

Magyar Nemzeti Bank



Szolgáltatási Utasítás

láncolt, nem minősített hitelesítés-szolgáltatás



NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Nyilvántartási szám (OID): ---- **1.3.6.1.4.1.3555.1.13.20070627**

A Szabályzat hatályának kezdőnapja: ----- 2007. június 28.

OLDALAK SZÁMA: ----- 45, AZAZ NEGYVENÖT

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

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

Jóváhagyás dátuma: ----- **2007. 06. 27.**

Jóváhagyom:

PH.

Verziókezelés

Verzió-szám	Dátum	Módosította	Módosítás leírása	Fájl név
0.1	2007.05.23.	Dr. Szűcs Katalin	Dokumentum létrehozása	Szolgáltatasi_utasitas_070517
0.2	2007.06.14.	Dr. Nagy Zsolt	Pontosítások	Szolgáltatasi_utasitas_070614a
0.3	2007.06.22.	Dr. Nagy Zsolt	Kommentek átvezetése	Szolgáltatasi_utasitas_070622a
1.0	2007.06.26.	Dr. Nagy Zsolt	Regisztrációs rend módosítása	Szolgáltatasi_utasitas_070626
1.1	2007.06.26.	Dr. Nagy Zsolt	Véglegesítés	Szolgáltatasi_utasitas_070626

Tartalomjegyzék

1	Bevezetés	6
1.1	Áttekintés.....	6
1.2	Dokumentum neve és azonosítása.....	9
1.3	PKI közösség.....	10
1.4	Alkalmazhatóság.....	11
1.5	Kapcsolattartás.....	11
1.6	Fogalmak és rövidítések.....	12
2	Közzététel és tanúsítványtár	16
2.1	Az információ közzététele.....	16
2.2	Tanúsítványokkal kapcsolatos információk.....	16
2.3	A közzététel gyakorisága.....	17
2.4	Hozzáférs ellenőrzések.....	17
3	Azonosítás és hitelesítés.....	18
3.1	Elnevezések.....	18
3.2	Kezdeti azonosítás.....	19
3.3	Azonosítás tanúsítvány kulcscseréje esetén	20
3.4	Visszavonási kérelem	20
4	Működésre vonatkozó követelmények.....	21
4.1	Tanúsítványigénylés.....	21
4.2	Tanúsítványkérelem feldolgozása.....	21
4.3	A tanúsítványok kibocsátása és hozzáférhetővé tétele	25
4.4	Tanúsítványelfogadás.....	25
4.5	A kulcpár és a tanúsítvány használata	26
4.6	Tanúsítvány megújítása	27
4.7	Kulcscsere.....	28
4.8	Tanúsítvány módosítása.....	28
4.9	Tanúsítvány függesztése és visszavonása	28
4.10	Tanúsítvány-állapot információk közzététele	31
4.11	Kulcs letétbe helyezése és visszaállítása.....	32
5	Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések.....	33
5.1	Fizikai óvintézkedések.....	33
5.2	A Láncolt Hitelesítés-szolgáltató leállítása.....	33
5.3	Kulcpár előállítás és telepítés.....	34
5.4	A magánkulcsok védelme.....	35
5.5	Aktíváló adatok	37
6	Tanúsítvány és visszavonási lista profilok.....	38

6.1	Tanúsítványprofilok.....	38
6.2	Tanúsítvány visszavonási lista profilok	39
7	Üzleti és jogi tudnivalók.....	40
7.1	Bizalmasság, adatvédelem.....	40
7.2	Jogok és kötelezettségek.....	40
7.3	Felelősség	43
7.4	Változtatási eljárás.....	44
7.5	Hivatkozott jogszabályok, szabványok és egyéb dokumentumok	45

1 Bevezetés

1.1 Áttekintés

A jelen dokumentum a Magyar Nemzeti Bank (a továbbiakban: MNB) nem minősített aláírás és titkosítás célú tanúsítványok hitelesítés-szolgáltatásra vonatkozó Szolgáltatási Utasítása (a továbbiakban: Szolgáltatási Utasítás vagy Utasítás).

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

MNB a NetLock Informatikai és Hálózatbiztonsági Szolgáltató Kft. által üzemeltetésébe adott láncolt hitelesítés-szolgáltatás használatával kijelenti, hogy azt jelen Szolgáltatási Utasítás alapján működteti, betartva jelen Utasításban foglalt valamennyi kötelezettségét.

1.1.1 Az Utasítás

Jelen Utasítás az MNB nem minősített, munkatársi aláíró és munkatársi titkosító tanúsítványokkal kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazza.

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

1.1.2 Az Utasítás hatálya

1.1.2.1 Tárgyi hatály

A Szabályzat tárgyi hatálya az 1.1.4 pontban ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.

1.1.2.2 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.

1.1.2.3 Személyi hatály

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

1.1.3 A Szolgáltató

A jelen Utasításban Szolgáltatónak nevezett entitás a NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság. Cégjegyzékszám: 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.

Önkéntes akkreditáció, egyéb minősítések:

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

A Szolgáltató felelős az MNB hitelesítés-szolgáltatási tevékenységért. A Szolgáltató felelőssége, hogy az általában elvárható magatartás szerint a jelen és kapcsolódó Szabályzatokat, Utasításokat betartsa, betartassa, azok betartását ellenőrizze, és előírja az esetleges Utasítástól eltérő működés megszüntetésének feltételeit.

1.1.4 Szolgáltatások

Az MNB tanúsítvány-szolgáltatásban való közreműködést, és ezzel összefüggésben intelligens kártya megsemmisítési feladatokat lát el. Az MNB tevékenysége a következő fő elemekből áll:

- Regisztrációs szolgáltatás
- Aláíró és titkosító tanúsítvány létrehozási szolgáltatás
- Aláíró eszköz szolgáltatás
- Egyedi név szolgáltatás
- Tanúsítványszétosztási szolgáltatás
- Tanúsítványarchiválási szolgáltatás
- Adattárolási szolgáltatás
- Állapotinformációs szolgáltatás
- Tanúsítványmegújítási szolgáltatás
- Visszavonás kezelési szolgáltatás

1.1.5 Szabványok és előírások

1.1.5.1 Szolgáltatási Utasítás

Az Utasítás az RFC 3647 [8] szabványa alapján készült. Az Utasítás 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 [15], valamint az x.509 [9] szabvány ajánlásait.

