

# NetLock Kft. MKB Kihelyezett Szolgáltató Alegységének Szolgáltatási Szabályzat Kiegészítése

## láncolt, nem minősített hitelesítés- szolgáltatás



NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Nyilvántartási szám (OID): ---- 1.3.6.1.4.1.3555.1.43.20071217

A Szabályzat hatályának kezdőnapja: ----- 2007. december 5.

OLDALAK SZÁMA: -----**48**

© **COPYRIGHT NETLOCK KFT.** ----- **MINDEN JOG FENNTARTVA**

Jóváhagyta: ----- **Rózsahegyi Zsolt**, Szabályzatvezető

Jóváhagyás dátuma: ----- **2007. november 21.**

Jóváhagyom: .....

PH.

## Verziókezelés

Verzió-szám	Dátum	Módosította	Módosítás leírása	Fájl név
0.1	2007.08.06.	Dr. Szűcs Katalin	Dokumentum létrehozása	Szolgáltatasi_Szabalyzat_Kiegeszites_MKB_LHSZ_070806
0.2	2007.08.14.	Dr. Szűcs Katalin	Dokumentum módosítása	Szolgáltatasi_Szabalyzat_Kiegeszites_MKB_LHSZ_070814
0.3	2007.08.16.	Dr. Szűcs Katalin	Személyes egyeztetésnek megfelelően a dokumentum pontosítása	Szolgáltatasi_Szabalyzat_Kiegeszites_MKB_LHSZ_070816
0.4	2007.09.21.	Dr. Szűcs Katalin	Személyes egyeztetésnek megfelelően a dokumentum pontosítása	Szolgáltatasi_Szabalyzat_Kiegeszites_MKB_LHSZ_070921
0.5	2007.10.05.	Dr. Szűcs Katalin	Telefonos egyeztetésnek megfelelően a dokumentum pontosítása	Szolgáltatasi_Szabalyzat_Kiegeszites_MKB_LHSZ_071005
0.6	2007.11.21.	Dr. Szűcs Katalin	Végző ellenőrzés	Szolgáltatasi_Szabalyzat_Kiegeszites_MKB_LHSZ_071121
0.7	2007.12.17.	Dr. Szűcs Katalin	Végleges verzió	Szolgáltatasi_Szabalyzat_Kiegeszites_MKB_LHSZ_071217

## Tartalomjegyzék

<b>1</b>	<b><i>Bevezetés</i></b> .....	<b>5</b>
1.1	Áttekintés.....	5
1.2	Dokumentum neve és azonosítása.....	8
1.3	PKI közösség.....	9
1.4	Alkalmazhatóság.....	10
1.5	Kapcsolattartás.....	11
1.6	Fogalmak és rövidítések.....	12
<b>2</b>	<b><i>Közzététel és tanúsítványtár</i></b> .....	<b>16</b>
2.1	Az információ közzététele.....	16
2.2	Tanúsítványokkal kapcsolatos információk.....	16
2.3	A közzététel gyakorisága.....	17
2.4	Hozzáférs ellenőrzések.....	17
<b>3</b>	<b><i>Azonosítás és hitelesítés</i></b> .....	<b>19</b>
3.1	Elnevezések.....	19
3.2	Kezdeti azonosítás.....	20
3.3	Azonosítás tanúsítvány kulcscseréje esetén .....	21
3.4	Visszavonási kérelem .....	21
<b>4</b>	<b><i>Működésre vonatkozó követelmények</i></b> .....	<b>22</b>
4.1	Tanúsítványigénylés.....	22
4.2	Tanúsítványkérelem feldolgozása.....	22
4.3	A tanúsítványok kibocsátása és hozzáférhetővé tétele .....	26
4.4	Tanúsítványelfogadás.....	26
4.5	A kulcpár és a tanúsítvány használata .....	27
4.6	Tanúsítvány megújítása .....	29
4.7	Kulcsre.....	29
4.8	Tanúsítvány módosítása.....	29
4.9	Tanúsítvány függesztése és visszavonása .....	29
4.10	Tanúsítvány-állapot információk közzététele .....	33
4.11	Kulcsletébe helyezése és visszaállítása.....	34
<b>5</b>	<b><i>Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések</i></b> .....	<b>35</b>
5.1	Fizikai óvintézkedések.....	35
5.2	A Láncolt Hitelesítés-szolgáltató leállítása.....	35
5.3	Kulcpár előállítás és telepítés.....	36
5.4	A magánkulcsok védelme.....	37
5.5	Aktívizáló adatok .....	39
<b>6</b>	<b><i>Tanúsítvány és visszavonási lista profilok</i></b> .....	<b>40</b>

<b>6.1</b>	<b>Tanúsítványprofilok.....</b>	<b>40</b>
<b>6.2</b>	<b>Tanúsítvány visszavonási lista profilok .....</b>	<b>42</b>
<b>7</b>	<b><i>Üzleti és jogi tudnivalók.....</i></b>	<b>43</b>
<b>7.1</b>	<b>Bizalmasság, adatvédelem.....</b>	<b>43</b>
<b>7.2</b>	<b>Jogok és kötelezettségek.....</b>	<b>43</b>
<b>7.3</b>	<b>Felelőség .....</b>	<b>46</b>
<b>7.4</b>	<b>Változtatási eljárás.....</b>	<b>47</b>
<b>7.5</b>	<b>Hivatkozott jogszabályok, szabványok és egyéb dokumentumok .....</b>	<b>48</b>

# 1 Bevezetés

## 1.1 Áttekintés

A Szolgáltató az MKB Bank Zrt.-nél (a továbbiakban: MKB) Kihelyezett Szolgáltató Alegységet működtet (Kihelyezett Szolgáltató Alegység vagy MKB Kihelyezett Szolgáltató Alegység). Jelen dokumentum a Kihelyezett Szolgáltató Alegységnek nem minősített aláírás és titkosítás célú tanúsítványok kibocsátására vonatkozó részletes eljárási és egyéb működési szabályokat tartalmazó Szolgáltatási Szabályzat Kiegészítése (a továbbiakban: Szolgáltatási Szabályzat Kiegészítés vagy Szabályzat).

Jelen Szabályzat kizárólag 'B' hitelesítési osztályú, nem minősített aláíró, nem minősített ideiglenes aláíró és titkosító tanúsítványok (a továbbiakban: aláíró tanúsítvány, ideiglenes tanúsítvány és titkosító tanúsítvány, együttesen: tanúsítványokra) kibocsátására vonatkozó szabályokat tartalmazza.

Jelen Szabályzatban nem szabályozott kérdésekben Szolgáltató Nem minősített Hitelesítés-szolgáltatás Szolgáltatási Szabályzatában, Általános Szerződési Feltételeiben, illetve egyéb szabályzataiban foglaltak az irányadók.

Az MKB a Kihelyezett Szolgáltató Alegység üzemeltetési feladataiban működik közre, részt vesz a tanúsítvány-szolgáltatásban, valamint ezzel összefüggésben intelligens kártya megszemélyesítési feladatokat lát el.

A jelen Szabályzat tartalmára és felépítésére az RFC 3647 [6] dokumentum adott útmutatót, mely struktúráját az Szabályzat követi.

### 1.1.1 A Szolgáltatási Szabályzat Kiegészítés hatálya

#### 1.1.1.1 Tárgyi hatály

A Szabályzat tárgyi hatálya az 1.1.3 pontban ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.

#### 1.1.1.2 Időbeli hatály

A Szabályzat időbeli hatálya a jelen verzió hatálybalépésének dátumától kezdődik, és a szolgáltatási tevékenység beszüntetéséig, illetve egy újabb szabályzat verzió hatályba lépéséig tart.

#### 1.1.1.3 Személyi hatály

A Szabályzat személyi hatálya a teljes Közösség (ld. 1.3 alfejezet) természetes személy tagjaira terjed ki.

### 1.1.2 A Szolgáltató

A jelen Szabályzatban a Szolgáltató entitás a NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság. Cégjegyzékszáma: 01-09-563961.

A Nemzeti Hírközlési Hatóság (NHH) 2001. október 27-én vette nyilvántartásba a Szolgáltatót nem minősített szolgáltatóként. NHH regisztrációs szám: FA 6133-5/2001.

A Nemzeti Hírközlési Hatóság (NHH) 2003. március 19-én vette nyilvántartásba a Szolgáltatót minősített szolgáltatóként. NHH regisztrációs szám: MH-1372-12/2003.

A Szolgáltató Kihelyezett Szolgáltató Alegységének nyilvántartásba vétele: 2007. november 29., nyilvántartásba vételi szám: HL-37885-2/2007

Önkéntes akkreditáció, egyéb minősítések:

- Ernst and Young AICPA/CICA WebTrust for Certification Authorities audit (2000)
- ISO 9001:2000 (2001)
- ISO 27001 (korábban: BS 7799-2:2002 (2005))

A Szolgáltató felelőssége, hogy az általában elvárható magatartás szerint a jelen és kapcsolódó Szabályzatokat betartsa, betartassa, azok betartását ellenőrizze, és előírja az esetleges Szabályzattól eltérő működés megszüntetésének feltételeit.

### 1.1.3 Szolgáltatások

Az MKB Kihelyezett Szolgáltató Alegység tevékenysége a következő fő elemekből áll:

- Regisztrációs szolgáltatás;
- Aláíró és titkosító tanúsítvány létrehozási szolgáltatás;
- Egyedi név szolgáltatás;
- Tanúsítványszétosztási szolgáltatás;
- Tanúsítványarchiválási szolgáltatásban;
- Adattárolási szolgáltatás;
- Állapotinformációs szolgáltatás;
- Visszavonás kezelési szolgáltatás;
- Kulcsletét szolgáltatás.

### 1.1.4 Szabványok és előírások

#### 1.1.4.1 Szolgáltatási Szabályzat Kiegészítés

A Szabályzat az RFC 3647 [6] szabványa alapján készült. A Szabályzat tartalmi vonatkozásokban eleget tesz az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] (továbbiakban: Törvény), az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendelet [2] (továbbiakban: Rendelet) előírásainak és ajánlásainak, és felhasználja az ETSI 102 042 [10], valamint az x.509 [6] szabvány ajánlásait.

#### 1.1.4.2 Lenyomatképző algoritmusok azonosítói

- SHA-1           OID ::= { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }

#### 1.1.4.3 Kriptográfiai algoritmusok azonosítói

- RSA       OID ::= { iso(1) member-body (2) USA (840) RSADSI (113549) PKCS (1) 1 }

#### 1.1.4.4 Tanúsítvány kiterjesztések azonosítói

- KeyUsage                      OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 15 }
- EnhancedKeyUsage        OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 37 }
- BasicConstraints            OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 19 }
- CertificatePolicies        OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 32 }

#### 1.1.4.5 Alkalmazott formátumok

Tétel	Alkalmazott / elfogadott formátum, szabvány
Alírási létrehozó adat	PKCS12 PEM, PKCS12 DER
Kérelem	PKCS10 PEM, X509 selfsigned PEM, SPKAC
Tanúsítvány	X509 PEM, X509 DER, X509 PKCS7, WAP WTLS
CRL	X509 PEM, X509 DER, X509 PKCS7

#### 1.1.5 Hitelesítés-szolgáltatás és tanúsítványfajták

A Szolgáltató Kihelyezett Szolgáltató Alegysége előzetes entitásazonosítás után az igénylők (kétsős alanyok) számára munkatársi aláíró, ideiglenes munkatársi aláíró és titkosító tanúsítványokat bocsát ki.

A tanúsítvány a hitelesítés-szolgáltató, illetve láncolt hitelesítés-szolgáltatás keretében kibocsátott igazolás, amely a nyilvános kulcsot egy meghatározott alanyhoz vagy szervezethez kapcsolja, és igazolja az alany azonosító adatait vagy valamely más tény fennállását.

A jelen Szabályzat szerint szabályozott végfelhasználói tanúsítványfajták összefoglaló táblázata az alábbi. A tanúsítványfajtákhoz tartozó profilok leírását a 6. fejezet tartalmazza.

Fajta	Alany	Engedélyezett alkalmazások	Tiltott alkalmazások	Felelősség biztosítás összege	Joghatás
Munkatársi aláíró	Természetes személy az MKB Bank Zrt., vagy MKB Üzemeltetési Kft. munkatársaként	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	A tanúsítványban szereplő érték, de maximum 500.000 forint	Írásbeliség (magánokirat)
Ideiglenes munkatársi aláíró	Természetes személy az MKB Bank Zrt., vagy MKB Üzemeltetési Kft. munkatársaként	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	A tanúsítványban szereplő érték, de maximum 500.000 forint	Írásbeliség (magánokirat)
Munkatársi titkosító	Természetes személy az MKB Bank Zrt., vagy MKB Üzemeltetési Kft. munkatársaként	Titkosítási műveletek végrehajtása	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	A tanúsítványban szereplő érték, de maximum 500.000 forint	-

Az MKB Kihelyezett Szolgáltató Alegység egyéni joga és felelőssége, hogy a fentiek közül egy adott célra milyen tanúsítványt alkalmaz.

## 1.1.6 Aláíró eszköz szolgáltatás

Az MKB Kihelyezett Szolgáltató Alegység a tanúsítványok kibocsátása során aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatást nem végez. A kulcsgenerálást a regisztrációs felületre (portál) történő belépést követően felhasználó maga végzi.

A hatályos jogszabályok és a jelen Szabályzat rendelkezéseinek figyelembe vételével az Alany a kulcspár generálása során az alábbiak szerint jár el:

Az aláíró tanúsítványok kulcspárjai generálása és a tanúsítvány kibocsátása során a Szolgáltató Kihelyezett Szolgáltató Alegységén keresztül:

- biztosítja, hogy az Alany az aláíró kulcsokat a fokozott biztonságú elektronikus aláírások céljaira alkalmas algoritmus [16] felhasználásával generálja;
- megszemélyesíti az aláírás létrehozó eszközt;
- gondoskodik arról, hogy a kulcs hossza és az alkalmazott nyilvános kulcsú algoritmus [16] a fokozott biztonságú elektronikus aláírás céljaira alkalmas legyen;
- a kulcsok generálása során az Alany a szükséges előírásokat és biztonsági intézkedéseket betartsa;
- biztosítja az aláíró kulcsok titkosságát, valamint az aláírás-ellenőrző adat sértetlenségét;
- gondoskodik róla, hogy az Alany aláírás-létrehozó adata a szolgáltatás nyújtása során visszafejtésre alkalmas módon ne kerüljön tárolásra;
- gondoskodik arról, hogy az Alany által generált magán kulcsokról semmilyen másolat ne kerüljön tárolásra;
- gondoskodik az MKB által biztosított aláírás-létrehozó eszköz kibocsátásakor az eljárás biztonságosságáról;
- biztosítja, hogy az aláírás-létrehozó eszköz a szándék szerinti, hitelesített Aláíróhoz kerül;
- aláíró eszköz biztosítása esetén a regisztrációs felület aktivizáló adatát az aláírás-létrehozó eszköztől elkülönítve juttatja el az Aláíróhoz;
- gondoskodik róla, hogy a saját munkavállalói ne élhessenek vissza az aláírás-létrehozó eszközzel a következőképpen: PIN számok, portál kódok megismerése, magánkulcsok, tanúsítványok használata;
- az aláírás-létrehozó eszköz előkészítése és továbbítása során alkalmazza a biztonsági eljárásokat.

