Digitoll Informatikai és Szolgáltató Kft.
1124. Budapest, Stromfeld A. út 9.
Tel.: +361 487 9900
Fax: +361 487 9901
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

Hitelesítési Rend

Fokozott biztonságú elektronikus aláíráshoz kapcsolódó
hitelesítés-szolgáltatásokhoz

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.24206.2.16.2
Verziószám: 1.2
Jóváhagyta: Németh Viktor Péter
Jóváhagyás dátuma: 2011. 07.06.
Hatályba lépés dátuma: 2011.07.10

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat	2011.05.10.	Németh Ágnes Krisztina Németh Viktor Péter
1.1	Módosítás a NMHH észrevételeinek megfelelően	2011.07.10	Németh Ágnes Krisztina Németh Viktor Péter
1.2	Technikai paraméter változások az NMHH észrevételeinek megfelelően. A regisztrációs eljárás során az NMHH által nyilvántartásba vett változat.	2011.07.10	Németh Ágnes Krisztina Németh Viktor Péter

Tartalomjegyzék

1. Általános információ 7
1.1. Szolgáltató adatai 7
2. Bevezetés 8
2.1. A Szabályzat hatálya 8
2.1.1. Időbeli hatálya 8
2.1.2. Személyi hatálya 8
2.2. Dokumentum név és azonosító 8
2.3. PKI résztvevők 9
2.4. Hitelesítő hatóság - CA (Certification Authority) 9
2.5. Regisztrációs hatóságok- RA (Registration Authority) 10
2.6. Végfelhasználók 11
2.7. Egyéb egységek 11
2.8. Tanúsítvány használat, alkalmazási lehetőségek 12
2.8.1. A Szolgáltató által támogatott profilok 12
2.8.1.1. Természetes személyek tanúsítvány profiljai 13
2.8.1.2. Szervezetek tanúsítvány profiljai 13
2.8.1.3. Szolgáltatók tanúsítvány profiljai 13
2.9. Szabályzat adminisztráció 13
2.9.1. Szervezeti dokumentum adminisztráció 13
2.9.2. Kapcsolattartó személyek 13
2.9.3. Elfogadási folyamatok 14
2.9.4. Fogyasztóvédelem 14
2.9.5. Felügyeleti szerv 14
2.10. Meghatározások és rövidítések 14
3. Közzététel, nyilvánosságra hozatal, tanúsítványtár 18
3.1. A szolgáltatói információ közzététele 18
3.1.1. Szabályzatok, kikötések és feltételek közzététele 18
3.1.2. Rendkívüli információk közzététele 18
3.2. A tanúsítvány állapot információk közzététele 19
3.2.1. A tanúsítványtár 19
3.2.1.1. Nyilvános tanúsítványtár 19
3.2.1.2. Tanúsítvány visszavonási lista (CRL) 19
3.3. Adattárak 20
3.4. A közzététel gyakorisága 20
3.4.1. Szabályzatok, kikötések és feltételek közzétételi gyakorisága 20
3.4.2. Rendkívüli információk közzétételi gyakorisága 20
3.4.3. Tanúsítványokkal kapcsolatos információk közzétételének gyakorisága 20
3.5. Adattárak hozzáférési szabályzása 21
4. Azonosítás és hitelesítés 21
4.1. Névtípusok 21
4.1.1. Márkanevek, védjegyek elismerése, hitelesítése 22
4.1.2. Álnevek használata 22