1.1.5.2 Lenyomatképző algoritmusok azonosítói

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

1.1.5.3 Kriptográfiai algoritmusok azonosítói

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

1.1.5.4 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 }
- Netscape Certificate Type OID ::= { Joint ISO/ITU-T assignment(2) Joint assignments by country(16) USA(840) US company arc(1) Netscape Communications Corp.(113730) Netscape certificate extension(1) 1 }
- Netscape Comment OID ::= { Joint ISO/ITU-T assignment(2) Joint assignments by country(16) USA(840) US company arc(1) Netscape Communications Corp.(113730) Netscape certificate extension(1) 13 }

1.1.5.5 Alkalmazott formátumok

Tétel	Alkalmazott / elfogadott formátum, szabvány
Aláírás 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

1.1.6 Hitelesítés-szolgáltatás és tanúsítványfajták

Az MNB előzetes entitásazonosítás után az igénylők (későbbi alanyok) számára aláíró és titkosító tanúsítványok kibocsátásában működik közre.

A tanúsítvány a hitelesítés-szolgáltató / 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, ideértve a hatósági (hivatali) jelleget.

Az MNB jelen utasítás 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 szervezet vagy hatóság munkatársaként	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgyi, értékbeli, időbeli stb.) megsejése	A tanúsítványban szereplő érték, de maximum 5 millió forint	Írásbeliség (magánokirat)
Munkatársi titkosító	Természetes személy szervezet vagy hatóság munkatársaként	Titkosítási műveletek végrehajtása	Bármilyen korlátozás (földrajzi, tárgyi, értékbeli, időbeli stb.) megsejése	A tanúsítványban szereplő érték, de maximum 5 millió forint	-

Az MNB egyéni joga és felelőssége, hogy a fentiek közül milyen tanúsítványt alkalmaz, illetve ezzel összefüggésben bocsát ki egy adott célra.

1.1.7 Aláíró eszköz szolgáltatás

Az MNB a tanúsítványok kibocsátása során aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatást végez. Az MNB kizárólag aláíró eszköz szolgáltatás keretében jogosult tanúsítványok kibocsátására.

A szolgáltatás keretében a hatályos jogszabályok és a jelen Utasítás rendelkezéseinek figyelembe vételével az alany számára kulcspárt generál az adott aláírás létrehozó eszközre.

Aláíró eszköz szolgáltatás biztosítása aláíró tanúsítványok kibocsátása során, mellyel összefüggésben az MNB:

- az aláíró kulcsokat a fokozott biztonságú elektronikus aláírások céljaira alkalmas algoritmus [23] felhasználásával generálja, illetve az eszközt megszemélyesíti;
- gondoskodik arról, hogy a kulcs hossza és az alkalmazott nyilvános kulcsú algoritmus [23] a fokozott biztonságú elektronikus aláírás céljaira alkalmas legyen;
- a kulcsok generálását és az Alanyhoz történő továbbítását megelőző tárolását biztonságosan végzi;
- 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 általa generált magán kulcsokról semmilyen másolat ne kerüljön tárolásra;
- gondoskodik az általa biztosított aláírás-létrehozó eszköz kibocsátásakor az eljárás biztonságosságáról;
- biztosítja, hogy az aláírás-létrehozó eszköz a szándék szerinti, hitelesített Aláíróhoz kerül;
- aláíró eszköz biztosítása esetén az aktivizáló adatokat 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 megismerése, magánkulcsok, tanúsítványok használata;
- az aláírás-létrehozó eszköz előkészítése és továbbítása során alkalmazza a biztonsági eljárásokat;
- az aláírás-létrehozó adat csak az átadás után lesz érvényes.

Aláíró eszköz szolgáltatás biztosítása titkosító tanúsítványok kibocsátása során, mellyel összefüggésben az MNB a fentiektől az alábbiakban tér el:

- a titkosító kulcsokat a titkosítás céljaira alkalmas algoritmus [23] felhasználásával generálja, illetve az eszközt megszemélyesíti;

1.2 Dokumentum neve és azonosítása

Jelen dokumentum:

- Teljes neve: Magyar Nemzeti Bank Szolgáltatási Utasítás (láncolt, nem minősített hitelesítés-szolgáltatás)
- Rövid neve: Szolgáltatási Utasítás
- Verziószáma: a fedlapon található verziószám

1.3 PKI közösség

A kibocsátott tanúsítványok, aláírás-létrehozó eszközök alkalmazó közössége az MNB, a tanúsítványok végfelhasználói és az érintett felek.

1.3.1 Hitelesítő Alegységek

Az MNB saját szervezetén belül Hitelesítő Alegységeket működtet, amelyek feladata a tanúsítványok központi létrehozása és kezelése a regisztrációs egységektől kapott kérelmeknek megfelelően.

1.3.1.1 Hitelesítő Alegység

Az MNB tanúsítványkiadási szolgáltatásait végző hitelesítő egysége. A Hitelesítő Alegység az előírt eljárási rend szerint a hozzá tartozó regisztrációs egységek kérelme alapján jóváhagyja az aláíró és a titkosító tanúsítványok kiadását, publikálását, visszavonását, felfüggesztését. Emellett gondoskodik a Tanúsítvány Visszavonási Lista (a továbbiakban: CRL) publikálásáról is.

Név:	MNB Nem Minősített Hitelesítő Egység
Egység:	MNB Bankbiztonság
Cím:	1054 Budapest, Szabadság tér 8-9..
Telefon:	(1) 428-2600 / 3096 / 3129
Internet cím:	www.mnb.hu
E-mail:	tanusitvanyok@mnb.hu

1.3.2 Regisztrációs Alegység

Az MNB saját szervezetén belül regisztrációs alegységet működtet, amelynek feladata a kezdeti regisztráció és a tanúsítvány kibocsátásával kapcsolatos egyéb tevékenységek elvégzése, tanúsítvány kezelési feladatok, ideértve a felhasználókkal való kapcsolattartást is.

