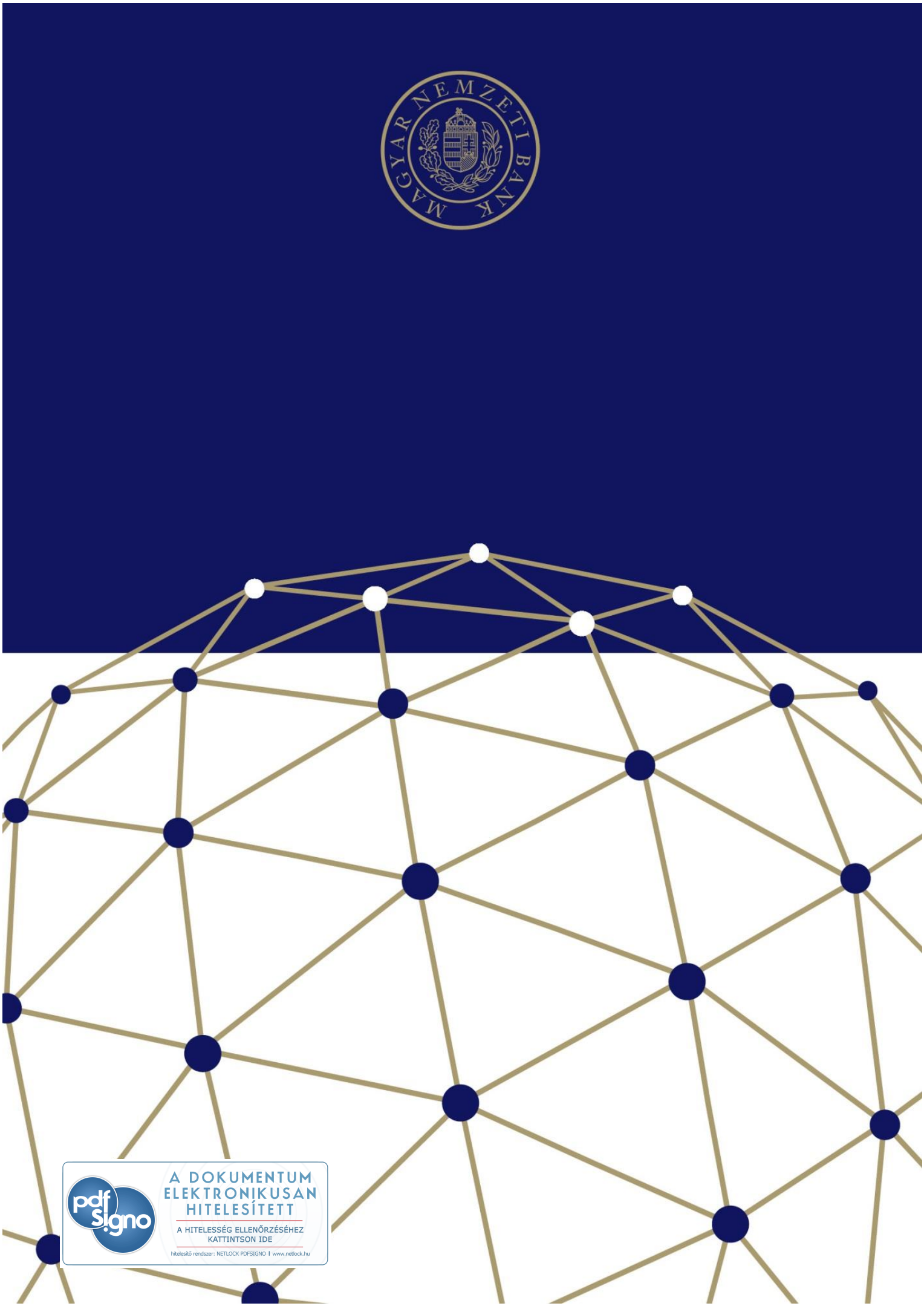

NETLOCK Kft. MNB-nél működő Kihelyezett Szolgáltató Alegységének Szolgáltatási Szabályzat Kiegészítése

(nem minősített hitelesítés-szolgáltatás)

Azonosító szám (OID):	**1.3.6.1.4.1.3555.1.13.20131210**
Azonosító szám kulcstároló eszközön kibocsátott tanúsítványokhoz (OID):	**1.3.6.1.4.1.3555.1.53. 20131210**
Jóváhagyás időpontja:	**2013.12.10.**
Hatály kezdőnapja:	**2013.12.15.**
Oldalak száma:	**42,** azaz **negyvenkettő**
Készítette:	**Lengyel Anett** szabályzat adminisztrátor
Jóváhagyta:	**dr. Szűcs Katalin** szabályzatvezető

NYILVÁNOS

Verziókezelés

Dátum	Módosította	Módosítás leírása
2007.05.23.	Dr. Szűcs Katalin	Dokumentum létrehozása
2007.06.14.	Dr. Nagy Zsolt	Pontosítások
2007.06.22.	Dr. Nagy Zsolt	Kommentek átvezetése
2007.06.26.	Dr. Nagy Zsolt	Regisztrációs rend módosítása
2007.06.26.	Dr. Nagy Zsolt	Véglegesítés
2011.05.10.	NetLock Szabályzat Elfogadó Egység (SzEE)	Szabályzat felülvizsgálata, aktualizálása
2012.07.11	NetLock Szabályzat Elfogadó Egység (SzEE)	Új OID kibocsátása az eszközszolgáltatás keretében kibocsátott tanúsítványok azonosításához; 1.1.5.2. és 1.1.5.5 frissítése [5] és [15] frissítése
2013.09.13	dr. Szentirmai László	A szabályozás „kihelyezett szolgáltató alegység” koncepció szerinti módosítása.
2013.12.10.	Lengyel Anett	NETLOCK székhely változása miatti módosítás

Tartalomjegyzék

1. BEVEZETÉS

1.1. Áttekintés

A szabályzat elkészítésének oka:

Jelen dokumentum a Szolgáltató Nem Minősített Szolgáltatási Szabályzatának a Kihelyezett Szolgáltató Alegység (lásd 1.3.1) tevékenységére vonatkozó, részletes eljárási és egyéb működési szabályokat tartalmazó Szolgáltatási Szabályzat Kiegészítése (a továbbiakban: Szolgáltatási Szabályzat Kiegészítés).

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

Jelen Szolgáltatási Szabályzatban nem szabályozott kérdésekben a Szolgáltató Nem Minősített Szolgáltatás Szolgáltatási Szabályzatában, illetve az Általános Szerződési Feltételeiben foglaltak az irányadók.

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

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

1.1.1. A Szabályzat hatálya

1.1.1.1. Tárgyi hatály

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

1.1.1.2. Időbeli hatály

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

1.1.1.3. Személyi hatály

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

1.1.2. A Szolgáltató

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

A Nemzeti Média- és Hírközlési Hatóság jogelődje, a Hírközlési Főfelügyelet 2001. október 27-én vette nyilvántartásba a Szolgáltatót nem minősített szolgáltatóként. HIF regisztrációs szám: FA 6133-5/2001.

A Hírközlési Főfelügyelet 2003. március 19-én vette nyilvántartásba a Szolgáltatót minősített szolgáltatóként. HIF regisztrációs szám: MH-1372-12/2003.

Egyéb tanúsítások:

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

Tekintettel arra, hogy Magyarországon az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] (továbbiakban: Törvény) 8/B. § szerinti önkéntes akkreditációs rendszer még nem működik, a Szolgáltató ilyen tanúsítással nem rendelkezik.

A Szolgáltató felelős a Magyar Nemzeti Bank (továbbiakban 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.