Titkosító tanúsítványok kibocsátása során a Szolgáltató fentiekől az alábbiakban tér el:

- a titkosító kulcsokat a titkosítás céljaira alkalmas algoritmus [16] felhasználásával az Alany generálja;
- a titkosító kulcsok generálása szoftveresen történik a kulcspár és a hozzá tartozó tanúsítvány a visszaállítás érdekében, és utólag kerül feltöltésre az intelligens kártyára;
- a titkosító tanúsítvány magánkulcsai megőrzésére a Szolgáltató Kihelyezett Szolgáltató Alegysége kulcsletét-szolgáltatást biztosít.

## 1.2 Dokumentum neve és azonosítása

Jelen dokumentum:

- Teljes neve: NetLock Kft. MKB Kihelyezett Szolgáltató Alegységének Szolgáltatási Szabályzat Kiegészítése (láncolt, nem minősített hitelesítés-szolgáltatás)
- Rövid neve: Szolgáltatási Szabályzat Kiegészítés vagy Szabályzat



- Verziószáma: a fedlapon található verziószám

## 1.3 PKI közösség

A kibocsátott tanúsítványok, aláírás-létrehozó eszközök alkalmazó közössége a Szolgáltató, a Szolgáltató Kihelyezett Szolgáltató Alegysége, a tanúsítványok végfelhasználói és az Érintett felek.

### 1.3.1 Hitelesítő Alegység

A Hitelesítő Alegység a Szolgáltató Kihelyezett Szolgáltató Alegységének tanúsítványkiadási szolgáltatásban részt vevő hitelesítő egysége. A Hitelesítő Alegység az előírt eljárási rend szerint a hozzá tartozó Regisztrációs Alegységek kérelme alapján közreműködik a jóváhagyott aláíró, ideiglenes aláíró és a titkosító tanúsítványok kiadásában, publikálásában, visszavonásában, felfüggesztésében. Emellett gondoskodik a Tanúsítvány Visszavonási Lista (a továbbiakban: CRL) publikálásáról is.

Név:	MKB Nem Minősített Hitelesítő Alegység
Egység:	Bankbiztonság / Eua team
Cím:	1056 Budapest, KassákLajos u. 18. fszt. 30.
Telefon:	+36 1 268 2382
Internet cím:	www.mkb.hu
E-mail:	euateam@mkb.hu

### 1.3.2 Regisztrációs Alegység

A Szolgáltató Kihelyezett Szolgáltató Alegysége Regisztrációs Alegységet működtet, amelynek feladata a kezdeti regisztrációban és a tanúsítvány kibocsátásával kapcsolatos egyéb tevékenységben való közreműködés, tanúsítvány kezelési feladatokban részvétel, ideértve a felhasználókkal való kapcsolattartást is.

A Regisztrációs Alegység a tanúsítvány-kibocsátási folyamat során a felhasználói adatellenőrzést végzésében működik közre, amely tevékenységet a mindenkor hatályos jogszabályi követelményeknek - így különösen az 1992. évi LXIII. törvénynek a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról - megfelelően végzi.

### 1.3.3 HelpDesk

A Szolgáltató Kihelyezett Szolgáltató Alegysége saját szervezetén belül HelpDesket működtet. A HelpDesk nem tagja a tanúsítványkezelő szervezetnek.

### 1.3.4 Végfelhasználók

A tanúsítványban mind annak alanya, mind a másodlagos alanya is megnevezésre kerül.

A Szolgáltató Kihelyezett Szolgáltató Alegysége jelen Szolgáltatási Szabályzat Kiegészítés alapján a következő entitások részére bocsát ki tanúsítványokat:

- az MKB vagy MKB Üzemeltetési Kft. alkalmazásában álló természetes személy – munkatársi aláíró tanúsítvány
- az MKB vagy MKB Üzemeltetési Kft. alkalmazásában álló természetes személy – ideiglenes munkatársi aláíró tanúsítvány

- az MKB vagy MKB Üzemeltetési Kft. alkalmazásában álló természetes személy – munkatársi titkosító tanúsítvány

A Szolgáltató, valamint a Szolgáltató Kihelyezett Szolgáltató Alegysége az Alanyokkal a Regisztrációs Alegységeken keresztül tart kapcsolatot.

Az alanyok kizárólag az MKB-val vagy az MKB Üzemeltetési Kft.-vel szerződéses viszonyban álló munkatársak lehetnek.

### **1.3.5 Érintett fél**

Az Érintett Fél a Közösség azon tagja, aki az elektronikus aláírási és titkosítási képesség ellenőrzése céljából a Szolgáltató által kibocsátott tanúsítványhoz fordul, illetőleg ezen tanúsítvány, érvényességének ellenőrzéséhez a Szolgáltató vagy a Szolgáltató Kihelyezett Szolgáltató Alegysége által és az MKB közreműködésével karbantartott nyilvántartásokat ellenőrzi.

A Szolgáltató az Érintett Féllel elsősorban a tanúsítványvisszavonási információkon keresztül tart kapcsolatot.

## **1.4 Alkalmazhatóság**

### **1.4.1 Engedélyezett alkalmazási lehetőségek**

A kibocsátott munkatársi aláíró, és ideiglenes munkatársi aláíró végfelhasználói tanúsítványok magánkulcs párijai kizárólag elektronikus dokumentumon (melybe egyéb nyilvános kulcsok nem értendők bele) elektronikus aláírások megtételére, míg a tanúsítványokban található nyilvános kulcsok az aláírások ellenőrzésére használhatók fel a tanúsítványban foglaltaknak megfelelően. (Lásd még 1.1.6 pont)

A kibocsátott munkatársi titkosító végfelhasználói tanúsítványok nyilvános kulcs párijai kizárólag a dokumentumon elektronikus titkosítások megtételére, míg az Alanynál található magánkulcs a titkosított dokumentum dekódolására használhatók fel a tanúsítványban foglaltaknak megfelelően.

A Szolgáltató Kihelyezett Szolgáltató Alegységének láncolt aláíró tanúsítványa (a továbbiakban: MKB Kihelyezett Hitelesítő Alegység szolgáltatói tanúsítvány) tanúsítványok tanúsítványhitelesítésre és CRL listák hitelesítésére használható fel.

### **1.4.2 Korlátozott alkalmazási lehetőségek**

Az egyes tanúsítványfajtáknak megfelelő konkrét korlátozásokat lásd még a tanúsítványfajtáknál (1.1.5 pont), illetve a tanúsítványfajtákhoz tartozó profiloknál (6. fejezet).

### **1.4.3 Tiltott alkalmazási lehetőségek**

A tanúsítványok használatára vonatkozó bármely korlátozást (ld. előző pont) megszegő alkalmazása tilos.

A végfelhasználói tanúsítványok magánkulcs párijai más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen hitelesítés-szolgáltatás nyújtásához történő alkalmazása tilos.

A Szolgáltató Kihelyezett Hitelesítő Alegységének szolgáltatói aláíró tanúsítványok magánkulcs párijai csak tanúsítványhitelesítésre és CRL listák hitelesítésére használhatók, egyéb más szolgáltatás nyújtásához történő alkalmazása tilos.

## 1.5 Kapcsolattartás

### 1.5.1 A Szolgáltató adatai

<b>Név:</b>	<b>NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság</b>
Egység:	NetLock Kft.
Székhely:	1023 Budapest, Zsigmond tér 10.
Telefon:	(1) 345-2255
Fax:	(1) 345-2250
Internet cím:	www.netlock.hu
Központi e-mail:	info@netlock.hu
Panaszok bejelentésének helye:	info@netlock.hu
Illetékes fogyasztóvédelmi felügyelőség:	Közép-magyarországi Regionális Közigazgatási Hivatal Fogyasztóvédelmi Felügyelőség, székhely: Budapest cím: 1052 Bp. V. Ker., Városház u. 7., levelezési cím: 1364 Bp. Pf.:270, Tel.: 318-2681, fax: 318-1639, e-mail: fogyasztovedelem@pest.b-m.hu

### 1.5.2 A Kihelyezett Szolgáltató Alegység adatai

<b>Név:</b>	<b>Kihelyezett Szolgáltató Alegység</b>
Egység:	Bankbiztonság / Eua team
Székhely:	1056 Budapest, Váci út 38.
Telefon:	+ 36 268 2382
Fax:	+ 36 268 7279
Internet cím:	www.mkb.hu
Központi e-mail:	euateam@mkb.hu

### 1.5.3 Ügyfélszolgálat és HelpDesk

A szolgáltatással kapcsolatos kérdésekkel, problémákkal a végfelhasználók a Szolgáltatóhoz, illetve a Szolgáltató Kihelyezett Szolgáltató Alegységéhez fordulhatnak szóban vagy írásban. A Szolgáltató az Interneten információs szolgáltatást működtet.

A Szolgáltató Internetes információs rendszere és e-mail fiókjai minden nap 0–24 óráig fogadják a bejelentéseket. A Szolgáltató a bejelentésre legkésőbb a következő 3 munkanap alatt reagál (válasz e-mail cím vagy telefonszám birtokában) és a tartalmi válasz várható idejét is jelzi.

A Szolgáltató Kihelyezett Szolgáltató Alegysége az MKB HelpDesk-jén keresztül fogadja a tanúsítványkibocsátással kapcsolatos kérdéseket, problémákat.

## 1.5.4 A Szolgáltatási Szabályzat Kiegészítéssel kapcsolatos kérdések

Jelen Szolgáltatási Szabályzat Kiegészítés karbantartását a Szolgáltató Szabályzatért Felelős Egysége végzi. A szabályzatokkal és szerződésekkel kapcsolatos kérdésekkel és észrevételekkel közvetlenül a Szolgáltató Szabályzatért Felelős Egysége kereshető meg a Szolgáltató info@netlock.hu e-mail címen (ld. még 1.5.1 pont).

## 1.5.5 Szabályzat-jóváhagyási eljárás

Lásd 7.4-es pont.

## 1.6 Fogalmak és rövidítések

### 1.6.1 Fogalmak

- **Alany:** A tanúsítvány alany (Subject) mezőjében megadott adatokkal meghatározott természetes személy, aki a tanúsítványban szereplő nyilvános kulcs párját jelentő magánkulcs felett rendelkezik.
- **Aláírás-ellenőrző adat:** Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.
- **Aláírás-létrehozó adat:** Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az Aláíró az elektronikus aláírás létrehozásához használ.
- **Aláírás-létrehozó eszköz:** Szoftver vagy hardver, melynek segítségével az Aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
- **Munkatársi tanúsítvány:** Olyan személyes tanúsítvány melyben az abban szereplő természetes személyt a másodlagos alany saját magához tartozónak ismeri el.
- **Alkalmazó Közösség:** A PKI rendszert alkalmazó, működtető entitások összessége.
- **Common Name (CN):** Az Alany tanúsítványban szereplő, szokásos megnevezéséből képzett neve.
- **Distinguished Name (DN):** A tanúsítványban szereplő, szokásos megnevezéséből, lakóhely vagy székhely szerinti város, ország megnevezéséből, valamint e-mail címéből képzett egyedi neve.
- **Elektronikus aláírás:** Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
- **Ellenőrzési lépések:** Az elektronikus aláírás ellenőrzésekor kötelezően végrehajtandó lépések, melyeket a Szolgáltatási Szabályzat Kiegészítés tartalmaz.
- **Eredeti példány:** Magán- vagy jogi személy azonosító okmány eredeti aláírásokat és pecsétet tartalmazó példánya, vagy ezek hitelesített másolata.
- **Érintett Fél:** Az a személy, aki elektronikus aláírás érvényességének ellenőrzése, illetve hiteles időpont megállapítása céljából a Szolgáltató által kibocsátott tanúsítványhoz, illetve időbélyeghez fordul.
- **Felügyelet:** Nemzeti Hírközlési Hatóság, a Hitelesítés-szolgáltatók felügyeleti szerve.
- **Fizikailag biztosított terület:** Olyan helyiség, amely ésszerű határok mellett képes megvédeni a benne elhelyezett eszközöket az elemi károktól, illetve a szándékos illetéktelen hozzáféréstől.
- **Fokozott biztonságú elektronikus aláírás:** Elektronikus aláírás, amely megfelel a következő követelményeknek:
  - alkalmas az Alany azonosítására és egyedülállóan hozzá köthető,

- olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak,
- a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető.
- **Folyamatosan elérhető szolgáltatás:** az év 365 napján a nap 24 órájában elérhető szolgáltatást jelenti (a karbantartási műveletek figyelembe vételével).
- **Hash:** Ld. Lenyomat.
- **Hitelesítő Alegységek:** Az MKB végfelhasználói tanúsítványokat létrehozásában közreműködő infrastruktúra alegységek, amely üzemeltetésében az MKB részt vesz.
- **Hozzáférések:** Egy adott számítógépes hálózat vagy annak egyes elemei elérésére vonatkozó szabályok összessége.
- **Információbiztonsági irányítási rendszer:** irányítási rendszer egy szervezet vezetésére és szabályozására, az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése szempontjából.
- **Kihelyezett Szolgáltató Alegység:** A jelen Szolgáltatási Szabályzat Kiegészítésben meghatározott feltételeknek megfelelő végfelhasználói tanúsítványok kibocsátásában, kezelésében való közreműködéssel kapcsolatos szolgáltatói feladatok összessége.
- **Késedelem nélküli cselekedet:** A mindenkorai technikai feltételek által megengedett lehető leggyorsabb intézkedést jelenti.
- **Közhiteles nyilvántartás:** olyan, hatóság által vezetett nyilvántartás, melynek tartalmát, az abban szereplő adatok valóságát az ellenkező bizonyításig mindenki köteles elfogadni. Ilyen közhiteles nyilvántartás a cégnyilvántartás, valamint a polgárok személyi és lakcím adatait tartalmazó nyilvántartás.
- **(Kriptográfiai) Kulcs:** Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.
- **Lenyomat:** Olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:
  - a képzett lenyomat egyértelműen származtatható az adott elektronikus dokumentumból,
  - a képzett lenyomattól az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés,
  - a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, amelyre alkalmazva a lenyomatképző eljárás eredményeképp az adott lenyomat keletkezik.
- **Magánkulcs védelme:** Mindazon tevékenységek összessége, melyek célja a magánkulcs megfelelő védelme, a magánkulcs teljes élettartama során annak generálásától, annak megsemmisítéséig, a hozzá tartozó tanúsítvány státuszától függetlenül.
- **Másolati példány:** Eredeti okmányról készült másolat.
- **Másodlagos alany:** Az jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amely a munkatársi tanúsítvány alanyával együttesen szerepel a tanúsítványban és aki az alanyt saját magához tartozónak ismeri el.
- **Minősített elektronikus aláírás:** olyan - fokozott biztonságú - elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.
- **MKB Kihelyezett Szolgáltató Alegység:** lásd: Kihelyezett Szolgáltató Alegység

