Központi Elszámolóház és Értéktár (Budapest) Zrt.

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

(nem minősített hitelesítés-szolgáltatás)

Azonosító szám (OID):	1.3.6.1.4.1.3555.1.51.20131210
Azonosító szám kulcstároló eszközön kibocsátott tanúsítványokhoz (OID)	1.3.6.1.4.1.3555.1.52.20131210
Jóváhagyás időpontja:	**2013.12.10.**
Hatály kezdőnapja:	**2013.12.15.**
Oldalak száma:	**50,** azaz **ötven**
Készítette:	**Lengyel Anett**, szabályzat adminisztrátor
Jóváhagyta:	**dr. Szűcs Katalin** szabályzatvezető

© COPYRIGHT, NETLOCK KFT. – MINDEN JOG FENNTARTVA

NYILVÁNOS

A DOKUMENTUM ELEKTRONIKUSAN HITELESÍTETT
A HITELESSÉG ELLENŐRZÉSÉHEZ KATTINTSON IDE
hitelesítő rendszer: NETLOCK PDFSIGNO I www.netlock.hu

Verzió -szám	Dátum	Módosította	Módosítás leírása
0.1	2011.12.06.	dr. Szűcs Katalin	Dokumentum létrehozása
0.2	2012.02.07.	dr. Szűcs Katalin	Dokumentum módosítása
0.3	2012.02.22.	dr. Szűcs Katalin	Személyes egyeztetésnek megfelelően a dokumentum pontosítása
0.4	2012.03.28.	dr. Tamás Gyöngyvér	Dokumentum pontosítása
0.5	2012.04.12.	dr. Szűcs Katalin	Dokumentum pontosítása
0.6	2012.10.16.	dr. Szűcs Katalin	Dokumentum véglegesítése a személyes egyeztetésen elhangzottaknak megfelelően
0.7	2013.03.12.	dr. Szentirmai László	NMHH észrevételek teljesítésének átvezetése
0.8	2013.12.10.	Lengyel Anett	NETLOCK székhely változása miatti módosítás
0.9	2014.01.02.	Lengyel Anett	Dokumentum pontosítása

1 TARTALOM

1 Bevezetés ... 7

1.1. Áttekintés ... 7

1.1.1 A Szolgáltatási Szabályzat Kiegészítés hatálya ... 7

1.1.2 A Szolgáltató ... 7

1.1.3 Szolgáltatások ... 8

1.1.4 Szabványok és előírások ... 8

1.1.5 Hitelesítés-szolgáltatás és tanúsítványfajták ... 10

1.1.6 Tanúsítvány-kibocsátás ... 10

1.2. Dokumentum neve és azonosítása ... 11

1.3. PKI közösség ... 11

1.3.1. Kihelyezett Szolgáltató Alegység ... 11

1.3.1.1. Hitelesítő Alegység ... 11

1.3.1.2. Regisztrációs Alegység ... 12

1.3.1.3. ServiceDesk ... 12

1.3.2. Végfelhasználók ... 12

1.3.3. Érintett fél ... 12

1.4. Alkalmazhatóság ... 12

1.4.1. Engedélyezett alkalmazási lehetőségek ... 12

1.4.2. Korlátozott alkalmazási lehetőségek ... 13

1.4.3. Tiltott alkalmazási lehetőségek ... 13

1.5. Kapcsolattartás ... 13

1.5.1. A Szolgáltató adatai ... 13

1.5.2. Jelen szabályzat szerinti Kihelyezett Szolgáltató Alegység adatai ... 14

1.5.3. Ügyfélszolgálat és ServiceDesk ... 14

1.5.4. A Szolgáltatási Szabályzat Kiegészítéssel kapcsolatos kérdések ... 14

1.6. Fogalmak és rövidítések ... 14

2 Közzététel és tanúsítványtár ... 18

2.1 Az információ közzététele ... 18

2.1.1 Közzétételi és tájékoztatási elvek ... 18

2.2 Tanúsítványokkal kapcsolatos információk ... 18

2.2.1 Tanúsítványok közzététele ... 18

2.2.2 A tanúsítvány visszavonásának nyilvánosságra hozatala ... 18

2.3 A közzététel gyakorisága ... 19

2.3.1 Tanúsítványok nyilvánosságra hozatalának gyakorisága ... 19

2.3.2 A tanúsítvány visszavonásának nyilvánosságra hozatali gyakorisága. 19
2.4 Hozzáférés ellenőrzések ... 19
2.4.1 Tanúsítványtárak ... 19
3 Azonosítás és hitelesítés ... 21
3.1 Elnevezések ... 21
3.1.1 Névtípusok ... 21
3.1.2 Álnév használata ... 22
3.1.3 Különböző elnevezési formák értelmezési szabályai ... 22
3.1.4 A nevek egyedisége ... 22
3.2 Kezdeti azonosítás ... 23
3.2.1 A magánkulcs birtoklásának bizonyítási módszere ... 23
3.2.2 Szervezeti azonosság hitelesítése ... 23
3.2.3 Személyazonosság hitelesítése ... 23
3.3 Azonosítás tanúsítvány kulcscseréje esetén ... 24
3.4 Visszavonási kérelem ... 24
4 Működésre vonatkozó követelmények ... 25
4.1 Tanúsítványigénylés ... 25
4.1.1 Igénylés feltételei ... 25
4.2 Tanúsítványkérelem feldolgozása ... 25
4.2.1 Általános regisztrációs szabályok ... 25
4.2.2 Regisztrációs eljárás ... 26
4.2.3 Szolgáltatási szerződés ... 27
4.2.4 A tanúsítványkérelmek jóváhagyásának követelményei ... 27
4.2.5 A tanúsítványok tartalma ... 27
4.2.6 A tanúsítványok jellemzői ... 28
4.2.7 Az igénylő (alany) tájékoztatása a kibocsátást megelőzően ... 28
4.2.8 Tanúsítványkérelmek elutasítása ... 28
4.2.9 A tanúsítványokra vonatkozó további rendelkezések ... 29
4.3 A tanúsítványok kibocsátása és hozzáférhetővé tétele ... 29
4.3.1 A tanúsítvány kibocsátásának időpontja ... 29
4.3.2 A tanúsítvány érvényessége ... 29
4.4 Tanúsítványelfogadás ... 29
4.4.1 A tanúsítvány elfogadása ... 29
4.4.2 A tanúsítványigénylő nyilatkozata ... 29
4.4.3 Tanúsítvány közzététele ... 30
4.5 A kulcspár és a tanúsítvány használata ... 30
4.5.1 Az alanyok számára szóló előírások ... 30
4.5.2 Ajánlás az Érintett Felek számára ... 31