1.1.3. Szolgáltatások

Az MNB tanúsítvány-szolgáltatásban való közreműködést, és ezzel összefüggésben intelligens kártya megszemélyesítési 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

1.1.4. Szabványok és előírások

1.1.4.1. Szolgáltatási Szabályzat Kiegészítés

A Szabályzat az RFC 3647 [6] szabványa alapján készült. A Szolgáltatási Szabályzat Kiegészítés tartalmi vonatkozásokban eleget tesz a Törvény [1], az elektronikus aláírásokkal kapcsolatos

szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendelet [2] (továbbiakban: Rendelet) előírásainak és ajánlásainak, és felhasználja az ETSI 102 042 [10], valamint az x.509 [7] szabvány ajánlásait.

1.1.4.2. Lenyomatképző algoritmusok azonosítói

- RIPE-MD160 OID ::= { iso(1) identified-organization(3) TeleTrusT(36) algorithm(3) hashAlgorithm(2) 1 }
- SHA-224 OID ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) 4 }
- SHA-256 OID ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) 1 }
- SHA-384 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha384(2)}
- SHA-512 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha512(3)}
- Whirlpool OID ::= { iso(1) standard(0) hash-functions(10118) part3(3) algorithm(0) 55

A Szolgáltató a Kihelyezett Szolgáltató Alegység tevékenysége során az itt meghatározott algoritmusokat legfeljebb az Algoritmus Határozatban [14] megjelölt időpontig használja.

1.1.4.3. Kriptográfiai algoritmusok azonosítói

- RSA OID ::= { iso(1) member-body (2) USA (840) RSADSI (113549) PKCS (1) 1 }
- DSA OID ::= { iso(1) member-body(2) us(840) x9-57 (10040) x9cm(4) 1 }
- Ecdsa OID ::= { iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA1(1) }

A Szolgáltató az itt meghatározott algoritmusokat legfeljebb a Felügyelet Algoritmus Határozatában [14] megjelölt időpontig használja.

1.1.4.4. Tanúsítvány kiterjesztések azonosítói

- KeyUsage OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 15 }
- ExtendedKeyUsage 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 }

1.1.4.5. 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

1.1.5. Hitelesítés-szolgáltatás és tanúsítványfajták

A Kihelyezett Szolgáltató Alegység közreműködik az előzetes entitásazonosítás után az igénylők (későbbi alanyok) számára történő munkatársi aláíró és titkosító tanúsítványok kibocsátásában.

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

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

Fajta	Alany	Engedélyezett alkalmazások	Tiltott alkalmazások	Felelősség biztosítás összege	Joghatás
Munkatársi aláíró	Természetes személy szervezet vagy hatóság munkatársaként	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	A tanúsítványban szereplő érték, de maximálisan 5 millió forint	Írásbeliség (magánokirat)
Munkatársi titkosító	Természetes személy szervezet vagy hatóság munkatársaként	Titkosítási műveletek végrehajtása	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	A tanúsítványban szereplő érték, de maximálisan 5 millió forint	-

A Kihelyezett Szolgáltató Alegység szolgáltatásait igénybevevő Alanyok egyéni joga és felelőssége, hogy a fentiek közül egy adott célra milyen tanúsítványt alkalmaznak.

1.1.6. Tanúsítvány-kibocsátás

A Kihelyezett Szolgáltató Alegység (a továbbiakban: KSZA) a tanúsítványok kibocsátása mellett az aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatás (aláíró eszköz szolgáltatás) nyújtásában is közreműködik.

A KSZA a Szolgáltató aláíró eszköz-szolgáltatása keretében a hatályos jogszabályok és a jelen Szolgáltatási Szabályzat Kiegészítés rendelkezéseinek figyelembe vételével az alany számára kulcspárt generál az adott aláírás létrehozó eszközre.

Aláíró eszköz szolgáltatás biztosítása aláíró tanúsítványok kibocsátása során, mellyel összefüggésben a KSZA:

- 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 a Szolgáltatóval közreműködve, 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 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;

Titkosító tanúsítványok kibocsátása során a KSZA az alábbiak szerint jár el:

- a titkosító kulcsok generálása az intelligens kártyán történik;

1.2. Dokumentum neve és azonosítása

Jelen dokumentum:

- Teljes neve: NETLOCK Kft. MNB -nél működő Kihelyezett Szolgáltató Alegységének Szolgáltatási Szabályzat Kiegészítése (nem minősített hitelesítés-szolgáltatás)
- Rövid neve: Szolgáltatási Szabályzat Kiegészítés
- Verziószáma: a fedlapon található verziószám

1.3. PKI közösség

A kibocsátott tanúsítványok, aláírás-létrehozó eszközök alkalmazó közössége a Szolgáltató, az MNB Kihelyezett Szolgáltató Alegység, a tanúsítványok végfelhasználói és az Érintett Felek.

1.3.1. Kihelyezett Szolgáltató Alegység

A Szolgáltató az MNB.-nél Kihelyezett Szolgáltató Alegységet működtet (a továbbiakban: Kihelyezett Szolgáltató Alegység vagy KSZA), melyen keresztül a Törvény hatálya alá tartozó hitelesítés-szolgáltatási tevékenységet végez az MNB. munkatársainak közreműködésével.

1.3.1.1. Hitelesítő Alegység

A Hitelesítő Alegység a Kihelyezett Szolgáltató Alegységnek a végfelhasználói tanúsítványok létrehozásában közreműködő hitelesítő egysége (a továbbiakban: Hitelesítő Alegység), melynek munkájában részt vesznek az MNB Bankbiztonsági igazgatóságának illetve az Informatikai igazgatóságának munkatársai. A Hitelesítő Alegység az előírt eljárási rend szerint a hozzá tartozó Regisztrációs Alegységek kérelme alapján közreműködik a jóváhagyott aláíró és titkosító tanúsítványok kiadásában, publikálásában, visszavonásában. Emellett gondoskodik a Tanúsítvány Visszavonási Lista (a továbbiakban: CRL) publikálásáról is.

Név:	**MNB Nem Minősített Hitelesítő Egység**
Egység:	MNB Bankbiztonsági igazgatóság

Cím:	1054 Budapest, Szabadság tér 8-9..
Telefon:	(1) 428-2600 /3129
Internet cím:	www.mnb.hu
E-mail:	tanusitvanyok@mnb.hu

1.3.1.2. Regisztrációs Alegység

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

A Regisztrációs Alegység a tanúsítvány-kibocsátási folyamat során a felhasználói adatellenőrzés végzésében működik közre, amely tevékenységet a mindenkor hatályos jogszabályi követelményeknek - így különösen a Törvénynek [1], illetve az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek - megfelelően végzi.

1.3.1.3. Felhasználó Támogatási Csoport

Az MNB saját szervezetén belül Felhasználó Támogatási Csoportot működtet. A Felhasználó Támogatási Csoportot nem tagja a tanúsítványkezelő szervezetnek.

Név:	**MNB Felhasználó Támogatási Csoport**
Egység:	MNB Informatikai igazgatóság
Cím:	1054 Budapest, Szabadság tér 8-9..
Telefon:	(1) 428-2600/1585
Internet cím:	www.mnb.hu
E-mail:	helpdesk@mnb.hu

1.3.2. Végfelhasználók

A Szolgáltató a Kihelyezett Szolgáltató Alegység közreműködésével a jelen Szolgáltatási Szabályzat Kiegészítés alapján az MNB-vel munkaviszonyban álló természetes személyek részére munkatársi aláíró, illetve titkosító tanúsítvány bocsát ki.