A regisztrációs alegység a tanúsítvány-kibocsátás során a felhasználói adatellenőrzést végzi, 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

Az MNB 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.

Az MNB jelen utasítás alapján a következő entitások részére bocsát ki aláíró tanúsítványokat:

- az MNB alkalmazásában álló természetes személy – munkatársi aláíró tanúsítvány
- az MNB alkalmazásában álló természetes személy – munkatársi titkosító tanúsítvány

Az alany és a másodlagos alany szerződéses viszonyban áll. Az MNB az alanyokkal a Regisztrációs Alegységeken keresztül tart kapcsolatot.

Az alanyok kizárólag az MNB-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 az MNB által kibocsátott tanúsítványhoz fordul, illetőleg ezen tanúsítvány, érvényességének ellenőrzéséhez az MNB által karbantartott nyilvántartásokat ellenőrzi.

Az MNB az Érintett Féllel elsősorban a tanúsítványvisszavonási információkon keresztül tart kapcsolatot.

1.4 Alkalmazhatóság

1.4.1 Engedélyezett alkalmazási lehetőségek

A kibocsátott 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.

Az MNB láncolt aláíró és titkosító főtanúsítványa (a továbbiakban: MNB 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 (1.1.6 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.

Az MNB 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

Név:	NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
Egység:	NetLock Kft.

Név:	NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
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 fogasztóvédelmi felügyelőség:	Budapest Főváros Közigazgatási Hivatal Fogasztóvédelmi Felügyelőség 1088 Budapest, József krt. 6.

1.5.2 Az MNB adatai

Név:	Magyar Nemzeti Bank
Egység:	MNB
Székhely:	1054 Budapest, Szabadság tér 8-9.
Telefon:	(1) 428-2600 / 3096 / 3129
Fax:	(1) 428-2585

1.5.3 Utasítással kapcsolatos kérdések

Jelen Szolgáltatási Utasítás 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).

1.5.4 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.
- **Személyes tanúsítvány:** Természetes személyek számára kibocsátott, kizárólag elektronikus aláírás előállítására használható tanúsítvány.

- **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.
- **Biztonságos aláírás-létrehozó eszköz (BALE):** A Törvény 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.
- **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. Az egyedi név komponensei személyes és munkatársi tanúsítvány esetén eltérhetnek.
- **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 az Utasítás 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.
- **Eszközszolgáltatás:** Az a szolgáltatás, melynek során az MNB a Törvény 6. § (1) bekezdésének c) pontja értelmében meghatározott, elektronikus aláíráshoz kapcsolódó aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatást végez, illetve a titkosító tanúsítványok kibocsátásához kapcsolódó kulcsgenerálási tevékenységet végez.
- **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 MNB végfelhasználói tanúsítványokat létrehozó infrastruktúra alegységek, amelyet az MNB üzemeltet.
- **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.
- **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 valódiságát az ellenkező bizonyításig mindenki köteles elfogadni. Ilyen közhiteles nyilvántartás a cégnyilvántartás, valamint a polgárok személyi és lakcím adatait tartalmazó nyilvántartás.
- **(Kriptográfiai) Kulcs:** Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításához, 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 lenyomathoz 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.
- **Munkatárs:** A természetes személyek azon köre, amelyeket egy adott szervezet saját magához tartozóként ismer el.
- **MNB Nem Minősített Hitelesítés-szolgáltatás:** 'B' hitelesítési osztályú nem minősített munkatársi aláíró és titkosító tanúsítványok kibocsátása.
- **MNB Hitelesítési-szolgáltatás:** MNB HSZ: A jelen Utasításban meghatározott feltételeknek megfelelő végfelhasználói tanúsítványok kibocsátásával, kezelésével kapcsolatos szolgáltatói feladatok összessége.
- **MNB Központ:** MNB hitelesítési rendszer irányításáért felelős szervezeti egység, az MNB Bankbiztonság Működési kockázatkezelési osztályának IT biztonsági csoportja.
- **Out-of-band:** Elektronikus információk szokásos használati környezetén kívül történő előállítás, továbbítási módja.
- **Összesített felelősség:** Tanúsítványok és káresemények 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 összegyűjtő, ellenőrző, tanúsítvány kibocsátási, felfüggesztési, visszavonási kérelmeket összeállító és a Hitelesítő Alegységhez továbbító egység, amelyet az MNB üzemeltet.

- **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.
- **Szolgáltató:** A NetLock Kft., amely az MNB számára a láncolt tanúsítványkiadó infrastruktúra működtetéséhez szükséges láncolt fő(root)tanúsítványt biztosítja.
- **Szolgáltatási Utasítás:** A Szolgáltatónak az adott Utasítás által szabályozott specifikus hitelesítési tevékenységgel kapcsolatos részletes kiegészítő és specifikus eljárási és egyén működési szabályokat tartalmazó nyilvános dokumentum.
- **Tanúsítvány:** A Szolgáltató által kibocsátott elektronikus igazolás, amely az aláírás-ellenőrző adatot a tanúsítvány alanyához kapcsolja.
- **Tanúsítvány-szolgáltatás:** azon eljárás, melynek során az MNB a Szolgáltatási Utasításban meghatározott eljárásban új vagy megújított, aláíró és titkosító célú tanúsítványt bocsát ki a felhasználó részére. A tanúsítvány-szolgáltatáshoz kapcsolódóan az MNB tanúsítványállapot-szolgáltatást is nyújt, melynek keretében fogadja a tanúsítvány-visszavonási- és felfüggesztési kérelmeket és a Szolgáltatási Utasításban meghatározott időközönként Tanúsítvány Visszavonási Listát bocsát ki.
- **Tanúsítványfajta:** Jelen Utasítás két megjelenési formáját ismeri: a személyeset és a munkatársit.
- **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 MNB által kibocsátott végfelhasználói tanúsítvánnyal rendelkezik.
- **Végfelhasználói tanúsítvány:** Az MNB által kibocsátott olyan tanúsítvány, amelyet az alany kizárólag elektronikus aláírás előállítására használhat, de más tanúsítvány hitelesítésére nem.