4.6 Tanúsítvány megújítása ... 32
4.6.1 Végfelhasználói tanúsítványok ... 32
4.6.2 A Kihelyezett Szolgáltató Alegység végfelhasználói tanúsítványok aláírására használt szolgáltatói tanúsítványa ... 32
4.7 Kulcscsere ... 32
4.8 Tanúsítvány módosítása ... 32
4.9 Tanúsítvány felfüggesztése és visszavonása ... 32
4.9.1 Általános rendelkezések ... 32
4.9.2 A visszavonás körülményei ... 32
4.9.3 Visszavonás kérelmezése ... 33
4.9.4 Visszavonási kérelemre vonatkozó eljárás ... 33
4.9.5 Visszavonási kérelemre vonatkozó türelmi idő ... 34
4.9.6 Visszavonásra vonatkozó egyéb szabályok ... 34
4.9.7 Kulcskompromittálódás esetére vonatkozó speciális követelmények ... 35
4.10 Tanúsítvány-állapot információk közzététele ... 35
4.10.1 Tanúsítvány Visszavonási Lista (CRL) ... 35
4.10.2 A CRL ellenőrzési követelményei az Érintett Fél számára ... 35
4.10.3 Valós idejű visszavonási állapot ellenőrzés elérhetősége ... 36
4.10.4 A visszavonási információ közzétételének egyéb formái ... 36
4.11 Kulcs letétbe helyezése és visszaállítása ... 36
5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések ... 37
5.1 Fizikai óvintézkedések ... 37
5.2 A KELER Kihelyezett Szolgáltató Alegység leállítása ... 37
5.2.1 Szolgáltatás megszűntetése ... 37
5.3 Kulcspár előállítás és telepítés ... 37
5.3.1 Kulcspár előállítás ... 37
5.3.2 Magánkulcs eljuttatása az alanyhoz ... 39
5.3.3 A Kihelyezett Szolgáltató Alegység által használt szolgáltatói nyilvános kulcs közzététele ... 39
5.3.4 Kulcsméretek ... 39
5.3.5 A nyilvános kulcs paraméterek generálása és megfelelőségük ellenőrzése ... 39
5.3.6 A kulcs használat célja (az X.509 v3 kulcshasználati mező tartalmának megfelelően) ... 39
5.4 A magánkulcsok védelme ... 39
5.4.1 A szolgáltatói kulcsokra vonatkozó általános szabályok ... 39
5.4.2 Magánkulcs letétbe helyezése ... 40
5.4.3 Magánkulcs mentése ... 40
5.4.4 Magánkulcs archiválása ... 40

5.4.5 Egyéb kulcskezelési rendelkezések ... 41
5.4.6 Nyilvános kulcs archiválása ... 41
5.4.7 A nyilvános és magánkulcsok használatának periódusa ... 41
5.4.8 Aktivizáló adatok előállítása és telepítése ... 41
5.4.9 Az aktivizáló adatok védelme ... 41
6 .Tanúsítvány és visszavonási lista profilok ... 42
6.1 Tanúsítványprofilok ... 42
6.1.1 Végfelhasználói aláíró tanúsítványok állandó elemei ... 42
6.1.2 Végfelhasználói autentikációs tanúsítványok állandó elemei ... 42
6.1.3 Végfelhasználói titkosító tanúsítványok állandó elemei ... 43
6.1.4 Szolgáltatói tanúsítvány profilja ... 43
6.2 Tanúsítvány visszavonási lista profilok ... 44
7 Üzleti és jogi tudnivalók ... 45
7.1 Bizalmasság, adatvédelem ... 45
7.1.1 Tanúsítvány visszavonására vonatkozó információ felfedése ... 45
7.2 Jogok és kötelezettségek ... 45
7.2.1 A Hitelesítő Alegység kötelezettségei ... 45
7.2.2 A Regisztrációs Alegység kötelezettségei ... 45
7.2.3 A végfelhasználó kötelezettségei ... 46
7.2.4 A KELER kötelezettségei ... 46
7.3 Felelősség ... 48
7.3.1 A Szolgáltató általános felelőssége ... 48
7.3.2 A végfelhasználó (Alany) felelőssége ... 48
7.3.3 A KELER felelőssége ... 49
7.3.4 Garancia ... 49
7.4 Változtatási eljárás ... 49
7.4.1 Szolgáltatási Szabályzat Kiegészítés változtatási eljárás ... 49
7.4.2 Szabályzatért Felelős Egység ... 49
7.5 Hivatkozott jogszabályok, szabványok és egyéb dokumentumok ... 50
7.6 Hatályon kívül kerülő szabályozó iratok ... 50

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, autentikációs, valamint titkosító tanúsítványok (a továbbiakban: aláíró tanúsítvány, authentikációs 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.

Jelen dokumentumban a KELER csoport alatt a KELER Zrt. és a KELER KSZF Zrt. cégeket és azok hivatkozásait együttesen kell értelmezni (a továbbiakban: KELER).

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

1.1.1 A Szolgáltatási Szabályzat Kiegészítés hatálya

1.1.1.1 Tárgyi hatály

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

1.1.1.2 Időbeli hatály

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

1.1.1.3 Személyi hatály

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

1.1.2 A Szolgáltató

A jelen Szolgáltatási Szabályzat Kiegészítésben a Szolgáltató 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.

Minősített archiválás szolgáltatóként a Nemzeti Média- és Hírközlési Hatóság 2010. szeptember 15-én vette nyilvántartásba Szolgáltatót HL/18188-4/2010 regisztrációs szám alatt..

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

1.1.3 Szolgáltatások

A Kihelyezett Szolgáltató Alegység tevékenysége a következő fő elemekből áll:

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

1.1.4 Szabványok és előírások

1.1.4.1 Szolgáltatási Szabályzat Kiegészítés

A Szabályzat az RFC 3647 [6] szabványa alapján készült. A 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, autentikációs 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 munkatársaként	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	A tanúsítványban szereplő érték, de maximálisan 500.000 forint	Írásbeliség (magán-okirat)
Autenti-kációs	Természetes személy munkatársaként	Természetes személy multifaktoros azonosítása elektronikus környezetben	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	A tanúsítványban szereplő érték	-
Munkatársi titkosító	Természetes személy munkatársaként	Titkosítási műveletek végrehajtása	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	A tanúsítványban szereplő érték	-

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 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:

- megszemélyesíti az aláírás létrehozó eszközt;
- a kulcsok generálását és az Aláíróhoz 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;
- biztosítja, hogy aláíró eszköz és az azt aktivizáló adatát az aláírás-létrehozó eszköztől elkülönítve jusson el az Aláíróhoz;
- gondoskodik róla, hogy a tevékenysége során közreműködők ne élhessenek vissza az aláírás-létrehozó eszközzel a következőképpen: PIN számok, portál kódok megismerése, magánkulcsok, tanúsítványok használata;
- az aláírás-létrehozó eszköz előkészítése és továbbítása során alkalmazza a biztonsági eljárásokat.

Titkosító tanúsítványok kibocsátása során a KSZA a fentiektől az alábbiakban tér el:

- a titkosító kulcsok generálása szoftveresen történik a kulcspár és a hozzá tartozó tanúsítvány a visszaállítás érdekében, és utólag feltöltésre kerülhet az intelligens kártyára;
- a titkosító tanúsítvány magánkulcsai megőrzésére a Kihelyezett Szolgáltató Alegység kulcsletét-szolgáltatást biztosít.

1.2. Dokumentum neve és azonosítása

Jelen dokumentum:

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

1.3. PKI közösség

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

1.3.1. Kihelyezett Szolgáltató Alegység

A Szolgáltató a KELER Zrt.-nél Kihelyezett Szolgáltató Alegységet működtet (a továbbiakban: Kihelyezett Szolgáltató Alegység vagy KSZA), melyen keresztül részben a Törvény hatálya alá tartozó hitelesítés-szolgáltatási tevékenységet végez a KELER Zrt. 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 résztvesznek a KELER Zrt. Biztonságmenedzsmentjének munkatársai. A Hitelesítő Alegység az előírt eljárási rend szerint a hozzá tartozó Regisztrációs Alegységek kérelme alapján közreműködik a jóváhagyott aláíró, authentikációs és a titkosító tanúsítványok kiadásában, publikálásában, visszavonásában. Emellett gondoskodik a Tanúsítvány Visszavonási Lista (a továbbiakban: CRL) publikálásáról is.