A Szolgáltató az alanyokkal a KSZA Regisztrációs Alegységén keresztül tart kapcsolatot.

1.3.3. Érintett fél

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

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

1.4. Alkalmazhatóság

1.4.1. Engedélyezett alkalmazási lehetőségek

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

A Kihelyezett Szolgáltató Alegység Szolgáltató által felülhitelesített köztes kiadói tanúsítványa végfelhasználói tanúsítványok, illetve ezen tanúsítványok státuszinformációit tartalmazó CRL hitelesítésére használható fel.

1.4.2. Korlátozott alkalmazási lehetőségek

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

1.4.3. Tiltott alkalmazási lehetőségek

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

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

A Hitelesítő Alegység szolgáltatói aláíró tanúsítványok magánkulcs párjai csak végfelhasználói tanúsítványok, illetve a végfelhasználói tanúsítványok státuszára vonatkozó CRL aláírására használhatók, egyéb, az Eat. hatálya alá tartozó, az elektronikus aláírással kapcsolatos szolgáltatás, illetve egyéb hitelesítés-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.
Székhely:	1101 Budapest, Expo tér 5-7.
Telefon:	(40) 22 55 22
Fax:	(1) 345-2250
Internet cím:	www.netlock.hu
Központi e-mail:	info@netlock.hu
Panaszok bejelentésének helye:	info@netlock.hu
Illetékes fogyasztóvédelmi felügyelőség:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelősége 1052 Budapest, Városház u. 7.

1.5.2. 1.5.2. Jelen szabályzat szerinti Kihelyezett Szolgáltató Alegység adatai

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

1.5.3. Ügyfélszolgálat és ServiceDesk

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

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

A Kihelyezett Szolgáltató Alegység a Felhasználó Támogatási Csoporton keresztül fogadja a tanúsítvány-kibocsátással kapcsolatos kérdéseket, problémákat.

1.5.4. A Szolgáltatási Szabályzat Kiegészítéssel kapcsolatos kérdések

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

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

- **Alany:** A tanúsítvány alany (Subject) mezőjében megadott adatokkal meghatározott természetes személy, aki a tanúsítványban szereplő nyilvános kulcs párját jelentő magánkulcs felett rendelkezik.
- **Aláírás-ellenőrző adat**: Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.
- **Aláírás-létrehozó adat**: Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az Aláíró az elektronikus aláírás létrehozásához használ.
- **Aláírás-létrehozó eszköz**: Szoftver vagy hardver, melynek segítségével az Aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

- **Munkatársi tanúsítvány:** Olyan személyes tanúsítvány melyben az abban szereplő természetes személyt a másodlagos alany saját magához tartozónak ismeri el.
- **Alkalmazó Közösség**: A PKI rendszert alkalmazó, működtető entitások összessége.
- **Common Name (CN):** Az Alany tanúsítványban szereplő, szokásos megnevezéséből képzett neve.
- **Distinguished Name (DN):** A tanúsítványban szereplő, szokásos megnevezéséből, lakóhely vagy székhely szerinti város, ország megnevezéséből, valamint e-mail címéből képzett egyedi neve.
- **Elektronikus aláírás:** Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
- **Ellenőrzési lépések:** Az elektronikus aláírás ellenőrzésekor kötelezően végrehajtandó lépések, melyeket az Utasítás tartalmaz.
- **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 a Kihelyezett Szolgáltató Alegység a Szolgáltatónak a Törvény 6. § (1) bekezdésének c) pontja értelmében meghatározott, elektronikus aláíráshoz kapcsolódó aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatásában közreműködik, illetve a titkosító tanúsítványok kibocsátásához kapcsolódó kulcsgenerálási tevékenységet végez.
- **Hatóság:** Nemzeti Média és Hírközlési Hatóság
- **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.
- **Hash:** Ld. Lenyomat.
- **Késedelem nélküli cselekedet:** A mindenkori 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 visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.
- **Lenyomat**: Olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:
  - a képzett lenyomat egyértelműen származtatható az adott elektronikus dokumentumból,
  - a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés,

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

- **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, jelen Utasítás vonatkozásában a Magyar Nemzeti Bank.
- **Out-of-band:** Elektronikus információk szokásos használati környezeten kívül történő előállítási, 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 részt vevő technikai eszközök, egységek, ezen tevékenységeket hivatalosan felügyelő és meghatározó intézmények, a felhasználók által alkalmazott kriptográfiai eszközök és tevékenységek összessége.
- **Regisztrációs Adminisztrátor:** Azon közreműködő természetes személy, aki a Regisztrációs Alegység feladatait végzi el
- **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 tanúsítványkiadó infrastruktúra működtetéséhez szükséges szolgáltatói alegység kiadói tanúsítványát biztosítja.
- **Szolgáltatási Szabályzat Kiegészítés:** A Szolgáltató meghatározott felhasználói kör részére nyújtott szolgáltatáshoz kapcsolódó, az adott tevékenységre vonatkozó kiegészítő, illetve specifikus eljárási és működési szabályokat tartalmazó nyilvános dokumentum.
- **Tanúsítvány**: A Szolgáltató részéről a Kihelyezett Szolgáltató Alegység közreműködésével kibocsátott elektronikus igazolás, amely az aláírás-ellenőrző adatot illetve a titkosításhoz használt nyilvános kulcsot a tanúsítvány alanyához kapcsolja.
- **Tanúsítvány-szolgáltatás:** azon eljárás, melynek során a Szolgáltató a Kihelyezett Szolgáltatási Alegység közreműködésével a Szolgáltatási Szabályzat Kiegészítésben meghatározott eljárásban új aláíró és titkosító célú tanúsítványt bocsát ki a felhasználó részére. A tanúsítvány-szolgáltatáshoz kapcsolódóan a KSZA tanúsítványállapot-szolgáltatást is nyújt, melynek keretében fogadja a tanúsítvány-visszavonási kérelmeket és a Szolgáltatási Szabályzat Kiegészítésben meghatározott időközönként Tanúsítvány Visszavonási Listát bocsát ki.
- **Tanúsítványállapot-nyilvántartás**: A legközelebb kibocsátásra kerülő Tanúsítvány Visszavonási Lista tartalmához kapcsolt on-line lekérdezhető információk. Ezen információk joghatással nem bírnak.
- **Tanúsítványtár:** A végfelhasználói a Kihelyezett Szolgáltató Alegység által végfelhasználói tanúsítványok aláírására szolgáló tanúsítványok, 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 a Kihelyezett Szolgáltató Alegység közreműködésével bocsát ki.

- **Végfelhasználó:** Szerződéses partner, aki a Szolgáltató részéről a Kihelyezett Szolgáltató Alegység. közreműködésével kibocsátott végfelhasználói tanúsítvánnyal rendelkezik.
- **Végfelhasználói tanúsítvány:** A Szolgáltató részéről a Kihelyezett Szolgáltató Alegység közreműködésével kibocsátott olyan tanúsítvány, amelyet az alany kizárólag elektronikus aláírás előállítására illetve titkosításra használhat, de más tanúsítvány hitelesítésére nem. A végfelhasználó tanúsítvány szervezet mezőjében kizárólag az MNB Zrt. kerülhet feltüntetésre.

2. KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR

2.1. Az információ közzététele

2.1.1. Közzétételi és tájékoztatási elvek

2.1.1.1. A Szolgáltatási Szabályzat Kiegészítésben nem tárgyalt elemek

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

2.1.1.2. A Szolgáltatási Szabályzat Kiegészítés 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.

A Kihelyezett Szolgáltató Alegység az általa megválaszolni nem tudott megkereséseket a beérkezett észrevételek 3 munkanapon belül továbbítja a Szolgáltató felé.