4.1.3. Nevek egyedisége 23
4.2. Kezdeti azonosítás 23
4.2.1. Igénylő személy személyazonosságának hitelesítése 23
4.2.2. Szervezet azonosságának hitelesítése 23
4.2.3. A magánkulcs birtokba adása 24
4.3. Azonosítás és hitelesítés az új kulcs-kérésnél 24
4.4. Azonosítás és hitelesítés tanúsítvány-megújítás esetén 24
4.5. Azonosítás és hitelesítés a felfüggesztési kérelemhez 24
4.6. Azonosítás és hitelesítés a visszavonási kérelemhez 24
5. A tanúsítvány életciklus működési követelményei 24
5.1. A tanúsítvány kérelem létrehozása 24
5.1.1. Az igénylés feltétele 24
5.1.2. A tanúsítványigénylés és feldolgozás folyamata 25
5.1.3. A tanúsítványigénylés elfogadásának feltételei 25
5.2. A tanúsítványkérelem feldolgozása 26
5.3. A tanúsítvány kibocsátása 26
5.4. A tanúsítvány elfogadása 27
5.5. Kulcspár és tanúsítvány használat 27
5.5.1. Tanúsítvány profilokra vonatkozó előfeltételek 27
5.5.1.1. Módosított tanúsítvány a letagadhatatlan elektronikus aláíráshoz 28
5.5.1.2. Tanúsítvány titkosításhoz, azonosításhoz és hitelesítéshez 28
5.5.1.3. SSL szerver tanúsítvány 28
5.5.1.4. TSA tanúsítvány 28
5.5.1.5. CA tanúsítvány 28
5.5.2. Az Aláíróra és az Érintett félre vonatkozó általános szabályok, ajánlások 29
5.5.3. Elektronikus aláírás készítése 29
5.5.4. Magánkulcs birtoklása 30
5.5.5. Az elektronikus aláírás ellenőrzése 30
5.6. Tanúsítvány csere 30
5.7. Tanúsítvány megújítás 30
5.8. Tanúsítvány felfüggesztése és visszavonása 30
5.8.1. A visszavonás körülményei 31
5.8.2. Visszavonás kérelemre vonatkozó eljárás 31
5.8.3. A felfüggesztés körülményei 31
5.8.4. Felfüggesztési kérelemre vonatkozó eljárás 31
5.8.5. A tanúsítvány visszaállítása 31
5.9. A tanúsítvány előfizetés vége 31
6. Létesítmény-, menedzsment- és működésellenőrzés 32
6.1. Fizikai óvintézkedések 32
6.1.1. Telephelyek, bérelt helyek elhelyezkedése 32
6.1.2. Fizikai hozzáférés 33
6.1.3. Áramellátás, légkondicionálás 33
6.1.4. Tűzvédelem 33
6.1.5. Vízvédelem (beázás, elázás) 33
6.1.6. Adathordozók tárolása 33

6.1.7. Bizalmas minősítésű adatok megsemmisítése, selejtkezelés 33
6.1.8. Mentési példányok fizikai elkülönítése 34
6.2. Folyamatellenőrzés 34
6.3. Személyzet ellenőrzése 34
6.3.1. A bizalmi munkakörök 35
6.4. Vizsgálati naplózás folyamatai 36
6.5. Feljegyzések archiválása 36
6.6. Informatikai biztonság 37
6.6.1. Jelszókezelés 37
6.6.2. Vírusirtás 37
6.6.3. Tűzfal 37
6.6.4. Biztonsági protokollok 37
6.6.4.1. Publikus elérés 37
6.6.4.2. Rendszerfrissítések 38
6.6.4.3. Adathordozók használata 38
6.7. Helyreállítás betörés vagy katasztrófa után 38
6.7.1. Sérült számítási erőforrások, szoftverek és/vagy adatok 38
6.7.2. Szolgáltatói egység kulcsának kompromittálódása 39
6.7.3. Helyreállítás természeti, vagy egyéb katasztrófát követően 39
6.8. CA vagy RA leállítás 39
7. Műszaki biztonsági ellenőrzés 40
7.1. Kulcspár-generálás és telepítés 40
7.1. Magánkulcs megsemmisítése 41
7.2. Alkalmazott eszközök 41
7.3. Privát kulcsok védelme és a kriptográfiai modul technikai ellenőrzése 42
7.4. A kulcspár-kezelés egyéb szempontjai 42
7.5. Aktivációs adatok 42
7.6. Hálózat és számítógép-biztonsági ellenőrzés 42
7.7. Időbélyegzés 43
8. Tanúsítvány-, és CRL-profilok 43
8.1. Tanúsítványprofil 43
8.1.1. Természetes személyek tanúsítvány profiljai 43
8.1.2. Szervezetek tanúsítvány profiljai 46
8.1.3. Szolgáltatók tanúsítvány profiljai 46
8.2. CRL-profil 48
8.3. Időbélyeg profilok 48
9. Egyéb üzleti és jogi kérdések 49
9.1. Díjak 49
9.2. Jogok, kötelezettségek 49
9.2.1. A Szolgáltató kötelezettségei 49
9.2.2. A végfelhasználók jogai és kötelezettségei 50
9.3. Anyagi felelősség - Felelősségek 50
9.3.1. A Szolgáltató általános felelőssége és felelősségének korlátai 50
9.3.2. A Szolgáltató pénzügyi felelőssége: 51
9.3.3. Felelősségbiztosítás 51