2 Közzététel és tanúsítványtár

2.1 Az információ közzététele

2.1.1 Közzétételi és tájékoztatási elvek

2.1.1.1 Az Utasításban nem tárgyalt elemek

Az MNB nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti. Az MNB több belső biztonsági és egyéb szabállyal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel.

2.1.1.2 Az Utasítás közzététele

Az MNB jelen szolgáltatási utasítást weboldalán (cdp.mnb.hu) keresztül hozza nyilvánosságra.

2.1.1.3 Észrevételek kezelése

Az Utasítással kapcsolatos észrevételeket Szolgáltató az info@netlock.hu címen fogadja.

2.2 Tanúsítványokkal kapcsolatos információk

2.2.1 Tanúsítványok közzététele

A Szolgáltató az általa működtetett szolgáltatási alegységek tanúsítványát a következő módszerekkel teszi közzé:

- saját szolgáltatói tanúsítványát közzéteszi tanúsítványtárában, illetve saját weboldalán

Az MNB a saját közreműködésével kibocsátott végfelhasználói tanúsítványokat az alany és a másodlagos alany hozzájárulása alapján tárolja tanúsítványtárában.

2.2.2 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala

A Szolgáltató az általa működtetett hitelesítő egység tanúsítványával kapcsolatos állapotinformációkat a következő módszerekkel teszi közzé:

- szolgáltatói tanúsítványainak állapotváltozását a saját tanúsítványtárában tünteti fel,

Az MNB az általa üzemeltetett hitelesítő egységek által kiadott végfelhasználói tanúsítványokkal kapcsolatos állapotinformációkat a következő módszerekkel teszi közzé:

- a végfelhasználói tanúsítványok állapotváltozását a tanúsítványtárában hozza nyilvánosságra (cdp.mnb.hu),
- végfelhasználói tanúsítvány visszavonását és felfüggesztését az MNB 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

Az MNB a nem minősített munkatársi aláíró és titkosító tanúsítványok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:

- Szolgáltató az MNB által használt láncolt fő(root)tanúsítványokat a kibocsátást követő 1 munkanapon belül teszi közzé,
- az MNB a végfelhasználói tanúsítványokat a tanúsítványtárban az előállítást követően 1 munkanapon belül helyezi el tanúsítványtárban.

2.3.2 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

Az MNB az általa működtetett hitelesítő egységek és felhasználók tanúsítványával kapcsolatos állapotinformációkat a 4.10.1 pontban tárgyalt gyakorisággal teszi közzé.

2.4 Hozzáférés ellenőrzések

Az MNB által közzétett kikötések és feltételek, tanúsítványok és állapotinformációk nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közlő közegek sajátosságainak megfelelően.

Az MNB által közzétett információkat az MNB kizárólag csak a Szolgáltatóval történő előzetes egyeztetést követően egészítheti ki, törölheti vagy módosíthatja. Az MNB különböző védelmi mechanizmusokkal akadályozza meg az információkhoz való jogosulatlan hozzáféréseket.

2.4.1 Tanúsítványtárak

Az MNB 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 az MNB által kiadott tanúsítványok (nem nyilvános rész) és a visszavont tanúsítványok listái (nyilvános rész) találhatók.

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

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

Az MNB a kibocsátott tanúsítványok nyilvántartása, a visszavonási nyilvántartások, valamint az online tanúsítvány állapot lekérdezési lehetőség legalább 99%-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 Névtypusok

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, SN = Vezetéknév), az UTF-8 kódolást használva,
- munkatársi tanúsítványokban az „*Organization*” mezőben mindig az MNB szerepel másodlagos alanyként, valamint az „*Organization-unit*” mezőben szerepelhet az MNB szervezeti egysége,
- a „*Locality*” mezőben az MNB székhelyeként Budapest kerül feltüntetésre,
- a az MNB az ISO 3166 [3] szabványban meghatározott kétkarakteres országkódként a „HU”-t alkalmazza.

3.1.2 Álnév használata

3.1.2.1 Általános szabályok

Az MNB nem jogosult álnevet tartalmazó tanúsítvány kibocsátására.

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*), a szervezet nevét (*Organization*), 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, *Surname* vezetéknévű természetes személy, aki az *Organization* nevű szervezet (jelen esetben: MNB) *Organization-unit* osztályához, illetve szervezeti egységéhez (jelen esetben: MNB szervezeti egysége) 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*.

Az *Organization* mezőben minden esetben az MNB kerül feltüntetésre.

3.1.4 A nevek egyedisége

Az MNB a 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

Az MNB 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

Az aláíró eszköz szolgáltatás esetében a Regisztrációs Alegység állítja elő az alany számára a kulcspárt, így az MNB nem igényel bizonyítékot arra, hogy az alany rendelkezik a hitelesítendő nyilvános kulcs magánkulcs párával.

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

3.2.2 Szervezeti azonosság hitelesítése

Az MNB által kibocsátott munkatársi tanúsítványban feltüntetésre kerül a felhasználó szervezet (másodlagos alany). Opcionálisan egyéb adatok is feltüntetésre kerülhetnek.

Tekintettel arra, hogy az MNB csak saját munkavállalói részére bocsát ki tanúsítványokat, a szervezet *Organization* mezőben minden esetben az MNB kerül feltüntetésre.

3.2.3 Személyazonosság hitelesítése

Az MNB a természetes személy azonosítását az egyes tanúsítványfajták esetében a 4.2.2 pont alatti táblázatban leírt módon végzi el.

A személyazonosításra alkalmas hivatalos igazolványban szereplő fénykép alapján az alanynak 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, az MNB megtagadja a tanúsítványkiadási kérelem teljesítését.

Az MNB továbbá megállapítja mindazon adatok hitelességét, melyeket a tanúsítványban feltüntet.

3.3 Azonosítás tanúsítvány kulcscseréje esetén

Tanúsítvány kulcscseréjét az MNB 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

Az MNB tanúsítvány 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

Tanúsítványt igényelhet

- a munkavállaló szervezeti egységének vezetője a munkavállaló részére feltüntetve a tanúsítványban, hogy meghatározott szervezethez, jelen esetben az MNB-hez tartozik,

Kizárólag a jelen Utasításban 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 MNB feldolgozza a tanúsítványkérelmet a következőkben bemutatott eljárásrend szerint.