Név:	**KELER Nem Minősített Hitelesítő Alegység**
Egység:	KELER Zrt.
Cím:	1075 Budapest, Asbóth u. 9-11.
Telefon:	+36 (1) 483-6100
Internet cím:	www.keler.hu
E-mail:	halozat.tamogatas@keler.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 adatellenőrzést 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. ServiceDesk

A Kihelyezett Szolgáltató Alegység saját szervezetén belül ServiceDesket működtet. A ServiceDesk nem tagja a tanúsítványkezelő szervezetnek.

1.3.2. Végfelhasználók

A Szolgáltató a Kihelyezett Szolgáltató Alegység közreműködésével a jelen Szolgáltatási Szabályzat Kiegészítés alapján a KELER Zrt. vagy KELER KSZF Zrt. alkalmazásában álló természetes személyek részére munkatársi aláíró, autentikációs, 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, authentikációs és titkosítási képesség ellenőrzése céljából a Kihelyezett Szolgáltató Alegység közreműködésével kibocsátott tanúsítványhoz fordul, illetőleg ezen tanúsítvány érvényességének ellenőrzéséhez a Szolgáltató vagy a Kihelyezett Szolgáltató Alegység által karbantartott nyilvántartásokat ellenőrzi.

A Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység 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 még1.1.6 pont)

A kibocsátott munkatársi autentikációs végfelhasználói tanúsítványok magánkulcs párjai kizárólag authentikációra megtételére, míg a tanúsítványokban található nyilvános kulcsok az authentikáció 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. (Lásd még 1.1.6 pont)

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

1.4.2. Korlátozott alkalmazási lehetőségek

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

1.4.3. Tiltott alkalmazási lehetőségek

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

A végfelhasználói tanúsítványok magánkulcs 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 listák 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) 700-1101
Internet cím:	www.netlock.hu
Központi e-mail:	info@netlock.hu
Panaszok bejelentésének helye:	info@netlock.hu
Illetékes fogyasztóvédelmi felügyelőség:	**Budapest Főváros Kormányhivatal, Fogyasztóvédelmi Felügyelőség** Cím: 1052 Budapest, V. ker. Városház u. 7. Levelezési cím: 1364 Budapest, Pf. 144. Telefon: +36 1 328-0185

Név:	NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
	Fax: +36 1 411-0116 E-mail: fogyved_kmf_budapest@nfh.hu

1.5.2. Jelen szabályzat szerinti Kihelyezett Szolgáltató Alegység adatai

Név:	Kihelyezett Szolgáltató Alegység
Egység:	KELER Zrt.
Székhely:	1075 Budapest, Asbóth u. 9-11.
Telefon:	+36 (1) 483-6100
Fax:	+36 (1) 342-3539
Internet cím:	www.keler.hu
Központi e-mail:	halozat.tamogatas@keler.hu

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 ServiceDesk-jén 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

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

- **Munkatársi tanúsítvány:** Olyan személyes tanúsítvány melyben az abban szereplő természetes személyt a másodlagos alany saját magához tartozónak ismeri el.
- **Alkalmazó Közösség**: A PKI rendszert alkalmazó, működtető entitások összessége.
- **Common Name (CN):** Az Alany tanúsítványban szereplő, szokásos megnevezéséből képzett neve.
- **Distinguished Name (DN):** A tanúsítványban szereplő, szokásos megnevezéséből, lakóhely vagy székhely szerinti város, ország megnevezéséből, valamint e-mail címéből képzett egyedi neve.
- **Elektronikus aláírás:** Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
- **Ellenőrzési lépések:** Az elektronikus aláírás ellenőrzésekor kötelezően végrehajtandó lépések, melyeket a Szolgáltatási Szabályzat Kiegészítés tartalmaz.
- **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 ezen túlmenően 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.
- **Kulcscsere**: az a folyamat, amelynek során egy megújított tanúsítvány kibocsátására úgy kerül sor, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai közül csak a nyilvános kulcs kerül lecserélésre.
- **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 a 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.
- **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, valamint az időbélyegzésben részt vevő technikai eszközök, egységek, ezen tevékenységeket hivatalosan felügyelő és meghatározó intézmények, a felhasználók által alkalmazott kriptográfiai eszközök és tevékenységek összessége.
- **Regisztrációs 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 Szolgáltató jelen és kapcsolódó szabályzatok kialakításáért, elfogadásáért és adminisztrációjáért felelős szolgáltatói egysége.
- **Szolgáltatási Szabályzat**: A [1] Törvény 2. § (20) alapján a Szolgáltató hitelesítési tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum.
- **Szolgáltatási Szabályzat Kiegészítés:** A 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, a titkosításhoz, illetve az autentikációhoz használt nyilvános kulcsot a tanúsítvány alanyához kapcsolja.
- **Tanúsítvány módosítása**: az a folyamat, amelynek során a tanúsítvány kibocsátója úgy bocsát ki egy módosított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai – a nyilvános kulcs kivételével – változnak, és a tanúsítvány az új adatokkal, valamint a régi nyilvános kulccsal kerül kiadásra
- **Tanúsítvány-szolgáltatás**: azon eljárás, melynek során a Szolgáltató a Kihelyezett Szolgáltatási Alegység közreműködésével a Szolgáltatási Szabályzat Kiegészítésben meghatározott eljárásban új aláíró, titkosító és autentikációs 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.
- **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 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, autentikációra, illetve titkosításra használhat, de más tanúsítvány hitelesítésére nem. A végfelhasználó tanúsítvány szervezet mezőjében kizárólag az KELER Zrt.és a KELER KSZF 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

A Szolgáltató a Szolgáltatási Szabályzatot Kiegészítést weboldalán (www.netlock.hu) keresztül hozza nyilvánosságra, valamint az Alanyok számára a KELER belső intranet weblapján is elérhető.

2.1.1.3 Észrevételek kezelése

A Szolgáltatási Szabályzat Kiegészítéssel kapcsolatos észrevételeket Szolgáltató az info@netlock.hu címen, valamint a KELER Kihelyezett Szolgáltató Alegység a halozat.tamogatas@keler.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 és a másodlagos alany hozzájárulása alapján közzéteszi nyilvános tanúsítványtárában.

2.2.2 A tanúsítvány visszavonásának 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 visszavonási listán, illetve a tanúsítványtárában hozza nyilvánosságra,
- végfelhasználói tanúsítvány visszavonását Kihelyezett Szolgáltató Alegység akkor is nyilvánosságra hozza, ha a tanúsítvány közzétételéhez az alany (igénylő) nem járult hozzá.

2.3 A közzététel gyakorisága

2.3.1 Tanúsítványok nyilvánosságra hozatalának gyakorisága

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

- Szolgáltató a közreműködő Kihelyezett Szolgáltató Alegység szolgáltatói tanúsítványait a kibocsátást követő 10 munkanapon belül teszi közzé,
- a Kihelyezett Szolgáltató Alegység a kibocsátott végfelhasználói tanúsítványokat az alany és a másodlagos alany hozzájárulása alapján közzéteszi nyilvános tanúsítványtárában.

2.3.2 A tanúsítvány visszavonásának 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 a KELER kizárólag csak a Szolgáltatóval történő előzetes egyeztetést követően egészítheti ki, törölheti vagy módosíthatja. A KELER különböző védelmi mechanizmusokkal akadályozza meg az információkhoz való jogosulatlan hozzáféréseket.