2.2. Tanúsítványokkal kapcsolatos információk

2.2.1. Tanúsítványok közzététele

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

- saját szolgáltatói tanúsítványát közzéteszi tanúsítványtárában, illetve saját weboldalán;
- a Kihelyezett Szolgáltató Alegység végfelhasználói tanúsítványok aláírására használt szolgáltatói tanúsítványát közzéteszi a tanúsítványtárban, illetve saját weboldalán.

A Szolgáltató a Kihelyezett Szolgáltató Alegység közreműködésével kibocsátott végfelhasználói tanúsítványokat az alany hozzájárulása alapján közzéteszi az MNB tanúsítványtárában.

2.2.2. A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala

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

- Kihelyezett Szolgáltató Alegység végfelhasználói tanúsítványok aláírására használt szolgáltatói tanúsítványának állapotváltozását a saját tanúsítványtárában tünteti fel.

A Kihelyezett Szolgáltató Alegység a Hitelesítő Alegysége közreműködésével 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 a közreműködő Kihelyezett Szolgáltató Alegység által használt kiadói tanúsítványokat a kibocsátást követő 1 munkanapon belül teszi közzé,

– a Kihelyezett Szolgáltató Alegység a végfelhasználói tanúsítványokat a tanúsítványtárában az előállítást követően 1 munkanapon belül helyezi el tanúsítványtárában.

2.3.2. A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

A Kihelyezett Szolgáltató Alegység a kibocsátott végfelhasználói tanúsítványával kapcsolatos állapotinformációkat a 4.10.1 pontban tárgyalt gyakorisággal teszi közzé.

2.4. Hozzáférés ellenőrzések

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

A Szolgáltató által közölt információkat az MNB kizárólag csak a Szolgáltatóval történő előzetes egyeztetést követően egészítheti ki, törölheti vagy módosíthatja. Az MNB különböző védelmi mechanizmusokkal akadályozza meg az információk jogosulatlan módosítását.

2.4.1. Tanúsítványtárak

A Kihelyezett Szolgáltató Alegység 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), mely szabványos HTTP, illetve HTTPS protokollokkal érhető el az ott megvalósított lekérdezési műveletekkel. A tanúsítványtárban a Szolgáltató részéről a Kihelyezett Szolgáltató Alegység közreműködésével kibocsátott tanúsítványok és a visszavont tanúsítványok listái (nyilvános rész) találhatók.

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

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

3. AZONOSÍTÁS ÉS HITELESÍTÉS

3.1. Elnevezések

A nevek regisztrációjának szabályai valamennyi tanúsítványfajtára vonatkoznak.

3.1.1. Névtípusok

3.1.1.1. Általános szabályok

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

- a tanúsítványban az adatok speciális és vezérlő karakterek nélkül szerepelnek,
- a nevek egyes egységeit szóköz választja el,
- a nevek alapértelmezetten tanúsítványban az alábbiak szerint kerülnek feltüntetésre: a személyazonosság igazolására elfogadott hatósági igazolványban (lásd 3.2.3 pont) foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve CN és opcionálisan SN mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév), általában az UTF-8 kódolást használva; a nevek egyes egységeit szóköz választja el. Ezen szabályoktól a Szolgáltató Kihelyezett Szolgáltató Alegysége kivételesen, eltérhet, amennyiben a *Common Name*, *Organization* és *Organization Unit* mezőkre vonatkozó méretbeli korlátok nem teszik lehetővé az ilyen formában történő teljes adatrögzítést.
- a tanúsítványban kivételesen, egyedileg meghatározott esetben, a vonatkozó szabványok szerinti meghatározott maximális karakterszámot meghaladó elnevezések esetén rövidítés használata lehetséges,
- a tanúsítványban a „*CN”* mező nem üres,
- a „*Title*” mező opcionálisan tartalmazhatja az alany beosztását,
- 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.
- a tanúsítvány „*SubjectAltname*” mezőjében szereplő elektronikus levelezési cím struktúrája megfelel az RFC 822 előírásainak.

3.1.1.2. Speciális szabályok a CertificatePolicies mező használatára vonatkozóan

Ha a tanúsítvány tartalmaz CertificatePolicies mezőt, akkor amennyiben a tanúsítvány kriptográfiai kulcsa a Kihelyezett Szolgáltató Alegység közreműködésével eszközszolgáltatás keretében került kibocsátásra, akkor a tanúsítvány tartalmazza az 1.3.6.1.4.1.3555.1.52.ÉÉÉÉHHNN azonosítót, ahol az ÉÉÉÉHHNN jelen Szolgáltatási Szabályzat Kiegészítés mindenkor hatályos verziószámát, azon belül is az elfogadásának napját jelenti.

3.1.2. Álnév használata

3.1.2.1. Általános szabályok

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

3.1.3. Különböző elnevezési formák értelmezési szabályai

3.1.3.1. Kibocsátó azonosító

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

Az *Issuer* mező a tanúsítvány kibocsátójának székhely szerinti országkódját (*Country*), 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* vezetéknevű 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

A Kihelyezett Szolgáltató Alegység fenntartja magának a jogot a név kiosztással kapcsolatos mindennemű döntés tekintetében. A tanúsítvány alanynak 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 vesztette.

3.2. Kezdeti azonosítás

3.2.1. A magánkulcs birtoklásának bizonyítási módszere

Az aláíró tanúsítványhoz tartozó kulcspár generálását a Regisztrációs Adminisztrátor végzi az intelligens kártyán: a Kihelyezett Szolgáltató Alegység által alkalmazott ellenőrzési folyamatok biztosítják, hogy az aláíró tanúsítványhoz kapcsolódó kulcspár ténylegesen a chipkártyán került generálásra.

3.2.2. Szervezeti azonosság hitelesítése

A Kihelyezett Szolgáltató Alegység 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

A Kihelyezett Szolgáltató Alegység a természetes személy azonosításában az egyes tanúsítványfajták esetében a 4.2.2.1 pont alatt leírt módon vesz részt.

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.

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

3.3. Azonosítás tanúsítvány kulcscseréje esetén

Tanúsítvány kulcscseréjét a Kihelyezett Szolgáltató Alegység 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

A Kihelyezett Szolgáltató Alegység tanúsítvány visszavonási és felfüggesztési szolgáltatásokat egyaránt nyújt. Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait a 0 pont tárgyalja.

4. MŰKÖDÉSRE VONATKOZÓ KÖVETELMÉNYEK

4.1. Tanúsítványigénylés

4.1.1. Igénylés feltételei

A Kihelyezett Szolgáltató Alegységnél tanúsítványt igényelhet:

- a munkavállaló felügyeletét ellátó vezető 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 a Kihelyezett Szolgáltató Alegység feldolgozza a tanúsítványkérelmet a következőkben bemutatott eljárásrend szerint.