4.2.1 Általános regisztrációs szabályok

A 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 az MNB saját Regisztrációs Adminisztrátorai végzik. A tanúsítványkérelmet a regisztrációs adminisztrátorok felelősek kezelni, miután azonosították az alanyt a kapcsolódó tanúsítványfajta által meghatározott követelményeknek megfelelően.

4.2.1.1 Általános regisztrációs lépések

- az igénylő tanúsítványigénylési kérelmet juttat el az MNB-hez, melynek során elfogadja a tanúsítványkibocsátáshoz kapcsolódó feltételeket; személyesen bemutatja a személyazonosító dokumentumait az MNB regisztrációs munkatársai előtt,
- az MNB fogadja a kérelmet, illetve ellenőrzi annak szabályosságát,
- az MNB azonosítja az igénylő természetes személyt, és a szervezeti adatokat,
- a Regisztrációs Alegység elkészíti szolgáltatási szerződését, előkészíti a további regisztrációhoz szükséges dokumentumokat,

- az MNB - amennyiben a személy- és szervezetazonosítás rendben lezárult, átveszi az alannal (és a másodlagos alannal) kötött szolgáltatási szerződését -, és összeveti az abban foglalt adatokat a személy- és szervezetazonosítás során ellenőrzött adatokkal,
- a kulcspárt az MNB generálja az igénylő számára az aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatás keretében,
- az MNB összeállítja a kibocsátandó tanúsítványt,
- az MNB dokumentálja a regisztrációs lépéseket,
- az MNB kibocsátja a tanúsítványt az összes ellenőrzés pozitív lezárása esetén.
- Az MNB eljuttatja az alanyhoz a kulcspárt és a tanúsítványt tartalmazó aláírás-létrehozó eszközt.

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.

Az MNB 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. Alanyregisztrációja	Munkavállaló adatainak (név, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az alany az elektronikus regisztrált adatait alátámasztó dokumentumok eredeti példányát, illetve a szervezeti egysége vezetőjének igazolását (a Kártyakísérő Űrlapon) a regisztrációs alegység munkatársai előtt bemutatja. Személyazonosság ellenőrzésekor kizárólag személyazonosításra alkalmas dokumentum, azaz személyi igazolvány vagy útlevél vagy „új” típusú (bankkártya méretű) jogosítvány és a lakcímkártya fogadható el.
2. Másodlagos alany regisztrációja (kapcsolt regisztráció)	Szervezet adatainak, jelen esetben az MNB (név, székhely, telefon, fax, e-mail cím) elektronikus regisztrációja. Az adatok karbantartása, naprakészességének biztosítása a Regisztrációs Alegység feladata.
3. Regisztráció jóváhagyása	Végrehajtani jogosult: Hitelesítő Egység
4. Kulcspár generálása eszközön és kérelem készítése	Végrehajtani jogosult: Regisztrációs Alegység.
5. Tanúsítvány előállítás	Végrehajtani jogosult: Regisztrációs Alegység
6. Tanúsítvány hordozó eszközre való letöltése és a tanúsítványtárban való közzététele	Végrehajtani jogosult: Regisztrációs Alegység.
7. Alany személyazonosságának ellenőrzése	Végrehajtani jogosult: Regisztrációs Alegység.

Eljárási lépés	Tanúsítványfajta
	Munkatársi
8. Kártyakísérő űrlap aláírása és másolatának átadása az alanynak	Végrehajtani jogosult: Regisztrációs Alegység.
9. Hordozóeszköz átadása az aláírónak	Végrehajtani jogosult: Regisztrációs Alegység.
10. Dokumentáció archiválása	Végrehajtani jogosult: Regisztrációs Alegység munkatársa.

4.2.3 Szolgáltatási szerződés

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

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

A nyilatkozat, vagy melléklete legalább a következőket tartalmazza:

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

A nyilvános kulcs lenyomat karaktereinek átírása:

0 - NULLA, 1 - EGY, 2 - KETTŐ, 3 - HÁROM, 4 - NÉGY, 5 - ÖT, 6 - HAT, 7 - HÉT, 8 - NYOLC, 9 - KILENC, A - ADÉL, B - BÉLA, C - CECIL, D - DÉNES, E - ELEMÉR és F – FERENC

Az elfogadó nyilatkozatot az igénylő természetes személy írja alá.

4.2.4 A tanúsítványkérelmek jóváhagyásának követelményei

Az MNB 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 alanyal,
- a kérelemben szereplő adatok ellenőrizhetők és pontosak.

4.2.5 A tanúsítványok tartalma

A tanúsítványok tartalmazzák az alábbiakat:

- a tanúsítvány azonosító kódját,
- az MNB megnevezését, benne székhelyének 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 (kivétel: láncolt hitelesítés szolgáltatáshoz használt tanúsítvány esetén),
- 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 Láncolt Hitelesítés-szolgáltató elektronikus aláírását.

4.2.6 A tanúsítványok jellemzői

Az MNB 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 MNB nem minősített láncolt tanúsítvány szolgáltatói kulcsával vannak aláírva,
- a tanúsítványok aláírása ellenőrizhető a tanúsítványban szereplő adatok és az MNB megfelelő nyilvános kulcsának felhasználásával.

4.2.7 Az igénylő (alany) tájékoztatása a kibocsátást megelőzően

Az MNB 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

Az MNB elutasítja a tanúsítványkérelmeket, amennyiben

- a tanúsítványigénylés nem teljes,
- a tanúsítványigénylés nem helyes,
- a bemutatott iratok és okmányok eredetiségével, valóságával vagy érvényességével kapcsolatban 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, illetve annak kódja. 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 előállítás során az MNB 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 és Hitelesítő 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 az MNB 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 alanynak, illetve a másodlagos alanynak 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 és a magánkulcsot, illetve a tanúsítványt átvette.