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 Intranet 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 Kihelyezett Szolgáltató Alegység a tanúsítványtár elérhetőségét folyamatosan (az év minden napján, 0–24h) biztosítja a karbantartáshoz szükséges idők kivételével (folyamatosan elérhető szolgáltatás). A KELER a tervezett karbantartásokat lehetőleg 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 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 tanúsítvány SN mezőjének feltüntetése nem kötelező.
- a „*Title*" mezőben az Alany beosztása szerepelhet,
- a „*State*" mezőben az ország, a megye, vagy megyei jogú város neve kerülhet feltüntetésre,
- az „*Organization*" mezőben kizárólag a KELER Zrt. és a KELER KSZF Zrt. valamelyike szerepelhet,míg az „*Organization-unit*" mezőben a másodlagos Alany szervezeti egysége kerül feltüntetésre,
- a „*Locality*" mezőben a másodlagos Alany székhelyeként Budapest kerül feltüntetésre,
- a KELER 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 által 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. Az aláíró tanúsítvány magánkulcs párja a jogszabályok szerint fokozott biztonságú elektronikus aláírások létrehozására alkalmas.

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

3.1.3.2 Alanyazonosító

3.1.3.2.1 Általános szabályok

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

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

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

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

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

3.1.4 A nevek egyedisége

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

3.1.4.1 Eljárások a nevekre vonatkozó vitás kérdések megoldására

A 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, illetve autentikációs tanúsítványhoz tartozó kulcspár generálását a Regisztrációs Adminisztrátor végzi szoftveresen vagy az intelligens kártyára.

Aláíró, illetve autentikációs tanúsítványok eszköz szolgáltatása esetén a Kihelyezett Szolgáltató Alegység által alkalmazott ellenőrzési folyamatok biztosítják, hogy az aláíró tanúsítványhoz kapcsolódó kulcspár a chipkártyán került generálásra. Szoftveresen történő kulcsgenerálás esetén a Kihelyezett Szolgáltató Alegység megfelelő biztosítékokat és garanciát alkalmaz arra vonatkozóan, hogy az Alanynak történő átadást követően az aláíró magánkulcsok visszaállíthatatlan módon törlésre kerülnek, illetve azzal kapcsolatban semmilyen visszaélés nem történik.

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

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

3.2.2 Szervezeti azonosság hitelesítése

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

A szervezet *Organization* mezőben minden esetben a KELER Zrt. vagy a KELER KSZF Zrt. kerül feltüntetésre. A tanúsítványba kerülő szervezetek adatai a Humánpolitikai Rendszerben minden esetben megtalálhatóak.

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, a Szolgáltató 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 3.2.3 pont).

3.4 Visszavonási kérelem

A Kihelyezett Szolgáltató Alegység a tanúsítvány visszavonási szolgáltatásban közreműködik. 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:

- természetes személy saját részére, feltüntetve a tanúsítványban, hogy meghatározott szervezethez, jelen esetben a KELER Zrt-hez vagy a KELER KSZF Zrt-hez tartozik,
- a munkavállaló szervezeti egységének vezetője a munkavállaló részére, feltüntetve a tanúsítványban, hogy az meghatározott szervezethez, jelen esetben a KELER Zrt-hez vagy a KELER KSZF Zrt-hez tartozik,

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

4.2 Tanúsítványkérelem feldolgozása

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

A tanúsítványigénylés feltételeinek teljesülése esetén 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 igénylőlap kitöltésével és elektronikus úton való megküldésével (e-mail) tanúsítványigénylési kérelmet juttat el a Kihelyezett Szolgáltató Alegységhez, melynek során elfogadja a tanúsítvány kibocsátáshoz kapcsolódó feltételeket;
- a Kihelyezett Szolgáltató Alegység fogadja a kérelmet, illetve ellenőrzi annak szabályosságát,
- az igénylő személyesen bemutatja a személyazonosító dokumentumait a regisztrációs munkatársai előtt
- a Regisztrációs 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, ha a személy- és szervezetazonosítás rendben lezárult – amennyiben értelmezett - egy intelligens kártyát allokál a felhasználó részére, és azt összerendeli a felhasználóval
- a Regisztrációs Adminisztrátor a Szolgáltató rendszerében elvégzi a kulcsgenerálást;
- a Hitelesítő Alegység munkatársa – ellenőrzést követően – a Szolgáltató rendszeréből kiadja a tanúsítványt;
- a Regisztrációs vagy a Hitelesítő Alegység munkatársa a felhasználót és a ServiceDesket is értesíti, 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 Regisztrációs Alegység összerendeli a kiadott tanúsítványt a kulccsal (feltölti az eszközre, illetőleg szoftveres tanúsítvány esetén PKCS#12-es formátumban a hordozó eszközre tölti és a végfelhasználó rendelkezésére bocsátja).

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,
- az ügyfélnek a rá vonatkozó kötelezettségekkel elfogadása,
- egyéb, a tanúsítványokhoz, valamint azok kibocsátáshoz 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
Alany regisztrációja	Tanúsítványigénylés indítása Service Desk-re írt e-mailen keresztül történik. Személyazonosság ellenőrzésekor személyazonosításra alkalmas dokumentum, azaz személyi igazolvány vagy útlevél vagy „új” típusú (bankkártya méretű) jogosítvány és a lakcímkártya fogadható el.
Másodlagos alany regisztrációja (kapcsolt regisztráció)	Szervezet adatainak, jelen esetben a KELER Zrt.-nek vagy KELER KSZF Zrt.-nek (név, telefon, fax, e-mail cím) elektronikus regisztrációja. A szervezet adatait a Humánpolitikai Rendszer tartalmazza.
Alany személyazonosságának ellenőrzése	Az Alany személyazonosságát a Hordozóeszköz/Aláírás létrehozó eszköz átadását megelőzően a Regisztrációs Alegység munkatársa személyazonosító fényképes igazolvány segítségével ellenőrzi.
Kulcspár generálása kérelem készítése	Végrehajtani jogosult: Regisztrációs Alegység Az aláíró, illetve authentikációs tanúsítvány magánkulcsának generálása szoftveresen vagy az eszközön történik, míg titkosító tanúsítvány magánkulcsának generálására szoftveresen kerül sor és utólagosan kerülhet feltöltésre az intelligens kártyára.
Tanúsítvány előállítása	Végrehajtani jogosult: Hitelesítő Alegység

Eljárási lépés	Tanúsítványfajta
	Munkatársi
Tanúsítvány hordozó eszközre/Aláírás létrehozó eszközre való letöltése	Regisztrációs/Hitelesítő Alegység
Tanúsítvány tanúsítványtárban való közzététele	Végrehajtani jogosult: Regisztrációs Alegység, az Alany hozzájárulása esetén.
Dokumentáció archiválása	Végrehajtani jogosult: Regisztrációs Alegység.
Hordozóeszköz/Aláírás létrehozó eszköz átadása az aláírónak	A személyazonosság ellenőrzését követően a Regisztrációs/Hitelesítő Egység munkatársa a személyazonosság ellenőrzését követően adja át az intelligens kártyát vagy egyéb, a kulcspár és a tanúsítvány biztonságos tárolására alkalmas eszközt.