9.3.4. A Végfelhasználók felelőssége 52
9.3.5. Szolgáltatóval szembeni kártérítés 52
9.4. Üzleti információ titkossága 53
9.5. Adatkezelés, bizalmasság 53
9.5.1. Adatkezelési szabályok, titoktartási kötelezettség 53
9.5.2. Adatok nyilvánosságra hozatala 53
9.5.3. Bizalmas jellegű információk 53
9.5.4. Nem bizalmas jellegű információk 53
9.6. Személyi adatok bizalmas kezelése 53
9.7. Szellemi tulajdonjogok 54
9.8. Garanciák jogi nyilatkozatai 54
9.9. Érvényesség, módosítás 55
9.9.1. A Hitelesítési Rend érvényessége 55
9.9.2. Érvénytelenség, fennmaradás 55
9.9.3. A Hitelesítési Rend értelmezése 55
9.10. Egyedi értesítések és kommunikáció a résztvevőkkel - Felek közötti kommunikáció 56
9.11. Módosítások 56
9.11.1. A Szabályzat módosítása 56
9.12. Rendelkezések a viták rendezéséről 57
9.13. Jogi szabályozás 57
9.14. Megfelelés az alkalmazandó törvényeknek 57
9.15. Vis major 57

1. Általános információ

Jelen dokumentum a Digitoll Informatikai és Szolgáltató Kft. (továbbiakban: Szolgáltató) nem minősített hitelesítés-szolgáltatására (továbbiakban: Szolgáltatás) vonatkozó Hitelesítési Rendje.

A hitelesítési rend olyan szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.

Jelen Hitelesítési Rend célja, hogy, összefoglalja mindazon minimum követelményeket, szabályokat, amelyek nem minősített, fokozott biztonságú tanúsítványok igénylésére, kibocsátására, használatára és életciklusára vonatkoznak.

A Hitelesítési Rendnek megfelelően kibocsátott tanúsítványok tartalmazhatnak egy azonosítót, amelyet az érintett felek arra használhatnak, hogy meghatározzák a tanúsítványok alkalmazhatóságát és megbízhatóságát egy adott alkalmazás tekintetében.

Jelen Hitelesítési Rend tartalmi vonatkozásokban eleget tesz a 2001. évi XXXV. törvény az elektronikus aláírásról (továbbiakban: EAT) és egyéb hazai jogszabályok előírásainak és ajánlásainak, tartalmában és felépítésében követi az IETF RFC 3647 ajánlást.

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).

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) 487 9900

Visszavonási ügyelet (0-24):	(+36-1) 567 8900
Telefax szám:	(+36-1) 487 9901
Email cím:	ugyfelszolgalat@digitoll.co.hu
	digitoll@digitoll.co.hu
Internet cím:	http://www.digitoll.co.hu
	http://ds.digitoll.co.hu

A Szolgáltató önkéntes akkreditációs rendszer keretében nem lett tanúsítva.

2. Bevezetés

2.1. A Szabályzat hatálya

2.1.1. 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. 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 dokumentum hivatalos elnevezése: Digitoll Informatikai és Szolgáltató Kft. Fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatás Hitelesítés Rendje, melynek azonosító paraméterei a Hitelesítési Rend fedőlapján találhatóak.