4.4.2 A tanúsítványigénylő nyilatkozata

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

- ismeri, érti és elfogadja a tanúsítványkibocsátáshoz kapcsolódó szabályzatokat,
- a tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályoknak és törvényi előírásoknak megfelelően használja,

- minden adat, amit az MNB-nek a tanúsítvány kiadásának céljából átadott, a valóságnak megfelel, és azok átadása önkéntes volt,
- a tanúsítványban szereplő minden adat a tudomásával és egyetértésével került a tanúsítványba,
- a tanúsítvány érvényességét befolyásoló tényekről, valamint az igénylés során megadott személyes adatok megváltozása esetén haladéktalanul értesíti az MNB-t,
- 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 MNB-t a tanúsítvány közzétételével, és saját vagy más nyilvános tanúsítványgyűjtő helyeken történő elhelyezésével.

4.4.3 Tanúsítvány közzététele

Az MNB a kiadott tanúsítványt 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 MNB-vel szerződésben rögzített korlátozásnak megfelelően használhatja,
- b) a megfelelő tanúsítvány lejártá 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 (MNB) 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 kell ellátni. A kulcs elvesztéséből, véletlen vagy szándékos nyilvánosságra hozatalából eredő károkért az Alany felelős. A kulcs kompromittálódását az előírt módon az MNB-be be kell jelenteni. A szabályosan bejelentett letiltási kérelem után a jelen Utasításban 4.9.1 pontjában meghatározott módon felel a felmerült károkért az Alany, a másodlagos alany, illetve a Szolgáltató.

Az MNB a 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 az MNB – 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 (lásd még 7.3.3 pont).

4.6 Tanúsítvány megújítása

4.6.1 Végfelhasználói tanúsítványok

A végfelhasználói tanúsítványok megújítása az MNB láncolt szolgáltatása során nem támogatott.

4.6.2 Szolgáltatói tanúsítványok

Az MNB láncolt szolgáltatáshoz tanúsítványát a Szolgáltató 5 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 MNB a láncolt szolgáltatás során nem jogosult kulcscserével történő tanúsítvány kibocsátására.

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 módosítására az MNB nem jogosult.

4.9 Tanúsítvány felfüggesztése és visszavonása

4.9.1 Általános rendelkezések

Az MNB 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 az MNB 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 MNB-hez 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 MNB 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, 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 az MNB regisztrációs munkatársai számára történő, meghatározott formanyomtatványon kitöltésével kezdeményezhető. A visszavonási kérelem benyújtható:

- személyesen, a Regisztrációs Alegységnél,
- az MNB-nek küldött e-mailben, illetve faxon.

Ügyfélszolgálati időben (megegyezik az MNB törzsidővel) a Regisztrációs Alegységnél, illetve a Bankbiztonság Fegyveres Biztonsági Őrségének (FBŐ) őrparancsnokánál:

- személyesen

Ügyfélszolgálati időn kívül Bankbiztonság Fegyveres Biztonsági Őrségének (FBŐ) őrparancsnokánál:

- személyesen

A visszavonási kérelemnek legalább a következő adatokat kell tartalmaznia:

- a tanúsítvány sorszáma vagy egyedi neve,
- a visszavonást kérő megnevezése,
- a visszavonást kérő elérhetősége,
- a visszavonást kérő kapcsolata a tanúsítvány alanyával,
- a visszavonás oka,
- személyazonosításhoz használt személyazonosító dokumentum megnevezése és száma.

A visszavonásra irányuló kérelmeket az MNB más kérelmeket megelőzően, soron kívül bírálja el.

A visszavonási eljárás során az MNB 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 az MNB 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 kiléte vagy a visszavonásra való jogosultság nem állapítható meg, akkor az MNB a tanúsítvány visszavonását megtagadhatja.

Helyes és hiteles kérelem esetén az MNB 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 az MNB folyamatosan fogadja és haladéktalanul megkezd azok feldolgozását. A feldolgozás megkezdése és a tanúsítvány státuszváltásról való döntést követően az MNB 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.

Az MNB 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 az MNB-hez. A felfüggesztési kérelmet a visszavonási kérelemmel megegyező módon dolgozza fel az MNB.

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 munkanapig. Ez alól a kibocsátás során az MNB általi technikai felfüggesztés időtartama jelent kivételt, mely során a tanúsítvány legfeljebb 30 naptári napig lehet felfüggesztett állapotban. Ezen technikai felfüggesztésre csak egy alkalommal kerülhet sor és a tanúsítvány kibocsátásától annak aktiválásáig tart. Minden egyéb esetben a felfüggesztés ideje legfeljebb 5 munkanap lehet. A tanúsítvány visszavonásáról, illetve újbóli érvényesre állításáról az MNB-nek 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, MNB 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 végrehajtandóak. 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)

Az MNB X.509 V2 típusú tanúsítvány visszavonási listák kibocsátását és tanúsítvány visszavonási kiterjesztések alkalmazását támogatja.

- Az MNB 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.

- Az MNB 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 az MNB 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 tanúsítványállapot-változásnak az MNB nyilvántartásában való átvezetést követő 1 órán belül a kérelem szerint módosított visszavonási állapotot közlésezi.

A visszavonási listák mindig tartalmazzák a következő lista kibocsátásnak idejét, melyet megelőzve is kibocsáthat az MNB 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.

Az MNB-t nem terheli felelősség a visszavonási listában közzétett tanúsítványok elfogadásából keletkező esetleges károkért.

4.10.3 A visszavonási információ közzétételének egyéb formái

A visszavonási hirdetmények csak az MNB tanúsítványtárában és annak biztonsági másolataiban, érhetőek el.

4.11 Kulcs letétbe helyezése és visszaállítása

Az MNB az által kibocsátott végfelhasználói aláíró és titkosító tanúsítványok esetén nem nyújt magánkulcs letéti szolgáltatást, illetve az alany aláíró magánkulcsát semmilyen más módon nem tárolja el vagy menti.

Az MNB a saját, szolgáltatói magánkulcsait elmentve is tárolja, illetve azt a Szolgáltató is tárolja.

5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A regisztrációs és hitelesítő 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

Az MNB láncolt hitelesítés-szolgáltatói infrastruktúrájára vonatkozó fizikai-biztonsági követelmények külön dokumentumban találhatóak.