4.2.3 Szolgáltatási szerződés

A természetes személy és a magánkulcs összetartozásának dokumentálására, illetve a kötelező tájékoztatásra a Kihelyezett Szolgáltató Alegység szolgáltatási szerződést alkalmaz. A szerződés feltételeit a KELER szabályzatai, jelen Szolgáltatási Szabályzat Kiegészítés, illetve az aláíró elfogadó nyilatkozata tartalmazza, melyek együttese jelenti a szolgáltatási szerződést. 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 (amennyiben lehetséges),
- a kiadandó tanúsítvány „*Subject”* mezője (alanyazonosító),
- az alany azonosításához szükséges egyéb adatok,
- a korlátozások, elfogadások,
- a Szolgáltató által adatlapon közölt adatok.

Az elfogadó nyilatkozatot az igénylő természetes személy írja alá.

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

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 (akinek nevében az igénylő eljár) azonos a kérelemben szereplő alannyal,
- a kérelemben szereplő adatok ellenőrizhetők és pontosak.

4.2.5 A tanúsítványok tartalma

A végfelhasználói tanúsítványok tartalmazzák az alábbiakat:

- a tanúsítvány azonosító kódját,
- a KELER Zrt. vagy KELER KSZF Zrt. megnevezését, ország-azonosítóját,
- a tanúsítvány érvényességi idejének kezdetét és végét (amely nem lehet az érvényesség kezdete időpontnál korábbi); az érvényesség időtartama nem haladja meg a 2 évet,
- az Alany nevét,

- azt az aláírás-ellenőrző adatot (nyilvános kulcs), amely az Alany által birtokolt aláírást készítő adat párjának (magánkulcs) felel meg,
- a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
- az adott tanúsítvány kibocsátásában közreműködő, Kihelyezett Szolgáltató Alegység elektronikus aláírását.

4.2.6 A tanúsítványok jellemzői

A Szolgáltató által kibocsátott tanúsítványok megfelelnek a következő követelményeknek:

- a tanúsítványazonosító a kibocsátóra nézve egyedi,
- a tanúsítványban foglalt megkülönböztetett név (DN, Distinguished Name) egyedi,
- a kiadott tanúsítványokhoz tartozó kulcsok egyediek,
- a tanúsítványok a Kihelyezett Szolgáltató Alegység nem minősített szolgáltatói 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

A Kihelyezett Szolgáltató Alegység 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 lehetősége,
- a szolgáltatói nyilvános kulcs, valamint annak elérhetősége,
- a panaszok benyújtására, a jogviták rendezésére vonatkozó szabályok.

4.2.8 Tanúsítványkérelmek elutasítása

A Kihelyezett Szolgáltató Alegység elutasítja a tanúsítványkérelmeket, amennyiben

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

Az elutasított kérelmekről az igénylő értesítést kap, melyben szerepel az elutasítás indoka, 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 előállítása 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 Alegység a 4.2.2 pontban leírt módon feldolgozza a kérelmet, illetve előállítja a tanúsítványt. A kész tanúsítvány a Tanúsítványtárba kerül.

4.3.1 A tanúsítvány kibocsátásának időpontja

A tanúsítvány kibocsátásának időpontja az az időpont, amikor a Kihelyezetett Szolgáltató Alegység az aláírt tanúsítványt elérhetővé teszi a tanúsítványtárban (lásd 2.4.1 pontban).

4.3.2 A tanúsítvány érvényessége

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

4.4 Tanúsítványelfogadás

4.4.1 A tanúsítvány elfogadása

A magánkulcs használatba vétele előtt az alanynak, illetve a másodlagos alanynak kötelessége ellenőrizni a tanúsítványban 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/kulcstárló eszközt 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 amely a tanúsítványban szerepel a valóságnak megfelel, és azok átadása önkéntes volt,
- a tanúsítványban szereplő minden adat a tudomásával és egyetértésével került a tanúsítványba,

- a tanúsítvány érvényességét befolyásoló tényekről, valamint az igénylés során megadott személyes adatok megváltozása esetén haladéktalanul értesíti a 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,
- tisztában van az autentikációs műveletek végzésére vonatkozó szabályokkal és követelményekkel,
- minden aláírás az elfogadott és érvényes (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, autentikációs 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 tanúsítvány előfizetője, illetve az alany és másodlagos alany hozzájárulása alapján közzéteszi.

4.5 A kulcspár és a tanúsítvány használata

4.5.1 Az alanyok számára szóló előírások

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

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

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

a) magánkulcsát és tanúsítványát csak a Kihelyezett Szolgáltató Alegységgel szerződésben rögzített korlátozásnak megfelelően használhatja,

b) a megfelelő tanúsítvány lejárta után nem használhatja tovább magánkulcsát.

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

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

Az autentikációs tanúsítványok adott rendszerbe való belépést tesznek lehetővé.

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 (KELER Zrt. vagy KELER KSZF Zrt.) 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 a Szolgáltató nyilatkozatain és szerződésein alapul, melyeket a felek a következő módon fogadnak el:

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

4.5.2 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.

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 A Kihelyezett Szolgáltató Alegység végfelhasználói tanúsítványok aláírására használt szolgáltatói tanúsítványa

A Kihelyezett Szolgáltató Alegység végfelhasználói tanúsítványok aláírására használt szolgáltatói tanúsítványát a Szolgáltató 7 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 Kihelyezett Szolgáltató Alegység tanúsítvány felfüggesztési szolgáltatást nem végez.

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

A visszavont és visszavonandó 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,
- az alany és a másodlagos alany kötelezettségeinek be nem tartása,
- a Felügyelet, bíróság vagy más hatóság erre vonatkozó, jogerős és végrehajtható határozata,
- a szolgáltatási szerződés megszűnése,
- a hitelesítési szolgáltatói tevékenység megszűnése,
- visszavonást jogszabály teszi kötelezővé.

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

4.9.3 Visszavonás kérelmezése

A visszavonást az alábbi entitások kérelmezhetik:

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

A Szolgáltató a KELER Zrt. 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 számára történő benyújtásával kezdeményezhető. A visszavonási kérelem benyújtható:

Üzemidőben (7:00-22:00):

- személyesen, Regisztrációs Egységnél és/vagy a ServiceDesk-nél,
- a KELER-nek küldött e-mailben
- a Szolgáltatónak küldött e-mailben.

Üzemidőn kívül (22:00-7:00):

- Portaszolgálat telefonon +36 (1) 483-6100 (Soron kívüli tanúsítvány visszavonó).

Végfelhasználói tanúsítvány visszavonása egy visszavonási kérelem az MSCA webes felületén és a ServiceDesk-en keresztül vagy írásban kezdeményezhető. Kivételt képez ez alól a kulcskompromittálódás, a kulcshordozó eszköz elvesztése, eltulajdonítása képez, ekkor a tanúsítvány visszavonás minél gyorsabb végrehajtása érdekében a felhasználó telefonon keresztül is

kezdeményezheti a tanúsítvány visszavonását üzemidőben a megjelölt helyeket, illetve üzemidőn kívül a soron kívüli tanúsítvány visszavonónál.

Soron kívüli visszavonási kérelem esetében az alábbi információkat kell a felhasználótól bekérni:

- a tanúsítvány sorszáma vagy egyedi neve,
- visszavonást kérő megnevezése, beosztása, elérhetősége;
- visszavonandó kártya adatai (amennyiben értelmezett);
- a visszavonást kérő kapcsolata a tanúsítvány alanyával,
- a visszavonás oka,
- személyazonosításhoz használt személyazonosító dokumentum megnevezése és száma.