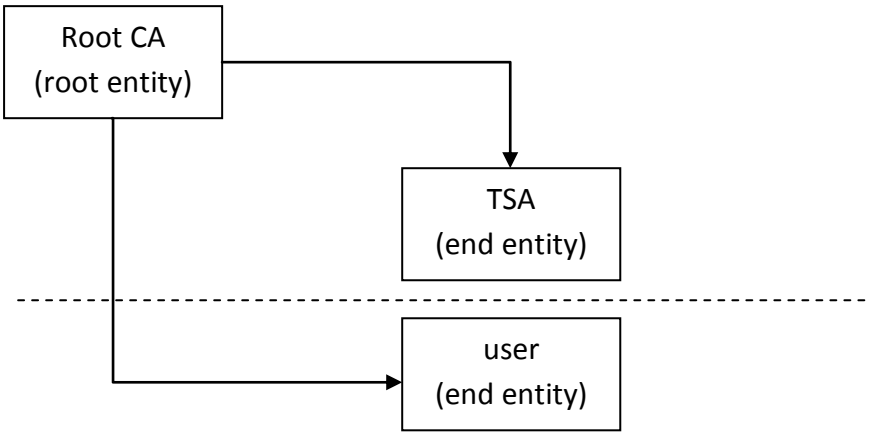
A Hitelesítési Rend, és ahhoz elválaszthatatlanul kapcsolódó mindenkori Általános Szerződési feltételek (továbbiakban: ÁSzF), Szolgáltatási Szabályzat (továbbiakban: Szabályzat) és Időbélyegzési Rend elérhető a Szolgáltató ügyfélszolgálati irodájában, vagy elektronikusan a http:/ds.digitoll.co.hu/ internetes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

2.3. PKI résztvevők

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

2.4. Hitelesítő hatóság - CA (Certification Authority)

A Szolgáltató, saját szervezetén belül Hitelesítő hatóságot működtet, melynek fő feladata a Regisztrációs hatósághoz 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 a szervezet 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:
  EA : 92 : 0D : 0E : D0 : 6E : E2 : 46 : 73 : B6 : E8 : 78 :
  81 : A8 : C3 : BF : 60 : 0C : 2A : C4
- SHA-256:
  A3 : 66 : A2 : 7A : 0D : 96 : B1 : 4A : F0 : 4C : A7 : DC :
  B3 : D4 : 2A : 91 : 45 : 0E : 59 : 97 : 94 : A6 : 01 : EC :
  14 : CD : 3E : 60 : 09 : 1B : 6C : D8

2.5. Regisztrációs hatóságok- RA (Registration Authority)

A Szolgáltató, saját szervezetén belül Regisztrációs hatóságot 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 hatóságnak.

- Tanúsítványokkal kapcsolatos feladatok:
  - Az aláírás létrehozó adat és az aláírás ellenőrző adat generálásának felügyelete és annak elhelyezése az biztonságos aláírást-létrehozó eszközön (továbbiakban: BALE),
  - A CA-tól lekért tanúsítvány elhelyezése a BALE-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 hatóság 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 hatóság 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 (Szolgáltatási szerződés, továbbiakban: Szerződés) 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 tanúsítványt csak az arra jogosultak, és csak a hatályos törvényben, a Szolgáltató szabályzataiban és a megkötött Szerződésben meghatározott célra használhatják. A tanúsítvány minden más célú használata tiltott.

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

- a kibocsátott nem minősített aláíró tanúsítványok kizárólag aláírási célra használhatók fel,
- a kibocsátott nem minősített authentikációs tanúsítványok kizárólag authentikációs célra használhatók fel,
- tanúsítványokhoz tartozó aláírás létrehozó adat tanúsítványok aláírására történő felhasználása, vagy bármilyen egyéb hitelesítés szolgáltatás nyújtásához történő alkalmazása tilos,
- a Szolgáltató a végfelhasználói tanúsítványok felhasználását a Szerződésben tovább korlátozhatja.

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

A tanúsítványhasználat függ a tanúsítvány profiljától.

2.8.1. A Szolgáltató által támogatott profilok

A tanúsítvány profilok, melyek kötelezően használandóak a tanúsítvány kibocsájtásnál, függenek a szükséges tanúsítvány tervezett felhasználási céljaitól. Így a tanúsítványok kibocsáthatóak adat aláírásra, adat titkosításra, hitelesítés elvégzésére (pl. SSL kliens- vagy szerver-hitelesítés).