5.2 A Láncolt Hitelesítés-szolgáltató leállítása

5.2.1 Szolgáltatás megszüntetése

Amennyiben az MNB 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, illetve a Szolgáltatót,
- b) A szolgáltatás megszűnése előtt 30 nappal e-mail címmel rendelkező ügyfelei számára a szolgáltatás befejezéséről elektronikus levélben értesítőt küld.
- c) Az MNB 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 kibocsátásra vonatkozó szabályzatokat és az aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását. A mentett adatállományokat a az MNB védi jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását, valamint az adatoknak megőrzési időn belüli, jogosultak számára való hozzáférhetőségét és értelmezhetőségét.
- e) A láncolt szolgáltatáshoz használt magánkulcsokat a Szolgáltatóval együttműködve megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat a Szolgáltató visszavonja.
- f) Az MNB a tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is eleget tesz.
- g) Az MNB a Szolgáltatóval történő együttműködés megszűnésének bejelentését követően az együttműködés keretében új tanúsítványokat 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 eszközszolgáltatás keretében aláírás-létrehozó eszközön az MNB végzi.	A láncolt szolgáltató kulcspárt a Szolgáltató generálja, hitelesíti és adja át az MNB részére.
	Kulcs méretek	A végfelhasználók minimum 1024 bites RSA kulccsal rendelkeznek	A Szolgáltató legalább 2048 bites RSA kulcsokat generál.
	Kulcs felhasználási célok	Aláíró kulcspárt generálás a.	- végfelhasználói tanúsítvány, CRL validációk aláírása;
Magánkulcs védelme	Magánkulcs többszemélyes kontrollja	Az MNB eszközszolgáltatás esetén többszemélyes kontrollt vagy ennek megfelelő technikai védelmet biztosít a magánkulcsok generálásakor és kezelésékor.	-
	Magánkulcs mentése	Magánkulcsot az MNB nem ment.	Az MNB láncolt szolgáltatásához használt magánkulcsokat a Szolgáltató menti.
	Magánkulcs aktiválása	A magánkulcsokat aláíró eszköz át vételét követően használhatók, külön aktiválásra nincs szükség.	Az MNB láncolt szolgáltatói magánkulcsai nak aktiválását a Szolgáltató végzi.
	Magánkulcs deaktiválása	A magánkulcsok deaktiválását a felhasználó alkalmazás végzi működésének befejezésekor.	A magánkulcsok deaktiválását a Szolgáltató végzi.
	Magánkulcs megsemmisítése	Végfelhasználó köteles kezdeményezni aláíró magánkulcsának megsemmisítését annak érvényességi idejének lejáta után.	Az MNB szolgáltatói magánkulcsait és azok minden előfordulását az érvényesség lejáratakor a Szolgáltató megsemmisíti.
Egyéb tevékenységek	Nyilvános kulcs archiválása	A végfelhasználói és szolgáltatói nyilvános kulcsokat az MNB az elektronikus aláírásról szóló törvényben meghatározott ideig archivformában megőrzi (ld. 4.2.2.1 pont).	
	Kulcsok felhasználási ideje	A magánkulcs érvényességi ideje megegyezik a hozzá tartozó tanúsítvány érvényességi idejével, de maximálisan 2 év. A nyilvános kulcs a kriptográfiai biztonságáig érvényes.	

Az MNB valamennyi láncolt szolgáltatói kulcspárát 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 Hitelesítő Egység	Rainbow iKey 2032 FIPS USB Token	iKeyDriver Version 3.4.7.118
Végfelhasználói eszköz	Kulcspár és tanúsítványtárolás áramkalmas aláírás-létrehozó eszköz	-

5.3.2 Magánkulcs eljuttatása az alanyhoz

Mivel a Szolgáltató valamennyi kulcspárja helyben generálódik (ld. 5.3.1 pont), azokat nem kell továbbítani.

Az MNB az eszköz-szolgáltatás keretében generált a végfelhasználói kulcspárt biztonságos módon közvetlenül juttatja el az alanyhoz és adja át annak.

5.3.3 A szolgáltatói nyilvános kulcs közzététele

A Szolgáltató az MNB 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 MNB-nek a munkatársi aláíró és munkatársi titkosító tanúsítványok aláírásához használt magánkulcsát, ezeken kívül csak a tanúsítvány visszavonási lista (CRL) aláírására szabad felhasználnia.

5.4 A magánkulcsok védelme

5.4.1 A szolgáltatói kulcsokra vonatkozó általános szabályok

A 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 FIPS 140, Level 3 tanúsítvánnyal rendelkező kriptográfiai modulban kerülnek előállításra, tárolásra,
- a kulcsokat kizárólag az arra felhatalmazottak használhatják, a létrehozás céljának megfelelő funkcióra,
- az MNB rendszerei a láncolt hitelesítés szolgáltatás során használt kulcsai 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 az MNB – együttműködve a Szolgáltatóval, melyek ténylegesen felülírják a kulcsok összes előfordulását az összes olyan tárolóeszközön, melyen a kulcs példányai előfordulhattak,
- biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálását az MNB a Szolgáltató gondoskodása mellett 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 magánkulcsot nem lehet letétbe helyeztetni.

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

Az MNB sem a láncolt hitelesítés-szolgáltatás során használt magán aláíró kulcsot, sem a végfelhasználói aláíró és titkosító tanúsítványok magánkulcsait nem archiválja. A kulcspár gondozásának egyéb szempontjai

5.4.5 Egyéb kulcskezelési rendelkezések

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

5.4.6 Nyilvános kulcs archiválása

A regisztrációs alegység minden az MNB által 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).

A 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.

Az MNB az Aláíró magánkulcsát nem archiválja. (Lásd 5.4.4 pont.)

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

Az MNB az aláírás-létrehozó eszközhöz tartozó aktivizáló adatokat (PIN kód) biztonságos módon, az eszközöktől elkülönítetten, a szolgáltatást igénybe vevő személy közreműködésével állítja elő. A PIN kód beállítása az aláírás-létrehozó eszköz tanúsítója által előírt módon történik.

5.5.2 Az aktivizáló adatok védelme

Az MNB az aláírás-létrehozó eszközhöz tartozó aktivizáló adatokat (PIN kód) nem rögzíti, azt a szolgáltatást igénybe vevő személy adja meg.