A visszavonásra irányuló kérelmeket a Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység más kérelmeket megelőzően, soron kívül bírálja el.

A visszavonási eljárás során a Regisztrációs Alegysége ellenőrzi a visszavonási kérelemben szereplő adatokat, a kérelmező személyazonosságát, a kérelem előterjesztésére való jogosultságot, a kérelemben foglalt indokok (lásd 4.9.2 pont) valóságalapját, illetve visszavonásra való alkalmasságát. A kérelemre vonatkozó fenti adatokat a Kihelyezett Szolgáltató Alegység 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 az Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység további mérlegelés nélkül intézkedik a tanúsítvány visszavonása érdekében: a visszavonási kérelmek azonnal végrehajtásra kerülnek, és 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 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 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, így az joghatással sem rendelkezik.. Visszavont autentikációs tanúsítvánnyal autentikáció nem végezhető. Visszavont titkosító tanúsítvány továbbiakban titkosító műveletek végzésére nem használható.

4.9.7 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.

- 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.
- A CRL tartalmazhatja a tanúsítvány visszavonásának okát.
- A CRL ellenőrzése ajánlott minden Érintett Fél részére az elektronikus aláírás ellenőrzési eljárásának részeként, az elvárható gondosság követelményének megfelelően. A CRL-en szereplő, azaz érvénytelen tanúsítvány elfogadásából keletkező bárminemű kár az Érintett Felet terheli.
- 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 tanúsítványok kerülnek feltüntetésre, amelyek érvényességi ideje még nem járt le.

A visszavonási lista kibocsátása a Kihelyezett Szolgáltató Alegységnek 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.

Tanúsítvány visszavonása 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 24 óra.

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 hirdetményeket elsősorban a Kihelyezett Szolgáltató Alegység saját oldalán teszi közzé, de a Szolgáltató oldalán és annak biztonsági másolataiban is elérhetők.

4.11 Kulcs letétbe helyezése és visszaállítása

A Kihelyezett Szolgáltató Alegység a közreműködésével kibocsátott végfelhasználói aláíró, illetve autentikációs 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 közreműködésével kibocsátott végfelhasználói titkosító tanúsítványok esetén magánkulcs letéti szolgáltatást biztosít. Titkosító tanúsítvány magánkulcsának visszaállítását kizárólag a felhasználó kezdeményezheti. A magánkulcsok tárolása és visszaállítása kiemelt védelmi szabályok szerint történik.

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

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

A Regisztrációs Alegység 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 A KELER Kihelyezett Szolgáltató Alegység leállítása

5.2.1 Szolgáltatás megszűntetése

Amennyiben a Kihelyezett Szolgáltató Alegység tevékenységét tervezetten megszűnteti vagy tartósan szünetelteteti, 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 a KELER 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	KSZA Szolgáltatói kulcspár
Kulcs-generálás és installáció	Kulcsgenerálás, tárolás	A kulcsgenerálást a Regisztrációs Alegység munkatársa végzi.	A Kihelyezett Szolgáltató Alegység által használt szolgáltatói kulcspárt a Szolgáltató generálja, hitelesíti és adja át a közreműködő Kihelyezett Szolgáltató Alegység részére.

		Végfelhasználói kulcspár	KSZA Szolgáltatói kulcspár
	Kulcs méretek	A végfelhasználóknak legalább 2048 bites kulccsal kell rendelkezniük.	A Kihelyezett Szolgáltató Alegység által használt szolgáltatói kulcspárok hossza megfelel a kibocsátáskor hatályos iránymutatást tartalmazó felügyeleti határozatban előírt hosszúságnak.
	Kulcs felhasználási célok	Aláíró kulcspár generálása Titkosítás Autentikáció	Végfelhasználói tanúsítvány, CRL válaszok aláírása;
Magánkulcs védelme	Magánkulcs több-személyes kontrollja	A Kihelyezett Szolgáltató Alegység megfelelő technikai védelmet biztosít a magánkulcsok generálásakor és kezelésekor.	-
	Magánkulcs mentése	Az aláíró, illetve autentikációs tanúsítvány magánkulcsot a Szolgáltató, illetve KELER Kihelyezett Szolgáltató Alegység nem ment, titkosító tanúsítvány magánkulcsának mentésére kulcsletét szolgáltatást biztosít.	A Kihelyezett Szolgáltató Alegység által használt szolgáltatói magánkulcsait a Szolgáltató menti.
	Magánkulcs aktiválása	A magánkulcsok 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 a Kihelyezett Szolgáltató Alegység, illetve a Szolgáltató, illetve az elektronikus aláírásról szóló törvényben meghatározott ideig archív formában megőrzi (lásd 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 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 Kihelyezett Szolgáltató Egység	ProtectServer Gold (hardware verzió: B2, firmware verzió: 2.03.00)	ProtectServer Gold (hardver verzió: B2, firmware verzió: 2.03.00) drivere,
Végfelhasználói eszköz	ID-One Cosmo v7.0.1-n kártya IAS ECC 1.0.1 alkalmazással (applet version 1121), NXP P5CC081 V1A (Standard) komponenssel	Oberthur-höz tartozó driverek

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 nyomonkövetésére, 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 Alegység a munkatársi aláíró, munkatársi authentikációs és munkatársi titkosító tanúsítványok aláírásához használt szolgáltatói magánkulcsát ezeken kívül csak a tanúsítvány visszavonási lista (CRL) aláírására használja fel.

5.4 A magánkulcsok védelme

5.4.1 A szolgáltatói kulcsokra vonatkozó általános szabályok

A Kihelyezett Szolgáltató Alegység szolgáltatói kulcsokra az alábbi szabályok vonatkoznak:

- a kulcsok létrehozása, tárolása, mentése, helyreállítása, megsemmisítése fizikailag biztosított területen környezetben, a Szolgáltató vagy a Kihelyezett Szolgáltató Alegység által kettős személyi ellenőrzés mellett valósul meg,
- a hitelesítő egységek kulcsai tanúsítvánnyal rendelkező kriptográfiai modulban kerülnek előállításra, tárolásra,
- a kulcsokat kizárólag az arra felhatalmazottak használhatják, a létrehozás céljának megfelelő funkcióra,
- a Kihelyezett Szolgáltató Alegységnek rendszerei a szolgáltatás során használt kulcsainak 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 a Szolgáltató végzi és gondoskodik a kulcs védelméről,
- élettartamuk végén a kulcsokat a Szolgáltató olyan módon semmisíti meg, hogy az aláíró kulcsok ne legyenek visszanyerhetőek,

5.4.2 Magánkulcs letétbe helyezése

A szolgáltatói és végfelhasználói aláíró és autentikációs 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, Kihelyezett Szolgáltató Alegységek 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 a végfelhasználói aláró és autentikációs tanúsítványok magánkulcsait nem, a végfelhasználói titkosító tanúsítványok magánkulcsát archiválja.

5.4.5 Egyéb kulcskezelési rendelkezések

A Szolgáltató, illetve a Kihelyezett Szolgáltató Alegység 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 Szolgáltató az aláíró, illetve az autentikációs tanúsítvány magánkulcsát nem archiválja.

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: 7 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.

5.4.8 Aktivizáló adatok előállítása és telepítése

Az intelligens kártyához tartozó tanúsítványt az, aktivizáló adatot a végfelhasználó adja meg. . A szoftveren tárolt tanúsítvány esetében a hordozó eszközre mentett PKCS#12-es formátumot aktiváló PIN-kódot szintén a végfelhasználó adja meg.