A Szolgáltató által kibocsátott tanúsítványok profilok leírása, táblázatos formában kerül megjelenítésre (jelen Hitelesítési Rend 8. pontjában). Az adattartalom szempontjából nincs különbség a tanúsítványok között attól függően, hogy milyen eszközre kerül (SSCD/HwSCDev/SwSCDev) a titkos kulcs.

SSCD Secure Signature-creation Device (Biztonságos Aláírás-létrehozó Eszköz)
A jogszabályi követelményeknek megfelelő terméktanúsítással rendelkező HwSCDev.

HwSCDev Hardware Signature-creation Device
Kriptográfiai adatok tárolására alkalmas eszköz (pl. chipkártya, USB token).
SwSCDev Software Signature-creation Device
Kriptográfiai adatok tárolására alkalmas állomány (pl. PKCS#12).

2.8.1.1. Természetes személyek tanúsítvány profiljai

- Magánszemély fokozott biztonságú tanúsítványa titkosításra, hitelesítésre SSCD/HwSCDev/SwSCDev használatával
- Magánszemély fokozott biztonságú tanúsítványa letagadhatatlan elektronikus aláírásra SSCD/HwSCDev/SwSCDev használatával
- Szervezeti személy fokozott biztonságú tanúsítványa titkosításra, hitelesítésre SSCD/HwSCDev/SwSCDev használatával
- Szervezeti személy fokozott biztonságú tanúsítványa letagadhatatlan elektronikus aláírásra SSCD/HwSCDev/SwSCDev használatával

2.8.1.2. Szervezetek tanúsítvány profiljai

- Szervezet fokozott biztonságú tanúsítványa elektronikus aláírásra SSCD/HwSCDev/SwSCDev használatával

2.8.1.3. Szolgáltatók tanúsítvány profiljai

- CA tanúsítványa SSCD/HwSCDev használatával
- TSA fokozott biztonságú végtanúsítványa SSCD/HwSCDev használatával
- SSL szerver fokozott biztonságú tanúsítványa SwSCDev használatával

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: 061 487 99 00
  - 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: 061 487 9900
  - E-mail: info@digitoll.co.hu

Technikai támogatás, felelős vezető

- Név: Németh Viktor
  - Telefon: 061 487 9900
  - E-mail: support@digitoll.co.hu

2.9.3. Elfogadási folyamatok

Jelen Hitelesítési Rend elfogadását a felelős vezetőnek kell elvégeznie.

2.9.4. Fogyasztóvédelem

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

Név:	Nemzeti Fogyasztóvédelmi Hatóság Közép-magyarországi Regionális Felügyelősége
Cím:	1052 Budapest, Városház u. 7.
Postai cím:	1364 Budapest, Pf. 144.
Telefonszám:	(+36-1) 328 0185
Email cím:	fogyved_kmf_budapest@nfh.hu
Internet cím:	http://www.nfh.hu

2.9.5. Felügyeleti szerv

Név:	Nemzeti Média- és Hírközlési Hatóság
Cím:	1015 Budapest, Ostrom u. 23-25.
Postacím:	1525 Budapest, Pf. 75
Telefonszám:	(+36-1) 457 7100
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.
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.

1124. Budapest, Stromfeld A. út 9.
Tel.: +361 487 9900
Fax: +361 487 9901
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

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:

- Rövidítések:

ANSI	The American National Standards Institute (Amerikai Nemzeti Szabványügyi Intézet)
CA	Certification Authority (Hitelesítő hatóság)
CC	Common Criteria (Közös szempontrendszer)
CP	Certificate Policy (Hitelesítési Rend)
CPS	Certification Practice Statement (Hitelesítés Szolgáltatási Szabályzat)
CRL	Certificate Revocation List (Tanúsítvány visszavonási lista)
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 hatóság)
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 hatóság)
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)

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 szolgáltatások 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_16_2.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 Hitelesítési Renddel kapcsolatos új verziók közzététele jelen Hitelesítési Rend 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 tartalmazza.