4.2.1. Általános regisztrációs szabályok

A Kihelyezett Szolgáltató Alegység által végzett regisztrációs eljárásra vonatkozó alapelvek:

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

4.2.1.1. Általános regisztrációs lépések

- az igénylő tanúsítványigénylési kérelmet juttat el a Kihelyezett Szolgáltató Alegységhez, melynek során elfogadja a tanúsítványkibocsátáshoz kapcsolódó feltételeket; személyesen bemutatja a személyazonosító dokumentumait az MNB regisztrációs munkatársai előtt,
- a Kihelyezett Szolgáltató Alegység fogadja a kérelmet, illetve ellenőrzi annak szabályosságát,
- a Kihelyezett Szolgáltató Alegység azonosítja az igénylő természetes személyt, és a szervezeti adatokat,

- a Regisztrációs Alegység elkészíti szolgáltatási szerződését, előkészíti a további regisztrációhoz szükséges dokumentumokat,
- a Regisztrációs Alegység - amennyiben a személy- és szervezetazonosítás rendben lezárult - átveszi az alannyal (és a másodlagos alannyal) kötött szolgáltatási szerződését, és összeveti az abban foglalt adatokat a személy- és szervezetazonosítás során ellenőrzött adatokkal,
- a Regisztrációs Alegység, ha a személy- és szervezetazonosítás rendben lezárult – amennyiben értelmezett - egy intelligens kártyát allokál a felhasználó részére, és azt összerendeli a felhasználóval
- a Regisztrációs Adminisztrátor az MNB tanúsítványmenedzsment rendszerében rögzíti a tanúsítványigényt
- a Hitelesítő Alegység munkatársa – ellenőrzést követően – az összes pozitív ellenőrzés lezárása esetén az MNB tanúsítványmenedzsment rendszerében jóváhagyja a tanúsítványigényt;
- a Regisztrációs Adminisztrátor az MNB tanúsítványmenedzsment rendszerében jóváhagyott igény alapján a Szolgáltató rendszerében elvégzi a kulcsgenerálást, összeállítja a kibocsátandó tanúsítványt és a Szolgáltató rendszeréből kiadja a tanúsítványt, összerendeli a kiadott tanúsítványt a kulccsal (feltölti a kártyára) és azt a végfelhasználó rendelkezésére bocsátja
- a Regisztrációs vagy a Hitelesítő Alegység munkatársa értesíti a felhasználót, hogy átvehető a kártya/hordozóeszköz;
- a kártya/hordozóeszköz átvételének feltételeként a felhasználó aláírja a felhasználói nyilatkozatot és a Regisztrációs Adminisztrátor ismerteti vele a Felhasználói tájékoztató elérhetőségét.
- a Kihelyezett Szolgáltató Alegység dokumentálja a regisztrációs lépéseket,

4.2.1.2. A regisztráció során nyilvántartásba vett adatok köre

- az igénylő természetes személyazonosító adatai, illetve az azokat igazoló dokumentumok egyedi azonosító adatai vagy azonosító számai,
- a munkavállaló munkaviszonyára vonatkozó, a tanúsítványigényléssel összefüggő adatok,
- a kártyahasználatról való tájékoztatás tudomásul vétele,
- az ügyfélnek a rá vonatkozó kötelezettségek elfogadása,
- a kérelmet elfogadó egység azonosítója,
- egyéb, a tanúsítványokhoz, valamint azok kibocsátásához kapcsolódó információ.

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

4.2.2. Regisztrációs eljárás

4.2.2.1. A regisztráció folyamata

Eljárási lépés	Tanúsítványfajta
	Munkatársi

Eljárási lépés	Tanúsítványfajta
	Munkatársi
1. Alany regisztrációja	Munkavállaló adatainak (név, születési idő, e-mail cím, törzsszám, személyazonosításra alkalmas dokumentum sorszáma) elektronikus regisztrációja melynek során a Regisztrációs alegység a személyazonosító okmány érvényességét és az abban foglalt adatok valódiságát közhiteles nyilvántartásban ellenőrzi. A regisztráció támogatására az alany az elektronikusan regisztrált személyazonosító adatait alátámasztó dokumentumok eredeti példányát 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, naprakészségének biztosítása a Regisztrációs Alegység feladata.
3. Tanúsítvány kérelem jóváhagyása	Végrehajtani jogosult: Hitelesítő Alegység
4. Kulcspár generálása eszközön és kérelem készítése	Végrehajtani jogosult: Regisztrációs Alegység.
5. Tanúsítvány előállítása	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.
8. Tanúsítványigénylő lap 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 (Tanúsítványigénylő lap)

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.

A Kihelyezett Szolgáltató Alegység közreműködésével 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

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

- benyújtották a kérelmét a tanúsítvány kibocsátónak,
- a természetes személy azonos a kérelemben szereplő alannyal,
- 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 aláíró tanúsítványok esetében 2 év, titkosító tanúsítványok esetében 2 év;
- 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 tanúsítvány kibocsátásában közreműködő, Kihelyezett Szolgáltató Alegység 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 a Kihelyezett Szolgáltató Alegység nem minősített kiadói kulcsával vannak aláírva,
- a tanúsítványok aláírása ellenőrizhető a tanúsítványban szereplő adatok és a Kihelyezett Szolgáltató Alegység 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, valódiságával vagy érvényességével kapcsolatban, valamint a személyazonosság ellenőrzése során egyéb okból kétség 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 a Kihelyezett Szolgáltató Alegység 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 a Kihelyezett Szolgáltató Alegység 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 legfeljebb 2 évig használhatók aláíró tanúsítványok esetében elektronikus aláírások készítésére, míg titkosító tanúsítványok esetében titkosításra. A nyilvános kulcs a kriptográfiai biztonságának periódusában használható aláírás ellenőrzésére, illetve titkosításra. 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 feltűntetett 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 tanúsítvány kibocsátáshoz kapcsolódó szabályzatokat,
- a tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályoknak és törvényi előírásoknak megfelelően használja,
- minden adat, amelyet a tanúsítvány kiadása céljából a Kihelyezett Szolgáltató Alegység részére 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 a Kihelyezett Szolgáltató Alegységet, illetve a Szolgáltató arra illetékes szervét,
- tisztában van azzal, hogy a magánkulcs védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége,
- tisztában van a titkosítási műveletek készítésére vonatkozó szabályokkal és követelményekkel,
- minden aláírás az elfogadott és érvényes (nem felfüggesztett, visszavont vagy lejárt) tanúsítvány alapján készül,
- minden egyes elektronikus aláírást, amely a tanúsítványban szereplő nyilvános kulcs párjával készült, a saját aláírásának ismeri el,
- jogosulatlan személy nem férhet hozzá magánkulcsához,
- ismeri az elektronikus aláírás és elektronikus titkosítás megfelelő használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,
- tudomása van arról, hogy a fokozott biztonságú elektronikus aláírással ellátott elektronikus okiratok az írásbeliség, vagyis az egyszerű magánokirat jogszabályi követelményeinek felelnek meg,
- az alany végfelhasználó, azaz nem hitelesítés-szolgáltató, és nem fogja a tanúsítványban megadott nyilvános kulcs párját újabb tanúsítványok vagy bármely más formátumú tanúsított

nyilvános kulcs, visszavonási lista, időbélyeg, OCSP válasz, viszontazonosítási válasz hitelesítésére és egyéb, hitelesítés-szolgáltatói funkciókra használni;

- amennyiben az alany beleegyezett a tanúsítvány nyilvánosságra hozatalába, felhatalmazza a Kihelyezett Szolgáltató Alegységet, illetve a Szolgáltatót a tanúsítvány közzétételével, és saját vagy más nyilvános tanúsítványgyűjtő helyeken történő elhelyezésével.

4.4.3. Tanúsítvány közzététele

A Kihelyezett Szolgáltató Alegység, illetve a Szolgáltató a kiadott tanúsítványt a Tanúsítványtárban közzéteszi.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. Az alanyok számára szóló előírások

Az aláíró tanúsítványok elektronikus aláírások 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:

- magánkulcsát és tanúsítványát csak a Kihelyezett Szolgáltató Alegységgel szerződésben rögzített korlátozásnak megfelelően használhatja,
- a megfelelő tanúsítvány lejárta után nem használhatja tovább magánkulcsát.