5.4.9 Az aktivizáló adatok védelme

A Kihelyezett Szolgáltató Alegység sem az eszközszolgáltatás során használt, aláírás-létrehozó eszközhöz tartozó, sem pedig egyéb hordozó eszközre mentett PKCS#12-es formátumot aktiváló PIN-kódot PIN kódot nem rögzít, azt a szolgáltatást igénybe vevő személy helyben adja meg

6 .TANÚSÍTVÁNY ÉS VISSZAVONÁSI LISTA PROFILOK

6.1 Tanúsítványprofilok

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

6.1.1 Végfelhasználói aláíró tanúsítványok állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyazonosító igazolványában szereplő írásmódon, ékezethelyesen, UTF-8-ban kódolva
Organization	KELER Zrt. vagy KELER KSZF Zrt.
Organization Unit	Szervezeti egység(ek) neve(i) vagy üres
Country	Székhely (vagy opcionálisan lakcím) szerinti országkód, Magyarország esetén HU
Locality	Székhely vagy telephely (vagy opcionálisan lakcím) szerinti város
Email	Email cím
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	(kritikus kiterjesztés) cA = FALSE
KeyUsage	(kritikus kiterjesztés) NonRepudiation, DigitalSignature
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége (az érvényesség kezdete a tanúsítvány kibocsátásának ideje, az érvényesség vége a tanúsítvány kibocsátásától számított maximum 730 nap)
Issuer	Kibocsátó megnevezése
Signature	sha256WithRSAEncryption
Subject Key Identifier	Tanúsítvány egyedi azonosítója
Authority Key Identifier	Kibocsátó tanúsítvány egyedi azonosítója
CRL Distribution Points	Visszavonási lista elérhetőségét tartalmazó URL (több URL)
Authority Info Access,CAIssuers	A kibocsátó tanúsítványának elérhetőségét tartalmazó URL (több URL)
Extended Key Usage	Secure Email, TLS Web Client
Subject Alternative Name	Email cím
certificatePolicies	Policyidentifier= fedlapon szereplő megfelelő OID azonosító CPS.1='http://cpsdokumentumelerhetősége" UserNotice.1="Feltüntetni kívánt szöveg a tanúsítványkiadásról módjáról"

6.1.2 Végfelhasználói autentikációs tanúsítványok állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyazonosító igazolványában szereplő írásmódon, ékezethelyesen, UTF-8-ban kódolva
Organization	KELER Zrt. vagy KELER KSZF Zrt.
Organization Unit	Szervezeti egység(ek) neve(i) vagy üres
Country	Székhely (vagy opcionálisan lakcím) szerinti országkód, Magyarország esetén HU
Locality	Székhely vagy telephely (vagy opcionálisan lakcím) szerinti város
Email	Email cím
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	(kritikus kiterjesztés) cA = FALSE
KeyUsage	(kritikus kiterjesztés) DigitalSignature
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége

Mező	Tartalom
	(az érvényesség kezdete a tanúsítvány kibocsátásának ideje, az érvényesség vége a tanúsítvány kibocsátásától számított maximum 730 nap)
Issuer	Kibocsátó megnevezése
Signature	sha256WithRSAEncryption
Subject Key Identifier	Tanúsítvány egyedi azonosítója
Authority Key Identifier	Kibocsátó tanúsítvány egyedi azonosítója
CRL Distribution Points	Visszavonási lista elérhetőségét tartalmazó URL (több URL)
Authority Info Access,CAIssuers	A kibocsátó tanúsítványának elérhetőségét tartalmazó URL (több URL)
Extended Key Usage	Email Protection , Client Auth.
Subject Alternative Name	Email cím
certificatePolicies	Policyidentifier= fedlapon szereplő megfelelő OID azonosító CPS.1='http://cpsdokumentumelerhetősége" UserNotice.1="Feltüntetni kívánt szöveg a tanúsítványkiadásról módjáról"

6.1.3 Végfelhasználói titkosító tanúsítványok állandó elemei

Mező	Tartalom
Common Name	Magánszemély neve a személyazonosító igazolványában szereplő írásmódon, ékezethelyesen, UTF-8-ban kódolva
Organization	KELER Zrt. vagy KELER KSZF Zrt.
Organization Unit	Szervezeti egység(ek) neve(i) vagy üres
Country	Székhely (vagy opcionálisan lakcím) szerinti országkód, Magyarország esetén HU
Locality	Székhely vagy telephely (vagy opcionálisan lakcím) szerinti város
Email	Email cím
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	(kritikus kiterjesztés) cA = FALSE
KeyUsage	(kritikus kiterjesztés) Key Encipherment, DataEncipherment
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége (az érvényesség kezdete a tanúsítvány kibocsátásának ideje, az érvényesség vége a tanúsítvány kibocsátásától számított maximum 730 nap)
Issuer	Kibocsátó megnevezése
Signature	sha256WithRSAEncryption
Subject Key Identifier	Tanúsítvány egyedi azonosítója
Authority Key Identifier	Kibocsátó tanúsítvány egyedi azonosítója
CRL Distribution Points	Visszavonási lista elérhetőségét tartalmazó URL(több URL)
Authority Info Access,CAIssuers	A kibocsátó tanúsítványának elérhetőségét tartalmazó URL(több URL)
Extended Key Usage	Email Protection
Subject Alternative Name	Email cím
certificatePolicies	Policyidentifier= fedlapon szereplő megfelelő OID azonosító CPS.1='http://cpsdokumentumelerhetősége" UserNotice.1="Feltüntetni kívánt szöveg a tanúsítványkiadásról módjáról"

6.1.4 Szolgáltatói tanúsítvány profilja

Mező	Tartalom
Common Name	A hozzárendelt kiadókhoz kapcsolódó név
Organization	NetLock Kft.
Organization Unit	Tanúsítványkiadók (Certification Services)
Country	HU
Public Key	Szolgáltatói tanúsítvány nyilvános kulcsa

Mező	Tartalom
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	A szolgáltatói tanúsítványt kiadó tanúsítványkiadó neve
Signature	sha256WithRSAEncryption
CRL Distribution Points	Visszavonási lista elérhetőségét tartalmazó URL, (több URL)
Basic Constraints	(kritikus kiterjesztés) cA = TRUE, pathlen = 0
KeyUsage	(kritikus kiterjesztés) Certificate Signing, CRL Signing
Subject Key Identifier	Tanúsítvány egyedi azonosítója
Authority Key Identifier	Kibocsátó tanúsítvány egyedi azonosítója
Authority Info Access,CAIssuers	A kibocsátó tanúsítványának elérhetőségét tartalmazó URL (több URL)

6.2 Tanúsítvány visszavonási lista profilok

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

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

7 ÜZLETI ÉS JOGI TUDNIVALÓK

7.1 Bizalmasság, adatvédelem

7.1.1 Tanúsítvány visszavonására 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 Alegység kötelezettségei

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

b) szabványos X509 tanúsítvány kibocsátásában, visszavonásában való közreműködés a Regisztrációs Alegység által küldött erre vonatkozó kérelem esetén,

c) tanúsítvány 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 a Szolgáltató késedelem nélküli értesítése elektronikusan (pl. elektronikus levélben), illetve out-of-band módon (pl. postai úton) továbbá a Szolgáltató Szabályzatért Felelős Egysége bármely tagjának írásban vagy személyesen történő megkeresésével.

