jogvitáikat mindenkor megkísérlik békés úton tárgyalások útján rendezni.

Amennyiben a Felek közötti egyeztetés valamelyik fél által kezdeményezetett egyeztetés napjától számított 30 napon belül nem vezet eredményre, arra az esetre a Felek értékhatártól függően kölcsönösen alávetik magukat a Fővárosi Bíróság / PKKB kizárólagos illetékességének.

A Szerződésben nem szabályozott kérdésekben a mindenkor hatályos magyar jogszabályok rendelkezései irányadók, különös tekintettel a Polgári Törvénykönyv, EAT, illetve az adatvédelmi jogszabályok rendelkezései.

A Szolgáltató tevékenységével kapcsolatos kifogásokat és panaszokat Szolgáltató elérhetőségein lehet megtenni.

A Szolgáltatásokkal kapcsolatos bármely vitás kérdés vagy panasz felmerülése esetén a vita jogi útra terelése előtt az Előfizetőnek és/vagy Aláírónak kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően.

Az jogviták esetén követendő eljárás további részleteit az ÁSZF ide vonatkozó fejezete tartalmazza.

## 10.14. Jogi szabályozás

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők. A legfontosabb jogszabályok felsorolását az ÁSZF ide vonatkozó pontja tartalmazza.

A legfontosabb jogszabályok:

- 2001. évi XXXV. törvény az elektronikus aláírásról (EAT)
- 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 aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelmények

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

## 10.15. Megfelelés az alkalmazandó törvényeknek

A Szolgáltató köteles a saját mindenkori szabályzatainak (ÁSzF, Szolgáltatási szabályzat, Hitelesítési Rend, Időbélyegzési Rend, működési szabályzatok, Szolgáltatási szerződés) megfelelően a Szolgáltatásait nyújtani, megfelelve a mindenkori magyar jogrendszernek és törvényeknek.

A Szolgáltató kötelezettséget vállal, hogy minden lehetséges és törvényes eszközzel biztosítja a Szolgáltatás problémamentes működését.

## 10.16. Vis major

A Szolgáltató és előfizetői (Felek) Szolgáltatásokra kötendő szerződéseire vonatkozóan a "vis major" a Felek érdekkörén kívül álló olyan nem látható eseményt jelenti, amely a Szerződés megkötése után következik be, annak ésszerű teljesítését akadályozza, a Felek ellenőrzésén kívülálló, általuk elháríthatatlan és nem látható előre. Ebben az esetben a Felek mentesülnek szerződésszegésük jogkövetkezményei alól, ha a szerződésszegés "vis major" miatt következett be. "Vis major" esetében Felek legkésőbb 5 napon belül írásban értesítik egymást az ilyen késedelem okairól.

## 10.17. Felek közötti kommunikáció

### *10.17.1. Általános kommunikáció*

A Szolgáltató a Szolgáltatásairól tájékoztatás nyújthat telefonon, írásban illetve az internetes oldalán.

1124. Budapest, Stromfeld Aurél út 9.
Tel.: +361 567 8912
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu


A Szolgáltató az Előfizetőket és/vagy Aláírókat írásban tájékoztatja az esetleges módosításokról, változásokról és egyéb információkról. Ezt megteheti írásban (elektronikusan vagy postai úton) illetve közzététellel.

Az Előfizető Szolgáltatóval való kommunikációja történhet írásban aláírva (elektronikusan vagy postai úton) vagy személyesen, kivétel ez alól a tanúsítvány felfüggesztésének kérelme, ami történhet telefonon is.