- **Munkatárs:** A természetes személyek azon köre, amelyeket egy adott szervezet saját magához tartozóként ismer el.
- **MKB Központ:** MKB hitelesítési rendszer irányításáért felelős szervezeti egység, az MKB Bankbiztonság Működési kockázatkezelési osztályának IT biztonsági csoportja.
- **Out-of-band:** Elektronikus információk szokásos használati környezetén kívül történő előállítási, továbbítási módja.
- **Összesített felelősség:** Tanúsítványok és kéresemények alapján történő összesítés szerinti felelősség, a tranzakciók, elektronikus aláírások, és alkalmazások számától függetlenül.
- **Publikus (Nyilvános) Kulcsú Infrastruktúra:** A tanúsítványok kibocsátásában és kezelésében, valamint az időbélyegzésben részt vevő technikai eszközök, egységek, ezen tevékenységeket hivatalosan felügyelő és meghatározó intézmények, a felhasználók által alkalmazott kriptográfiai eszközök és tevékenységek összessége.
- **Regisztrációs Alegység:** Az ügyfelek adatait ellenőrző, tanúsítvány kibocsátási, felfüggesztési, visszavonási kérelmeket összeállításban közreműködő egység, amelynek üzemeltetésében az MKB közreműködik.
- **Subject Name (SN):** Az alany megnevezése, egyedi neve (DN).
- **Szabályzatért Felelős Egység:** A jelen és kapcsolódó szabályzatok kialakításáért, elfogadásáért és adminisztrációjáért felelős szolgáltatói egység.
- **Szolgáltatási Szabályzat:** A [1] Törvény 2. § (20) alapján a Szolgáltató hitelesítési tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum.
- **Szolgáltatási Szabályzat Kiegészítés:** A Szolgáltatónak az adott Szolgáltatási Szabályzat Kiegészítés által szabályozott specifikus hitelesítési tevékenységgel kapcsolatos részletes kiegészítő és specifikus eljárási és egyén működési szabályokat tartalmazó nyilvános dokumentum.
- **Szolgáltató:** A NetLock Kft., amely az MKB Kihelyezett Szolgáltató Alegység számára a szükséges láncolt szolgáltatói tanúsítványt biztosítja.
- **Tanúsítvány:** A Szolgáltató által kibocsátott elektronikus igazolás, amely az aláírás-ellenőrző adatot a tanúsítvány alanyához kapcsolja.
- **Tanúsítvány-szolgáltatás:** azon eljárás, melynek során az MKB Kihelyezett Szolgáltató Alegység Szolgáltatási Szabályzat Kiegészítésben meghatározott eljárásban új vagy megújított, aláíró és titkosító célú tanúsítványt bocsát ki a felhasználó részére. A tanúsítvány-szolgáltatáshoz kapcsolódóan a Kihelyezett Szolgáltató Alegység tanúsítványállapot-szolgáltatást is nyújt, melynek keretében fogadja a tanúsítvány-visszavonási- és felfüggesztési kérelmeket és a Szolgáltatási Szabályzat Kiegészítésben meghatározott időközönként Tanúsítvány Visszavonási Listát bocsát ki.
- **Tanúsítványfajta:** Jelen Szolgáltatási Szabályzat Kiegészítés egy megjelenési formáját ismeri: a munkatársi.
- **Tanúsítványállapot-nyilvántartás:** A legközelebb kibocsátásra kerülő Tanúsítvány Visszavonási Lista tartalmához kapcsolt on-line lekérdezhető információk. Ezen információk joghatással nem bírnak.
- **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.
- **Végfelhasználó:** Szerződéses partner, aki az MKB által kibocsátott végfelhasználói tanúsítvánnyal rendelkezik.

- **Végfelhasználói tanúsítvány:** Az MKB Kihelyezett Szolgáltató Alegység által kibocsátott olyan tanúsítvány, amelyet az alany kizárólag elektronikus aláírás előállítására használhat, de más tanúsítvány hitelesítésére nem. A végfelhasználó tanúsítvány szervezet mezőjében kizárólag az MKB Bank Zrt., illetve az MKB Üzemeltetési Kft. kerülhet feltüntetésre.

## **2 Közzététel és tanúsítványtár**

### **2.1 Az információ közzététele**

#### **2.1.1 Közzétételi és tájékoztatási elvek**

##### **2.1.1.1 A Szolgáltatási Szabályzat Kiegészítésben nem tárgyalt elemek**

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti. Szolgáltató több belső biztonsági és egyéb szabállyal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen Szabályzat több ilyen is megemlít). Jelen Szolgáltatási Szabályzat Kiegészítésben nem tárgyal kérdések kapcsán a Szolgáltató egyéb szabályzatai az irányadóak.

##### **2.1.1.2 A Szolgáltatási Szabályzat Kiegészítés közzététele**

A Szolgáltató a Szolgáltatási Szabályzatot Kiegészítést weboldalán ([www.netlock.hu](http://www.netlock.hu)) keresztül hozza nyilvánosságra, valamint az Alanyok számára az MKB belső weblapján is elérhető.

##### **2.1.1.3 Észrevételek kezelése**

A Szolgáltatási Szabályzat Kiegészítéssel kapcsolatos észrevételeket Szolgáltató az [info@netlock.hu](mailto:info@netlock.hu) címen, valamint a Kihelyezett Szolgáltató Alegység a [euateam@mkb.hu](mailto:euateam@mkb.hu) címen fogadja.

A Kihelyezett Szolgáltató Alegység a beérkezett észrevételek 3 munkanapon belül továbbítja a Szolgáltató felé.

### **2.2 Tanúsítványokkal kapcsolatos információk**

#### **2.2.1 Tanúsítványok közzététele**

A Szolgáltató saját, illetve Kihelyezett Szolgáltató Alegységének tanúsítványát a következő módszerekkel teszi közzé:

- saját szolgáltatói tanúsítványát közzéteszi tanúsítványtárában, illetve saját weboldalán;
- minden Kihelyezett Szolgáltató Alegységének tanúsítványát közzéteszi a tanúsítványtárban, illetve saját weboldalán.

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat az alany és a másodlagos alany hozzájárulása alapján közzéteszi nyilvános tanúsítványtárában.

#### **2.2.2 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala**

A Szolgáltató az általa működtetett Kihelyezett Hitelesítő Alegységek tanúsítványával kapcsolatos állapotinformációkat a következő módszerekkel teszi közzé:



- szolgáltatói tanúsítványainak állapotváltozását a saját tanúsítványtárában tünteti fel.

A Szolgáltató hitelesítő egységei által kiadott végfelhasználói tanúsítványokkal kapcsolatos állapotinformációkat a következő módszerekkel teszi közzé:

- a végfelhasználói tanúsítványok állapotváltozását a tanúsítványtárában hozza nyilvánosságra,
- végfelhasználói tanúsítvány visszavonását és felfüggesztését Szolgáltató akkor is nyilvánosságra hozza, ha a tanúsítvány közzétételéhez az alany (igénylő) nem járult hozzá.

## **2.3 A közzététel gyakorisága**

### **2.3.1 Tanúsítványok nyilvánosságra hozatalának gyakorisága**

A Szolgáltató a nem minősített munkatársi aláíró, ideiglenes munkatársi aláíró és titkosító tanúsítványok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:

- Szolgáltató a Kihelyezett Szolgáltató Alegység láncolt szolgáltatói tanúsítványait a kibocsátást követő 1 munkanapon belül teszi közzé,
- a Szolgáltató a kibocsátott végfelhasználói tanúsítványokat az alany és a másodlagos alany hozzájárulása alapján közzéteszi nyilvános tanúsítványtárában.

### **2.3.2 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága**

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokkal kapcsolatos állapotinformációkat a 4.10.1 pontban tárgyalt gyakorisággal teszi közzé.

## **2.4 Hozzáférés ellenőrzések**

A Szolgáltató által közzétett kikötések és feltételek, rendkívüli információk, tanúsítványok és állapotinformációk nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közlő közegek sajátosságainak megfelelően. A tanúsítványok és állapotinformációk elérése kapcsán az Érintett Felek részére a Szolgáltató által kibocsátott tanúsítványok, illetve időpont hitelesítésének ellenőrzésére jelen Szabályzat tartalmaz ajánlásokat.

A Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató különböző védelmi mechanizmusokkal akadályozza meg az információkhoz való jogosulatlan hozzáféréseket.

### **2.4.1 Tanúsítványtárak**

A Szolgáltató az Érintett Felek számára a rendelkezésére álló legpontosabb adatokat biztosítja a lehetőségeknek, vállalásoknak megfelelően leghamarabb, és ennek érdekében nyilvános Tanúsítványtárat üzemeltet az Internet címén (lásd 1.5 pont). A tanúsítványtárban a Szolgáltató, valamint a Szolgáltató Kihelyezett Szolgáltató Alegységei által kibocsátott tanúsítványok és a visszavont tanúsítványok listái (nyilvános rész) találhatóak.

A Szolgáltató tanúsítványtára szabványos HTTP, illetve HTTPS protokollokkal érhető el a Szolgáltató Internetes oldalain keresztül (ld. 1.5 alfejezet), az ott megvalósított lekérdezési műveletekkel.

A Szolgáltató tanúsítványtár elérhetőségét folyamatosan (az év minden napján, 0–24h) biztosítja a karbantartáshoz szükséges idők kivételével (folyamatosan elérhető szolgáltatás). A Szolgáltató a tervezett karbantartásokat lehetőleg munkaidőn kívüli időszakokra ütemezi.

A Szolgáltató által kibocsátott tanúsítványok nyilvántartása, a visszavonási nyilvántartások, valamint az online tanúsítvány állapot lekérdezési lehetőség legalább 99,9%-os rendelkezésre állással elérhető, egyúttal az eseti szolgáltatás kiesések nem haladják meg a 24 órás időtartamot.

## 3 Azonosítás és hitelesítés

### 3.1 Elnevezések

A nevek regisztrációjának szabályai valamennyi tanúsítványfajtára vonatkoznak.

#### 3.1.1 Névtípusok

##### 3.1.1.1 Általános szabályok

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

- a tanúsítványban az adatok speciális és vezérlő karakterek nélkül szerepelnek,
- a nevek egyes egységeit szóköz választja el,
- a „*Title*” mező opcionálisan tartalmazhatja az alany beosztását,
- a tanúsítványban a „*CN*” mező nem üres,
- a tanúsítványban a „*CN*” mező a személyazonosság igazolására elfogadott hatósági igazolványban (lásd 3.2.3 pont) foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint van feltüntetve „*CN*” és „*SN*” mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév), az UTF-8 kódolást használva,
- munkatársi tanúsítványokban az „*Organization*” mezőben mindig az MKB Bank Zrt. vagy az MKB Üzemeltetési Kft. szerepel másodlagos alanyként, valamint az „*Organization-unit*” mezőben szerepelhet az MKB Bank Zrt., illetve az MKB Üzemeltetési Kft. szervezeti egysége,
- a „*Locality*” mezőben az MKB Bank Zrt., illetve MKB Üzemeltetési Kft. székhelye vagy telephelye kerül feltüntetésre,
- a az MKB Bank Zrt., illetve az MKB Üzemeltetési Kft. az ISO 3166 [3] szabványban meghatározott kétkarakteres ország kódként a „HU”-t alkalmazza.

#### 3.1.2 Álnév használata

##### 3.1.2.1 Általános szabályok

A Szolgáltató Kihelyezett Szolgáltató Alegysége nem működik közre álnevet tartalmazó tanúsítvány kibocsátásában.

#### 3.1.3 Különböző elnevezési formák értelmezési szabályai

##### 3.1.3.1 Kibocsátó azonosító

A kibocsátó azonosítója úgy értelmezendő, hogy a tanúsítványt a NetLock Kft. mint Hitelesítés-szolgáltató adta ki (székhely, elérhetőség: ld. 1.5 alfejezet). Az aláíró tanúsítvány magánkulcs párja a jogszabályok szerint fokozott biztonságú elektronikus aláírások létrehozására alkalmas.

Az *Issuer* mező a tanúsítvány kibocsátójának székhely szerinti országkódját (*Country - HU*), a szervezet nevét (*Organization - Szolgáltató*), szervezeti egységét (*Organization Unit*) és az adott tanúsítványkiadó megnevezését (*Common Name*) tartalmazza.

### 3.1.3.2 Alanyazonosító

#### 3.1.3.2.1 Általános szabályok

Az alany azonosítója úgy értelmezendő, hogy a tanúsítvány alanya a *Common Name* nevű természetes személy, aki az *Organization* nevű szervezet (jelen esetben: MKB Bank Zrt. vagy MKB Üzemeltetési Kft.) *Organization-unit* osztályához, illetve szervezeti egységéhez tartozik. Az azonosításban egyéb mezők is értelmezettek lehetnek.

A természetes személy nevei (családi, elő- és utóneve) betű szerint megegyezően, ékezetes betűket eredeti írásmódjuk szerint feltüntetve – UTF-8 kódolással - olyan sorrendben szerepelnek a *Common Name* mezőben, ahogyan azok a személyazonosságát igazoló okmányban. A nevek egyes egységeit szóköz választja el.

A szervezet székhelye vagy telephelye a *Country* országban, *Locality* településén található. Amennyiben feltüntetésre kerül, a *Title* mező tartalmazza az alany beosztását.

Az alanyazonosító mezőnek célja, hogy a tanúsítvány alanyát (a felhasználó egységen belül) azonosítani lehessen. Az alany és a másodlagos alany egység(ek) együttes megjelenítése a tanúsítványban azt jelenti, hogy a másodlagos hozzájárult az alany(ok) és az egység(ek) nevének együttes feltüntetéséhez.

Az alany e-mail címe az igénylő egységgel összefüggésben a *SubjectAltName*-ben az *rfc822Name*.

### 3.1.4 A nevek egyedisége

A Szolgáltató által kibocsátott összes tanúsítvány esetében a tanúsítványok alanyait egymástól egyértelműen megkülönbözteti a tanúsítványban rögzített összes személyes adatuk (név, lakóhely ország, lakóhely város, e-mail cím, illetve a szolgáltató által esetleg generált sorszám) segítségével (egyedi név).

#### 3.1.4.1 Eljárások a nevekre vonatkozó vitás kérdések megoldására

A Szolgáltató fenntartja magának a jogot a név kiosztással kapcsolatos mindennemű döntés tekintetében. A tanúsítvány alanyának bizonyítani kell a jogát egy adott név használatára. A nevek kiosztása érkezési sorrend alapján történik, azaz a később érkező nem kérheti egy már korábban kiosztott név újrakiosztását még akkor sem, ha a kívánt névvel kapcsolatos tanúsítvány már érvényét veszítette.

## 3.2 Kezdeti azonosítás

### 3.2.1 A magánkulcs birtoklásának bizonyítási módszere

A kulcspár generálását az Alany végzi az intelligens kártyára. A Szolgáltató által alkalmazott ellenőrzési folyamatok biztosítják, hogy az aláíró tanúsítványhoz kapcsolódó kulcspár a chipkártyán került

generálásra. A titkosító tanúsítványhoz tartozó magánkulcs generálása szoftveresen történik, és utólag kerül feltöltésre az intelligens kártyára.