7.2.2 A Regisztrációs Alegység kötelezettségei

a) úgy működni, hogy semmilyen módon ne sértse a szolgáltatás biztonságát,

b) tevékenységét saját maga ellátni,

c) az igénylő (alany) tanúsítványra vonatkozó kérelmeinek (kibocsátás, 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 szolgáltatás területére belépés lehetővé tétele a Szolgáltató Szabályzatért Felelős Egysége számára.

7.2.3 A végfelhasználó kötelezettségei

7.2.3.1 A végfelhasználó általános kötelessége:

a) megismerni és betartani a tanúsítvány, illetve a magánkulcs kezelésére 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 kérni a Kihelyezett Szolgáltató Alegységtől.

7.2.3.3 A végfelhasználó kötelessége a tanúsítványának kezelése során:

a) a tanúsítványkiadáshoz előírt regisztrációs eljárásrend alapján felvett adatainak valódiságát a szükséges okmányok eredetijének, hiteles másolatának, továbbá másolatának bemutatásával alátámasztani,

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

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

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 A KELER kötelezettségei

A KELER általános kötelessége:

a) a Kihelyezett Szolgáltató Alegység és a tanúsítványtár felügyeletében, üzemeltetésében való közreműködés;

b) a szolgáltatásainak a hatályos jogi szabályozással, jelen Szolgáltatási Szabályzat Kiegészítéssel 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 készítésében és rendszeres felülvizsgálatában való közreműködés,

b) megfelelő szakmai végzettséggel rendelkező, a folyamatos, szabályzatokban előírt működés biztosításához elégséges számú kezelőszemélyzet biztosítása,

c) a szabályzatokban előírt PKI folyamatok elvégzésére alkalmas, megfelelően beállított szoftver és hardver infrastruktúra biztosítása, a szükséges változtatások megtételében való közreműködés,

d) az infrastruktúra működtetésében, javításában és karbantartásában közreműködő felelős személyzet munkájának és szakmai felkészültségének folyamatos ellenőrzése, a szükséges változtatások megtétele,

e) az előző pontokban előírt infrastruktúra folyamatos, biztonságos üzemeltetésében, hibajavításában való közreműködés és az infrastruktúrába tartozó eszközökre előírt szabványos karbantartás elvégzésének segítése,

f) Üzleti Folytonossági Terv készítése, alkalmazása,

g) a szabályzatokban előírt módon folytatott tevékenység során keletkező adatok jelen és kapcsolódó szabályzatokban meghatározott kezelésére, tárolására, archiválására alkalmas szoftver és hardver eszközök biztosításában, működtetésében, karbantartásában való közreműködés,

h) a PKI folyamatokat végző és az azok során keletkező adatokat tároló szoftver és hardver rendszer jelen és kapcsolódó szabályzatokban előírt logikai és fizikai védelmét biztosító szoftver és hardver eszközök biztosításában való közreműködés,

i) a logikai és fizikai védelmet megteremtő eszközök megfelelő üzemeltetésében, az informatikai, fizikai, adminisztrációs és üzleti biztonság megteremtésében és fenntartásában való közreműködés.

7.2.4.2 A Szabályzatért Felelős Egység kötelezettségei

a) a felügyelendő dokumentumok, továbbá a belső ügyviteli folyamatok azok helyszínén való ellenőrzése és a Szolgáltató vezetésének tájékoztatása a megfigyelésekről,

b) a Szolgáltatóhoz, illetve a Kihelyezett Szolgáltató Alegységéhez érkező szabályzatokkal kapcsolatos észrevételek és javaslatok fogadása,

c) a szabályzatok aktualizálásának előkészítése, egyeztetése és végrehajtása,

d) a különböző hitelesítés-szolgáltatási rendek specifikálása, jóváhagyása és karbantartása.

7.2.4.3 A tanúsítványtár kötelezettségei és vele kapcsolatos tevékenységek

A Tanúsítványtár kötelessége az üzemeltetés során:

a) a Tanúsítványtár részben nyilvános, minden Érintett Fél számára elérhető módon való üzemeltetése a KELER Intranetes oldalán (lásd 1.5 fejezet), valamint az Alanyok által elérhető belső oldalán;
b) bizalmas információkat, nem nyilvános adatokat a Tanúsítványtárban meg nem jeleníteni,
c) a Tanúsítványtár 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 hogy az általában elvárható magatartás szerint a jelen és kapcsolódó szabályzatokat, utasításokat betartsa, betartassa, azok betartását ellenőrizze és előírja az esetlegesen Szolgáltatási Szabályzat Kiegészítéstől eltérő működés megszüntetésének feltételeit.

Szolgáltató a Törvényben és kapcsolódó rendeletiben meghatározott feltételrendszerű és mértékű felelősségbiztosítással rendelkezik. A Szolgáltató felelőssége és összesített felelőssége korlátozott a kötelezettségeinek megszegéséből eredő 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 ÁSZF-ben rögzítettek.

A felelősségi korlátozások vonatkoznak

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

7.3.1.2 A felelősség kizárása

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

- Olyan esetben, mely a tanúsítványok jelen és kapcsolódó szabályzatok, előírások, utasítások ellentmondó felhasználásából ered
- A végfelhasználói magánkulcs kompromittálódásából eredő kár tekintetében, figyelemmel az 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

A végfelhasználó a jelen Szabályzat szerinti kötelezettségeinek be nem tartásával okozott vagyoni és nem vagyoni kárt köteles megtéríteni.

7.3.3 A KELER felelőssége

Jelen és kapcsolódó Szabályzatoknak, Szolgáltatási Szabályzat Kiegészítésnek megfelelő tevékenység, különösen a Regisztrációs és Hitelesítő Alegységre, valamint a tanúsítványkezelésre és regisztrációs tevékenységre vonatkozó előírások tekintetében.

7.3.4 Garancia

Szolgáltató garantálja a Közösség számára

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

7.4 Változtatási eljárás

7.4.1 Szolgáltatási Szabályzat Kiegészítés változtatási eljárás

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

A Szolgáltatási Szabályzat Kiegészítés módosított változatai mindig új verziószámmal kerülnek a KELER Kihelyezett Szolgáltató Alegységnek átadásra. A Szolgáltatási Szabályzat Kiegészítés a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente egyszer történik, a Szabályzatért Felelős Egység és a KELER Kihelyezett Szolgáltató Alegység biztonsági vezetője által - felelősség– és hatáskörükben eljárva - legkésőbb jelen szabályzat hatályba lépését követő évben, a hatályba lépés hónapjának utolsó munkanapján történik. A Szolgáltatási Szabályzat Kiegészítés rendkívüli felülvizsgálatára és módosítására a jogszabályi változások esetén kerül sor.

7.4.2 Szabályzatért Felelős Egység

7.4.2.1 A Szabályzatért Felelős Egység összetétele

A Szabályzatért Felelős Egység a következő összetételű munkacsoportként működik:

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

7.4.2.2 A Szabályzatért Felelős Egység működése

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

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

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

7.5 Hivatkozott jogszabályok, szabványok és egyéb dokumentumok

Jelen dokumentum az alábbi jogszabályok, szabványok és egyéb dokumentumokra hivatkozik:

[1]. 2001. évi XXXV. Törvény az elektronikus aláírásról

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

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

[4]. FIPS PUB 140-2 (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]. 9/2005. IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

[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

[15]. 4-20 IBSZ_V1_1

7.6 Hatályon kívül kerülő szabályozó iratok

Jelenleg nincs.