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

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

4.5.1.1. Elektronikus aláírás készítése

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

Amennyiben az alany nem körültekintően jár el, úgy az ebből származó kárért ő, valamint a tanúsítványban feltüntetésre került másodlagos alany (MNB) felel.

4.5.1.2. Aláíró tanúsítvány esetén a magánkulcs megőrzése

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

A Kihelyezett Szolgáltató Alegység az aláíró tanúsítványok magánkulcsait nem őrzi meg.

4.5.1.3. Érvényes elektronikus aláírás következményei

Az elektronikusan aláírt dokumentumok jogi hatással bírnak, amely a jogszabályokon kívül a felek – az Aláíró, az Érintett Fél és 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. Ajánlás az Érintett Felek számára

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 a Kihelyezett Szolgáltató Alegység nem minősített hitelesítés-szolgáltatása során nem támogatott.

4.6.2. Szolgáltatói tanúsítványok

A Kihelyezett Szolgáltató Alegység végfelhasználói tanúsítványok aláírására használt szolgáltatói tanúsítványát a Szolgáltató 5 év időtartamra bocsátja ki.

4.7. Kulcscsere

Kulcscserét a Kihelyezett Szolgáltató Alegység nem végez.

4.8. Tanúsítvány módosítása

Tanúsítvány módosítását a Kihelyezett Szolgáltató Alegység nem végez.

4.9. Tanúsítvány felfüggesztése és visszavonása

4.9.1. Általános rendelkezések

A Kihelyezett Szolgáltató Alegység a tanúsítványok érvényességének kezelésére közreműködik a tanúsítvány visszavonási szolgáltatások nyújtásában.

A felfüggesztett és visszavont tanúsítványok érvénytelenek. A felfüggesztett tanúsítvány azonban csak a felfüggesztés időtartama alatt érvénytelen. A felfüggesztés meghatározott időtartamra szól, annak letelte után a Kihelyezett Szolgáltató Alegység 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 kérelemnek a Kihelyezett Szolgáltató Alegységhez történő megérkezéséig az alany, illetve a másodlagos alany felelős a felmerülő károkért,
- a Kihelyezett Szolgáltató Alegység felel azért, hogy a beérkezett visszavonási kérelem jogosságának elbírálása 3 órán belül megtörténjen, és jogos kérelem esetén az elbírálást követő

egy órán belül a tanúsítvány állapotának változását közzétegye a tanúsítvány-visszavonási listán;

- 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 Kihelyezett Szolgáltató Alegység végfelhasználói tanúsítványok aláírására használt szolgáltatói tanúsítvány vagy a szolgáltatói magánkulcs kompromittálódása,
- a tanúsítvány alanyának kérelme,
- szervezeti egység vezető kérelme,
- a tanúsítvány használatának visszautasítása hibás tanúsítvány miatt,
- a Kihelyezett Szolgáltató Alegység vagy a Szolgáltató tudomására jutott tény, vagy megalapozott vélelem a regisztrációs adatok valótlanságáról,
- a tanúsítványban foglalt adatok megváltozása,
- a tanúsítvány felfüggesztési idejének lejárata,
- az alany és a másodlagos alany kötelezettségeinek be nem tartása,
- a Hatóság, 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, a munkavállaló felügyeletét ellátó vezető, a tanúsítvány alanya
Kihelyezett Szolgáltatói Alegység tanúsítványa	Kihelyezett Szolgáltató Alegység, Hatóság

A Szolgáltató az MNB haladéktalan értesítése mellett saját hatáskörben kezdeményezheti a Kihelyezett Szolgáltatói Alegység tanúsítványának visszavonását, amennyiben a rendelkezésre álló információk alapján:

- a tanúsítványkiadási eljárásra vonatkozó előírások súlyos megsértését észleli;
- a Kihelyezett Szolgáltatói Alegység tanúsítványa, illetve a nyújtott tanúsítványkiadási szolgáltatás kompromittálódott.

4.9.4. Visszavonási kérelemre vonatkozó eljárás

Végfelhasználói tanúsítvány visszavonása egy visszavonási kérelem a Kihelyezett Szolgáltató Alegység regisztrációs munkatársai számára történő, meghatározott formanyomtatvány kitöltésével kezdeményezhető. A visszavonási kérelem benyújtható:

- személyesen, a Regisztrációs Alegységnél,
- elektronikus formában a Bankbiztonsági Igénykezelő Rendszeren (BIR) keresztül,
- telefonon.

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

- személyesen,
- elektronikus formában a Bankbiztonsági Igénykezelő Rendszeren (BIR) keresztül,

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

- személyesen vagy telefonon

A visszavonási kérelemnek legalább a következő adatokat kell tartalmaznia:

- a tanúsítvány alanyának 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 a Kihelyezett Szolgáltató Alegység más kérelmeket megelőzően, soron kívül bírálja el.

A visszavonási eljárás során a Regisztrációs Alegység ellenőrzi a visszavonási kérelemben szereplő adatokat, a kérelmező személyazonosságát, a kérelem előterjesztésére való jogosultságot, a kérelemben foglalt indokok (ld. □ pont) valóságalapját, 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 a Kihelyezett Szolgáltató Alegység a tanúsítvány visszavonását megtagadhatja.

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

4.9.5. Visszavonási kérelemre vonatkozó türelmi idő

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

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

4.9.6. Visszavonásra vonatkozó egyéb szabályok

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

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

4.9.7. A felfüggesztés körülményei

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

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

4.9.8. Felfüggesztés kérelmezése

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

4.9.9. Felfüggesztési kérelemre vonatkozó eljárás

A felfüggesztési kérelem a visszavonási kérelemhez hasonlóan (lásd előzőekben) nyújtható be a Kihelyezett Szolgáltató Alegységhez, melyet az a felfüggesztési kérelmet a visszavonási kérelemmel megegyező módon dolgoz fel.

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 a Kihelyezett Szolgáltató Alegység 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 a Kihelyezett Szolgáltató Alegységnek a lehető leghamarabb intézkednie kell. A felfüggesztett állapot kezdő időpontja a felfüggesztési kérelem elfogadásától számítandó. Ha ez idő alatt a visszavonáshoz vezető körülmények gyanúja cáfolatot nem nyer, a Kihelyezett Szolgáltató Alegység 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)

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

[1]. a Kihelyezett Szolgáltató Alegység 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.

[2]. A CRL tartalmazhatja a tanúsítvány visszavonásának okát.

[3]. 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 bárminemű kár az Érintett Felet terheli.

[4]. A Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység 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 a Kihelyezett Szolgáltató Alegység nyilvántartásában való átvezetést követő 1 órán belül a kérelem szerint módosított visszavonási állapotot közzéteszi.

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

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

4.10.2. A CRL ellenőrzési követelményei az Érintett Fél számára

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

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

4.10.3. Valós idejű visszavonási állapot ellenőrzés elérhetősége

A Kihelyezett Szolgáltató Alegység valós idejű visszavonási állapot-szolgáltatásokat nem nyújt.

4.10.4. A visszavonási információ közzétételének egyéb formái

A visszavonási hirdetmények csak a Kihelyezett Szolgáltató Alegység tanúsítványtárában és annak biztonsági másolataiban érhetők el.

4.11. Kulcs letétbe helyezése és visszaállítása

A Kihelyezett Szolgáltató Alegység közreműködésével 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.

A Kihelyezett Szolgáltató Alegység 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

A Kihelyezett Szolgáltató Alegységnél üzemeltetett hitelesítés-szolgáltatói infrastruktúrájára vonatkozó fizikai-biztonsági követelmények külön dokumentumban találhatóak.