A Szolgáltató ellenőrzi, hogy a nyilvános kulcs korábban nem került-e kiosztásra más alany számára.

### **3.2.2 Szervezeti azonosság hitelesítése**

A Szolgáltató MKB Kihelyezett Szolgáltató Alegysége által kibocsátott tanúsítványokban feltüntetésre kerül a felhasználó szervezet (másodlagos alany). Opcionálisan egyéb adatok is feltüntetésre kerülhetnek.

A szervezet *Organization* mezőben minden esetben az MKB Bank Zrt. vagy az MKB Üzemeltetési Kft. kerül feltüntetésre. A tanúsítványba kerülő szervezetek adatai a Humánpolitikai Rendszerben naprakészen minden esetben megtalálhatóak.

### **3.2.3 Személyazonosság hitelesítése**

A Szolgáltató Kihelyezett Szolgáltató Alegysége a természetes személy azonosításában az egyes tanúsítványfajták esetében a 4.2.2 pont alatti táblázatban leírt módon vesz részt.

A személyazonosításra alkalmas hivatalos igazolványban szereplő fénykép alapján az alanynek egyértelműen felismerhetőnek kell lennie, a benne szereplő aláírásának meg kell egyeznie a szolgáltatási szerződésen tett aláírásával. Amennyiben kétség merül fel a fénykép vagy az aláírás megfeleltethetősége kapcsán, a Szolgáltató megtagadja a tanúsítványkiadási kérelem teljesítését.

A Szolgáltató továbbá megállapítja mindazon adatok hitelességét, melyeket a tanúsítványban feltüntet.

## **3.3 Azonosítás tanúsítvány kulcscseréje esetén**

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 (lásd 4.2.2 pont).

## **3.4 Visszavonási kérelem**

Szolgáltató visszavonási és -felfüggesztési szolgáltatásokat egyaránt nyújt. Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait a 4.9.4 pont tárgyalja.

## 4 Működésre vonatkozó követelmények

### 4.1 Tanúsítványigénylés

#### 4.1.1 Igénylés feltételei

A Szolgáltató Kihelyezett Szolgáltató Alegységétől tanúsítványt igényelhet:

- természetes személy saját részére, feltüntetve a tanúsítványban, hogy meghatározott szervezethez, jelen esetben az MKB-hez, vagy az MKB Üzemeltetési Kft.-hez tartozik,
- a munkavállaló szervezeti egységének vezetője a munkavállaló részére, feltüntetve a tanúsítványban, hogy meghatározott szervezethez, jelen esetben az MKB-hez, vagy az MKB Üzemeltetési Kft.-hez tartozik,

Kizárólag a jelen Szolgáltatási Szabályzat Kiegészítésben megadott és hivatkozott fajtájú és profilú tanúsítványok igényelhetők.

### 4.2 Tanúsítványkérelem feldolgozása

Végfelhasználói tanúsítványok kibocsátására a tanúsítványigénylési eljárás lefolytatását követően kerül sor. A tanúsítvány elkészítésére az új tanúsítványigénylés során a kérelemben megadott, a szolgáltatási szerződésben megerősített, ellenőrzött, illetve érvényesnek elismert adatok alapján kerül sor.

A tanúsítványigénylés feltételeinek teljesülése esetén az MKB Kihelyezett Szolgáltató Alegység feldolgozza a tanúsítványkérelmet a következőkben bemutatott eljárásrend szerint.

#### 4.2.1 Általános regisztrációs szabályok

A Kihelyezett Szolgáltató Alegység által végzett regisztrációs eljárásra vonatkozó alapelvek

- az eljárást a Regisztrációs Alegység munkatársai végzik el,
- az eljárást minden új tanúsítványigénylés esetében teljes egészében le kell folytatni,
- az eljárás részben automatizált, elektronikus rendszereken keresztül zajló, részben humán beavatkozással végzett folyamat,
- a megadott személyes és szervezeti adatok ellenőrzését a Kihelyezett Szolgáltató Alegység saját Regisztrációs Adminisztrátorai végzik. A tanúsítványkérelmet a regisztrációs adminisztrátorok felelősek kezelni, miután azonosították az alanyt.

##### 4.2.1.1 Általános regisztrációs lépések

- az igénylő tanúsítványigénylési kérelmet juttat el az MKB Kihelyezett Szolgáltató Alegységhez, melynek során elfogadja a tanúsítványkibocsátáshoz kapcsolódó feltételeket;
- az MKB Kihelyezett Szolgáltató Alegység fogadja a kérelmet, illetve ellenőrzi annak szabályosságát,
- megtörténik a tanúsítványigénylési kérelem jóváhagyása a felettes vezető, vagy annak helyettese által;

- az MKB Kihelyezett Szolgáltató Alegység azonosítja az igénylő természetes személyt, és a szervezeti adatokat,
- a Regisztrációs Alegység elkészíti szolgáltatási szerződését, előkészíti a további regisztrációhoz szükséges dokumentumokat,
- az MKB Kihelyezett Szolgáltató Alegység, amennyiben a személy- és szervezetazonosítás rendben lezárult, értesíti a felhasználóhoz tartozó Lokális Regisztrációs Adminisztrátort, hogy allokáljon egy kártyát a felhasználó részére.
- a Regisztrációs Adminisztrátor meghatározott lépésekben összerendeli a kártyát a felhasználóval;
- a Regisztrációs Adminisztrátor értesíti a folyamat befejezéséről a Lokális Regisztrációs Adminisztrátort, aki átadja a kártyát a felhasználónak;
- a kártya átvételének feltételeként a felhasználó aláírja a felhasználói nyilatkozatot és a Lokális Regisztrációs Adminisztrátor ismerteti vele a Felhasználói tájékoztató elérhetőségét;
- a felhasználó e-mailben értesítést kap a további teendőkről, illetve megkapja az egyszer használatos kódot a felhasználói portálhoz;
- a kártya és az egyszer használatos kód segítségével a felhasználó belép a kártyamenedzsment portálra, inicializálja a kártyát és megkapja rá az igényelt és jóváhagyott tanúsítványokat.

#### 4.2.1.2 A regisztráció során nyilvántartásba vett adatok köre

- az azonosítási dokumentumok egyedi azonosító adatai, és azonosító számai,
- a kérelem és az azonosítási dokumentumok – beleértve az Aláíró féllel kötött megállapodást – másolatainak tárolási helyszíne,
- az ügyfélnek a rá vonatkozó kötelezettségekkel történő egyetértése,
- a kérelmet elfogadó egység azonosítója,
- minden, a tanúsítványok kiadásához kapcsolódó információ.

A Szolgáltató a nyilvántartásokat a jogszabályi előírásoknak megfelelően addig, ameddig a tanúsítványokra jogi eljárások során bizonyítási célból szükség lehet, megőrzi.

## 4.2.2 Regisztrációs eljárás

### 4.2.2.1 A regisztráció folyamata

Eljárási lépés	Tanúsítványfajta
	Munkatársi
1. Alany regisztrációja	Munkavállaló adatai elektronikus úton, a Humánpolitikai Rendszerből kerülnek átvételre. A regisztráció támogatásárára az alany az elektronikus regisztrált adatait alátámasztó dokumentumok eredeti példányát a regisztrációs alegység munkatársai előtt bemutatja. Személyazonosság ellenőrzésekor személyazonosításra alkalmas dokumentum, az az személyi igazolvány vagy útlevél vagy „új” típusú (bankkártya méretű) jogosítvány és a lakcímkártya fogadható el.
2. Másodlagos alany regisztrációja (kapcsolt regisztráció)	Szervezet adatait a Humánpolitikai Rendszer napra készen tartalmazza.
3. Igénylés jóváhagyása	Végrehajtani jogosult: felettes vezető, illetve annak helyettese
4. Regisztráció jóváhagyása	Végrehajtani jogosult: Regisztrációs Egység

Eljárási lépés	Tanúsítványfajta
	Munkatársi
5. Alany személyazonosságának ellenőrzése	Az Alany személyazonosságát a Hordozóesz köz átadását megelőzően a Lokális Regisztrációs Adminisztrátor személyazonosító fényképes igazolvány segítségével ellenőrzi.
6. Kártyakísérő űrlap aláírása és másolatának átadása az alanynak	A személyazonosság ellenőrzését követően a Lokális Regisztrációs Adminisztrátor aláírja a kártyakísérő űrlapot.
7. Hordozóesz köz átadása az aláírónak	A személyazonosság ellenőrzését követően a Lokális Regisztrációs Adminisztrátor kártyakísérő űrlap aláírását követően átadja az intelligens kártyát és a kártyaolvasót.
8. Kulcspár generálása kérelem készítése	Végrehajtani jogosult: Alany. Az aláíró tanúsítvány magánkulcsának generálása az esz közön történik, míg titkosító tanúsítvány magánkulcsának generálására szoftveresen kerül sor és utólagosan kerül feltöltésre az intelligens kártyára.
9. Tanúsítvány előállítás	Végrehajtani jogosult: Regisztrációs Alegység
10. Tanúsítvány hordozó esz közre való letöltése	Végrehajtani jogosult: Alany.
11. Tanúsítvány tanúsítványtárban való közzététele	Végrehajtani jogosult: Regisztrációs Alegység, az Alany hozzájárulása esetén.
12. Dokumentáció archíválása	Végrehajtani jogosult: Regisztrációs Alegység.

### 4.2.3 Szolgáltatási szerződés

A természetes személy és a magánkulcs összetartozásának dokumentálására, illetve a kötelező tájékoztatásra a Szolgáltató szolgáltatási szerződést alkalmaz. A szerződés feltételeit a Szolgáltató szabályzatai, jelen Szolgáltatási Szabályzat Kiegészítés, illetve az aláíró elfogadó nyilatkozata tartalmazza. A szolgáltatási szerződést ezen dokumentumok együttese jelenti. A tanúsítvány kiadásának feltétele ezen szerződés létrejötte.

Az MKB Kihelyezett Szolgáltató Alegység által kibocsátott tanúsítvány esetében az aláírás-hitelesítést a Regisztrációs Alegység előtt kell elvégezni.

A nyilatkozat, vagy melléklete legalább a következőket tartalmazza:

- a kiadandó tanúsítvány „*Subject*” mezője (alanyazonosító),
- az alany azonosításához szükséges egyéb adatok,
- a korlátozások, elfogadások,
- a Szolgáltató által adatlapon közölt adatok.

Az elfogadó nyilatkozatot az igénylő természetes személy írja alá.

### 4.2.4 A tanúsítványkérelmek jóváhagyásának követelményei

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

- benyújtották a kérelmet a tanúsítvány kibocsátónak,
- a természetes személy (akinek nevében az igénylő eljár) azonos a kérelemben szereplő alannal,
- a kérelemben szereplő adatok ellenőrizhetők és pontosak.

### 4.2.5 A tanúsítványok tartalma

A végfelhasználói tanúsítványok tartalmazzák az alábbiakat:



- a tanúsítvány azonosító kódját,
- az MKB Bank Zrt., illetve az MKB Üzemeltetési Kft. megnevezését, benne székhelyének vagy telephelyének megnevezését, ország-azonosítóját,
- a tanúsítvány érvényességi idejének kezdetét és végét (amely nem lehet az érvényesség kezdete időpontnál korábbi); az érvényesség időtartama nem haladja meg a 2 évet,
- az Alany nevét,
- azt az aláírás-ellenőrző adatot (nyilvános kulcs), amely az Alany által birtokolt aláírást készítő adat párjának (magánkulcs) felel meg,
- a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
- az adott tanúsítványt kibocsátó alárendelt hitelesítés-szolgáltató elektronikus aláírását.

#### **4.2.6 A tanúsítványok jellemzői**

A Szolgáltató által kibocsátott tanúsítványok megfelelnek a következő követelményeknek:

- a tanúsítványazonosító a kibocsátóra nézve egyedi,
- a tanúsítványban foglalt megkülönböztetett név (DN, Distinguished Name) egyedi,
- a kiadott tanúsítványokhoz tartozó kulcsok egyediek, ez alól természetesen kivételt jelent a megújított tanúsítványban szereplő kulcs,
- a tanúsítványok az MKB Kihelyezett Szolgáltató Alegység nem minősített szolgáltatói kulcsával vannak aláírva,
- a tanúsítványok aláírása ellenőrizhető a tanúsítványban szereplő adatok és az MKB Kihelyezett Szolgáltató Alegység megfelelő nyilvános kulcsának felhasználásával.

#### **4.2.7 Az igénylő (alany) tájékoztatása a kibocsátást megelőzően**

A Szolgáltató a tanúsítvány igénylőjét (alanyát) magyar nyelven, közérthetően és egyértelműen tájékoztatja a következőkről:

- a szolgáltatás igénybevételének feltételei,
- a felhasználó jogai és kötelezettségei,
- a magánkulcs felhasználásának és kezelésének gyakorlati módszere és szabályai,
- a magánkulcs elvesztésének, kompromittálódásának veszélyei,
- a tanúsítványok kibocsátásának körülményei,
- a tanúsítvány használatának feltételei,
- a tanúsítvánnyal kapcsolatos, a tanúsítványban meghatározott tárgybeli, időbeli, földrajzi vagy egyéb korlátozások,
- a tanúsítvány érvényessége, érvényességi idejének lejárta,
- az aláírás-létrehozó adat használatával kapcsolatosan szükséges biztonsági intézkedések,
- az aláírás létrehozó eszköz használata,
- az Alany és az aláírást ellenőrizni kívánó felek felelőssége, kötelezettségei,
- a tanúsítvány minősége, a tanúsítvány magánkulcs párjával végzett műveletek joghatásai,
- a tanúsítványok visszavonásának, felfüggesztésének lehetősége,
- a szolgáltatói nyilvános kulcs, valamint annak elérhetősége,
- a panaszok benyújtására, a jogviták rendezésére vonatkozó szabályok.

#### **4.2.8 Tanúsítványkérelmek elutasítása**

A Szolgáltató Kihelyezett Szolgáltató Alegysége elutasítja a tanúsítványkérelmeket, amennyiben

- a tanúsítványigénylés nem teljes,
- a tanúsítványigénylés nem helyes,
- a felettes személy, illetve annak helyettese a tanúsítványigénylést nem hagyta jóvá,
- a személyazonosság ellenőrzése során kétsége merül fel,
- a személy szervezethez tartozása nem egyértelmű,
- a személy kiléte nem állapítható meg minden kétséget kizáróan,
- az igénylő felhatalmazása a tanúsítvány kibocsátásának kérésére nem egyértelmű.

Az elutasított kérelmekről az igénylő értesítést kap, melyben szerepel az elutasítás indoka. Amennyiben az elutasítás oka harmadik fél által szolgáltatott információ, az értesítés megnevezi az elutasítást eredményező információforrást is.

#### **4.2.9 A tanúsítványokra vonatkozó további rendelkezések**

A tanúsítvány előállításánál a Szolgáltató biztosítja a tanúsítványt kérő üzenet sértetlenségét, az adatforrás hitelességét, és ahol szükséges, annak bizalmasságát, illetve a személyhez fűződő jogok védelmét.