- commonName (CN)

A “commonName” típusa szabadszöveges mező. Ez a névelem nem tartalmazhat álnevet, kizárólag a személyazonosításra használt okmányban szereplő név alapján kerülhet kitöltésre.

- localityName (L)

A “localityName” lista előredefiniált 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

A tanúsítványok CommonName (CN) mezőiben valós neveknek kell szerepelniük, a jelen Hitelesítési rend kizárja az álnév használatát.

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.

A részletes eljárásrendet a Szabályzat tartalmazza.

4.2.2. 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 részletes eljárásrendet a Szabályzat tartalmazza.

4.2.3. 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 tanúsítvány-megújítás esetén

A vonatkozó eljárásrendet a Szabályzat tartalmazza.

4.5. Azonosítás és hitelesítés a felfüggesztési kérelemhez

A vonatkozó eljárásrendet a Szabályzat tartalmazza.

4.6. Azonosítás és hitelesítés a visszavonási kérelemhez

A vonatkozó eljárásrendet a Szabályzat tartalmazza.

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.

Igénylésben az Igénylő fél megadja a tanúsítványba kerülő adatait, megnevezi, hogy pontosan milyen tanúsítványt igényel, és felhatalmazza a Szolgáltatót az adatok kezelésére. Az igénylés történhet személyesen a Szolgáltató Ügyfélszolgálati irodájában, vagy előre egyeztetett külső helyszínen is.

A tanúsítványigénylés részletes folyamatát a Szabályzat idevonatkozó pontja tartalmazza.

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.

Ha a beérkező adatokat a Szolgáltató hiányosnak, vagy valótlannak találja, felhívást küldhet az Igénylőnek hiánypótlásra, pontosításra.

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

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

Jelen folyamatoktól külön írásos megállapodás keretében el lehet térni.

Jelen folyamatokat a Szolgáltató Regisztrációs hatósága végzi.

A tanúsítvány feldolgozásának részletes leírását, feltételeit a Szabályzat, kapcsolódó pontja tartalmazza.

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 (RA) 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 Tanúsítványok kibocsátása tanúsítványigénylési és regisztrációs folyamat végén kerül sor, és az Előfizető illetve Aláíró által megadott adatok alapján történik. A regisztrációt követően a Regisztrációs hatóság az Előfizetőtől kapott adatok alapján kiállítja a tanúsítvány kérelmet, melyet a Hitelesítő hatóság jóváhagy, majd kiállítja a Tanúsítványt. A kiállított Tanúsítványt a Regisztrációs hatóság átadja az Előfizetőnek illetve az Aláírónak. A Szolgáltató a kibocsátást követően közzéteszi a tanúsítványt a Nyilvános tanúsítványtárában, ha az Előfizető ehhez előzetesen írásban hozzájárult.

A folyamat részleteit a Szabályzat idevonatkozó pontja tartalmazza.

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 aláírás-létrehozó eszközön (BALE) 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 BALE-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

5.5.1. Tanúsítvány profilokra vonatkozó előfeltételek

Az előre megadott tanúsítvány-profilok tartalmaznak előfeltételeket a keyUsage és extKeyUsage kiegészítőkhöz, melyek beállításai határozzák meg a használható funkciókat és protokollokat, mint az SSL vagy TLS.

A táblázatok a különböző tanúsítvány típusokhoz tartozó keyUsage és extKeyUsage kiegészítők előre beállított értékeit tartalmazzák.

5.5.1.1. Módosított tanúsítvány a letagadhatatlan elektronikus aláíráshoz

mező/kiterjesztés	beállítások	jelző
Key Usage	Digital Signature (0) Non Repudiation (1)	critical

5.5.1.2. Tanúsítvány titkosításhoz, azonosításhoz és hitelesítéshez

mező/kiterjesztés	beállítások	jelző
Key Usage	Digital Signature (0) Key Encipherment (2) Data Encipherment (3) Key Agreement (4)	critical
Extended Key Usage	TLS WWW client authentication Email protection Microsoft Smartcard Logon	