5.5.3 Az aktivizáló adatok egyéb szempontjai

Az MNB az aláírás-létrehozó eszközhöz tartozó aktivizáló adatot (PIN kód) az aláírás-létrehozó eszköztől elkülönítve juttatja el az alanyhoz, amennyiben nem személyesen történik az aláírás-létrehozó eszköz átadása.

6 Tanúsítvány és visszavonási lista profilok

6.1 Tanúsítványprofilok

Az MNB az X.509 [7] ajánlason alapuló tanúsítványokat bocsát ki.

6.1.1 Munkatársi végfelhasználói aláíró tanúsítványok profiljainak állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyazonosító igazolványában szereplő írás módon, ékezhelyesen, UTF-8-ban kódolva
Organization	Szervezet(ek), azaz a másodlagos alany(ok) neve vagy üres
Organization Unit	Szervezeti egység(ek) neve(i) vagy üres
Country	Székhely (vagy opcionálisan lakóhely) szerinti ország kód, Magyarország esetén HU
Locality	Székhely (vagy opcionálisan lakóhely) szerinti város
Public Key	Tanúsítványtulajdonosának 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
Issuer	Kibocsátó megnevezése
Signature	sha1RSA

6.1.2 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	Szervezet(ek), azaz a másodlagos alany(ok) neve vagy üres
Organization Unit	Szervezeti egység(ek) neve(i) vagy üres
Country	Székhely (vagy opcionálisan lakóhely) szerinti ország kód, Magyarország esetén HU
Locality	Székhely (vagy opcionálisan lakóhely) szerinti város
Public Key	Tanúsítványtulajdonosának 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
Issuer	Kibocsátó megnevezése
Signature	sha1RSA

6.1.3 „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

Mező	Tartalom
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

6.2 Tanúsítvány visszavonási lista profilok

Az MNB az x.509 [9] megfelelő visszavonási listákat (CRL) bocsát ki.

Mező	Tartalom
Version	V2
Issuer	Kibocsátó megnevezése
Last update	Utolsó kibocsátás dátuma
Next update	Következő kibocsátás dátuma
Signature	Kibocsátó elektronikus aláírása
CRL entry	Az érvénytelenített tanúsítvány sorozatszáma, érvénytelenítés dátuma, időpontja

7 Üzleti és jogi tudnivalók

7.1 Bizalmasság, adatvédelem

7.1.1 Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése

Az MNB az általa kibocsátott tanúsítványok visszavonását és felfüggesztését a Tanúsítvány Visszavonási Listában teszi közzé, a tanúsítvány sorszámának és opcionálisan a visszavonás okának a jelölésével. Az MNB 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 hitelesítő egységek közös kötelezettségei

- a) Az alegységek eszközeit kizárólag az erre felhatalmazott, megfelelően kioktatott kezelőszemélyzet kezelheti,
- b) szabványos X509 tanúsítvány kibocsátása, megújítása, felfüggesztése, reaktiválása, visszavonása 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 tanúsítványkibocsátásra 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 az MNB-t,
- 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 lejártá után,
- d) amennyiben magánkulcsa kompromittálódásának lehetősége fennáll, a lehető leghamarabb tanúsítványának visszavonását, illetve felfüggesztését kérni a Szolgáltatótól.

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 az MNB-t,
- c) a regisztrált adatainak a kibocsátott tanúsítványának érvényességi ideje alatt történő megváltozásáról késedelem nélkül az MNB-t 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 MNB egyéb kötelezettségei

Az MNB általános kötelessége:

- a) a hitelesítő és regisztrációs egységek és a tanúsítványtár felügyelete, üzemeltetése;
- b) a szolgáltatásainak a hatályos jogi szabályozással, jelen Szolgáltatási Utasítással és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban való nyújtása;

- c) a magas színvonalú és biztonságos szolgáltatások folyamatos biztosítása;

7.2.4.1 A Szolgáltatói egységek közös kötelezettségei

Az MNB-hez tartozó szervezetek, regisztrációs és hitelesítő egységek köteleessége:

- a) a Közösség elektronikus hitelesítéssel kapcsolatos tevékenységeinek, alapelveinek meghatározása, ezek alapján a működést részletesen tárgyaló szabályzatok készítése és rendszeres felülvizsgálata,
- 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 megtétele,
- d) az infrastruktúra működtetéséért, javításáért és karbantartásáért felelős személyzet munkájának és szakmai felkészültségének folyamatos ellenőrzése, a szükséges változtatások megtétele,
- e) az előző pontokban előírt infrastruktúra folyamatos, biztonságos üzemeltetése, hibajavítása és az infrastruktúrába tartozó eszközökre előírt szabványos karbantartás elvégzése,
- 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 biztosítása, működtetése, karbantartása,
- 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 biztosítása,
- i) a logikai és fizikai védelmet megteremtő eszközök megfelelő üzemeltetése, az informatikai, fizikai, adminisztrációs és üzleti biztonság megteremtése és fenntartása.

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 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 az MNB Internetes oldalán (ld. 1.5 alfejezet),
- 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:

- Az MNB hitelesítés-szolgáltatási tevékenységért,
- Hogy az általában elvárható magatartás szerint a jelen és kapcsolódó szabályzatokat, utasításokat betartsa, betartassa, azok betartását ellenőrizze és előíja az esetlegesen Utasítástól 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 bármintemű 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 Az MNB felelőssége

Jelen és kapcsolódó Szabályzatoknak, Utasításoknak megfelelő tevékenység, különösen a Regisztráció és Hitelesítő Alegségre, valamint a tanúsítványkezelésre és regisztrációs tevékenységre vonatkozó előírások tekintetében.

7.3.4 Garancia

Szolgáltató garantálja a Község számára

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

7.4 Változtatási eljárás

7.4.1 Szolgáltatási Utasítás változtatási eljárás

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

A Szolgáltatási Utasítás módosított változatai mindig új verziószámmal kerülnek az MNB-nek átadásra. Az Utasítás a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente kétszer történik. Az Utasítás 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 Község 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 profildefiníciók 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)