### **4.3 A tanúsítványok kibocsátása és hozzáférhetővé tétele**

A Regisztrációs Alegységek a 4.2.2 pontban leírt módon feldolgozzák a kérelmet, illetve előállítják a tanúsítványt. A kész tanúsítvány a Tanúsítványtárba kerül.

#### **4.3.1 A tanúsítvány kibocsátásának időpontja**

A tanúsítvány kibocsátásának időpontja az az időpont, amikor a Szolgáltató az aláírt tanúsítványt elérhetővé teszi a tanúsítványtárban (ld. 2.4.1 alfejezet).

#### **4.3.2 A tanúsítvány érvényessége**

A tanúsítványban szereplő nyilvános kulcs magán párja csak a tanúsítványban megjelölt időintervallumban, de maximum 2 évig használható elektronikus aláírások készítésére. A nyilvános kulcs a kriptográfiai biztonságának periódusában használható aláírás ellenőrzésére. A tanúsítvány érvényességének ellenőrzése a tanúsítványt használó alany, illetve Érintett Fél felelőssége.

### **4.4 Tanúsítványelfogadás**

#### **4.4.1 A tanúsítvány elfogadása**

A magánkulcs használatba vétele előtt az alany, illetve a másodlagos alany kötelessége ellenőrizni a tanúsítványban feltüntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál, a magánkulcsot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonása érdekében.

A magánkulcs és a tanúsítvány elfogadottnak tekintendő, ha az alany a hordozóeszközt átvette, a kulcsgenerálást az Alany hajtotta végre (tanúsítvány fajtától függően az eszközön, illetve szoftveren), valamint a tanúsítványt letöltötte.

## 4.4.2 A tanúsítványigénylő nyilatkozata

A tanúsítvány elfogadásával együtt az alany, illetve a másodlagos alany kijelenti, hogy:

- ismeri, érti és elfogadja a tanúsítványkiadásához kapcsolódó szabályzatokat,
- a tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályoknak és törvényi előírásoknak megfelelően használja,
- minden adat amely a tanúsítványban szerepel a valóságnak megfelel, és azok átadása önkéntes volt,
- a tanúsítványban szereplő minden adat a tudomásával és egyetértésével került a tanúsítványba,
- a tanúsítvány érvényességét befolyásoló tényekről, valamint az igénylés során megadott személyes adatok megváltozása esetén haladéktalanul értesíti a Szolgáltató Kihelyezett Szolgáltató Alegységét, illetve a Szolgáltató arra illetékes szervét,
- tisztában van azzal, hogy a magánkulcs védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége,
- tisztában van a titkosítási műveletek készítésére vonatkozó szabályokkal és követelményekkel,
- minden aláírás az elfogadott és érvényes (nem felfüggesztett, visszavont vagy lejárt) tanúsítvány alapján készül,
- minden egyes elektronikus aláírást, amely a tanúsítványban szereplő nyilvános kulcs párjával készült, a saját aláírásának ismeri el,
- jogosulatlan személy nem férhet hozzá magánkulcsához,
- ismeri az elektronikus aláírás és elektronikus titkosítás megfelelő használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,
- tudomása van arról, hogy a fokozott biztonságú elektronikus aláírással ellátott elektronikus okiratok az írásbeliség, vagyis az egyszerű magánokirat jogszabályi követelményeinek felelnek meg,
- az alany végfelhasználó, azaz nem hitelesítés-szolgáltató, és nem fogja a tanúsítványban megadott nyilvános kulcs párját újabb tanúsítványok vagy bármely más formátumú tanúsított nyilvános kulcs, visszavonási lista, időbélyeg, OCSP válasz, viszontazonosítási válasz hitelesítésére és egyéb, hitelesítés-szolgáltatói funkciókra használni;
- amennyiben az alany beleegyezett a tanúsítvány nyilvánosságra hozatalába, felhatalmazza az Szolgáltatót a tanúsítvány közzétételével, és saját vagy más nyilvános tanúsítványgyűjtő helyeken történő elhelyezésével.

## 4.4.3 Tanúsítvány közzététele

A Szolgáltató a kiadott tanúsítványt a tanúsítvány előfizetője, illetve az alany és másodlagos alany hozzájárulása alapján közzéteszi.

## 4.5 A kulcspár és a tanúsítvány használata

### 4.5.1 Az alanyok számára szóló előírások

Az aláíró tanúsítványok elektronikus aláírások és ezzel üzenetek, dokumentumok integritásának ellenőrzésére használandók. Az elektronikus aláírás ellenőrzésével lehet meggyőződni arról, hogy

- az elektronikus aláírás a tanúsítványban szereplő nyilvános kulcs titkos párjával készült,
- az aláírt üzenet nem változott meg az elektronikus aláírás elkészülte óta.

Amennyiben a nyilvános kulcsú kódolást használó felek a szabályzatok és törvényi előírások szerint járnak el az elektronikus aláírások használatakor, akkor az elektronikus aláírt dokumentummal kapcsolatos jogos érdekeiket bíróság előtt érvényesíthetik. Ennek kapcsán az alany:

- a) magánkulcsát és tanúsítványát csak az Szolgáltatóval szerződésben rögzített korlátozásnak megfelelően használhatja,
- b) a megfelelő tanúsítvány lejárta után nem használhatja tovább magánkulcsát.

A titkosító tanúsítványok elektronikus üzenetek, dokumentumok titkosítására használhatók, ezzel biztosítva a dokumentumok, üzenetek bizalmasságát. A titkosított üzenet dekódolásával lehet meggyőződni arról, hogy

- a titkosítás a tanúsítványban szereplő nyilvános kulccsal készült
- a titkosított üzenet tartalma nem változott a feladás óta.

#### **4.5.1.1 Elektronikus aláírás készítése**

Az elektronikusan aláírt dokumentum előállításának folyamatáért elsősorban az Alany a felelős. Az Alany birtokolja a magánkulcsot, ismeri az aláírandó üzenet tartalmát, dönt az aláírási szándékról és üzemelteti az aláírást elvégző technikai eszközt.

Amennyiben az alany nem körültekintően jár el, úgy az ebből származó kárért ő, valamint a tanúsítványban feltüntetésre került másodlagos alany (MKB Bank Zrt. vagy az MKB Üzemeltetési Kft.) felel.

#### **4.5.1.2 Magánkulcs megőrzése**

Az elektronikus aláírás csak akkor biztonságos, ha a magánkulcs az Alanyon kívül soha, senki más számára nem hozzáférhető. A kulcsot hardvervédelemmel lehet ellátni. A kulcs elvesztéséből, véletlen vagy szándékos nyilvánosságra hozatalából eredő károkért az Alany felelős. A kulcs kompromittálódását az előírt módon az MKB Kihelyezett Szolgáltató Alegységéhez, vagy a Szolgáltatóhoz be kell jelenteni. A szabályosan bejelentett leiltási kérelem után a jelen Szolgáltatási Szabályzat Kiegészítés 4.9.1 pontjában meghatározott módon felel a felmerült károkért az Alany, a másodlagos alany, illetve a Szolgáltató.

A Szolgáltató az aláíró tanúsítványok magánkulcsait nem őrzi meg.

#### **4.5.1.3 Érvényes elektronikus aláírás következményei**

Az elektronikusan aláírt dokumentumok jogi hatással bírnak, amely a jogszabályokon kívül a felek – az Aláíró, az Érintett Fél és a Szolgáltató nyilatkozatain és szerződésein alapul, melyeket a felek a következő módon fogadnak el:

- az Alany a szolgáltatási szerződés aláírásával, a tanúsítványkérelem benyújtásával, illetve a tanúsítvány elfogadásával,
- az Érintett Fél az aláírás ellenőrzéséhez szükséges tanúsítvány, illetve az aláírt dokumentum elfogadásával.

## **4.5.2 Az Érintett Felek számára szóló előírások**

Nem érvényes elektronikus aláírás esetén, vagy ha az ellenőrzés nem a szabályzatok pontjainak megfelelően történt, az aláírás nem tekinthető valódinak és az elfogadásból eredő minden kár és kockázat az Érintett Felet terheli.

## **4.6 Tanúsítvány megújítása**

### **4.6.1 Végfelhasználói tanúsítványok**

A végfelhasználói tanúsítványok megújítását a Szolgáltató Kihelyezett Szolgáltató Alegysége nem végez.

### **4.6.2 Szolgáltatói tanúsítványok**

Az MKB Kihelyezett Szolgáltató Alegység láncolt szolgáltatói tanúsítványát a Szolgáltató 7 év időtartamra bocsátja ki.

## **4.7 Kulcscsere**

A kulcscsere az a folyamat, amelynek során egy megújított tanúsítvány kibocsátására úgy kerül sor, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai közül csak a nyilvános kulcs kerül lecserélésre.

Az MKB Kihelyezett Szolgáltató Alegysége kulcscserével történő tanúsítvány kibocsátási szolgáltatás nyújtást nem végez.

## **4.8 Tanúsítvány módosítása**

A tanúsítvány-módosítás az a folyamat, amelynek során a tanúsítvány kibocsátója úgy bocsát ki egy módosított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai – a nyilvános kulcs kivételével – változnak, és a tanúsítvány az új adatokkal, valamint a régi nyilvános kulccsal kerül kiadásra.

Tanúsítvány módosítását az MKB Kihelyezett Szolgáltató Alegysége nem végez.

## **4.9 Tanúsítvány felfüggesztése és visszavonása**

### **4.9.1 Általános rendelkezések**

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatásokat nyújt.

A felfüggesztett és visszavont tanúsítványok érvénytelenek. A felfüggesztett tanúsítvány azonban csak a felfüggesztés időtartama alatt érvénytelen. A felfüggesztés meghatározott időtartamra szól, annak letelte után a Szolgáltató, vagy a Szolgáltató Kihelyezett Szolgáltató Alegysége végleges döntést hoz (ld. még 4.9.10 pont).

A visszavont, illetve felfüggesztett tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. Amennyiben van rá lehetőség, a visszavont tanúsítványhoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni (ld. még 4.11 pont). A felfüggesztett, visszavont vagy lejárt tanúsítványokban szereplő nyilvános kulcsokat kizárólag addig lehet aláírás ellenőrzésre használni, amíg azok kriptográfiai biztonsága megfelelő.

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

- a visszavonási/felfüggesztési kérelem Szolgáltatóhoz, vagy a Szolgáltató Kihelyezett Szolgáltató Alegységéhez történő megérkezéséig az alany, illetve a másodlagos alany felelős a felmerülő károkért,
- az érvénytelen állapot tanúsítványtárban való megjelenése után az Érintett Fél felelős a felmerülő károkért.

#### 4.9.2 A visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásához a következő körülmények vezetnek:

- végfelhasználói, a láncolt szolgáltatói vagy a szolgáltatói magánkulcs kompromittálódása,
- a tanúsítvány alanyának kérelme,
- szervezeti egység vezető kérelme,
- a tanúsítvány használatának visszautasítása hibás tanúsítvány miatt,
- az MKB Kihelyezett Szolgáltató Alegység vagy a Szolgáltató tudomására jutott tény, vagy megalapozott vélelem a regisztrációs adatok valótlanágáról,
- a tanúsítványban foglalt adatok megváltozása,
- a tanúsítvány felfüggesztési idejének lejáratára,
- az alany és a másodlagos alany kötelezettségeinek be nem tartása,
- a NHH, bíróság vagy más hatóság erre vonatkozó jogerős és végrehajtható határozata,
- a szolgáltatási szerződés megszűnése,
- a hitelesítési szolgáltatói tevékenység megszűnése,
- visszavonást jogszabály teszi kötelezővé.

Kompromittálódott magánkulcs soha többet nem használható, és megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes magánkulcs.

#### 4.9.3 Visszavonás kérelmezése

A visszavonást az alábbi entitások kérelmezhetik:

Tanúsítványok	Visszavonást kérheti
Végfelhasználói tanúsítvány	Szolgáltató, Kihelyezett Szolgáltató Alegység, Felügyelet, Munkáltató (szervezeti egység vezetője)
Láncolt Szolgáltatói tanúsítvány	Munkáltató (szervezeti egység vezetője), Szolgáltató, Felügyelet

#### 4.9.4 Visszavonási kérelemre vonatkozó eljárás

Végfelhasználói tanúsítvány visszavonása egy visszavonási kérelem Szolgáltató, vagy a Szolgáltató Kihelyezett Szolgáltató Alegysége számára történő benyújtásával kezdeményezhető. A visszavonási kérelem benyújtható:

Ügyfélszolgálati időben:

- személyesen, a Szolgáltató székhelyén, a Központi Regisztrációs Egységnél,
- a Szolgáltatónak küldött e-mailben, illetve faxon,
- a kártyamenedzsment rendszer felületén,
- a Szolgáltató székhelyére küldött levélben.

Ügyfélszolgálati időben és azon kívül:

- Soronkívüli tanúsítvány visszavonónál,
- telefonon, a Szolgáltató ügyeleti rendszerén keresztül

Végfelhasználói tanúsítvány visszavonása egy visszavonási kérelem a kártyamenedzsment rendszer webes felületén kezdeményezhető. Kivételt képez ez alól a kulcskompromittálódás, a kulcshordozó eszköz elvesztése, eltulajdonítása képez, ekkor a tanúsítvány visszavonás minél gyorsabb végrehajtása érdekében a felhasználó telefonon keresztül is kezdeményezheti a tanúsítvány visszavonását 7x24-es időben elérhető Soronkívüli tanúsítvány visszavonónál.

Soronkívüli visszavonási kérelem esetében az alábbi információkat kell a felhasználótól bekérni:

- visszavonást kérő megnevezése, beosztása, elérhetősége;
- visszavonandó kártya adatai;
- a visszavonás oka,
- személyazonosításhoz használt személyazonosító dokumentum megnevezése és száma.

A visszavonásra irányuló kérelmeket a Szolgáltató, illetve a Szolgáltató Kihelyezett Szolgáltató Alegysége más kérelmeket megelőzően, soron kívül bírálja el. A Szolgáltató arra jogosult munkatársa a Soronkívüli visszavonási kérelmeket haladéktalanul továbbítja Kihelyezett Szolgáltató Alegységének.

A visszavonási eljárás során a Kihelyezett Szolgáltató Alegység Regisztrációs Alegysége ellenőrzi a visszavonási kérelemben szereplő adatokat, a kérelmező személyazonosságát, a kérelem előterjesztésére való jogosultságot, a kérelemben foglalt indokok (ld. 4.9.2 pont) valóságát, illetve visszavonásra való alkalmasságát. A kérelemre vonatkozó fenti adatokat a Szolgáltató Kihelyezett Szolgáltató Alegysége lehetőleg független, illetve az alany által megadott forrásból ellenőrzi. A visszavonási kérelem hitelességének megállapításának alapjául a tanúsítvány kibocsátásakor alkalmazott ellenőrzési rend szolgál kiindulásként vagy egy az alany magánkulcsának felhasználásával aláírt dokumentum vagy a személyes megjelenés esetén történő személyazonosság megállapítás.