5.5.1.3. SSL szerver tanúsítvány

mező/kiterjesztés	beállítások	jelző
Key Usage	Digital Signature (0) Key Encipherment (2) Data Encipherment (3) Key Agreement (4)	critical
Extended Key Usage	TLS WWW server authentication	

5.5.1.4. TSA tanúsítvány

mező/kiterjesztés	beállítások	jelző
Key Usage	Non Repudiation (1)	critical
Extended Key Usage	Timestamping(1.3.6.1.5.5.7.3.8)	critical

5.5.1.5. CA tanúsítvány

mező/kiterjesztés	beállítások	jelző
Key Usage	Certificate Signing (5) CRL Signing(6)	critical

5.5.2. 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 a Szabályzatban illetve Szerződésben 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.

5.5.3. 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.

5.5.4. 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.

5.5.5. 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 csere (új tanúsítvány kibocsátása régi kulccsal) a Szolgáltatónál nem elérhető.

5.7. Tanúsítvány megújítás

A vonatkozó eljárásrendet a Szabályzat tartalmazza.

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 vonatkozó eljárásrendet a Szabályzat tartalmazza.

5.8.2. Visszavonás kérelemre vonatkozó eljárás

A vonatkozó eljárásrendet a Szabályzat tartalmazza.

5.8.3. A felfüggesztés körülményei

A vonatkozó eljárásrendet a Szabályzat tartalmazza.

5.8.4. Felfüggesztési kérelemre vonatkozó eljárás

A vonatkozó eljárásrendet a Szabályzat tartalmazza.

5.8.5. A tanúsítvány visszaállítása

A vonatkozó eljárásrendet a Szabályzat tartalmazza.

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 a Szolgáltatási Szabályzat, az ÁSzF és a Szerződés tartalmazza.

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

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 óvintézkedések

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 fizikai 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 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 logokról, 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 policyból 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 2003. évi XXXV. elektronikus aláírás törvény 16. §-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.

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 köztes hitelesítő egységeinek kulcsa 2048 bites,
- 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.

7.1. Magánkulcs megsemmisítése

A hitelesítő szervezet 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.

7.2. Alkalmazott eszközök

Szolgáltató a szolgáltatás nyújtásához (kulcskezelés, tárolás, előállítás) nCipher nShield Connect 500 (nShield F3 500e nC4033E-500N) típusú HSM eszközt használ.

A végfelhasználói eszközök kulcspár és tanúsítvány tárolására alkalmas aláírás-létrehozó eszközök, melyek megfelelő minősítéssel rendelkeznek.

7.3. 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.

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.

7.4. A kulcspár-kezelés egyéb szempontjai

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

7.5. Aktivációs adatok

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

7.6. Hálózat és számítógép-biztonsági ellenőrzés

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

7.7. 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 (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
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_16_2.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
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_16_2.pdf

3) 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
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_16_2.pdf

4) 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
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_16_2.pdf

8.1.2. Szervezetek 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
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_16_2.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_16_2.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_16_2.pdf

3) 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
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_16_2.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 (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 (1.3.6.1.4.1.24206.3.16.1)
messageImprint	kötelező; időbélyeghez kapcsolódó lenyomatképző algoritmus azonosítója és lenyomat

serialNumber	kötelező; időbélyeg sorszáma
genTime	kötelező; időbélyeg kibocsátásának dátuma és időpontja

9. Egyéb üzleti és jogi kérdések

9.1. 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.

9.2. Jogok, kötelezettségek

9.2.1. A Szolgáltató kötelezettségei

A Szolgáltató alapvető kötelezettsége, hogy a Szolgáltatást jelen Hitelesítési Renddel és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a saját belső szabályzataival összhangban nyújtsa.

Így a Szolgáltatónak kötelessége:

- a Szolgáltatásnak megfelelő jogi-, működési keretek megteremtése,
- magas színvonalú és biztonságos szolgáltatás nyújtása a vonatkozó szabályzatok szerint,
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése,
- a szolgáltatás biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket,

- a nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az Interneten keresztül.

A Szolgáltató jogait és további kötelezettségeit a Szabályzat és ÁSzF tartalmazza.

9.2.2. 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 és/vagy Aláíró köteles a szolgáltatásokat kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a 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 Hitelesítési rend, Szabályzat, Időbélyegzési Rend, Szerződés).

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.

A Végfelhasználók további jogait és kötelezettségeit a Szabályzat és ÁSzF tartalmazza.

9.3. 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 §-sa szerinti mértékben.

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

9.3.1. A Szolgáltató általános felelőssége és felelősségének korlátai

A Szolgáltató felelősséget vállal a szabályzataiban és szerződéseiben 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. 339. §) 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.

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 egyéb felelősségét és felelősségének korlátozását a Szabályzat és ÁSzF tartalmazza.

9.3.2. A Szolgáltató pénzügyi felelőssége:

A Szolgáltató a kártérítés felső határát tanúsítványonként és összességében is (az összes tanúsítvánnyal és káreseménnyel kapcsolatban) korlátozza, melynek mértékét a Szerződés tartalmazza.

A Szolgáltató pénzügyi felelősségével kapcsolatos további részleteket a Szabályzat tartalmazza.

9.3.3. Felelősségbiztosítás

A Szabályzat ide vonatkozó pontja szerint.

9.3.4. 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 Aláírók, 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 egyéb és felelősségeit a Szabályzat és ÁSzF tartalmazza.

9.3.5. 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.

9.4. Üzleti információ titkossága

A Szabályzat ide vonatkozó pontja szerint.

9.5. Adatkezelés, bizalmasság

A Szabályzat ide vonatkozó pontja szerint.

9.5.1. Adatkezelési szabályok, titoktartási kötelezettség

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

9.5.2. Adatok nyilvánosságra hozatala

A Szabályzat ide vonatkozó pontja szerint.

9.5.3. Bizalmas jellegű információk

A Szabályzat ide vonatkozó pontja szerint.

9.5.4. Nem bizalmas jellegű információk

A Szabályzat ide vonatkozó pontja szerint.

9.6. Személyi adatok bizalmas kezelése

A Szolgáltató kötelezettséget vállal arra, hogy a hitelesítés-szolgáltatás során tudomására jutott személyes adatokat a személyes adatok védelméről és a közérdekű adatok nyilvántartásáról szóló 1992. évi LXIII. 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.

9.7. 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.

9.8. Garanciák jogi nyilatkozatai

A Szolgáltató kötelezettséget vállal, hogy minden lehetséges és törvényes eszközzel biztosítja a szolgáltatások 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.

9.9. Érvényesség, módosítás

9.9.1. A Hitelesítési Rend érvényessége

Jelen Hitelesítési Rend visszavonásig, vagy újabb verzió hatályba lépéséig érvényes.

9.9.2. Érvénytelenség, fennmaradás

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

A Hitelesítési Rend 9. fejezete érvényben marad a Hitelesítési Rend hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, melyet a Szolgáltató a Hitelesítési Rend hatálya alatt bocsátott ki.

9.9.3. A Hitelesítési Rend értelmezése

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

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

9.10. 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 internetes oldalán közzéteszi: http://ds.digitoll.co.hu/.

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 reklamációt és hibabejelentést nyilvántartásba vesz és kivizsgál. A számlareklamációkkal kapcsolatos feltételeket az ÁSzF tartalmazza.

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.

9.11. Módosítások

9.11.1. A Szabályzat módosítása

Jelen Hitelesítési Rendet a Szolgáltató egyoldalúan módosíthatja. A módosításról a Hitelesítési Rend 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.

Minden Hitelesítési Rend egyedi azonosítóval rendelkezik (verziószám).

A módosított Hitelesítési Rendet minden esetben a Szolgáltató felügyeleti szerve az NMHH bevizsgálja és hatályba lépés előtt és jóváhagyja vagy módosíttatja azt, majd nyilvántartásba

veszi. A Hitelesítési Rend csak írott és hitelesített formában módosítható, a NMHH által vezetett szabályzat-nyilvántartásban való átvezetés mellett.

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

9.12. Rendelkezések a viták rendezéséről

A Szabályzat ide vonatkozó pontja szerint.

9.13. Jogi szabályozás

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 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 is tartalmazza.

9.14. 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.

9.15. 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.