5.2. Az MNB Kihelyezett Szolgáltató Alegység leállítása

5.2.1. Szolgáltatás megszűntetése

Amennyiben a Kihelyezett Szolgáltató Alegység tevékenységét tervezetten megszűnteti vagy tartósan szüneteltetni, a tevékenység leállását megelőzően közreműködik a kibocsátott, és még vissza nem vont tanúsítványokat visszavonásában. Ezt követően 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, illetve visszavonására vonatkozó adatokat, valamint a tanúsítvány kibocsátásában való közreműködésre vonatkozó szabályzatokat és az aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását. Ezt követően a mentett állományokat a Kihelyezett Szolgáltató Alegység átadja a Szolgáltatónak, melyeket az átadásig a KSZA védi jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását. Az átadást követően ezen követelményeket a Szolgáltató biztosítja, illetve ezen túlmenően gondoskodik az adatoknak megőrzési időn belüli, jogosultak számára való hozzáférhetőségéről és értelmezhetőségéről.

Az adatátadást követően a Szolgáltató Az MNB Kihelyezett Szolgáltató Alegység magánkulcsait megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat a Szolgáltató visszavonja.

A Szolgáltató a tanúsítványok visszavonását követően a tevékenység befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is eleget tesz.

A Kihelyezett Szolgáltató Alegység új tanúsítványok kibocsátásában a megszűnés bejelentése után nem működik közre.

5.3. Kulcspár előállítás és telepítés

5.3.1. Kulcspár előállítás

		Végfelhasználói kulcspár	**Szolgáltatói alegység kulcspár**
Kulcsgenerá-lás és installáció	Kulcsgenerálás, tárolás	A kulcsgenerálást eszközszolgáltatás keretében aláírás-létrehozó eszközön az MNB végzi.	A Kihelyezett Szolgáltató Alegység által használt szolgáltatói kulcspárt a Szolgáltató generálja, hitelesíti és adja át a Kihelyezett Szolgáltató Alegység részére.
	Kulcs méretek	A végfelhasználók minimum 2048 bites RSA kulccsal rendelkeznek.	A Szolgáltató legalább 2048 bites RSA kulcsokat generál.
	Kulcs felhasználási célok	Aláírás létrehozása Titkosítás	- végfelhasználói tanúsítvány, CRL válaszok aláírása;
Magánkulcs védelme	Magánkulcs több-személyes kontrollja	A Kihelyezett Szolgáltató Alegység megfelelő technikai védelmet biztosít a magánkulcsok generálásakor és kezelésekor.	-

		Végfelhasználói kulcspár	Szolgáltatói alegység kulcspár
	Magánkulcs mentése	Az aláíró tanúsítvány magánkulcsot a Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység nem menti, titkosító tanúsítvány magánkulcsának mentésére kulcsletét szolgáltatást nem biztosít.	A Kihelyezett Szolgáltató Alegység által használt szolgáltatói magánkulcsait a Szolgáltató menti.
	Magánkulcs aktiválása	A magánkulcsok az aláíró eszköz átvételét követően használhatók, külön aktiválásra nincs szükség.	A Kihelyezett Szolgáltató Alegység által használt szolgáltatói magánkulcsainak 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 lejárta után .	A Kihelyezett Szolgáltató Alegység az általa használt szolgáltatói magánkulcsait és azok minden előfordulását az érvényesség lejáratakor a Szolgáltató megsemmisíti.
Egyéb tevékenységek	Nyilvános kulcs archiválása	A végfelhasználói és szolgáltatói nyilvános kulcsokat a Kihelyezett Szolgáltató Alegység az elektronikus aláírásról szóló törvényben meghatározott ideig archív formában 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.	

A Kihelyezett Szolgáltató Alegység által használt valamennyi szolgáltatói kulcspárt 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 Kihelyezett Szolgáltató Alegység által használt 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	ProtectServer Gold (hardware verzió: B2, firmware verzió: 2.03.00)	ProtectServer Gold (hardver verzió: B2, firmware verzió: 2.03.00) drivere,
Végfelhasználói eszköz	ActivIdentity 64K V2C	-

Szolgáltató folyamatosan figyelemmel kíséri az általa bejelentett eszközök tanúsításának érvényességét, illetve az alkalmazásukra vonatkozó esetleges újabb korlátozásokat. Ennek érdekében egyrészt meghozza a szükséges belső adminisztrációs lépéseket a tanúsítások érvényességének nyilvántartására, illetve az Európai Unión belül elvégzett tanúsítások érvényességei változásainak nyomon követésére, másrészt szorosabb kapcsolatot alakít ki a tanúsítással érintett eszközök importőreivel, hogy minél hamarabb értesülhessen a tanúsítások változásairól.

5.3.2. Magánkulcs eljuttatása az alanyhoz

A Kihelyezett Szolgáltató Alegység által használt valamennyi szolgáltatói kulcspárját a Szolgáltató generálja, védett kriptográfiai hardver modulban. A generált magánkulcsok mentést (klónozást) leszámítva, teljes életciklusuk alatt a kriptográfiai hardverekben marad, megsemmisítéséig azt sehová nem kell továbbítani. Amennyiben a Kihelyezett Szolgáltató Alegység által használt 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.

Az eszköz-szolgáltatás keretében generált a végfelhasználói kulcspárt, akkor az eszközt biztonságos módon, közvetlenül juttatja el az Alanyhoz és adja át annak. Amennyiben a kulcspár előállítása szoftveresen történik, azok Alanyhoz való eljuttatására megfelelő biztonsági intézkedések mellett kerül sor.

5.3.3. A Kihelyezett Szolgáltató Alegység által használt szolgáltatói nyilvános kulcs közzététele

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

5.3.4. Kulcsméretek

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 (statisztikailag 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)

A Kihelyezett Szolgáltató Alegységnek 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 Kihelyezett Szolgáltató Alegység szolgáltatói kulcsokra az alábbi szabályok vonatkoznak:

- a kulcsok létrehozása, tárolása, mentése, helyreállítása, megsemmisítése fizikailag biztonságos környezetben, a Szolgáltató által kettős személyi ellenőrzés mellett valósul meg,
- a hitelesítő egységek kulcsai FIPS 140, Level 3 tanúsítvánnyal rendelkező kriptográfiai modulban kerülnek előállításra, tárolásra,
- a kulcsokat kizárólag az arra felhatalmazottak használhatják, a létrehozás céljának megfelelő funkcióra,
- a Kihelyezett Szolgáltató Alegység rendszerei a hitelesítés szolgáltatásban való közreműködés során használt kulcsai használata előtt meggyőződnek arról, hogy az ezen kulcsokhoz kapcsolódó tanúsítványok érvényesek,
- a Kihelyezett Szolgáltató Alegység által használt szolgáltatói kulcsok frissítése out-of-band cserével történik,
- a Kihelyezett Szolgáltató Alegység által használt szolgáltatáshoz használt kulcsok megsemmisítése során olyan biztonságos törlési folyamatokat alkalmaz a Szolgáltató, melyek ténylegesen felülírják a kulcsok összes előfordulását az összes olyan tárolóeszközön, melyen a kulcs példányai előfordulhattak,
- biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálását 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 aláíró magánkulcsot nem lehet letétbe helyeztetni. Végfelhasználói titkosító tanúsítványok magánkulcsai esetén a Kihelyezett Szolgáltató Alegység kulcsletét szolgáltatást biztosíthat.

5.4.3. Magánkulcs mentése

A Szolgáltatónál az összes, a Kihelyezett Szolgáltató Alegység által a szolgáltatáshoz használt magánkulcs mentésre (illetve duplikálásra, klónozásra) kerülhet.