Ha az adatok helytelenek, az igénylő kérése vagy a visszavonásra való jogosultság nem állapítható meg, akkor a Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység a tanúsítvány visszavonását megtagadhatja.

Helyes és hiteles kérelem esetén az Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység további mérlegelés nélkül intézkedik a tanúsítvány visszavonása érdekében: a visszavonási kérelmek azonnal végrehajtásra kerülnek, a tanúsítvány visszavont státusza bekerül a tanúsítványtárba (ún. tanúsítványállapot-adatbázisba), valamint a tanúsítvány bekerül a következő alkalommal kibocsátott visszavonási listába.

#### **4.9.5 Visszavonási kérelemre vonatkozó türelmi idő**

A visszavonási lépések késedelem nélkül követik egymást. A visszavont tanúsítvány státusza azonnal bekerül a tanúsítványtárba. A tanúsítványállapot-változást követő 1 órán belül új visszavonási lista kiadására kerül sor, mely tartalmazza a tanúsítvány megváltozott státuszát.

A humán beavatkozást igénylő visszavonási és felfüggesztési kérelmeket a Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység folyamatosan fogadja és haladéktalanul megkezdi azok feldolgozását. A feldolgozás megkezdése és a tanúsítvány státuszváltásról való döntést követően a Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység a tanúsítványállapot-adatbázist szükség esetén késedelem nélkül frissíti. A humán beavatkozást igénylő visszavonási és felfüggesztési kérelmek feldolgozásának ideje legfeljebb 3 óra.

#### **4.9.6 Visszavonásra vonatkozó egyéb szabályok**

Amennyiben egy tanúsítvány visszavonásra került, azt nem lehet újra használatba venni.

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

#### **4.9.7 A felfüggesztés körülményei**

A tanúsítvány felfüggesztéséhez a visszavonáshoz vezető körülmények fennállására vonatkozó alapos gyanú vezethet.

A Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység saját belátása szerint, a visszavonási kérelmeket ideiglenesen kielégítheti felfüggesztéssel is, amennyiben a bejelentett körülmények kivizsgálását szükségesnek tartja.

#### **4.9.8 Felfüggesztés kérelmezése**

A felfüggesztést ugyanazok kérelmezhetik, akik a visszavonást (ld. 4.9.3 pont), kiegészítve olyan harmadik felekkel, akik hitelt érdemlő módon bizonyítani tudják a visszavonáshoz vagy felfüggesztéshez vezető körülmények alapos gyanújának a fennállását.

#### **4.9.9 Felfüggesztési kérelemre vonatkozó eljárás**

A felfüggesztési kérelem a visszavonási kérelemhez hasonlóan (lásd előzőekben) nyújtható be a Szolgáltatóhoz, illetve a Szolgáltató Kihelyezett Szolgáltató Alegységhez. A felfüggesztési kérelmet a visszavonási kérelemmel megegyező módon dolgozza fel a Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység.

#### **4.9.10 A felfüggesztés időtartamára vonatkozó korlátozások**

Érvényes tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 5 naptári napig. A tanúsítvány visszavonásáról, illetve újbóli érvényesre állításáról a Szolgáltatónak, illetve a Kihelyezett Szolgáltató Alegységének a lehető leghamarabb intézkednie kell. A felfüggesztett állapot kezdő időpontja a felfüggesztési kérelem elfogadásától számítandó. Ha ez idő alatt a visszavonáshoz vezető körülmények gyanúja cáfolatot nem nyer, a Szolgáltató, illetve Kihelyezett Szolgáltató Alegysége a tanúsítványt visszavonja.

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



#### 4.9.10.1 Újraérvényesítés módja

A tanúsítvány újbóli érvénybe helyezését az alany és a másodlagos alany kérelmezheti a visszavonásra vonatkozó eljárási rend szerinti módon.

#### 4.9.11 Kulcskompromittálódás esetére vonatkozó speciális követelmények

Magánkulcs kompromittálódása vagy vélelmezett kompromittálódása esetén a visszavonási eljárásban leírt lépések végrehajtandók. Kompromittálódott magánkulcs soha többet nem használható, és megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes magánkulcs. Az alany, illetve a másodlagos alany kötelessége a kompromittálódott magánkulcs által esetlegesen érintett felek értesítése, és minden intézkedés megtétele az esetleges károk megelőzése vagy enyhítése érdekében.

### 4.10 Tanúsítvány-állapot információk közzététele

#### 4.10.1 Tanúsítvány Visszavonási Lista (CRL)

A Szolgáltató X.509 V2 típusú tanúsítvány visszavonási listák kibocsátását és tanúsítvány visszavonási kiterjesztések alkalmazását támogatja.

- A Szolgáltató a CRL listán jelöli annak érvényességi idejét. CRL egy előző CRL érvényességi ideje alatt is kibocsátható. Amennyiben egy időben több érvényes CRL is létezik, a legutolsó az irányadó.
- A CRL tartalmazhatja a tanúsítvány visszavonásának okát.
- A CRL ellenőrzése ajánlott minden Érintett Fél részére az elektronikus aláírás ellenőrzési eljárásának részeként, az elvárható gondosság követelményének megfelelően. A CRL-en szereplő, azaz érvénytelen tanúsítvány elfogadásából keletkező bármilyen kár az Érintett Felet terheli.
- A Szolgáltató az egyes CRL-eket és a kapcsolódó egyéb adatokat a [1] Törvény 9. § (7) bekezdésében előírt határidőig (jelenleg: 10 év) őrzi meg.

A visszavonási listán azon visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre, amelyek érvényességi ideje még nem járt le.

A visszavonási lista kibocsátása a Szolgáltató, illetve Kihelyezett Szolgáltató Alegységének tanúsítványtárába történik. A listák kibocsátása közt legfeljebb 24 óra telik el. Ezen időközönként CRL akkor is kibocsátásra kerül, ha a legutóbbi kibocsátás óta nem történt tanúsítvány visszavonás vagy felfüggesztés.

Tanúsítvány visszavonása vagy felfüggesztése esetén a a tanúsítványállapot-változásnak a Szolgáltató nyilvántartásában való átvezetést követő 1 órán belül a kérelem szerint módosított visszavonási állapotot közzéteszi.

A visszavonási listák mindig tartalmazzák a következő lista kibocsátásnak idejét, melyet megelőzve is kibocsáthat a Szolgáltató új listát. A listák érvényességi ideje legfeljebb 25 óra.

A felfüggesztett tanúsítványok az újbóli érvényesítés hatására kerülhetnek ki a listából.

#### **4.10.2 A CRL ellenőrzési követelményei az Érintett Fél számára**

A visszavonási lista ellenőrzése érintett felek részére ajánlott a tanúsítványok elfogadását megelőzően tekintettel a 4.5.2 pontban foglaltakra. A lista ellenőrzésének arra kell vonatkozni, hogy a kérdéses tanúsítványt a lista tartalmazza-e, a lista hiteles és sértetlen-e, és a kérdéses tranzakció szempontjából időben releváns-e.

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

#### **4.10.3 Valós idejű visszavonási állapot ellenőrzés elérhetősége**

A Szolgáltató Kihelyezett Szolgáltató Alegysége által kibocsátott tanúsítványok esetében valós idejű visszavonási állapot-szolgáltatásokat nem nyújt.

#### **4.10.4 A visszavonási információ közzétételének egyéb formái**

A visszavonási hirdetmények az MKB oldalán, a Szolgáltató oldalán és annak biztonsági másolataiban érhetők el.

### **4.11 Kulcs letétbe helyezése és visszaállítása**

A Szolgáltató az általa kibocsátott végfelhasználói aláíró, ideiglenes aláíró tanúsítványok esetén nem nyújt magánkulcs letéti szolgáltatást, illetve az alany aláíró magánkulcsát semmilyen más módon nem tárolja el vagy menti.

A Szolgáltató az általa kibocsátott végfelhasználói titkosító tanúsítványok esetén magánkulcs letéti szolgáltatást biztosít. Titkosító tanúsítvány magánkulcsának visszaállítását kizárólag a felhasználó kezdeményezheti. A magánkulcsok tárolása és visszaállítása kiemelt védelmi szabályok szerint történik.

A Szolgáltató az MKB Kihelyezett Szolgáltató Alegység, valamint a saját szolgáltatói magánkulcsait elmentve tárolja.

## 5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A Regisztrációs Alegységek eszközeit kizárólag az erre felhatalmazott, megfelelően kioktatott és ellenőrzött tudású, szakértelmű kezelőszemélyzet kezeli.

Az egységek megfelelő működésének biztosítása érdekében a rendszer szoftver és hardver elemein az operációs dokumentumokban meghatározott módon és rendszerességgel, az arra kijelölt személyek belső karbantartást végeznek, a munka naplózásával.

### 5.1 Fizikai óvintézkedések

A Szolgáltató láncolt hitelesítés-szolgáltatói infrastruktúrájára vonatkozó fizikai-biztonsági követelmények külön dokumentumban találhatóak.

### 5.2 A Láncolt Hitelesítés-szolgáltató leállítása

#### 5.2.1 Szolgáltatás megszüntetése

Amennyiben a Szolgáltató Kihelyezett Szolgáltató Alegységének tevékenységét tervezetten megszünteti vagy tartósan szünetelteti, a tevékenység leállítását megelőzően legalább az alábbi eljárásokat hajtja végre:

- a) A tevékenység befejezését legalább 60 nappal megelőzően értesíti az általa kibocsátott és még vissza nem vont tanúsítványokban Alanyként megjelölt személyeket,
- b) A szolgáltatás megszűnése előtt 30 nappal e-mail címmel rendelkező ügyfelei számára a szolgáltatás közreműködésében való befejezéséről elektronikus levélben értesítőt küld.
- c) A Szolgáltató a tevékenység befejezését legalább 20 nappal megelőzően az általa kibocsátott, és még vissza nem vont tanúsítványokat visszavonja.
- d) A regisztrációs információk, és az eseménynapló archívumok megőrzése érdekében, időbélyegzővel ellátott teljes körű mentést hajt végre. A mentésnek tartalmaznia kell a tanúsítványokkal kapcsolatos korábbi változások adatait, a tanúsítványok helyzetére, esetleges felfüggesztésére, illetve visszavonására vonatkozó adatokat, valamint a tanúsítvány kibocsátásában való közreműködésre vonatkozó szabályzatokat és az aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását. A mentett adatállományokat a Szolgáltató védi jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását, valamint az adatoknak megőrzési időn belüli, jogosultak számára való hozzáférhetőségét és értelmezhetőségét.
- e) A Szolgáltató a Kihelyezett Szolgáltató Alegység láncolt szolgáltatói magánkulcsait megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat a Szolgáltató visszavonja.
- f) A Szolgáltató a tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is eleget tesz.
- g) A Szolgáltató új tanúsítványokat a megszűnés bejelentése után nem bocsát ki.

## 5.3 Kulcspár előállítás és telepítés

### 5.3.1 Kulcspár előállítás

		Végfelhasználói kulcspár	Láncolt-Szolgáltatói kulcspár
Kulcsgenerálás és installáció	Kulcsgenerálás, tárolás	A kulcsgenerálást a felhasználó maga végzi.	A láncolt szolgáltató kulcspárt a Szolgáltató generálja, hitelesíti és adja át az MKB Kihelyezett Szolgáltató Alegység részére.
	Kulcs méretek	A végfelhasználók minimum 1024 bites RSA kulccsal rendelkeznek.	A Szolgáltató legalább 2048 bites RSA kulcsokat generál.
	Kulcs felhasználási célok	Aláíró kulcspár generálása.	Végfelhasználói tanúsítvány, CRL válaszok aláírása;
Magánkulcs védelme	Magánkulcs többszemélyes kontrollja	A Szolgáltató megfelelő technikai védelmet biztosít arra, hogy a kulcsgenerálást a felhasználó maga végezze és a kulcsgenerálás kulcstároló eszközben jöjjön létre.	-
	Magánkulcs mentése	Az aláíró tanúsítvány magánkulcsot a Szolgáltató nem ment, titkosító tanúsítvány magánkulcsának mentésére kulcsetét szolgáltatást biztosít.	Az MKB Kihelyezett Szolgáltató Alegység láncolt szolgáltatói magánkulcsokat a Szolgáltató menti.
	Magánkulcs aktiválása	A magánkulcsok külön aktíválásra nincs szükség.	Az MKB Kihelyezett Szolgáltató Alegység láncolt szolgáltatói magánkulcsainak aktiválását a Szolgáltató végzi.
	Magánkulcs deaktiválása	A magánkulcsok deaktiválását a felhasználó alkalmazás végzi működések befejezésekor.	A magánkulcsok deaktiválását a Szolgáltató végzi.
	Magánkulcs megsemmisítése	Végfelhasználó köteles kezdeményezni aláíró magánkulcsának megsemmisítését annak érvényességi idejének lejáta után.	Az MKB Kihelyezett Szolgáltató Alegység láncolt szolgáltatói magánkulcsait és azok minden előfordulását az érvényesség lejátakor a Szolgáltató megsemmisíti.
Egyéb tevékenységek	Nyilvános kulcs archiválása	A végfelhasználói és szolgáltatói nyilvános kulcsokat a Szolgáltató az elektronikus aláírásról szóló törvényben meghatározott ideig archiv formában megőrzi (ld. 4.2.2.1 pont).	
	Kulcsok felhasználási ideje	A magánkulcs érvényességi ideje megegyezik a hozzá tartozó tanúsítvány érvényességi idejével, de maximum 2 év. A nyilvános kulcs a kriptográfiai biztonságáig érvényes.	

Az MKB Kihelyezett Szolgáltató Alegység valamennyi láncolt szolgáltatói kulcspárját a Szolgáltató generálja, védett kriptográfiai hardver modulban. A generált magánkulcsok mentést (klónozást) leszámítva, teljes életciklusuk alatt a kriptográfiai hardverekben marad, megsemmisítéséig azt sehová nem kell továbbítani. Amennyiben a láncolt szolgáltatói kulcspár, bármely okból történő megsemmisítése válik szükségessé, úgy az az eszköz tanúsítványában előírt módon két személyes kontroll mellett történik. A megsemmisítést a Szolgáltató végzi.

#### 5.3.1.1 Alkalmazott eszközök

Aláíró eszközök	Hardver specifikáció	Szoftver specifikáció
Nem Minősített Kihelyezett Szolgáltató Alegység	Protect Server Gold PSG PCI HSM 25	-
Végfelhasználói eszköz	Kulcspár és tanúsítványtárolás áramkímélő eszköz	-

### 5.3.2 Magánkulcs eljuttatása az alanyhoz

A Szolgáltató saját székhelyén megfelelő biztonsági intézkedések mellett generálja a Láncolt szolgáltatói kulcspárt, és megfelelő biztonsági intézkedések mellett gondoskodik annak Kihelyezett Szolgáltató Alegységéhez való eljuttatásáról.

A felhasználó maga generálja a végfelhasználói tanúsítványhoz tartozó kulcspárt, így azok Alany számára történő eljuttatására külön nincs szükség.

### **5.3.3 A szolgáltatói nyilvános kulcs közzététele**

A Szolgáltató Kihelyezett Szolgáltató Alegysége által használt tanúsítványokat saját tanúsítványtárában teszi mindenki számára elérhetővé.

### **5.3.4 Kulcsméreték**

Lásd 5.3.1 pont.

### **5.3.5 A nyilvános kulcs paraméterek generálása és megfelelőségük ellenőrzése**

#### **5.3.5.1 A paraméterek megfelelőségének ellenőrzése**

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

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

A véletlenszám-generálás megfelelőségének ellenőrzésének alapja, hogy a rendszerben használt valamennyi kriptográfiai hardver modul képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül.

A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám-generálásukat, melyek hibás teszt esetén leállnak.

### **5.3.6 A kulcs használat célja (az X.509 v3 kulcshasználati mező tartalmának megfelelően)**

Az MKB Kihelyezett Szolgáltató Alegység a munkatársi aláíró, ideiglenes munkatársi aláíró és munkatársi titkosító tanúsítványok aláírásához használt láncolt hitelesítés-szolgáltatói magánkulcsát ezeken kívül csak a tanúsítvány visszavonási lista (CRL) aláírására használja fel.

## **5.4 A magánkulcsok védelme**

### **5.4.1 A szolgáltatói kulcsokra vonatkozó általános szabályok**

A Kihelyezett Szolgáltató Alegység szolgáltatói kulcsokra az alábbi szabályok vonatkoznak:

- a kulcsok létrehozása, tárolása, mentése, helyreállítása, megsemmisítése fizikailag biztonságos környezetben, a Szolgáltató által kettős személyi ellenőrzés mellett valósul meg,
- a hitelesítő egységek kulcsai tanúsítással rendelkező kriptográfiai modulban kerülnek előállításra, tárolásra,

- a kulcsokat kizárólag az arra felhatalmazottak használhatják, a létrehozás céljának megfelelő funkcióra,
- a Szolgáltató Kihelyezett Szolgáltató Alegységének rendszerei a láncolt hitelesítés szolgáltatás során használt kulcsainak használata előtt meggyőződnek arról, hogy az ezen kulcsokhoz kapcsolódó tanúsítványok érvényesek,
- a láncolt szolgáltatói kulcsfrissítés out-of-band cserével történik,
- a láncolt szolgáltatáshoz használt kulcsok megsemmisítése során olyan biztonságos törlési folyamatokat alkalmaz a Szolgáltató, melyek ténylegesen felülírják a kulcsok összes előfordulását az összes olyan tárolóeszközön, melyen a kulcs példányai előfordulhattak,
- biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálását a Szolgáltató végzi és gondoskodik a kulcs védelméről,
- élettartamuk végén a kulcsokat a Szolgáltató olyan módon semmisíti meg, hogy az aláíró kulcsok ne legyenek visszanyerhetőek,

#### **5.4.2 Magánkulcs letétbe helyezése**

A szolgáltatói és végfelhasználói aláíró magánkulcsot nem lehet letétbe helyeztetni. Végfelhasználói titkosító tanúsítványok magánkulcsai esetén a Szolgáltató kulcsletét szolgáltatást biztosít.

#### **5.4.3 Magánkulcs mentése**

A Szolgáltatónál az összes láncolt szolgáltatáshoz használt magánkulcs mentésre (illetve duplikálásra, klónozásra) kerülhet.

A mentés során a tanúsítvány-aláíró magánkulcsot generáló kriptográfiai hardver modulból intelligens kártyákra több darabban, védetten másolódik át a magánkulcs.

- A mentés funkció kiváltásához speciális eszközök kellenek.
- A mentési funkció első lépéseként a kettős ellenőrzés mellett működő végrehajtók hitelesítik magukat.
- Sikeres hitelesítés esetén a mentés rejtjeles formában hajtódik végre.
- A mentett példányok a továbbiakban ugyanolyan jellegű és erősségű védelem alatt állnak, mint a kulcsgenerálást végző hardver modul eredeti példánya.

#### **5.4.4 Magánkulcs archiválása**

A Szolgáltató Kihelyezett Szolgáltató Alegysége a végfelhasználói aláíró tanúsítványok magánkulcsait nem archiválja. A Szolgáltató Kihelyezett Szolgáltató Alegysége a végfelhasználói titkosító tanúsítványok magánkulcsát archiválja.

#### **5.4.5 Egyéb kulcskezelési rendelkezések**

A Szolgáltató a szolgáltatások nyújtásához használt elektronikus aláírási termékeit elkülönítetten kezeli és működteti az egyéb tevékenységeihez használt termékektől.

#### **5.4.6 Nyilvános kulcs archiválása**

A Szolgáltató minden előállított tanúsítványt archivál, az alábbi időszakra:

- nem végfelhasználói tanúsítványok: az érvényesség lejártától számított 10 évig,
- végfelhasználói tanúsítványok: az érvényesség lejártától számított jogszabályban meghatározott ideig (jelen Szabályzat hatályba lépésekor 10 évig).

Szolgáltatói, illetve láncolt szolgáltatói kulcs használati idejének végén archiválható, hogy esetleg később (nem meghatározott idő múlva) újra használatba vehető legyen. Ez különösen az elektronikus aláírás ellenőrzésére szolgáló nyilvános kulcsokra vonatkozik.

A Szolgáltató az Aláíró magánkulcsát nem archiválja.

#### **5.4.7 A nyilvános és magánkulcsok használatának periódusa**

A láncolt szolgáltatáshoz használt tanúsítványok és a bennük foglalt nyilvános kulcsok magán párijai:

- nem minősített tanúsítvány- és CRL aláíró magánkulcs: 5 év

A végfelhasználói aláíró kulcsokhoz tartozó tanúsítványoknak és a bennük foglalt nyilvános kulcsok magán párijainak érvényességi ideje maximálisan 2 év. Az érvényességi periódus a tanúsítványban feltüntetésre kerül. A tanúsítványok érvényességének kezdete a kibocsátás időpontjával egyezik meg.

A magánkulcs érvényességi ideje megegyezik a tanúsítvány érvényességi idejével. Valamennyi fenti tanúsítványban szereplő nyilvános kulcs érvényességi ideje annak kriptográfiai biztonságának megfelelő voltáig tart.

### **5.5 Aktivizáló adatok**

#### **5.5.1 Aktivizáló adatok előállítása és telepítése**

A Kihelyezett Szolgáltató Alegység Regisztrációs Alegysége a tanúsítvány igénylést kiszolgáló kártyamenedzsmet rendszerhez kapcsolódó egyszer használatos aktivizáló adatot biztonságos módon állítja elő. A kártyamenedzsmet rendszer az aktivizáló adatot véletlenszerűen, automatikusan állítja elő. Az aktivizáló adat használata csak egyszer, és csak a megfelelő aláírás-létrehozó eszközzel együtt lehetséges.

#### **5.5.2 Az aktivizáló adatok védelme**

A Szolgáltató az aláírás-létrehozó eszközhöz PIN kódot nem határoz meg és nem rögzíti, azt a szolgáltatást igénybe vevő személy adja meg.

#### **5.5.3 Az aktivizáló adatok egyéb szempontjai**

A Kihelyezett Szolgáltató Alegység Regisztrációs Alegysége a kártyamenedzsmet rendszerhez kapcsolódó egyszer használatos PIN kódot e-mailben juttatja el, vagy személyesen adja át a felhasználónak.

## 6 Tanúsítvány és visszavonási lista profilok

### 6.1 Tanúsítványprofilok

A Szolgáltató az X.509 [7] ajánláson alapuló tanúsítványokat bocsát ki.

#### 6.1.1 Munkatársi végfelhasználói aláíró tanúsítványok profiljainak állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyesítő igazolványában szereplő írás módon, ékezhelyesen, UTF-8-ban kódolva
Organization	MKB Bank Zrt. vagy MKB Üzemeltetési Kft.
Organization Unit	Szervezeti egység(ek) neve(i) vagy üres
Country	Székhely (vagy opcionálisan lakcím) szerinti ország kód, Magyarország esetén HU
Locality	Székhely vagy telephely (vagy opcionálisan lakcím) szerinti város
Email	Email cím
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	(kritikus kiterjesztés) cA = FALSE
KeyUsage	(kritikus kiterjesztés) NonRepudiati on, DigitalSignature
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége (az érvényesség kezdete a tanúsítvány kibocsátásának ideje, az érvényesség vége a tanúsítvány kibocsátásától számított 365 nap)
Issuer	Kibocsátó megnevezése
Signature	sha1RSA
Subject Key Identifier	Tanúsítvány egyedi azonosítója
Authority Key Identifier	Kibocsátó tanúsítvány egyedi azonosítója
CRL Distribution Points	Visszavonási lista elérhetőségét tartalmazó URL
Authority Info Access	A kibocsátó tanúsítványának elérhetőségét tartalmazó URL
Enhanced Key Usage	Secure Email
Subject Alternative Name	Email cím

#### 6.1.2 Munkatársi végfelhasználói ideiglenes aláíró tanúsítványok profiljainak állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyesítő igazolványában szereplő írás módon, ékezhelyesen, UTF-8-ban kódolva
Organization	MKB Bank Zrt. vagy MKB Üzemeltetési Kft.
Organization Unit	Szervezeti egység(ek) neve(i) vagy üres
Country	Székhely (vagy opcionálisan lakcím) szerinti ország kód, Magyarország esetén HU
Locality	Székhely vagy telephely (vagy opcionálisan lakcím) szerinti város
Email	Email cím
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	(kritikus kiterjesztés) cA = FALSE
KeyUsage	(kritikus kiterjesztés) NonRepudiati on, DigitalSignature
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége (az érvényesség kezdete a tanúsítvány kibocsátásának ideje, az érvényesség vége a tanúsítvány



Mező	Tartalom
	kibocsátásától számított 7 nap)
Issuer	Kibocsátó megnevezése
Signature	sha1RSA
Subject Key Identifier	Tanúsítvány egyedi azonosítója
Authority Key Identifier	Kibocsátó tanúsítvány egyedi azonosítója
CRL Distribution Points	Visszavonási lista elérhetőségét tartalmazó URL
Authority Info Access	A kibocsátó tanúsítványának elérhetőségét tartalmazó URL
Enhanced Key Usage	Secure Email
Subject Alternative Name	Email cím

### 6.1.3 Munkatársi végfelhasználói titkosító tanúsítványok profiljainak állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyazonosító igazolványában szereplő írás módon, ékezhelyesen, UTF-8-ban kódolva
Organization	MKB Bank Zrt. vagy MKB Üzemeltetési Kft.
Organization Unit	Szervezeti egység(ek) neve(i) vagy üres
Country	Székhely (vagy opcionálisan lakcím) szerinti ország kód, Magyarország esetén HU
Locality	Székhely vagy telephely (vagy opcionálisan lakcím) szerinti város
Email	Email cím
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	(kritikus kiterjesztés) cA = FALSE
Key Usage	(kritikus kiterjesztés) Key Encipherment
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége (az érvényesség kezdete a tanúsítvány kibocsátásának ideje, az érvényesség vége a tanúsítvány kibocsátásától számított 730 nap)
Issuer	Kibocsátó megnevezése
Signature	sha1RSA
Subject Key Identifier	Tanúsítvány egyedi azonosítója
Authority Key Identifier	Kibocsátó tanúsítvány egyedi azonosítója
CRL Distribution Points	Visszavonási lista elérhetőségét tartalmazó URL
Authority Info Access	A kibocsátó tanúsítványának elérhetőségét tartalmazó URL
Enhanced Key Usage	Secure Email
Subject Alternative Name	Email cím

### 6.1.4 „B” osztályú szolgáltatói (tanúsítvány- és visszavonási lista aláíró) tanúsítvány profilja

Mező	Tartalom
Common Name	NetLock Üzleti (Class B) Tanúsítványkiadó
Organization	NetLock Kft.
Organization Unit	Tanúsítványkiadók
Country	HU
Public Key	Szolgáltatói tanúsítvány nyilvános kulcsa
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	NetLock Üzleti (Class B) Tanúsítványkiadó
Signature	sha1RSA

Mező	Tartalom
Netscape Cert Type	SSL CA, SMIME CA
Netscape Comment	FIGYELEM! Ezen tanúsítvány a NetLock Kft. Hitelesítés Szolgáltatási Utasításában leírt eljárások alapján készült. Az elektronikus aláírás elfogadásának feltétele az előírt ellenőrzési eljárás megtétele. Az eljárás leírása megtalálható a Szolgáltató Tanúsítványtarabában, vagy kerhető a Szolgáltató e-mail címén: info@netlock.hu. IMPORTANT! The issuance and the use of this certificate is subject to the NetLock Practice statement, available at Internet site or e-mail address of NetLock Ltd.
CRL Distribution Points	Visszavonási lista elérhetőségét tartalmazó URL
Basic Constraints	(kritikus kiterjesztés) cA = TRUE, pathlen = 0
KeyUsage	(kritikus kiterjesztés) Certificate Signing, CRL Signing

## 6.2 Tanúsítvány visszavonási lista profilok

A Szolgáltató az x.509 [9] megfelelő visszavonási listákat (CRL) bocsát ki.

Mező	Tartalom
Version	V2
Issuer	Kibocsátó megnevezése
Last update	Utolsó kibocsátás dátuma
Next update	Kibocsátott CRL érvényességének vége
Signature	Kibocsátó elektronikus aláírása
CRL entry	Az érvénytelenített tanúsítvány sorszám, érvénytelenítés dátuma, időpontja
AuthorityKeyIdentifier	Kibocsátó tanúsítvány egyedi azonosítója
CA Version	V0.0
CRL Number	Kiadott CRL sorszáma
Next CRL Publish	Legközelebbi CRL kibocsátás várható időpontja

## 7 Üzleti és jogi tudnivalók

### 7.1 Bizalmasság, adatvédelem

#### 7.1.1 Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése

A Szolgáltató tanúsítványok visszavonását és felfüggesztését a Tanúsítvány Visszavonási Listában teszi közzé, a tanúsítvány sorszámának és opcionálisan a visszavonás okának a jelölésével. A Szolgáltató a Tanúsítvány Visszavonási Listában a tanúsítvány azonosítója szerint is keresési lehetőséget biztosít (ld. még 4.6 alfejezet).

### 7.2 Jogok és kötelezettségek

#### 7.2.1 A Kihelyezett Szolgáltató Alegységek közös kötelezettségei

- a) a Kihelyezett Szolgáltató Alegység eszközeit kizárólag az erre felhatalmazott, megfelelően kioktatott kezelőszemélyzet kezelheti,
- b) szabványos X509 tanúsítvány kibocsátásában, megújításában, felfüggesztésében, reaktiválásában, visszavonásában való közreműködés a Regisztrációs Alegység által küldött erre vonatkozó kérelem esetén,
- c) tanúsítvány felfüggesztésének vagy visszavonásának publikálása CRL-en,
- d) saját tanúsítványának nyilvánosságra hozatala,
- e) saját magánkulcsának teljes körű védelme, a kulcs dedikált kriptográfiai hardver modulban történő tárolásával,
- f) a hitelesítő kulcspár kompromittálódásának feltételezése, a kulcspár sérülése, megsemmisülése esetén az alkalmazó Közösség tagjainak késedelem nélküli értesítése elektronikusan (pl. elektronikus levélben, Internet oldalon közzététellel), illetve out-of-band módon (pl. postai úton, napilapban közzététellel) továbbá a Szabályzatért Felelős Egység bármely tagjának írásban vagy személyesen történő megkeresésével.

#### 7.2.2 A Regisztrációs Alegységek közös kötelezettségei

- a) úgy működni, hogy semmilyen módon ne sértsék a szolgáltatás biztonságát,
- b) tevékenységüket saját maguk ellátni,
- c) az igénylő (alany) tanúsítványra vonatkozó kérelmeinek (kibocsátás, megújítás, felfüggesztés, visszavonás) kezelése,
- d) az ügyfeladatok összegyűjtése, ellenőrzése és döntés meghozatala azok valódiságára vonatkozóan,
- e) a nem nyilvános ügyfeladatok megfelelő szintű védelme,
- f) az alany (és az igénylő) és a Közösség többi tagjának értesítése a tanúsítvány kibocsátásáról és a tanúsítvánnyal végzett műveletekről,
- g) a tanúsítványnak az alany számára elérhetővé tétele,

- h) a belépés lehetővé tétele a belső és a Szolgáltatói Szabályzatért Felelős Egység számára a szolgáltatás területére.

### **7.2.3 A végfelhasználó kötelezettségei**

#### **7.2.3.1 A végfelhasználó általános kötelessége:**

- a) megismerni és betartani a tanúsítványkiadásra vonatkozó szabályzatot,
- b) a feltételeknek és szabályzatoknak megfelelően eljárni a szolgáltatások felhasználása során, beleértve a tanúsítvány és magánkulcs igénylését és alkalmazását,
- c) hozzájárulni a szolgáltatás biztonságához, elsősorban korrekt adatszolgáltatáson keresztül, valamint a nyilvános kulcsú infrastruktúra tudatos és felelősségteljes alkalmazásával,
- d) az aláírással vagy az így aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt – külön jogszabályban, illetve a szabályzatokban meghatározott – rendellenességről tájékoztatni a Szolgáltatót, vagy a Szolgáltató Kihelyezett Szolgáltató Alegységét,
- e) betartani a tanúsítványban jelzett esetleges korlátozásokat.

#### **7.2.3.2 A végfelhasználó kötelessége saját kulcs kezelése során:**

- a) a magánkulcsát biztonságos módon tárolni, kezelni,
- b) a kulcspárt és tanúsítványát rendeltetésszerűen használni,
- c) magánkulcsának megsemmisítését kezdeményezni a hozzá tartozó tanúsítvány lejáta után,
- d) amennyiben magánkulcsa kompromittálódásának lehetősége fennáll, a lehető leghamarabb tanúsítványának visszavonását, illetve felfüggesztését kérni a Szolgáltatótól, vagy a Szolgáltató Kihelyezett Szolgáltató Alegységétől.

#### **7.2.3.3 A végfelhasználó kötelessége a tanúsítványának kezelése során:**

- a) a tanúsítványkiadáshoz előírt regisztrációs eljárásrend alapján felvett adatainak valódiságát a szükséges okmányok eredetijének, hiteles másolatának, továbbá másolatának bemutatásával alátámasztani,
- b) az azonosításához szükséges személyazonosító adatokról és mindezek változásáról tájékoztatni a Szolgáltató Kihelyezett Szolgáltató Alegységét, vagy a Szolgáltatót,
- c) a regisztrált adatainak a kibocsátott tanúsítványának érvényességi ideje alatt történő megváltozásáról késedelem nélkül a Szolgáltató Kihelyezett Szolgáltató Alegységét, vagy a Szolgáltatót tájékoztatni,
- d) a tanúsítvány első felhasználása előtt ellenőrizni a tanúsítványban feltüntetett adatainak helyességét és amennyiben azok nem felelnek meg a valóságnak, akkor a tanúsítvány visszavonását kérni.
- e) A kötelezettségek értelemszerűen alkalmazandók a tanúsítvány és kulcs érvényességi időszaka alatt, és ha szükséges, akkor azt követően is.

### **7.2.4 Az MKB kötelezettségei**

Az MKB általános kötelessége:

- a) a Kihelyezett Szolgáltató Alegység és a tanúsítványtár felügyeletében, üzemeltetésében való közreműködés;
- b) tevékenységének a Szolgáltató utasításai szerint megfelelő végzése;
- c) a magas színvonalú és biztonságos szolgáltatások folyamatos biztosítása;

#### **7.2.4.1 A Szolgáltatói egységek közös kötelezettségei**

A Szolgáltatóhoz tartozó szervezetek, regisztrációs és hitelesítő alegységek kötelessége:

- a) a Közösség elektronikus hitelesítéssel kapcsolatos tevékenységeinek, alapelveinek meghatározása, ezek alapján a működést részletesen tárgyaló szabályzatok készítésében és rendszeres felülvizsgálatában való közreműködés,
- b) megfelelő szakmai végzettséggel rendelkező, a folyamatos, szabályzatokban előírt működés biztosításához elégséges számú kezelőszemélyzet biztosítása,
- c) a szabályzatokban előírt PKI folyamatok elvégzésére alkalmas, megfelelően beállított szoftver és hardver infrastruktúra biztosítása, a szükséges változtatások megtételében való közreműködés,
- d) az infrastruktúra működtetésében, javításában és karbantartásában közreműködő felelős személyzet munkájának és szakmai felkészültségének folyamatos ellenőrzése, a szükséges változtatások megtétele,
- e) az előző pontokban előírt infrastruktúra folyamatos, biztonságos üzemeltetésében, hibajavításában való közreműködés és az infrastruktúrába tartozó eszközökre előírt szabványos karbantartás elvégzésének segítése,
- f) Üzleti Folytonossági Terv készítése, alkalmazása,
- g) a szabályzatokban előírt módon folytatott tevékenység során keletkező adatok jelen és kapcsolódó szabályzatokban meghatározott kezelésére, tárolására, archiválására alkalmas szoftver és hardver eszközök biztosításában, működtetésében, karbantartásában való közreműködés,
- h) a PKI folyamatokat végző és az azok során keletkező adatokat tároló szoftver és hardver rendszer jelen és kapcsolódó szabályzatokban előírt logikai és fizikai védelmét biztosító szoftver és hardver eszközök biztosításában való közreműködés,
- i) a logikai és fizikai védelmet megteremtő eszközök megfelelő üzemeltetésében, az informatikai, fizikai, adminisztrációs és üzleti biztonság megteremtésében és fenntartásában való közreműködés.

#### **7.2.4.2 A Szabályzatért Felelős Egység kötelezettségei**

- a) a felügyelendő dokumentumok, továbbá a belső ügyviteli folyamatok azok helyszínén való ellenőrzése és a Szolgáltató vezetésének tájékoztatása a megfigyelésekről,
- b) a Szolgáltatóhoz, illetve Kihelyezett Szolgáltató Alegységéhez érkező szabályzatokkal kapcsolatos észrevételek és javaslatok fogadása,
- c) a szabályzatok aktualizálásának előkészítése, egyeztetése és végrehajtása,
- d) a különböző hitelesítés-szolgáltatási rendek specifikálása, jóváhagyása és karbantartása.

#### **7.2.4.3 A tanúsítványtár kötelezettségei és vele kapcsolatos tevékenységek**

A Tanúsítványtár kötelessége az üzemeltetés során:

- a) a Tanúsítványtár nyilvános, minden Érintett Fél számára elérhető módon való üzemeltetése a Szolgáltató Internetes oldalán (ld. 1.5 alfejezet), valamint az MKB Alanyok által elérhető belső oldalán;
- b) bizalmas információkat, nem nyilvános adatokat a Tanúsítványtárban meg nem jeleníteni,
- c) a Tanúsítványtárat minimum 99 %-os rendelkezésre állással működtetni, ezt a mutatót is figyelembe véve elérhetővé tenni az év valamennyi napján, 0–24 óráig; az eseti rendelkezésre állás kimaradások nem haladhatják meg a 24 órát,

## 7.3 Felelősség

### 7.3.1 A Szolgáltató általános felelőssége

A Szolgáltató felelős hogy az általában elvárható magatartás szerint a jelen és kapcsolódó szabályzatokat, utasításokat betartsa, betartassa, azok betartását ellenőrizze és előírja az esetlegesen Szolgáltatási Szabályzat Kiegészítéstől eltérő működés megszüntetésének feltételeit.

Szolgáltató a Törvényben és kapcsolódó rendeletiben meghatározott feltételrendszerű és mértékű felelősségbiztosítással rendelkezik. A Szolgáltató felelőssége és összesített felelőssége korlátozott a kötelezettségeinek megszegéséből eredő bármilyen kár tekintetében 15 millió, azaz tizenötmillió forint.

#### 7.3.1.1 A felelősség korlátai

Felek felelőssége a jelen és kapcsolódó szabályzatok, utasítások mellett a Szolgáltató ÁSZF-ben rögzítettek.

A felelősségi korlátozások vonatkoznak

- A Szolgáltató egészére,
- Bármilyen törvényszegés, szerződésszegés, visszaélés, mulasztás,
- Bármilyen egyéb közvetlen vagy közvetett károkozás esetére.

#### 7.3.1.2 A felelősség kizárása

A tanúsítványok kibocsátásában és menedzsmentjében részt vevő szervezeteknek nem áll fenn felelőssége

- Olyan esetben, mely a tanúsítványok jelen és kapcsolódó szabályzatok, előírások, utasítások ellentmondó felhasználásából ered
- A végfelhasználói magánkulcs kompromittálódásából eredő kár tekintetében, figyelemmel a Alany kötelezettségeknél meghatározottakra is
- Tanúsítvány Érintett Fél általi elfogadásáért, mely a benne foglalt adatok, vagy a tanúsítvány visszavonási lista alapján érvénytelen volt, vagy az adott esetben nem lett volna elfogadható,
- A tanúsítvány vagy a magánkulcs bármilyen meggondolatlan, hanyag, csalárd felhasználásáért akár az Alany, akár az Érintett Fél részéről.

### 7.3.2 A végfelhasználó (Alany) felelőssége

Ha a végfelhasználó az által a vonatkozó Szabályzatok, és a Törvény rendelkezéseinek be nem tartásáért okozott vagyoni és nem vagyoni kárt köteles megtéríteni, a károkozás maga után vonhatja a tanúsítvány visszavonását is.

### **7.3.3 Garancia**

Szolgáltató garantálja a Közösség számára

- A tanúsítványok kezelésének teljes időtartamára a jelen kapcsolódó szabályzatokban foglaltaknak megfelelő működést,
- A tanúsítványok kibocsátására való jogosultságot
- A tanúsítvány kibocsátási tevékenység feletti felügyeletet.

## **7.4 Változtatási eljárás**

### **7.4.1 Szolgáltatási Szabályzat Kiegészítés változtatási eljárás**

A Szolgáltatón belül Szabályzatért Felelős Egység működik, amely a Szolgáltatási Szabályzat, valamint és annak kiegészítései karbantartásáért felelős. A változtatási igényeket ezen egység gyűjti, a módosításokat elvégzi, s a változtatásokat életbe lépteti.

A Szolgáltatási Szabályzat Kiegészítés módosított változatai mindig új verziószámmal kerülnek a Kihelyezett Szolgáltató Alegységnek átadásra. A Szolgáltatási Szabályzat Kiegészítés a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente kétszer történik. A Szolgáltatási Szabályzat Kiegészítés rendkívüli felülvizsgálatára és módosítására a jogszabályi változások esetén kerül sor.

### **7.4.2 Szabályzatért Felelős Egység**

#### **7.4.2.1 A Szabályzatért Felelős Egység összetétele**

A Szabályzatért Felelős Egység a következő összetételű munkacsoportként működik:

- Szabályzat Vezető: a Szabályzatért Felelős Egység vezetője, feladata az Egység munkájának koordinálása, illetve határozatainak jóváhagyása.
- Szabályzat Adminisztrátor: a Szabályzatért Felelős Egység által felügyelt szabályzatokat alkalmazó Közösség felől a szabályzatok módosítása tekintetében érkező igények feldolgozására, illetve a szabályzatok módosításának kidolgozására és javaslat formában történő előterjesztésére kijelölt személy.

#### **7.4.2.2 A Szabályzatért Felelős Egység működése**

A Szabályzatért Felelős Egységet a Szabályzat Vezető hívja össze. A Szabályzatért Felelős Egység évente legalább kétszer a felügyelt szabályzatok rendelkezéseinek átfogó felülvizsgálata miatt kerül összehívásra.

Az Egység határozatait a szükséges változtatások előterjesztése és megvitatása után a Szabályzat Vezető hozza meg, melyeknek a szabályzatokba történő bevezetéséért a Szabályzat Adminisztrátor felelős.

A Szabályzatért Felelős Egység tagjainak mindenkor érvényes névsorát a Szabályzatért Felelős Egység tagjegyzéke tartalmazza. A Szabályzatért Felelős Egység üléseiről jegyzőkönyv készül.

## 7.5 Hivatkozott jogszabályok, szabványok és egyéb dokumentumok

Jelen dokumentum az alábbi dokumentumokra hivatkozik

- [1]. 2001. évi XXXV. Törvény az elektronikus aláírásról
- [2]. 3/2005. (III. 18.) IHM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- [3]. ISO 3166 English Country Names and Code Elements
- [4]. FIPS PUB 140-1 (1994. január 11): "Kriptográfiai modulok biztonsági követelményei"
- [5]. RFC 3280 (korábban RFC 2459) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány- és tanúsítvány visszavonási lista profil
- [6]. RFC 3647 (korábban RFC 2527) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer
- [7]. International Telecommunication Union X.509 "Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány-keretrendszer"
- [8]. 9/2005. IHM rendelet az elektronikus aláírási temékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról
- [9]. RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- [10]. ETSI 102 042 v1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates
- [11]. Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára
- [12]. 1992 évi XLIII. törvény a személyes adatok védelméről és a közhasznú adatok nyilvánosságáról
- [13]. Az Európai Parlament és a Tanács 1999/93/EK számú irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről
- [14]. Nem minősített tanúsítvány, visszavonási lista, OCSP és időbélyeg profildefiniciók mindenkor hatályos változata (e szabályzat hatályba lépésekor: 1.3.6.1.4.1.3555.1.24.20061027)
- [15]. A hitelesítés-szolgáltatás területén alkalmazható kriptográfiai algoritmusokról és paramétereikről szóló NHH határozat mindenkor hatályos változata (e szabályzat hatályba lépésekor: HL-20336-8/2005)
- [16]. A hitelesítés-szolgáltatás területén alkalmazható kriptográfiai algoritmusokról és paramétereikről szóló NHH határozat mindenkor hatályos változata (e szabályzat hatályba lépésekor: HL-20336-8/2005)