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

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

5.4.4. Magánkulcs archiválása

A Kihelyezett Szolgáltató Alegység sem a szolgáltatásban való közreműködés során használt kiadó magán aláíró kulcsát, sem a végfelhasználói aláró és titkosító tanúsítványok magánkulcsait nem archiválja.

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 Kihelyezett Szolgáltató Alegység minden, általa előállított tanúsítványt archivál, az alábbi időszakra:

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

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

A Kihelyezett Szolgáltató Alegység az Aláíró magánkulcsát nem archiválja. (Lásd 5.4.4 pont.)

5.4.7. A nyilvános és magánkulcsok használatának periódusa

A Kihelyezett Szolgáltató Alegység által nyújtott szolgáltatáshoz használt tanúsítványok és a bennük foglalt nyilvános kulcsok magán párjai:

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

A végfelhasználói aláíró kulcsokhoz tartozó tanúsítványoknak és a bennük foglalt nyilvános kulcsok magán párjainak 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 biztonságnak megfelelő voltáig tart.

5.5. Aktivizáló adatok

5.5.1. Aktivizáló adatok előállítása és telepítése

A Kihelyezett Szolgáltató Alegység 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

A Kihelyezett Szolgáltató Alegység 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] ajánláson alapuló tanúsítványokat bocsát ki.

6.1.1. Munkatársi végfelhasználói aláíró tanúsítványok profiljainak állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyazonosító igazolványában szereplő írásmódon, ékezethelyesen, 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 lakcím) szerinti országkód, Magyarország esetén HU
Locality	Székhely (vagy opcionálisan lakcím) szerinti város
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	(kritikus kiterjesztés) cA = FALSE
KeyUsage	(kritikus kiterjesztés) NonRepudiation, DigitalSignature
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	Kibocsátó megnevezése
Signature	sha256with RSAEnryption

6.1.2. Munkatársi végfelhasználói titkosító tanúsítványok profiljainak állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyazonosító igazolványában szereplő írásmódon, ékezethelyesen, 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 lakcím) szerinti országkód, Magyarország esetén HU
Locality	Székhely (vagy opcionálisan lakcím) szerinti város
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	(kritikus kiterjesztés) cA = FALSE
KeyUsage	(kritikus kiterjesztés) NonRepudiation, DigitalSignature

Mező	Tartalom
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	Kibocsátó megnevezése
Signature	sha256WithRSAEncryption

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
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	sha256WithRSAEncryption

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

A Kihelyezett Szolgáltató Alegység tanúsítványok visszavonását a Tanúsítvány Visszavonási Listában teszi közzé, a tanúsítvány sorszámának és opcionálisan a visszavonás okának a jelölésével, mely listában a tanúsítvány azonosítója szerint is keresési lehetőséget biztosít.

7.2. Jogok és kötelezettségek

7.2.1. A Hitelesítő Egység kötelezettségei

a) Az alegység eszközeit kizárólag az erre felhatalmazott, megfelelően kioktatott kezelőszemélyzet kezelheti,

b) szabványos X509 tanúsítvány kibocsátása, 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 Alegység 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, felfüggesztés, visszavonás) kezelése,

d) az ügyféladatok összegyűjtése, ellenőrzése és döntés meghozatala azok valódiságára vonatkozóan,

e) a nem nyilvános ügyféladatok 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 Szolgáltató Szabályzatért Felelős Egysége számára a szolgáltatás területére.

7.2.3. A végfelhasználó kötelezettségei

7.2.3.1. A végfelhasználó általános kötelessége:

a) megismerni és betartani a tanúsítvány kibocsátásra vonatkozó szabályzatot,

b) a feltételeknek és szabályzatoknak megfelelően eljárni a szolgáltatások felhasználása során, beleértve a tanúsítvány és magánkulcs igénylését és alkalmazását,

c) hozzájárulni a szolgáltatás biztonságához, elsősorban korrekt adatszolgáltatáson keresztül, valamint a nyilvános kulcsú infrastruktúra tudatos és felelősségteljes alkalmazásával,

d) az aláírással vagy az így aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt – külön jogszabályban, illetve a szabályzatokban meghatározott – rendellenességről tájékoztatni a Szolgáltatót vagy a Kihelyezett Szolgáltató Alegységet,

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 lejárta 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 bemutatásával alátámasztani,

b) az azonosításához szükséges személyazonosító adatokról és mindezek változásáról tájékoztatni a Kihelyezett Szolgáltató Alegységet,

c) a regisztrált adatainak a kibocsátott tanúsítványának érvényességi ideje alatt történő megváltozásáról késedelem nélkül a Kihelyezett Szolgáltató Alegységet 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 Kihelyezett Szolgáltató Alegység 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

A Szolgáltatóhoz tartozó szervezetek, regisztrációs és hitelesítő alegységek kötelessége:

a) a Közösség elektronikus hitelesítéssel kapcsolatos tevékenységeinek, alapelveinek meghatározása, ezek alapján a működést részletesen tárgyaló szabályzatok 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 részben nyilvános, a visszavonási információk tekintetében minden Érintett Fél számára elérhető módon való üzemeltetése az MNB internetes oldalán (http://cdp.mnb.hu) (ld. 1.5 alfejezet),

b) bizalmas információkat, nem nyilvános adatokat a Tanúsítványtárban meg nem jeleníteni,

c) a Tanúsítványtár a visszavonási információkat tartalmazó részét 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 általában elvárható magatartás szerint a jelen és kapcsolódó szabályzatok, utasítások betartásáért, ennek ellenőrzéséért, és az esetlegesen a Szolgáltatási Szabályzat Kiegészítéstől eltérő működés megszüntetéséért.

Szolgáltató ezen felül felel a Kihelyezett Szolgáltató Alegység hitelesítés-szolgáltatás során közreműködő tevékenységéért.

Szolgáltató a Törvényben és kapcsolódó rendeletiben meghatározott feltételrendszerű és mértékű felelősségbiztosítással rendelkezik. A Szolgáltató felelőssége és összesített felelőssége korlátozott a kötelezettségeinek megszegéséből eredő bárminemű 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 Általános Szerződési Feltételeiben 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 előírásainak, utasításainak 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

Az MNB felel a Kihelyezett Szolgáltató Alegység keretében jelen Szolgáltatási Szabályzat Kiegészítésben rögzített szabályok betartásáért, különös tekintettel a Regisztrációs és a Hitelesítő Alegységekre vonatkozó tanúsítványkezelési és regisztrációs előírásaira.

7.3.4. Garancia

Szolgáltató garantálja a Közösség 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 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 Közösség felől a szabályzatok módosítása tekintetében érkező igények feldolgozására, illetve a szabályzatok módosításának kidolgozására és javaslat formában történő előterjesztésére kijelölt személy.

7.4.2.2. A Szabályzatért Felelős Egység működése

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

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

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

7.5. Hivatkozott jogszabályok, szabványok és egyéb dokumentumok

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

[1]. az elektronikus aláírásról szóló 2001. évi XXXV. törvény

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

[3]. ISO 3166 English Country Names and Code Elements

[4]. FIPS PUB 140-2 (2001. május): "Kriptográfiai modulok biztonsági követelményei"

[5]. RFC 5280 (korábban RFC 3280) 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]. az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról szóló 9/2005. IHM rendelet

[9]. RFC 2560 Online Certificate Status Protocol (OCSP)

[10]. ETSI 102 042 v1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates

[11]. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

[12]. Az Európai Parlament és a Tanács 1999/93/EK számú irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről

[13]. 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)

[14]. A Nemzeti Média- és Hírközlési Hatóság EF/26838-8/2011 számú határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről