Minősített Szolgáltatás Szolgáltatási Szabályzat

NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

Azonosító szám (OID) BALE eszközön kibocsátott tanúsítványok esetében:	**1.3.6.1.4.1.3555.1.15.20130312**
Azonosító szám (OID) nem BALE eszközön kibocsátott tanúsítványok esetében:	**1.3.6.1.4.1.3555.1.50.20130312**
Jóváhagyás időpontja:	**2013.03.12**
Hatály kezdőnapja:	**2013.03.18**
Oldalak száma:	**98,** azaz **kilencvennyolc**
Készítette:	**Szentirmai László** szabályzat adminisztrátor
Jóváhagyta:	**Rózsahegyi Zsolt** szabályzatvezető

© COPYRIGHT, NETLOCK KFT. - MINDEN JOG FENNTARTVA

NYILVÁNOS

OID	Változás leírása	Készítő	Ellenőrző
1.3.6.1.4.1.3555.1.15.030317	A minősítési eljárás során NHH nyilvántartásba vett, első nyilvános verzió	Boromisza Zsolt	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20040301	Az egy éves minősített HSz tevékenység tapasztalatai alapján módosított, NHH nyilvántartásba vett verzió	Dr. Kovács Gábor	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20040929.0	Hatóság számára történő statisztikai célú adattovábbítás, szolgáltatói rendszer legalább évenkénti független felülvizsgálata. Szabályzat Elfogadó Egység által jóváhagyott, de NHH nyilvántartásba nem vett változat	Dr. Kovács Gábor	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20050331.0	Az álnevet tartalmazó tanúsítvány megengedése, tevékenység befejezése esetén követendő eljárás pontosítása, visszavonási lépések pontosítása. Szabályzat Elfogadó Egység által jóváhagyott, de NHH nyilvántartásba nem vett változat	Dr. Kovács Gábor	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20050713	3/2005. (III. 18.) IHM rendeletnek való megfelelés kialakítása, visszavonási szolgáltatások pontosítása, OCSP szolgáltatás bevezetése.	Dr. Kovács Gábor	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20060223.0	A közigazgatási ügyintézésben alkalmazható hitelesítési rend megfelelésével való kiegészítés	Dr. Szentirmai László	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20060411	A közigazgatási ügyintézésben alkalmazható hitelesítési rend megfelelésével való kiegészítés, NHH hiánypótlási felhívásának megfelelő módosítás	Dr. Szentirmai László	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20060728	Az éves NHH felülvizsgálat kapcsán megfogalmazott módosítási javaslatok átvezetése.	Dr. Szentirmai László	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20060828	NHH észrevételek alapján történő pontosítások	NetLock Szabályzat Elfogadó Egység (SzEE)	Rózsahegyi Zsolt
1.3.6.1.4.1.3555.1.15.20070926	NHH észrevételek alapján történő pontosítások	Dr. Tavaszi Éva	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20071115	NHH észrevételek alapján történő pontosítások	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20080107	NHH észrevételek alapján történő pontosítások	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20080206	NHH észrevételek alapján történő pontosítások	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20100318	NHH Algoritmus közleményének megfelelő módosítások, illetve NHH észrevételek alapján történő egyéb pontosítások	Ádám János	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20100830	NMHH felügyeleti eljárás során megkövetelt pontosítások	Ádám János	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20100922	NHH észrevételek alapján történő egyéb pontosítások	Ádám János	NetLock Szabályzat

OID	Változás leírása	Készítő	Ellenőrző
			Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20110706	NMHH észrevételek alapján történő pontosítások: - regisztrációs eljárás módosítása - hitelesítésszolgáltatás során használt eszközök specifikációjának pontosítása	Szentirmai László	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20110927	ORGA BALE eszköz kivezetése a szabályzatból	Szentirmai László	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20120127	- lejárt tanúsítású Micardo BALE eszköz kivezetése - újonnan bejelentett Oberthur 7.0.1, illetve Gemalto BALE eszköz felvétele - nyilvántartásban már szereplő Luna modulok beillesztése	Szentirmai László	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20120229	- április 1-én hatályba lépő Eat. módosításra való felkészülés, ennek keretében új OID kibocsátása a BALE eszközön történő tanúsítványkibocsátás megkülönböztetésére - NMHH hiánypótlás teljesítése - SafeNet eToken BALE eszköz felvétele	Szentirmai László	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.15.20120928	Használt eszközök tanúsítottságának követésére vonatkozó szabályok pontosítása	Szentirmai László	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.XX.20130312	Új eszközök felvétele a szabályzatba	Szentirmai László	NetLock Szabályzat Elfogadó Egység (SzEE)

Tartalomjegyzék

1 Bevezetés ... 10

1.1 Áttekintés ... 10
1.1.1 A Szabályzat ... 10
1.1.2 A Szabályzat hatálya ... 11
1.1.3 A Szolgáltató ... 11
1.1.4 Szolgáltatások ... 11
1.1.5 Szabványok és előírások ... 12
1.1.6 Hitelesítés-szolgáltatás és tanúsítványfajták ... 13
1.1.7 Időbélyegzés-szolgáltatás ... 14
1.1.8 Aláíró eszköz szolgáltatás ... 15

1.2 Dokumentum neve és azonosítása ... 16

1.3 PKI közösség ... 16
1.3.1 Hitelesítő egységek ... 16
1.3.2 Regisztrációs egységek ... 17
1.3.3 Végfelhasználók ... 18
1.3.4 Érintett Fél ... 18
1.3.5 Egyéb szereplők ... 18

1.4 Alkalmazhatóság ... 19
1.4.1 Engedélyezett alkalmazási lehetőségek ... 19
1.4.2 Korlátozott alkalmazási lehetőségek ... 19
1.4.3 Tiltott alkalmazási lehetőségek ... 19

1.5 Kapcsolattartás ... 20
1.5.1 A Szolgáltató adatai ... 20
1.5.2 Ügyfélszolgálat ... 20
1.5.3 Szabályzattal kapcsolatos kérdések ... 20
1.5.4 Szabályzat-jóváhagyási eljárás ... 20

1.6 Fogalmak és rövidítések ... 20
Fogalmak ... 20

2 Közzététel és tanúsítványtár ... 26

2.1 A Szolgáltatói információ közzététele ... 26
2.1.1 Közzétételi és tájékoztatási elvek ... 26
2.1.2 Kikötések és feltételek közzététele ... 26
2.1.3 Rendkívüli információk közzététele ... 26

2.2 Tanúsítványokkal kapcsolatos információk ... 26
2.2.1 Tanúsítványok közzététele ... 26
2.2.2 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala ... 27
2.2.3 Határidők meghatározása a tanúsítvány életciklusa kapcsán ... 27

2.3 A közzététel gyakorisága ... 27
2.3.1 Kikötések és feltételek közzétételi gyakorisága ... 27
2.3.2 Rendkívüli információk közzétételi gyakorisága ... 27
2.3.3 Tanúsítványok nyilvánosságra hozatalának gyakorisága ... 27
2.3.4 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága ... 28

2.4 Hozzáférés ellenőrzések ... 28
2.4.1 Tanúsítványtárak ... 28

3 Azonosítás és hitelesítés ... 29

3.1 Elnevezések ... 29
3.1.1 Névtípusok ... 29
3.1.2 Álnév használata ... 30
3.1.3 Különböző elnevezési formák értelmezési szabályai ... 30
3.1.4 A nevek egyedisége ... 31

3.1.5 Védjegyek elismerése, hitelesítése és szerepe ... 31

3.2 Kezdeti azonosítás ... 31
3.2.1 A magánkulcs birtoklásának bizonyítási módszere ... 31
3.2.2 Szervezeti azonosság hitelesítése ... 32
3.2.3 Személyazonosság hitelesítése ... 32

3.3 Azonosítás tanúsítvány kulcscseréje esetén ... 33

3.4 Visszavonási kérelem ... 33

4 Működésre vonatkozó követelmények - tanúsítványok ... 34

4.1 Tanúsítványigénylés ... 34
4.1.1 Igénylés feltételei ... 34

4.2 Tanúsítványkérelem feldolgozása ... 34
4.2.1 Általános regisztrációs szabályok ... 34
4.2.2 Regisztrációs eljárás ... 36
4.2.3 Szolgáltatási Szerződés ... 39
4.2.4 A tanúsítványkérelmek jóváhagyásának követelményei ... 39
4.2.5 A tanúsítványok tartalma ... 40
4.2.6 A tanúsítványok jellemzői ... 40
4.2.7 Az Igénylő (Alany) tájékoztatása a kibocsátást megelőzően ... 41
4.2.8 Tanúsítványkérelmek elutasítása ... 41
4.2.9 A tanúsítványokra vonatkozó további rendelkezések ... 42

4.3 A tanúsítványok kibocsátása és hozzáférhetővé tétele ... 42
4.3.1 A tanúsítvány kibocsátásának időpontja ... 42
4.3.2 A tanúsítvány érvényessége ... 42

4.4 Tanúsítványelfogadás ... 42
4.4.1 A tanúsítvány elfogadása ... 42
4.4.2 A tanúsítványigénylő nyilatkozata ... 43
4.4.3 Tanúsítvány közzététele ... 43

4.5 A kulcspár és a tanúsítvány használata ... 43
4.5.1 Az Alanyok számára szóló előírások ... 43
4.5.2 Az Érintett Felek számára szóló ajánlások ... 44

4.6 Tanúsítvány megújítása ... 44
4.6.1 Végfelhasználói tanúsítványok ... 44
4.6.2 Szolgáltatói tanúsítványok ... 46

4.7 Kulcscsere ... 46

4.8 Tanúsítvány módosítása ... 46

4.9 Tanúsítvány felfüggesztése és visszavonása ... 46
4.9.1 Általános rendelkezések ... 46
4.9.2 A visszavonás körülményei ... 47
4.9.3 Visszavonás kérelmezése ... 47
4.9.4 Visszavonási kérelemre vonatkozó eljárás ... 47
4.9.5 Visszavonási kérelemre vonatkozó türelmi idő ... 48
4.9.6 Visszavonásra vonatkozó egyéb szabályok ... 49
4.9.7 A felfüggesztés körülményei ... 49
4.9.8 Felfüggesztés kérelmezése ... 49
4.9.9 Felfüggesztési kérelemre vonatkozó eljárás ... 49
4.9.10 A felfüggesztés időtartamára vonatkozó korlátozások ... 50
4.9.11 Kulcskompromittálódás esetére vonatkozó speciális követelmények ... 50

4.10 Tanúsítvány-állapot információk közzététele ... 50
4.10.1 Tanúsítvány Visszavonási Lista (CRL) ... 50
4.10.2 Az ajánlott CRL ellenőrzés az Érintett Fél számára ... 51
4.10.3 Valós idejű visszavonási állapot ellenőrzés elérhetősége ... 51
4.10.4 Valós idejű visszavonás ellenőrzési követelmények ... 52
4.10.5 A visszavonási információ közzétételének egyéb formái ... 52

4.11 Tanúsítvány-előfizetés vége ... 52

4.12 Kulcs letétbe helyezése és visszaállítása ... 52

5 Működésre vonatkozó követelmények - időbélyegzés ... 53

5.1 Időbélyeg-szolgáltatás igénylése ... 53

5.2 Az időbélyeg- szolgáltatás teljesítése ... 53

5.3 Minősített Időbélyeg-szolgáltatás joghatása ... 54

6 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések ... 55

6.1 Fizikai óvintézkedések ... 55

6.1.1 A telephely elhelyezése és szerkezeti felépítése ... 55
6.1.2 A Second Site elhelyezése és szerkezeti felépítése ... 56
6.1.3 Fizikai hozzáférés ... 56
6.1.4 Áramellátás és légkondicionálás ... 56
6.1.5 Beázás és elárasztódás veszélyeztetettsége ... 57
6.1.6 Tűzmegelőzés és tűzvédelem ... 57
6.1.7 Adathordozók tárolása ... 57
6.1.8 Selejt kezelése, megsemmisítése ... 57
6.1.9 Fizikailag elkülönítetten őrzött mentési példányok ... 58

6.2 Eljárásbeli óvintézkedések ... 58

6.2.1 Bizalmi munkakörök ... 58
6.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok ... 59
6.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés ... 60
6.2.4 Változáskezelés ... 60

6.3 Személyzetre vonatkozó óvintézkedések ... 60

6.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények ... 61
6.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások ... 61
6.3.3 Képzési követelmények ... 61
6.3.4 Továbbképzési gyakoriságok és követelmények ... 61
6.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje ... 62
6.3.6 A felhatalmazás nélküli tevékenységek büntető következményei ... 62
6.3.7 A szerződéses munkavállalókra vonatkozó követelmények ... 62
6.3.8 A személyzet számára biztosított dokumentációk ... 62

6.4 A biztonsági naplózás folyamatai ... 62

6.4.1 A tárolt események típusai ... 62
6.4.2 A napló állomány feldolgozásának gyakorisága ... 63
6.4.3 A napló állomány megőrzési időtartama ... 63
6.4.4 A napló állomány védelme ... 63
6.4.5 A napló állomány mentési folyamatai ... 63
6.4.6 A napló gyűjtési rendszere ... 63
6.4.7 Az eseményeket kiváltó Alanyok értesítése ... 63
6.4.8 Sebezhetőség felmérése ... 63

6.5 Adatok archiválása ... 64

6.5.1 A tárolt események típusai ... 64
6.5.2 Az archívum megőrzési időtartama ... 64
6.5.3 Az archívum védelme és hozzáférési szabályok ... 64
6.5.4 Az archívum mentési folyamatai ... 64
6.5.5 A rekordok időbélyegzésére vonatkozó követelmények ... 64
6.5.6 Az archívum gyűjtési rendszere ... 65
6.5.7 Archív információ hozzáférését és ellenőrzését végző eljárások ... 65
6.5.8 Egyéb archiválási rendelkezések ... 65

6.6 Biztonsági rendelkezések ... 65

6.6.1 Biztonsági felülvizsgálati eljárások ... 65

6.7 Helyreállítás kompromittálódás és katasztrófa esetén ... 66

6.7.1 Incidens- és kompromittálódás-kezelési eljárások ... 66

6.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok ... 66
6.7.3 Egy szolgáltatói egység kulcsának kompromittálódása ... 66
6.7.4 Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően ... 66

6.8 A Szolgáltató leállítása ... 67
6.8.1 Szolgáltatás megszűntetése ... 67
6.8.2 Regisztrációs pont megszűnése ... 68

7 Műszaki biztonsági óvintézkedések ... 69

7.1 Kulcspár előállítás és telepítés ... 69
7.1.1 Kulcspár előállítás ... 69
7.1.2 Magánkulcs eljuttatása az Alanyhoz ... 71
7.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz ... 71
7.1.4 A szolgáltatói nyilvános kulcs közzététele ... 71
7.1.5 Kulcsméretek ... 71
7.1.6 A nyilvános kulcs paraméterek generálása és megfelelőségük ellenőrzése ... 71
7.1.7 A kulcs használat célja (az X.509 v3 kulcshasználati mezők tartalmának megfelelően) ... 72

7.2 A magánkulcsok védelme ... 72
7.2.1 A szolgáltatói kulcsokra vonatkozó általános szabályok ... 72
7.2.2 Magánkulcs letétbe helyezése ... 72
7.2.3 Magánkulcs mentése ... 72
7.2.4 Magánkulcs archiválása ... 73

7.3 A kulcspár gondozásának egyéb szempontjai ... 73
7.3.1 Egyéb kulcskezelési rendelkezések ... 73
7.3.2 Nyilvános kulcs archiválása ... 73
7.3.3 A nyilvános és magánkulcsok használatának periódusa ... 73

7.4 Aktivizáló adatok ... 74
7.4.1 Aktivizáló adatok előállítása és telepítése ... 74
7.4.2 Az aktivizáló adatok védelme ... 74
7.4.3 Az aktivizáló adatok egyéb szempontjai ... 74

7.5 Számítógép-biztonsági óvintézkedések ... 74
7.5.1 Speciális számítógép-biztonsági műszaki követelmények ... 74
7.5.2 Informatikai biztonsági osztályozás ... 75

7.6 Életciklusra vonatkozó műszaki óvintézkedések ... 75
7.6.1 Rendszerfejlesztési óvintézkedések ... 75
7.6.2 Biztonságkezelési óvintézkedések ... 75
7.6.3 Az életciklusra vonatkozó biztonság osztályozása ... 76

7.7 Hálózatbiztonsági óvintézkedések ... 76

7.8 A kriptográfiai modul ellenőrzése ... 76
7.8.1 Időforrás és időszinkronizáció ... 76
7.8.2 Az időforrások megnevezése ... 76
7.8.3 Időforrás pontossága ... 77
7.8.4 Alkalmazott eszközök ... 77

8 Tanúsítvány, -visszavonási lista és időbélyeg profilok ... 78

8.1 Tanúsítványprofilok ... 78
8.1.1 Személyes végfelhasználói tanúsítványok profiljainak állandó elemei ... 78
8.1.2 Munkatársi végfelhasználói tanúsítványok profiljainak állandó elemei ... 78

8.2 Szolgáltatói tanúsítványok profilja ... 79
8.2.1 Szolgáltatói (tanúsítvány- és visszavonási lista aláíró) főtanúsítvány profilja ... 79
8.2.2 Szolgáltatói (tanúsítvány- és visszavonási lista aláíró) kiadói tanúsítvány profilja ... 79
8.2.3 Szolgáltatói (visszavonási lista aláíró) tanúsítvány profilja ... 79
8.2.4 Szolgáltatói (időbélyegző) tanúsítványok profilja ... 80
8.2.5 Szolgáltatói (OCSP válasz aláíró) tanúsítványok profilja ... 80
8.2.6 Közigazgatási Gyökér Hitelesítés-Szolgáltató által felülhitelesített szolgáltatói (tanúsítvány- és visszavonási lista aláíró) tanúsítvány profilja ... 81

8.3 Tanúsítvány visszavonási lista profil ... 81

8.4 Időbélyeg-profil ... 81

9 A megfelelőség vizsgálata ... 83

9.1 A megfelelőség vizsgálatának gyakorisága ... 83

9.2 Az átvizsgáló egységek megnevezése ... 83

9.3 Az átvizsgáló egységek és a vizsgált fél kapcsolata ... 84

9.4 A vizsgálat által érintett területek ... 84

9.5 Hiányosságok esetén végrehajtandó tevékenységek ... 84

10 Üzleti és jogi tudnivalók ... 85

10.1 Díjak ... 85
10.1.1 Egyéb szolgáltatásokra vonatkozó díjak ... 85
10.1.2 Visszatérítési elvek ... 85

10.2 Pénzügyi felelősség ... 86

10.3 Bizalmasság, adatvédelem ... 86
10.3.1 Bizalmasan kezelendő információ típusok ... 87
10.3.2 Nem bizalmasnak tekintett információ típusok ... 87
10.3.3 Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése ... 87
10.3.4 Információszolgáltatás hatósági szervek részére ... 87
10.3.5 Információszolgáltatás polgári peres eljárás keretében ... 88
10.3.6 Egyéb információszolgáltatás ... 88
10.3.7 Az Alany kérésére történő felfedés ... 88
10.3.8 Egyéb információ harmadik félnek történő átadása ... 88

10.4 Szellemi alkotásokhoz fűződő jogok ... 88

10.5 Jogok és kötelezettségek ... 88
10.5.1 A hitelesítő egységek közös kötelezettségei ... 88
10.5.2 A Regisztrációs Egységek közös kötelezettségei ... 89
10.5.3 A végfelhasználó kötelezettségei ... 89
10.5.4 Ajánlások az Érintett Fél részére ... 90
10.5.5 Szolgáltató egyéb kötelezettségei ... 92

10.6 Felelősség ... 93
10.6.1 A Szolgáltató általános felelőssége ... 93
10.6.2 A végfelhasználó felelőssége ... 93
10.6.3 Az Érintett Fél felelőssége ... 94

10.7 Változtatási eljárás ... 94
10.7.1 Szabályzat-változtatási eljárás ... 94
10.7.2 Szabályzat Elfogadó Egység ... 94
10.7.3 Értesítés nélkül változtatható elemek ... 95
10.7.4 Értesítéssel változtatható elemek ... 95
10.7.5 Szabályzati objektumazonosítót vagy mutatót változtató módosítások ... 95

10.8 Panaszkezelési szabályok ... 95
10.8.1 Panaszok benyújtásának helye ... 95
10.8.2 Panaszok benyújtásának módja ... 95
10.8.3 Panaszok kezelésének eljárása ... 95
10.8.4 Illetékes fogyasztóvédelmi felügyelőség ... 96

10.9 Hivatkozott jogszabályok, szabványok és egyéb dokumentumok ... 96

10.10 Értelmezés és érvényesítés ... 97
10.10.1 Irányadó jog ... 97
10.10.2 A rendelkezések különválaszthatósága ... 97
10.10.3 A rendelkezések jogfolytonossága ... 98
10.10.4 A rendelkezések kiterjesztése ... 98

10.10.5 Vitás kérdések megoldására vonatkozó eljárások 98

1 Bevezetés

1.1 Áttekintés

A jelen szabályzat a NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (a továbbiakban: Szolgáltató) minősített hitelesítés-szolgáltatásra és egyéb aláírással kapcsolatos szolgáltatásaira vonatkozó Szolgáltatási Szabályzata (a továbbiakban: Szabályzat).

A Szolgáltató az elektronikus kommunikáció hitelességét és bizalmasságát biztosító elektronikus tanúsítványok kiadását, az ehhez kapcsolódó nyilvános adatbázisok, illetve infrastruktúra karbantartását és üzemeltetését végzi. A hitelesítés-szolgáltatói tevékenység mellett kiemelt terület a PKI tanácsadás és-integráció: vállalati és országos szintű elektronikus hitelesítési rendszerek tervezése és megvalósítása, valamint a hiteles és bizalmas kommunikációhoz elengedhetetlen eszközök, az elektronikus kulcsok biztonságos készítését, tárolását biztosító hardvereszközök (intelligens kártyák és USB kompatibilis egységek) telepítése és folyamatos támogatása.

A tanúsítványhitelesítés, PKI tanácsadás és rendszerintegráció mellett a Szolgáltató időbélyeg-szolgáltatást is végez, illetve elektronikus aláírást létrehozó adat elektronikus aláírást létrehozó eszközön való elhelyezése szolgáltatást is nyújt.

A Szolgáltató, mint Hitelesítés-szolgáltató minősített és nem minősített osztályokban kínál különböző tanúsítványfajtákat. A tanúsítványfajták elsősorban a kibocsátandó tanúsítványban szereplő entitások számában és jellegében, míg a tanúsítvány osztályok elsősorban az entitások adatainak és egyéb adatok ellenőrzésének szigorában különböznek. A nem minősített tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjaival készített, fokozott biztonságú aláírással ellátott elektronikus dokumentumokhoz az írásbeliség, míg a minősített tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjaival készített minősített vagy fokozott biztonságú aláírással ellátott elektronikus okiratokhoz a teljes bizonyító erejű magánokiratok jogkövetkezményeit fűzi a polgári perrendtartásról szóló 1952. évi III. törvény.

Jelen Szabályzat kizárólag a minősített tanúsítványokra, valamint a minősített időbélyegzés-szolgáltatásra vonatkozó szabályokat tartalmazza.

A Szolgáltató 2003. márciusában, jelen szolgáltatási szabályzat első változatának hatályba lépésekor vált az első olyan hitelesítés-szolgáltatóvá, amely a piaci magán- és szervezeti szereplők számára is nyújt tanúsítvány- és időbélyegszolgáltatást. A Szolgáltató tevékenysége megfelel a Hitelesítés-szolgáltatókkal szemben támasztott nemzetközi követelményeknek, ezt az Ernst & Young Kft. által kiadott WEB TRUST nemzetközi audit záródokumentuma igazolja. A folyamatos magas színvonalú szolgáltatás érdekében ISO 9001-es szabványnak megfelelő minőségbiztosítási rendszert üzemeltet, amelyet külső és belső, független szakértők évente több alkalommal is ellenőriznek. A Szolgáltató az általa kezelt információk, illetve általa nyújtott szolgáltatások bizalmasságának, integritásának és rendelkezésre állásának biztosítása érdekében ISO/IEC 27001 (korábban BS 7799-2:2002 elnevezésű) szabványnak megfelelő információbiztonsági irányítási rendszert is üzemeltet, amelynek megfelelőségét évente külső és belső, független ellenőrök és tanúsítók ellenőriznek.

A Szolgáltató szerepel minden Microsoft termék, a legújabb Mozilla termékek, és egy sor egyéb szoftver (KDE, Konqueror, Kmail, Safari, PGP, stb.) hitelesítés-szolgáltatói listáján világszerte. Szolgáltatásaiért viszontbiztosítással rendelkező magyar biztosító társaság vállal felelősséget.

1.1.1 A Szabályzat

Jelen Szolgáltatási Szabályzat a Szolgáltató minősített szolgáltatásokként nyújtott szolgáltatásaival kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazza.

A Szabályzat összefoglalóan tartalmazza mindazon szabályokat, információkat, melyek a Szolgáltató tevékenységével kapcsolatosak, és amelyeket a Szolgáltatóval valamilyen módon kapcsolatba

kerülőknek (elsősorban a végfelhasználóknak és érintett feleknek) érdemes tudni. Mint ilyen, a Szolgáltató működésének átláthatóságát biztosítja, és lehetővé teszi a felhasználók számára, hogy megállapítsák, hogy a Szolgáltató gyakorlata, illetve adott tanúsítványfajtája mennyiben felel meg elvárásaiknak. A Szabályzat ellenőrzésével a tanúsítvány elfogadói egyértelműen meg kell tudják állapítani a tanúsítvány kezelésének módját, az általa garantált biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat.

A jelen Szabályzat tartalmára és felépítésére az RFC 3647 [11] dokumentum, illetve a Minősített tanúsítványtípus minták minősített Hitelesítés-szolgáltatók számára [5] adott útmutatót, amelyek struktúráját a Szabályzat követi.

1.1.2 A Szabályzat hatálya

1.1.2.1 Tárgyi hatály

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

1.1.2.2 Időbeli hatály

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

1.1.2.3 Személyi hatály

A Szabályzat személyi hatálya a Felhasználóra és a Szolgáltatóra terjed ki.

1.1.3 A Szolgáltató

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

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

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

Önkéntes akkreditáció, egyéb minősítések:

- Ernst and Young AICPA/CICA WebTrust for Certification Authorities audit (2000)
- ISO 9001:2000 (2001. óta folyamtosan)
- BS 7799-2:2002 (2005)
- ISO/IEC 27001:2008 (2005. óta folyamatosan)

Tekintettel arra, hogy Magyarországon a Törvény 8/B § szerinti önkéntes akkreditációs rendszer még nem működik, a Szolgáltató ilyen tanúsítással nem rendelkezik.

1.1.4 Szolgáltatások

A Szolgáltató tevékenységi köre: hitelesítés-szolgáltatás, eszköz-szolgáltatás, időbélyeg-szolgáltatás. Ezen kívül a szolgáltatásokhoz kötődő fejlesztési, rendszerintegrációs és PKI tanácsadási tevékenységgel is foglalkozik, illetve a biztonságos aláíró eszközzel kapcsolatos kereskedelmi és megszemélyesítési feladatokat is ellát.

1.1.5 Szabványok és előírások

1.1.5.1 Szolgáltatási Szabályzat

A Szabályzat az RFC 3647 [11] szabványa alapján készült, az Informatikai és Hírközlési Minisztérium közigazgatási rendekre vonatkozó ajánlásának [18] megfelelően. A Szabályzat tartalmi vonatkozásokban eleget tesz az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] (továbbiakban: Törvény) és 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 TS 101 456 [8], az ETSI 102 042 [20], valamint az x.509 [13] szabvány ajánlásait.

1.1.5.2 Lenyomatképző algoritmusok azonosítói

- SHA-1 OID ::= { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }
- 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) 2}
- SHA-512 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) 3}
- Whirlpool OID ::= { iso(1) standard(0) hash-functions(10118) part3(3) algorithm(0) 55 }

A Szolgáltató az itt meghatározott algoritmusokat legfeljebb a FelügyeletAlgoritmus Határozatában [31] megjelölt időpontig használja.

1.1.5.3 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 [31] megjelölt időpontig használja.

1.1.5.4 Tanúsítvány kiterjesztések azonosítói

- Pseudonym OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) attributeType(4) 65}
- CRL Distribuion Point OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) objectClass(6) 19}
- 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 }
- QcEUCompliance OID ::= { ITU-T(0) ITU-T Identified Organization(4) ETSI(0) 1862 1 1 }
- QcEULimitValue OID ::= { ITU-T(0) ITU-T Identified Organization(4) ETSI(0) 1862 1 2 }
- QcEURetentionPeriod OID ::= { ITU-T(0) ITU-T Identified Organization(4) ETSI(0) 1862 1 3 }
- QcSSCD OID ::= { ITU-T(0) ITU-T Identified Organization(4) ETSI(0) 1862 1 4 }
- AIA:OCSP OID ::= {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) 1}
- AIA:CAIssuers OID::= {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) 2}

1.1.5.5 Alkalmazott formátumok

Tétel	Alkalmazott / elfogadott formátum, szabvány
Aláírás létrehozó adat	PKCS12 PEM, PKCS12 DER
Kérelem	PKCS10 PEM, X509 selfsigned PEM, SPKAC
Tanúsítvány	X509 PEM, X509 DER, X509 PKCS7, WAP WTLS
CRL	X509 PEM, X509 DER, X509 PKCS7
OCSP	RFC 2560 Online Certificate Status Protocol (OCSP)
Időbélyeg	RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

1.1.6 Hitelesítés-szolgáltatás és tanúsítványfajták

A Szolgáltató előzetes entitásazonosítás után az Igénylők (későbbi Alanyok) számára minősített tanúsítványt bocsát ki, amelyekbe foglalt nyilvános kulcsok magánkulcs párja BALE eszköz felhasználásával minősített elektronikus aláírás, nem BALE eszközön tárolva fokozott biztonságú aláírás létrehozására, maga a tanúsítvány pedig aláírások ellenőrzésére használható.

A tanúsítvány a hitelesítés-szolgáltató által kibocsátott igazolás, amely a nyilvános kulcsot egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.

A Szolgáltató által támogatott, végfelhasználói tanúsítványfajták összefoglaló táblázata az alábbi. A tanúsítványfajtákhoz tartozó profilok leírását a 8. fejezet tartalmazza.

Figyelem! A minősített tanúsítványokat is kibocsátó szolgáltatói tanúsítványok bizalmi hierarchiájában minősített és nem minősített (fokozott biztonságú) tanúsítványok szerepelnek. A tanúsítványok ellenőrzésénél ezért fokozott figyelmet kell fordítani a tanúsítványokban szereplő qcCompliance mező értelmezésére (ld. 8. fejezet).

Fajta	Alany	Engedélyezett alkalmazások	Tiltott alkalmazások	Osztály	Felelősség biztosítás összege	Joghatás
Személyes aláíró (BALE eszközön kibocsátott)	Természetes személy	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	Minősített	A tanúsítványban szereplő érték, de maximálisan 50 M forint	Teljes bizonyító erejű magánokirat
Személyes aláíró (nem BALE eszközön kibocsátott)	Természetes személy	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	Minősített	A tanúsítványban szereplő érték, de maximálisan 50 M forint	Teljes bizonyító erejű magánokirat
Munkatársi aláíró (BALE eszközön kibocsátott)	Természetes személy szervezet vagy hatóság munkatársa-ként	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	Minősített	A tanúsítványban szereplő érték, de maximálisan 50 M forint	Teljes bizonyító erejű magánokirat
Munkatársi aláíró (nem BALE eszközön kibocsátott)	Természetes személy szervezet vagy hatóság munkatársa-ként	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	Minősített	A tanúsítványban szereplő érték, de maximálisan 50 M forint	Teljes bizonyító erejű magánokirat
Szervezeti aláíró (BALE eszközön kibocsátott)	Szervezet vagy hatóság oldalán szereplő automatizmus	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	Minősített	A tanúsítványban szereplő érték, de maximálisan 50 M forint	Teljes bizonyító erejű magánokirat
Szervezeti aláíró (nem BALE eszközön kibocsátott)	Szervezet vagy hatóság oldalán szereplő automatizmus	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése	Minősített	A tanúsítványban szereplő érték, de maximálisan 50 M forint	Teljes bizonyító erejű magánokirat

Az Igénylőnek egyéni mérlegelési joga és felelőssége, hogy a Szolgáltató szabályzatai alapján meghatározza, milyen tanúsítványt alkalmaz egy adott célra. Ugyanígy az Érintett Félnek is egyéni mérlegelési joga és felelőssége, hogy a Szolgáltató szabályzatai alapján meghatározza, milyen tanúsítványt fogad el egy adott célra.

1.1.7 Időbélyegzés-szolgáltatás

Szolgáltató minősített időbélyegzés-szolgáltatást is nyújt.

Az időbélyegző az elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját. Az irat vagy dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető. Az elektronikus dokumentum egy adott pillanatban való létezését (időbélyegző elhelyezésének időpontja) kizárólag időbélyegzővel ellátott elektronikus dokumentum esetén lehet hitelesen megállapítani.

Időbélyegzés esetén a tanúsítványra, illetve az időbélyegzésre vonatkozó rendelkezéseket kell megfelelően alkalmazni.

Típus	Igénylő	Joghatás
Minősített időbélyeg	Természetes személy vagy szervezet	Az ellenkező bizonyításáig vélelmezni kell, hogy a dokumentumban foglalt adatok az időbélyegző elhelyezése óta változatlan formában léteztek.

A Szolgáltató időbélyegzés-szolgáltatás nyújtása során biztosítja, hogy az időbélyegző válasz – az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve – ugyanazokat az adatokat tartalmazza amelyeket a kérelem tartalmazott. Az időbélyegzés szolgáltatás során a Szolgáltató a technológia jellegéből adódóan nem ismeri meg az időbélyegzett dokumentum tartalmát, csak az abból képzett lenyomatot.

A Szolgáltató az időbélyegző elhelyezése során biztosítja, hogy a számára átadott elektronikus dokumentum vagy lenyomat tartalmát csak az időbélyegző elhelyezéséhez szükséges mértékben módosítja. A Szolgáltató az időbélyegzőt oly módon hozza létre, hogy az összekösse az aktuális időt (az időadatot), egyedi sorszámot és az időbélyegzővel ellátni kívánt elektronikus dokumentumot vagy annak lenyomatát.

1.1.8 Aláíró eszköz szolgáltatás

A Szolgáltató aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatást végez.

A szolgáltatás keretében a hatályos jogszabályok és a jelen Szabályzat rendelkezéseinek figyelembe vételével az Alany számára kulcspárt generál az adott aláírás létrehozó eszközre vagy azon kívül.

Az aláírás-létrehozó eszköznek szerepelnie kell a Felügyelet által vezetett nyilvántartásban.

Aláíró eszköz szolgáltatás biztosítása során a Szolgáltató:

- az aláíró kulcsokat a minősített elektronikus aláírások céljaira alkalmas algoritmus felhasználásával generálja, illetve az eszközt megszemélyesíti;
- gondoskodik arról, hogy a kulcs hossza és az alkalmazott nyilvános kulcsú algoritmus a minősített elektronikus aláírás céljaira alkalmas legyen;
- a kulcsok generálását és az Aláíró félhez történő továbbítását megelőző tárolását biztonságosan végzi;
- ha a kulcspár előállítása az aláírás-létrehozó eszközön kívül történik, a Szolgáltató a kulcspárt biztonságos módon juttatja az aláírás-létrehozó eszközbe és az aláírás-létrehozó eszközben történt elhelyezése után a magánkulcs aláírás-létrehozó eszközön kívüli másolatait megsemmisíti;
- biztosítja az aláíró kulcsok titkosságát, valamint az aláírás-ellenőrző adat sértetlenségét;
- gondoskodik róla, hogy az Aláíró aláírás-létrehozó adata a szolgáltatás nyújtása során – tehát a kulcsok Aláíró félnek történő átadásig - visszafejtésre alkalmas módon ne kerüljön tárolásra;
- gondoskodik arról, hogy az Aláíró aláírás-létrehozó adata az Aláírónak történő átadást követően semmilyen módon ne kerüljön tárolásra;
- amennyiben az aláírás-létrehozó eszközt harmadik fél biztosítja, az aláírás-létrehozó eszköz előkészítése előtt ellenőrzi, hogy az aláírás-létrehozó eszköz a Felügyelet által nyilvántartásba vett biztonságos aláírás-létrehozó eszköz-e;
- gondoskodik az általa biztosított aláírás-létrehozó eszköz kibocsátásakor az eljárás biztonságosságáról;
- biztosítja, hogy a kulcsgenerálást követően, az aláírás-létrehozó eszköz a szándék szerinti, hitelesített Aláíróhoz kerül;
- aláíró eszköz biztosítása esetén az aktivizáló adatokat az aláírás-létrehozó eszköztől elkülönítve juttatja el az Aláíróhoz;
- gondoskodik róla, hogy a saját munkavállalói ne élhessenek vissza az aláírás-létrehozó eszközzel a következőképpen: PIN számok megismerése, magánkulcsok, tanúsítványok használata;
- az aláírás-létrehozó eszköz előkészítése és továbbítása során alkalmazza a biztonsági eljárásokat;

- az aláírás-létrehozó adat csak az aláírást-létrehozó eszközön és csak az átadás után lesz érvényes.

1.1.8.1 Biztonságos aláírás-létrehozó eszköz

A biztonságos aláírás-létrehozó eszköz (BALE) olyan eszköz, amely biztosítja a következőket:

- az aláírás készítéséhez használt aláírás-létrehozó adat Aláírónként biztosan mindig különbözik és titkossága kellően biztosított,
- az aktuálisan elérhető technológiával kellő bizonyossággal garantálható, hogy az aláírás készítéséhez használt aláírás-létrehozó adat nem rekonstruálható, megvalósítható annak a jogosulatlan felhasználókkal szembeni védelme, illetve az aláírás nem hamisítható;
- a biztonságos aláírás-létrehozó eszközöknek nem szabad az aláírandó elektronikus dokumentumot az aláírás elhelyezéséhez szükséges mértéken felül módosítaniuk, illetőleg nem akadályozhatják meg azt, hogy az Aláíró a dokumentumot az aláírási eljárás előtt megjelenítse.

1.2 Dokumentum neve és azonosítása

Jelen dokumentum:

- Teljes neve: NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság Minősített Szolgáltatási Szabályzata
- Rövid neve: Minősített Szolgáltatási Szabályzat
- Verziószáma: a fedőlapon található egyedi azonosító (OID)

A Szabályzat hivatalos és aktuális verziója megtalálható és letölthető:

- Szolgáltató internetes oldalairól: www.netlock.hu (ld. még 2.1.2 pont).
- A Felügyelet internetes oldaláról: http://www.nmhh.hu.

A Szabályzat alapján a Szolgáltató a következő hitelesítési rendnek való megfelelést vállalja:

- [18] Biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rendek
- Ügyfelekre vonatkozó hitelesítési rend: OID 0.2.216.1.100.42.101.1.2.1 (az általános szabályoktól eltérő, ezen hitelesítési rendnek megfelelő szabályozás jelölése: MHR_Ü)
- Közigazgatási köztisztviselőkre vonatkozó hitelesítési rend: OID 0.2.216.1.100.42.101.2.2.1 (az általános szabályoktól eltérő, ezen hitelesítési rendnek megfelelő szabályozás jelölése: MHR_K)
- NetLock Aláírás Célú Tanúsítvány Hitelesítési Rend [29]
- NetLock Általános Időbélyegzési Rend [30]

1.3 PKI közösség

A kibocsátott tanúsítványok, időbélyegzők, aláírás-létrehozó eszközök alkalmazó közössége a Szolgáltató, a vele szerződéses kapcsolatban álló regisztrációs és egyéb közreműködő szervezetek, a tanúsítványok végfelhasználói és az érintett felek.

1.3.1 Hitelesítő egységek

A Szolgáltató saját szervezetén belül hitelesítő egységeket működtet, amelyek feladata a tanúsítványok központi létrehozása és kezelése a regisztrációs egységektől kapott kérelmeknek megfelelően.

1.3.1.1 Minősített Hitelesítő Egység

A Szolgáltató minősített szolgáltatásait végző hitelesítő egysége. A Minősített Hitelesítő Egység a minősített eljárási rend szerint a hozzá tartozó regisztrációs egységek kérelme alapján a minősített tanúsítványok kiadását, publikálását, visszavonását, felfüggesztését, valamint a Minősített Tanúsítvány Visszavonási Lista (a továbbiakban: CRL) publikálását végző automatizált szolgáltatói egység.

Név:	**Minősített Hitelesítő Egység**
Egység:	NetLock Kft.
Cím:	1023 Budapest, Zsigmond tér 10.
Telefon:	(40) 22-55-22
Fax:	(1) 700-1101
Internet cím:	www.netlock.hu
E-mail:	info@netlock.hu

1.3.2 Regisztrációs egységek

A Szolgáltató Központi Regisztrációs Egységet, Mobil Regisztrációs Munkatársakat, Kihelyezett Regisztrációs Egység(ek)et, valamint Regisztrációs és Kézbesítési Megbízottakat alkalmaz, amelyek feladata a kezdeti regisztráció és a tanúsítvány kibocsátásával kapcsolatos egyéb tevékenységekben való részvétel.

Minden esetben a Központi Regisztrációs Egység feladata az Alany – ha van, akkor a másodlagos Alany is – kezdeti azonosítása, adatainak ellenőrzése közhiteles nyilvántartásban, kibocsátás során elektronikus kérelem-feldolgozási tevékenység, eljárási lépések koordinálása, dokumentálás, s további tanúsítvány kezelési feladatok, többek között a felhasználókkal való kapcsolattartás. A kezdeti azonosításhoz szükséges okmányok begyűjtését a Központi Regisztrációs Egység, vagy a Központi Regisztrációs egység felügyelete és irányítása alatt álló Mobil Regisztráció Munkatársak, valamint a Kihelyezett Regisztrációs Egység munkatársai végzik. Az ügyfélszolgálati teendőket, valamint a felhasználókkal való elsődleges kapcsolattartást a Szolgáltató külön erre a feladatra alkalmazott vevőszolgálati munkatársai végzik. Az ügyfélszolgálati munkatársak a Központi Regisztrációs Egységen belül alkotnak önálló csoportot.

A fentieken túl a Központi Regisztrációs Egység a regisztrációs eljárás egészének helyességét és szabályzatoknak való megfelelését ellenőrzi. A Központi Regisztrációs Egység munkatársainak felelőssége a tanúsítvánnyal kapcsolatos végső döntések meghozatala is.

A Szolgáltatási Szerződés aláírására és/vagy az eszközátadásra az ügyfél választása alapján az alábbiak valamelyike szerint kerül sor:

- a Központi Regisztrációs Egység előtt, a Szolgáltató székhelyén, vagy
- a Mobil Regisztrációs Munkatárs előtt, az ügyfél által kért helyen, vagy
- a Regisztrációs és Kézbesítési Megbízott előtt, az ügyfél által kért helyen.

Mindezek mellett lehetőség van arra is, hogy a Szolgáltatási Szerződést az ügyfél a már meglévő, érvényes aláíró tanúsítványával írja alá és jutassa el a Szolgáltatónak.

A Szolgáltató az utolsó pont választása esetén előírhatja a Szolgáltatási Szerződés közokiratba foglalását, vagy 20 millió forint alatti ügyleti érték esetén az aláírás hitelesítését, adatellenőrzést. Ezen feltételeket tipikusan a Magyar Közjegyzői Kamara tagjainak közjegyzői közreműködésével lehet teljesíteni.

A regisztrációs munkatársak, valamint a Regisztrációs és Kézbesítési Megbízottak tanúsítvány-kibocsátás során, személyes megjelenés mellett, a felhasználói adatellenőrzést végzik, amely tevékenységüket a mindenkor hatályos jogszabályi követelményeknek - így különösen az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek - megfelelően

végzik. Az ügyfél választása szerint ők végzik az eszközátadást is, amennyiben az ügyfél nem jelent meg érte a Központi Regisztrációs Egység előtt.

A Szolgáltató a későbbiekben egyéb szervezetekkel is szerződést köthet regisztrációs szolgáltatások elvégzésére, illetve jogszabály megállapíthat egyéb regisztrációs egységként működő szervezeteket. Az így létrejövő regisztrációs pontok és közreműködők listáját a Szolgáltató honlapján publikálja.

Név:	**Központi Regisztrációs Egység**
Egység:	NetLock Kft.
Cím:	1023 Budapest, Zsigmond tér 10.
Telefon:	(40) 22-55-22
Fax:	(1) 700-1101
Internet cím:	www.netlock.hu
E-mail:	info@netlock.hu

1.3.3 Végfelhasználók

A tanúsítványban mind annak alanya, munkatársi tanúsítvány esetén annak másodlagos alanya is megnevezésre kerül.

A Szolgáltató a következő entitások részére bocsát ki minősített tanúsítványokat:

- természetes személyeknek – személyes tanúsítvány
- természetes személyeknek egy adott szervezethez tartozóként – munkatársi tanúsítvány
- szervezeteknek – szervezeti aláíró tanúsítvány

Az Alany és a másodlagos Alany a Szolgáltatóval az Általános Szerződési Feltételekben foglaltak szerint szerződéses viszonyban áll. A Szolgáltató az Alanyokkal elsősorban a regisztrációs egységeken keresztül tart kapcsolatot.

A Szolgáltató szabályzatai csak a tanúsítványfajták definiálásával korlátozzák az Alanyok körét, a Szolgáltató szerződéses feltételeinek teljesítésével, a szabályzatokban leírt jellemzőknek megfelelve bárki lehet Alany, illetve másodlagos Alany.

1.3.4 Érintett Fél

Az Érintett Fél a Közösség azon tagja, aki az elektronikus aláírás, illetve időpont hitelesítése céljából a Szolgáltató által kibocsátott tanúsítványhoz, illetve időbélyeghez fordul, illetőleg ezen tanúsítvány, illetve időbélyeg érvényességének ellenőrzéséhez a Szolgáltató által karbantartott nyilvántartásokat és szabályzatokat ellenőrzi.

A közigazgatási felhasználás tekintetében minden olyan felhasználó a közigazgatási bizalmi tartományon belül és kívül, aki a magyar közigazgatási nyilvános kulcsú infrastruktúrában kibocsátott tanúsítványokat ellenőrzi, alkalmazza.

A Szolgáltató az Érintett Féllel elsősorban a tanúsítványtáron keresztül tart kapcsolatot.

1.3.5 Egyéb szereplők

A Közigazgatási Gyökér Hitelesítés-Szolgáltató (KGyHSz) a magyar közigazgatásban használható tanúsítványokat kibocsátó hitelesítés-szolgáltatók szolgáltatókat felülhitelesítő szervezet.

A KGyHSz a felülhitelesítéssel igazolja, hogy a hitelesítés-szolgáltató adatait, valamint a megfelelő Hitelesítési rend és Szolgáltatási Szabályzat előírásainak megfelelőségét ellenőrizte, illetve hogy a felültanúsított hitelesítés-szolgáltató magára nézve kötelezőnek ismeri el a KGyHSz által kiadott szabályzatokat és a KGyHSz felügyeleti, ellenőrzési jogát.

1.4 Alkalmazhatóság

1.4.1 Engedélyezett alkalmazási lehetőségek

A kibocsátott végfelhasználói tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai kizárólag elektronikus dokumentumon (melybe egyéb nyilvános kulcsok nem értendők bele) elektronikus aláírások megtételére, míg a tanúsítványokban található nyilvános kulcsok az aláírások ellenőrzésére használhatók fel a tanúsítványban foglaltaknak megfelelően. (Lásd még 1.1.6 pont)

A Szolgáltatói aláíró tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai tanúsítványhitelesítésre és CRL listák hitelesítésére, a Szolgáltatói időbélyeg tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai időbélyegek kibocsátására, valamint a Szolgáltatói OCSP tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai az OCSP szolgáltatás hitelesítésére használhatók fel. A szolgáltatói viszontazonosítási aláíró tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai a viszontazonosítás (lásd 3.2.3.1 pont) során a megkereső hatóság részére küldött válasz aláírására használhatóak.

Jelen dokumentum egyúttal megfelel a közigazgatási felhasználásra vonatkozó követelményeknek ([3], [4], [18]), mely szerepel az NMHH Hivatala hatósági nyilvántartásában, a köztisztviselő és az ügyfél által használt, minősített aláíráshoz kapcsolódó hitelesítési rendek között. A külön jelzett („MHR_Ü”, „MHR_K”), szabályok alkalmazása esetén a kiadott tanúsítvány használható a közigazgatási ügyintézésben.

1.4.1.1 MHR_Ü, MHR_K

A fenti alkalmazási lehetőségeken túl a szolgáltatói viszontazonosítási aláíró tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai a viszontazonosítás (lásd 3.2.3.1 pont) során a megkereső hatóság részére küldött válasz aláírására is használhatóak.

1.4.2 Korlátozott alkalmazási lehetőségek

A Szolgáltató a jelen Szolgáltatási Szabályzatban leírt felhasználási feltételekkel korlátozza a kibocsátott tanúsítványok felhasználhatóságát (lásd 7.1.7 pont). A hatályos jogszabályok ugyancsak korlátozzák a kibocsátott tanúsítványok felhasználhatóságát.

Az egyes tanúsítványfajtáknak megfelelő konkrét korlátozásokat lásd még a tanúsítványfajtáknál (1.1.6 pont), illetve a tanúsítványfajtákhoz tartozó profiloknál (8. fejezet).

1.4.3 Tiltott alkalmazási lehetőségek

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

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

A szolgáltatói aláíró tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai csak tanúsítványhitelesítésre és CRL listák hitelesítésére használhatók, egyéb más szolgáltatás nyújtásához történő alkalmazása tilos. A szolgáltatói időbélyeg tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai csak időbélyegzés során használhatók fel, a szolgáltatói OCSP tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai pedig csak OCSP szolgáltatás során használhatók fel; egyéb más szolgáltatás nyújtásához történő alkalmazásuk tilos. A szolgáltatói viszontazonosítási aláíró tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai pedig csak a viszontazonosítás (lásd 3.2.3.1 pont) során, a megkereső hatóság részére küldött válasz aláírására használhatóak.

1.5 Kapcsolattartás

1.5.1 A Szolgáltató adatai

Név:	**NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság**
Egység:	NetLock Kft.
Székhely:	1023 Budapest, Zsigmond tér 10.
Telefon:	(40) 22-55-22
Fax:	(1) 700-1101
Internet cím:	www.netlock.hu
E-mail:	info@netlock.hu
Ügyfélfogadás/Nyitvatartás	Munkanapokon 9:00-17:00

1.5.2 Ügyfélszolgálat

A szolgáltatással kapcsolatos kérdésekkel, problémákkal a végfelhasználók a Központi Regisztrációs Egység ügyfélszolgálati munkatársaihoz fordulhatnak szóban vagy írásban. A Szolgáltató az Interneten információs szolgáltatást működtet.

A Szolgáltató Internetes információs rendszere, telefonközpontja és e-mail fiókjai minden nap 0–24 óráig fogadják a bejelentéseket. A Szolgáltató legkésőbb a bejelentést követő 3. munkanapon felveszi a kapcsolatot a bejelentővel (válasz e-mail cím vagy telefonszám birtokában) és a bejelentőt a tartalmi válasz megérkezésének várható idejéről is tájékoztatja.

A Szolgáltató ügyfélszolgálati munkatársai pontban meghatározott időpontban személyesen is fogadják az Ügyfeleket, Érintett Feleket, valamint az egyéb érdekelteket.

1.5.3 Szabályzattal kapcsolatos kérdések

A Szolgáltató szabályzatainak karbantartását a Szabályzat Elfogadó Egység végzi. A szabályzatokkal és szerződésekkel kapcsolatos kérdésekkel és észrevételekkel a regisztrációs egységek, a Szolgáltató ügyfélszolgálata vagy közvetlenül a Szabályzat Elfogadó Egység kereshető meg az info@netlock.hu e-mail címen (ld. még 1.3.1 pont).

1.5.4 Szabályzat-jóváhagyási eljárás

Lásd 10.7 pont.

1.6 Fogalmak és rövidítések

Fogalmak

- **Alany:** A tanúsítvány Alany (Subject) mezőjében megadott adatokkal meghatározott természetes személy, jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, illetve ezek képviselője, aki vagy amely 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.
- **Alárendelt elektronikus aláírással kapcsolatos szolgáltatások:** Olyan, a Törvény [1] hatálya alá tartozó szolgáltatás, melyet a szolgáltató entitás (alárendelt szolgáltató) saját nevében, de olyan módon nyújt, hogy egy másik szolgáltató entitás (jelen esetben a Szolgáltató) a szolgáltatás

nyújtására megállapodás alapján jelentős befolyással bír. A Szolgáltató ezen szolgáltatásait kizárólag előzetes - Hatóság felé történő - bejelentést követően nyújtja.

- **(Papír alapú) Aláírás-hitelesítés:** Az az eljárás, melynek során az Alany, vagy az őt képviselő természetes személy a személyazonosságának igazolása után a Szolgáltatási Szerződést a regisztrációs feladatot ellátó munkatárs, megbízott vagy közreműködő előtt kézjegyével ellátja, vagy a dokumentumokon levő aláírást a sajátjának ismeri el (a továbbiakban: aláírja), a regisztrációs feladatot ellátó munkatárs, megbízott vagy közreműködő pedig írásban igazolja az aláírás tényét, feltüntetve az aláíró személy személyazonosító adatait.
- **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.
- **Aláíró:** Lásd: Alany.
- **Alkalmazó Közösség:** A PKI rendszert alkalmazó, működtető entitások összessége.
- **Általános Szerződési Feltételek (ÁSZF):** A Szolgáltató szolgáltatásainak, tanúsítványainak igénybevételéhez szükséges feltételeket, illetve egyéb szerződési feltételeket leíró dokumentum.
- **Belépési Nyilatkozat:** Elsődlegesen az ÁSZF és a Szolgáltatási Szabályzat elfogadását jelző, aláírt dokumentum. A Belépési Nyilatkozat a Szolgáltató által meghatározott esetekben a Szolgáltatási Szerződéssel egyenértékűnek minősül (lásd: Szolgáltatási Szerződés).
- **Biztonságos aláírás-létrehozó eszköz (BALE):** A Törvény 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.
- **Common Name (CN):** Az Alany tanúsítványban szereplő, szokásos megnevezéséből képzett neve vagy az Alany által megjelölt álnévből képzett karaktersorozat.
- **CRL:** lásd: Tanúsítvány visszavonási lista
- **Distinguished Name (DN):** A tanúsítványban szereplő, szokásos megnevezéséből, lakóhely vagy székhely szerinti város, ország megnevezéséből, valamint e-mail címéből képzett egyedi neve. Az egyedi név komponensei személyes és munkatársi tanúsítvány esetén eltérhetnek.
- **Elektronikus aláírás:** Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat..
- **Ellenőrzési lépések:** Az elektronikus aláírás ellenőrzésekor kötelezően végrehajtandó lépések, melyeket a Szabályzat tartalmaz.
- **Előtanúsítvány:** A Szolgáltató által használt kifejezés azon ellenőrzött adathalmazra, mely a Szolgáltató elektronikus aláírásával ellátva tanúsítványt eredményez.
- **Eredeti példány:** Magán- vagy jogi személy azonosító okmány eredeti aláírásokat és pecsétet tartalmazó példánya, vagy ezek hitelesített másolata.
- **Érintett Fél: Az** a személy, aki elektronikus aláírás érvényességének ellenőrzése, illetve hiteles időpont megállapítása céljából a Szolgáltató által kibocsátott tanúsítványhoz, illetve időbélyeghez fordul.
- **Eszközszolgáltatás:** Az a szolgáltatás, melynek során a Szolgáltató a Törvény 6. § (1) bekezdésének c) pontja értelmében meghatározott, elektronikus aláíráshoz kapcsolódó aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatást végez.
- **Felhasználó:** Szerződéses partner, aki közvetlenül vagy közvetett módon, általa megbízott személyen keresztül igénybe veszi a Szolgáltató valamely szolgáltatását

- **Felügyelet**: Nemzeti Média- és Hírközlési Hatóság (röviditve: NMHH), a hitelesítés-, az időbélyegzés és az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatásokat nyújtó szolgáltatók felügyeleti szerve.
- **Fizikailag biztosított terület:** Olyan helyiség, amely ésszerű határok mellett képes megvédeni a benne elhelyezett eszközöket az elemi károktól, illetve a szándékos illetéktelen hozzáféréstől.
- **Fokozott biztonságú elektronikus aláírás**: Elektronikus aláírás, amely megfelel a következő követelményeknek:
  - alkalmas az Aláíró azonosítására és egyedülállóan hozzá köthető,
  - olyan eszközökkel hozták létre, amelyek kizárólag az Aláíró befolyása alatt állnak,
  - a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető.
- **Folyamatosan elérhető szolgáltatás**: Az év 365 napján a nap 24 órájában elérhető szolgáltatás , a Szolgáltató szabályzataiban meghatározott rendelkezésre állási időkkel.
- **Hash:** Ld. Lenyomat.
- **Hitelesítő Egységek**: A végfelhasználói tanúsítványokat létrehozó egységek a Szolgáltatónál.
- **Hitelesítési rend**: szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
- **Hozzáférések:** Egy adott számítógépes hálózat vagy annak egyes elemei elérésére vonatkozó szabályok összessége.
- **Hozzájáruló és Elfogadó Nyilatkozat:** Olyan, a minősített munkatársi tanúsítvány kibocstásához szükséges nyilatkozat, mellyel a természetes személyt az adott szervezet magához tartozónak ismeri el. Amennyiben a Szolgáltatási Szerződés a „munkatársi minősítésre" egyéb rendelkezéseket nem tartalmaz, akkor a Hozzájáruló és Elfogadó Nyilatkozat kitöltése kötelező.
- **Időbélyeg Szolgáltatás**: azon eljárás, melynek során a Szolgáltató a Szolgáltatási Szabályzatokban meghatározott módon az elektronikusan aláírt elektronikus dokumentumhoz időbélyegzőt kapcsol.
- **Időbélyegző**: az elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját. Az irat vagy dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető. Az elektronikus dokumentum egy adott pillanatban való létezését (időbélyegző elhelyezésének időpontja) kizárólag időbélyegzővel ellátott elektronikus dokumentum esetén lehet hitelesen megállapítani.
- **Időbélyegzési rend:** olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
- Igénylő: a Szolgáltató által nyújtott elektronikus aláírás hitelesítés-szolgáltatás igénybevételét kezdeményő Alany, vagy ezen célból annak nevében eljáró természetes személy.
- **Információbiztonsági irányítási rendszer**: irányítási rendszer egy szervezet vezetésére és szabályozására, az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése szempontjából.
- **Késedelem nélküli cselekedet**: A mindenkori technikai feltételek által megengedett lehető leggyorsabb intézkedést jelenti.
- **Ket.:** 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól és ennek végrehajtási rendeletei

- **Kihelyezett Regisztrációs Egység:** olyan, a Szolgáltatóval szerződéses jogviszonyban álló személy és/vagy szervezet, mely feladata, hogy a Szolgáltató munkáját segítse a tanúsítványkibocsátáshoz szükséges dokumentumok összegyűjtésében, ellássa a tanúsítvány kibocsátásával kapcsolatos koordinációs feladatokat, valamint – adott esetben – részt vegyen az ügyféllel való kapcsolattartásban.
- **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.
- **Láncolt hitelesítés-szolgáltatás:** A Törvény [1] hatálya alá tartozó, oly módon nyújtott hitelesítés-szolgáltatás, mely egy belföldi hitelesítés-szolgáltató szolgáltatói kulcsát egy, a szolgáltatótól elkülönülő másik belföldi szolgáltató entitás felülhitelesítette és ezzel a felülhitelesítő és a felülhitelesített között a tanúsítványhierarchiában alá-fölérendeltségi viszony jött létre. A Szolgáltató ezen szolgáltatásait kizárólag előzetes - Hatóság felé történő - bejelentést követően nyújtja.
- **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.
- **Magánkulcs védelme**: Mindazon tevékenységek összessége, melyek célja a magánkulcs megfelelő védelme, a magánkulcs teljes élettartama során annak generálásától, annak megsemmisítéséig, a hozzá tartozó tanúsítvány státuszától függetlenül.
- **Másodlagos Alany**: Az jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amely a munkatársi tanúsítvány esetében a természetes személy Alannyal együttesen szerepel a tanúsítványban és aki ezt az Alanyt saját magához tartozónak ismeri el.
- **Másolati példány**: Eredeti okmányról készült másolat.
- **Minősített elektronikus aláírás**: olyan - fokozott biztonságú - elektronikus aláírás, amelyet az Aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.
- **Munkatárs:** A természetes személyek azon köre, amelyeket egy adott szervezet saját magához tartozóként ismer el.
- **Munkatársi tanúsítvány**: Olyan személyes tanúsítvány melyben az abban szereplő természetes személyt a másodlagos Alany saját működési köre alá tartozónak ismeri el.
- **NetLock Minősített Hitelesítés-szolgáltatás**: Minősített tanúsítványok kibocsátása.
- **NetLock Minősített Időbélyeg Szolgáltatás**: Minősített időbélyeg kibocsátása elektronikus dokumentumokra.
- **Object Identifier (OID):** objektumok azonosítására használt, hierarchizált rendszer alapján definiált számsor.

- **OCSP (On-line Certificate Status Protokoll):** Valós idejű, on-line tanúsítvány állapot szolgáltatás. Az adott szolgáltatás keretében kibocsátott összes tanúsítvány aktuális visszavonási állapota (státusza) lekérdezhető. A lekérdezés azonnali, hiteles választ ad egy tanúsítvány állapotáról.
- **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.
- **PEM formátumú kérelem**: Szöveges formátumú tanúsítványkérelem.
- **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 Egység:** Az ügyfelek adatait összegyűjtő, ellenőrző, tanúsítvány kibocsátási, felfüggesztési, visszavonási kérelmeket összeállító és a Hitelesítő Egységhez továbbító egység.
- **Subject Name (SN):** Az Alany megnevezése, egyedi neve (DN).
- **Szabályzat Elfogadó Egység**: Jelen és más szabályzatok kialakításáért, elfogadásáért és adminisztrációjáért felelős szolgáltatói egység.
- **Személyes tanúsítvány:** Természetes személyek számára kibocsátott tanúsítvány, melyekbe foglalt nyilvános kulcs magán párja kizárólag elektronikus aláírás előállítására használható.
- **Szolgáltatási Szabályzat**: A [1] Törvény 2. § (20) alapján a Szolgáltató hitelesítési tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum (ld. 1.1.1).
- **Szolgáltatási Szerződés**: A Szolgáltató által nyújtott szolgáltatások igénybevételéhez szükséges dokumentum, melynek elfogadása és aláírása a szolgáltatás igénybevételének előfeltétele. A Szolgáltató által nyújtott szolgáltatások igénybe vétele Szolgáltatási Szerződés megkötése helyett Belépési Nyilatkozat (lásd fentebb) elfogadásával is történhet, továbbá Szolgáltató a Belépési Nyilatkozat elfogadását kötelezővé teheti.
- **Szolgáltató:** NetLock Kft., amely tevékenységi körében elsősorban tanúsítvány-szolgáltatást, eszközszolgáltatást, időbélyegzést végez.
- **Tanúsítvány:** A Szolgáltató által kibocsátott elektronikus igazolás, amely az aláírás-ellenőrző adatot a tanúsítvány Alanyához kapcsolja.
- **Tanúsítvány-szolgáltatás**: azon eljárás, melynek során a Szolgáltató a Szolgáltatási Szabályzatokban meghatározott eljárásban új vagy megújított, aláíró vagy egyéb célú tanúsítványt bocsát ki a felhasználó részére. A tanúsítvány-szolgáltatáshoz kapcsolódóan a Szolgáltató tanúsítványállapot-szolgáltatást is nyújt, melynek keretében fogadja a tanúsítvány-visszavonási- és felfüggesztési kérelmeket és a Szolgáltatási Szabályzatokban meghatározott időközönként Tanúsítvány Visszavonási Listát bocsát ki.
- **Tanúsítványfajta:** Jelen Szabályzat a tanúsítványok következő megjelenési formáiról rendelkezik: személyes, munkatársi .
- **Tanúsítványállapot-nyilvántartás**: A legközelebb kibocsátásra kerülő Tanúsítvány Visszavonási Lista tartalmához kapcsolt on-line lekérdezhető információk. Ezen információk joghatással nem bírnak.
- **Tanúsítványtár:** A végfelhasználói és szolgáltatói tanúsítványok, felfüggesztett, visszavont tanúsítványadatok, Szolgáltatói Szabályzatok publikálásáért, tárolásáért felelős alegység.
- **Tanúsítványok osztályai**: A Szolgáltató által végzett entitásazonosításhoz kapcsolódó ellenőrzési szintek megnevezése. A Szolgáltató által meghatározott aktuális tanúsítvány osztályok megjelölése

mindenkor megtalálható a Szolgáltató honlapján. Jelen Szabályzat kizárólag a minősített osztályra vonatkozik, emellett azonban a Szolgáltató nyújt nem minősített szolgáltatásokat is, melyekre külön szabályzatok vonatkoznak.

- **Tanúsítvány Visszavonási Lista (CRL – Certificate Revocation List):** Valamely okból visszavont, azaz érvénytelenített, illetve felfüggesztett, azaz ideiglenesen érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet meghatározott időközökkel a Szolgáltató bocsát ki.
- **Ügyfélmenü:** A Szolgáltató Internetes oldalain on-line regisztrációt követően létrejövő, az adott felhasználó saját kérelmeit, tanúsítványait és egyéb egyedi információit tartalmazó felhasználói profil.
- **Végfelhasználó:** Szerződéses partner, aki a Szolgáltató által kibocsátott végfelhasználói tanúsítvánnyal rendelkezik.
- **Végfelhasználói tanúsítvány**: A Szolgáltató által kibocsátott olyan tanúsítvány, amelyet az Alany kizárólag elektronikus aláírás előállítására használhat, de más tanúsítvány hitelesítésére nem.
- **Viszontazonosítás:** Azon eljárás, melynek során az ügyintéző hatóság megkeresésére a hitelesítés-szolgáltató összeveti az elektronikus aláírást használó ügyfélnek a hatóság által megküldött természetes azonosítóit az általa vezetett nyilvántartásban szereplő adatokkal és az adategyeztetés eredményét megküldi a hatóság részére.

2 Közzététel és tanúsítványtár

2.1 A Szolgáltatói információ közzététele

2.1.1 Közzétételi és tájékoztatási elvek

2.1.1.1 A szabályzatban nem tárgyalt elemek

Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti. Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen Szabályzat több ilyet is megemlít).

2.1.1.2 A Szabályzat közzététele

Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak tervezett hatályba lépését megelőzően megküldi a Felügyelet részére. A Szolgáltató alkalmanként ezt megelőzően is tájékoztathatja a Közösséget a tervezett változtatásairól. A jelen szabályzattal kapcsolatos közzéteendőket a 10.7.4 pont határozza meg.

2.1.1.3 Észrevételek kezelése

A közzétett szabályzatokkal kapcsolatos észrevételeket a Szolgáltató az info@netlock.hu címen fogadja. A Szabályzat észrevételekkel módosított változatát Szolgáltató az előző pont alapján teszi ismételten közzé.

2.1.2 Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában (Microsoft Word és PDF formátumokban) hozza nyilvánosságra Internetes oldalain keresztül (ld. 1.5 alfejezet). Itt a dokumentumok aktuális verziója mellett megtalálhatóak azok korábban érvényben lévő változatai is.

2.1.3 Rendkívüli információk közzététele

A Szolgáltató a következő eseményekről honlapján hirdetést jelentet meg:

- új szolgáltatás beindítása,
- valamely szolgáltatás tervezett beszüntetése vagy tartós (7 naptári napot meghaladó) szüneteltetése, ([1] Törvény 9. § 8. bek. alapján „A hitelesítés-szolgáltató tevékenységi köréből csak az új tanúsítvány kibocsátást szüneteltetheti.”),
- tevékenységének befejezése (ld. bővebben 6.8 alfejezet),
- rendkívüli üzemeltetési helyzetről tájékoztatás.

2.2 Tanúsítványokkal kapcsolatos információk

2.2.1 Tanúsítványok közzététele

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

- saját szolgáltatói tanúsítványát közzéteszi tanúsítványtárában, illetve kifüggeszti a vevőszolgálatán (ld. 1.5.1 alfejezet),

- minden hitelesítő egység tanúsítványát közzéteszi tanúsítványtárában, valamint Internetes honlapján keresztül.

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat csak abban az esetben teszi közzé a nyilvános tanúsítványtárában, ha az Alany és a másodlagos Alany ehhez a regisztrációs eljárás során hozzájárult.

2.2.2 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala

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

- saját fő (root) szolgáltatói tanúsítványainak állapotváltozásáról egy országos terjesztésű napilapban tesz közzé hirdetést, illetve az állapotváltozást saját tanúsítványtárában is feltünteti,
- egyéb szolgáltatói tanúsítványainak állapotváltozását a saját tanúsítványtárában tünteti fel,

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

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

2.2.3 Határidők meghatározása a tanúsítvány életciklusa kapcsán

A Szolgáltató egyes eljárási részcselekmények elvégzésére [pl. tanúsítvány meghosszabbításának kezdeményezése; az aláírt Szolgáltatási Szerződés (Belépési Nyilatkozat) Szolgáltatóhoz történő eljuttatására, stb.] határidőket írhat elő az Alanyok részére, melyeket a Szolgáltató az internetes oldalán (ld. 1.5 pont), illetve az Alanynak a regisztráció során megadott elektronikus levelezési címére küldött tájékoztatóban tesz közzé. Amennyiben az Alany nem tartja be a Szolgáltató által megjelölt határidőket, a tanúsítvánnyal kapcsolatos eljárási cselekmények késedelmes elvégzésének következményeit maga viseli, továbbá a Szolgáltató fenntartja magának a jogot, hogy a késedelmes ügyintézésért a Szolgáltató internetes oldalán közzétett mértékű külön eljárási díjat számoljon fel.

2.3 A közzététel gyakorisága

2.3.1 Kikötések és feltételek közzétételi gyakorisága

Jelen Szabályzattal kapcsolatos új verziók közzététele a 2.1 és 10.7 alfejezetben ismertetett eljárásoknak megfelelően történik.

Szolgáltató egyéb szabályzatai és szerződéses feltételei, illetve ezek újabb változatai szükség esetén kerülnek kibocsátására.

2.3.2 Rendkívüli információk közzétételi gyakorisága

Szolgáltató a rendkívüli információkat – amikor arra szükség van – a jogszabályi előírásoknak megfelelően, ennek hiányában késlekedés nélkül közzéteszi.

2.3.3 Tanúsítványok nyilvánosságra hozatalának gyakorisága

A Szolgáltató a minősített tanúsítványok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:

- saját szolgáltatói tanúsítványait a kibocsátást követő 10 munkanapon belül teszi közzé,

- az általa működtetett szolgáltatási egységek tanúsítványa a tanúsítványtárában és az Internetes honlapján (ld. 1.5.1 alfejezet) 10 munkanapon belül jelenik meg,
- a Szolgáltató a végfelhasználói tanúsítványokat a tanúsítványtárában az előállítást követően 10 munkanapon belül teszi közzé.
- Láncolt Hitelesítés-Szolgáltatás esetén a vonatkozó Szolgáltatási Utasításban, illetőleg Szolgáltatási Szabályzat Kiegészítésben a fentiektől el lehet térni.

2.3.4 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

A Szolgáltató az általa működtetett hitelesítő egységek és felhasználók 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 tanúsítványok és állapotinformációk elérése kapcsán az Érintett Felek részére a Szolgáltató által kibocsátott tanúsítványok, illetve időpont hitelesítésének ellenőrzésére jelen Szabályzat tartalmaz ajánlásokat (lásd 10.5.4 pont).

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

2.4.1 Tanúsítványtárak

A Szolgáltató az Érintett Felek számára a rendelkezésére álló legpontosabb adatokat biztosítja a lehetőségeknek, vállalásoknak megfelelően leghamarabb, és ennek érdekében nyilvános Tanúsítványtárat üzemeltet az Internet címén (lásd 1.5 pont). A tanúsítványtárban a Szolgáltató által kiadott tanúsítványok, a visszavont tanúsítványok listái, eljárási rendek, szerződési feltételek és más dokumentációk találhatók.

A Szolgáltató tanúsítványtára szabványos HTTP, illetve HTTPS protokollokkal érhető el a Szolgáltató Internetes oldalain keresztül (ld. 1.5 alfejezet), az ott megvalósított lekérdezési műveletekkel. A tanúsítványtár többszintű keresési lehetőséget biztosít a tárolt adatok eléréséhez.

A tanúsítványtár elérhetőségét Szolgáltató folyamatosan (az év minden napján, 0–24h) biztosítja a karbantartáshoz szükséges idők kivételével. A Szolgáltató a tervezett karbantartásokat munkaidőn kívüli időszakokra ütemezi, és ezekről a karbantartás megelőzően 24 órával értesítést tesz közzé honlapján.

A Szolgáltató a kibocsátott tanúsítványok nyilvántartása, a visszavonási nyilvántartások, valamint visszavonási állapot-közzététel legalább 99,9%-os rendelkezésre állással elérhetők, egyúttal az eseti szolgáltatás kiesések nem haladják meg a 3 órás időtartamot.

3 Azonosítás és hitelesítés

3.1 Elnevezések

A nevek regisztrációjának szabályai valamennyi tanúsítványfajtára vonatkoznak.

3.1.1 Névtípusok

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 egy szóköz választhatja el,
- a nevek ékezettel ellátottak vagy anélküliek,
- a nevek alapértelmezetten tanúsítványban az alábbiak szerint kerülnek feltüntetésre: a személyazonosság igazolására elfogadott hatósági igazolványban (lásd 3.2.3 pont), illetve a szervezeti azonosság igazolására szolgáló egyéb közokiratban foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve CN és - természetes személy esetén - opcionálisan SN mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév), UTF-8 kódolást használva; a nevek egyes egységeit egy szóköz választhatja el. Szolgáltató ettől kivételesen, egyedi esetben eltérhet.
- 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 szerepel, amennyiben lehetséges annak feltűntetése a tanúsítványtípus esetében, egyéb esetben nem kerül feltüntetésre,
- a „*State*” mezőben az ország, a megye vagy megyei jogú város neve kerülhet feltüntetésre, vagy nem kerül feltüntetésre
- a tanúsítvány Alany lakóhelyének, székhelyének ország megjelölésénél esetén a Szolgáltató az ISO 3166 [5] szabványban meghatározott kétkarakteres országkódot alkalmazza.
- a tanúsítvány „*SubjectAltname*” mezőjében szereplő elektronikus levelezési cím struktúrája megfelel az RFC 822 előírásainak.

3.1.1.1 MHR_Ü

Az általános szabályokat az alábbi eltérésekkel, illetve kiegészítésekkel kell alkalmazni:

- 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 SN mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév), az UTF-8 kódolást használva; a nevek egyes egységeit egy szóköz választhatja el,
- a „*State or province*” mező nem kerül feltüntetésre
- a „*Locality*” mezőben feltüntetésre kerül az Alany lakóhelyének vagy a másodlagos alany telephelyének városa, munkatársi tanúsítvány esetében,
- az „*Organization*” mezőben szerepelhet az másodlagos Alany, munkatársi tanúsítvány esetében,
- az „*Organization-unit*” mezőben szerepelhet az másodlagos Alany szervezeti egysége, munkatársi tanúsítvány esetében.

3.1.1.2 MHR_K

Az általános szabályokat az alábbi eltérésekkel, illetve kiegészítésekkel kell alkalmazni:

- 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 SN mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév), az UTF-8 kódolást használva; a nevek egyes egységeit egy szóköz választhatja el,
- a „*State or province*" mező nem kerül feltüntetésre,
- a „*Locality*" mezőben feltüntetésre kerül másodlagos Alany telephelyének városa,
- az „*Organization*" mezőben szerepel a másodlagos Alany közigazgatási szerv neve,
- az „*Organization-unit*" mezőben szerepel a másodlagos Alany közigazgatási szerv osztálya, illetve részlege.

3.1.1.3 Speciális szabályok a CertificatePolicies mező használatára vonatkozóan

Attól függően, hogy a tanúsítvány milyen aláírás-létrehozó eszközön került kibocsátásra, ezen mezőben a kibocsátásnak megfelelő, jelen szabályzat címlapján közzétett, megfelelő OID kerül feltüntetésre.

3.1.2 Álnév használata

A Szabályzat a Törvény [1], valamint a rendelet [4] rendelkezései alapján megengedi az álnév használatát a tanúsítványban.

A tanúsítvány Subject mezőjében álnév használata megengedett az "ALNEV" előtét, vagy a „(*)" utótag alkalmazása mellett. Az álnév feltünthethető a Pseudonym mezőben is, ez esetben a CN mező „álneves tanúsítvány" elnevezést tartalmaz.

Az álnevet az Alany választja, a Szolgáltató az álnevet nem ellenőrzi, az Alany az esetleges álnévvel kapcsolatos problémákért (szerzői jogi, .stb.) maga felel.

A Szolgáltató saját hatáskörében jogosult a jogi problémákba (akár valószínűsíthetően) ütköző álneves tanúsítvány kiadását megtagadni, a kiadott tanúsítványokat visszavonni.

3.1.3 Különböző elnevezési formák értelmezési szabályai

A Szolgáltató által kibocsátott tanúsítványoknak nem célja, hogy az alanyként megjelölt természetes személyek, jogi személyek, illetve jogi személyiség nélküli szervezetek számára digitális igazolványként funkcionáljon, illetve hogy őket kizárólag a tanúsítványban feltüntetett adatok alapján azonosítani lehessen. A munkatársi tanúsítvány önmagában képviseleti jogosultságot nem igazol.

Az azonosítók értelmezése érdekében Érintett Feleknek a jelen Szabályzatban leírtak alapján kell eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett Félnek segítségre van szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot. A Szolgáltató az Alany, illetve a másodlagos Alany egyéb adatairól többlettájékoztatást – a tanúsítványban feltüntetett adatok értelmezését segítő információn kívül – csak az erre vonatkozó felhatalmazás alapján ad ki (ld. 10.3.7 pont).

3.1.3.1 Kibocsátó azonosító

A kibocsátó azonosítója úgy értelmezendő, hogy a tanúsítványt a Szolgáltató, mint minősített Hitelesítés-szolgáltató hitelesítő egysége adta ki (székhely, elérhetőség: ld. 1.5 alfejezet). A tanúsítvány a jogszabályok szerinti minősített tanúsítványnak felel meg.

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

3.1.3.2 Alanyazonosító

Az Alany azonosítója úgy értelmezendő, hogy a tanúsítvány Alanya a *Common Name* nevű természetes személy, jogi személy vagy jogi személyiség nélküli szervezet, aki munkatársi, illetve szervezeti tanúsítvány esetén az *Organization* nevű szervezet O*rganization-unit* osztályához, illetve részlegéhez tartozik. Az azonosításban egyéb mezők is értelmezettek lehetnek. Amennyiben a szervezet gazdasági társaság, akkor ez az egység típusából látszódik.

A természetes személy nevei (családi, elő- és utóneve) – UTF-8 kódolással - olyan sorrendben szerepelnek a *Common Name* mezőben, ahogyan azok a személyazonosságát igazoló okmányban. A jogi személy, illetve a jogi személyiség nélküli szervezet neve – UTF-8 kódolással - olyan sorrendben szerepelnek a *Common Name* mezőben, ahogy a szervezetazonossági igazolására bemutatott okmányban.

A természetes személy lakóhelye, illetve a szervezet székhelye vagy telephelye a *Country* ország, *State* ország/megye, *Locality* településén található. Az Alany e-mail címe az Igénylő egységgel összefüggésben *E-mail*. Amennyiben a tanúsítványtípusnál lehetséges, 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.

3.1.4 A nevek egyedisége

A Szolgáltató a kibocsátott összes minősített tanúsítvány esetében a tanúsítványok Alanyait egymástól egyértelműen megkülönbözteti a tanúsítványban rögzített összes személyes adatuk (név, lakóhely ország, lakóhely város, e-mail cím, ha van, sorszám) segítségével (egyedi név).

3.1.4.1 Eljárások a nevekre vonatkozó vitás kérdések megoldására

Szolgáltató 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.

3.1.5 Védjegyek elismerése, hitelesítése és szerepe

Szolgáltató nem garantálja az ügyfelek számára védjegyeik feltüntetését a tanúsítványban. Az ügyfél részéről egy védjegy megszerzése nem tekinthető olyan eseménynek, amely szükségszerűen a tanúsítvány megújítását eredményezi.

A tanúsítványkérelemmel és elfogadással az ügyfél kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik személy jogait. Szolgáltatónak nem kötelessége a védjegyek jogos használatának az ellenőrzése.

3.2 Kezdeti azonosítás

3.2.1 A magánkulcs birtoklásának bizonyítási módszere

Az aláíró eszköz szolgáltatás és a hitelesítés-szolgáltatás esetében a Központi Regisztrációs Egység állítja elő az Alany számára a kulcspárt, így a Szolgáltató nem igényel bizonyítékot arra, hogy az Alany rendelkezik a hitelesítendő nyilvános kulcs magánkulcs párjával.

Amennyiben az ügyfél állítja elő a kulcspárt, úgy a Szolgáltató gondoskodik mindazon technikai és műszaki eljárás alkalmazásáról, melynek révén megbizonyosodhat arról, hogy az Igénylő ténylegesen birtokolja a nyilvános kulcshoz tartozó magánkulcsot.

A Szolgáltató – attól függetlenül, hogy a kulcspárt ki generálta – ellenőrzi, hogy a nyilvános kulcs korábban nem került-e kiosztásra más Alany számára.

3.2.2 Szervezeti azonosság hitelesítése

A Szolgáltató által kibocsátott munkatársi, illetve szervezeti tanúsítványban feltüntetésre kerül a felhasználó szervezet (másodlagos Alany). Opcionálisan egyéb adatok is feltüntetésre kerülhetnek.

A Szolgáltató a szervezetek azonosítását a 4.2.2 pont alatti táblázatban leírt módon végzi el.

3.2.2.1 Általános felhasználás esetén

Ha az Igénylő tanúsítványával kifejezetten jelezni kívánja, hogy ő egy adott szervezethez tartozik, akkor a személyazonosítás során fel kell mutatnia az adott szervezet nevében aláírásra jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében a tanúsítványt használja, az aláírásra jogosító aláírási címpéldányt, valamint a szervezet azonosságát is hitelesítő, közhiteles nyilvántartást vezető hatóság által kiadott igazolást.

Meghatározott szervezet nevében történő aláíráshoz igényelt tanúsítvány esetén az Igénylőnek fel kell mutatnia az adott szervezet nevében aláírásra jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében tanúsítványigénylést nyújthat be, ezen túlmenően az aláírásra jogosító aláírási címpéldányt, valamint a szervezet azonosságát is hitelesítő, közhiteles nyilvántartást vezető hatóság által kiadott igazolást.

A Szolgáltató weboldaláról (lásd 1.5.1 pont) letölthető az igényléshez szükséges meghatalmazás-minta.

Amennyiben az adott szervezet azonossága nem igazolható közhiteles nyilvántartást vezető hatóság által kiadott igazolással, úgy a szervezetet képviselő természetes személynek a személyazonosítás során fel kell mutatnia az adott szervezet által kiállított és közokiratba foglalt, a szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében a hitelesítés-szolgáltatónál előforduló ügyekben eljárjon, mely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti

3.2.2.2 MHR_K

A közigazgatási szerv nevében a tanúsítvány-kibocsátási eljárás során meghatalmazottként eljáró természetes személynek a személyazonosítás során fel kell mutatnia az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a hivatal képviseletében a hitelesítés-szolgáltatónál előforduló ügyekben eljárjon, mely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti

A Szolgáltató weboldaláról (lásd 1.5.1 pont) letölthető az igényléshez szükséges meghatalmazás-minta.

3.2.3 Személyazonosság hitelesítése

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

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

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

A regisztráció támogatására az Alany hozzájárulásával a személyazonosító dokumentumokról másolat készülhet, melyek archiválásra kerülnek. Amennyiben az Alany nem egyezik bele a másolat készítésébe, úgy a dokumentumokat személyesen is bemutathatja a Szolgáltató ügyfélszolgálatán a regisztrációs, vagy a mobil regisztrációt végző munkatársak előtt. A bemutatás megtagadása esetén a Szolgáltató a tanúsítványkiadási kérelmet elutasítja.

A személyazonosítás során a Szolgáltató regisztrációs munkatársai közhiteles nyilvántartásokban ellenőrzik a személyazonosság igazolására bemutatott dokumentumok azonosító adatait, a dokumentumok érvényességét, valamint hogy az ügyfél által megadott adatok megfelelnek-e a valóságnak.

3.2.3.1 MHR_Ü: természetes személy viszontazonosítása

A Szolgáltató a közigazgatásban felhasználható tanúsítványok esetében az ügyintéző hatóság elektronikus úton történő megkeresésére viszontazonosítást végez. Ennek során a Szolgáltató összeveti a megadott természetes személyazonosító adatokat az általa kezelt, beazonosított természetes személyazonosító adatokkal, és válaszként megküldi a hatóság részére, hogy a viszontazonosítás során megadott adatok megegyeznek-e az általa kezelt személyazonosító adatokkal.

A Szolgáltató a viszontazonosítási kérés során megvizsgálja az ügyintéző hatóság elektronikus aláírását és hiteles kérés esetén a választ haladéktalanul megküldi.

3.3 Azonosítás tanúsítvány kulcscseréje esetén

Tanúsítvány kulcscseréjét a szolgáltató alapesetben nem támogatja. Amennyiben kulcscsere válna szükségessé, abban az esetben új tanúsítvány-igénylést kell beadni, az ott meghatározott személyazonosítási szabályok szerint eljárva (lásd 4.2.2 pont).

3.4 Visszavonási kérelem

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

4 Működésre vonatkozó követelmények - tanúsítványok

4.1 Tanúsítványigénylés

4.1.1 Igénylés feltételei

Tanúsítványt igényelhet:

- természetes személy, saját részére,
- természetes személy saját részére, feltüntetve a tanúsítványban, hogy meghatározott szervezethez tartozik,
- természetes személy az általa képviselt szervezet részére
- közigazgatásban felhasználható tanúsítványt a természetes személy saját részére, feltüntetve a tanúsítványban, ha meghatározott szervezethez tartozik (MHR_Ü),
- közigazgatásban felhasználható tanúsítványt a köztisztviselő természetes személy feladata ellátásához, feltüntetve a tanúsítványban, hogy mely közigazgatási szervezet nevében jár el (MHR_K),
- közigazgatásban felhasználható tanúsítványt a hatóság a köztisztviselő természetes személy munkatársa részére, feltüntetve a tanúsítványban, hogy mely hatóság nevében jár el (MHR_K),

Kizárólag a jelen Szabályzatban megadott fajtájú és profilú tanúsítványok igényelhetők.

A regisztráció során a szolgáltatott adatok ugyan önkéntesek, de a már kibocsátott tanúsítványokhoz tartozó adatok a regisztrációs adatbázisból a Törvény [1] 9.§ (7) bekezdése alapján a kötelező megőrzési idő alatt nem törölhetők, még írásbeli kérés alapján – a tanúsítvány egyidejű visszavonása mellett – sem.

Az Igénylő köteles a tanúsítvány ellenértékét előre, a mindenkori díjtáblázatban fogalt díjak alapján a tanúsítvány kibocsátását megelőzően a Szolgáltató részére megfizetni. A díjfizetést megelőzően a tanúsítvány kibocsátásáról, annak egyéb feltételeiről (pl. külön eljárási díjáról) a Szolgáltató saját hatáskörén belül dönt. A tanúsítvány ellenértékének kiegyenlítésére vonatkozó szabályoktól a Szolgáltató egyedi esetekben, saját döntése alapján jogosult eltérni.

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, a tanúsítvány fajtájától függően ellenőrzött, illetve a Szolgáltató rendelkezésre álló és a tanúsítvány megújításának igénylése során (a megújítást igénylő űrlapon) érvényesnek elismert adatok alapján kerül sor.

A tanúsítványigénylés feltételeinek teljesülése esetén a Szolgáltató feldolgozza a tanúsítványkérelmet a következőkben bemutatott eljárásrend szerint.

A Szolgáltató a megadott elektronikus levelezési címre utasításokat továbbít, és erről a levelezési címről várja a tanúsítvány kiadására vonatkozó kérelem megerősítését.

4.2.1 Általános regisztrációs szabályok

A regisztrációs eljárásra vonatkozó alapelvek:

- az eljárást a Regisztrációs és Kézbesítési Megbízottak, Mobil Regisztrációs Munkatársak, a Kihelyezett Regisztrációs Egység és a Szolgáltató Központi Regisztrációs Egységének munkatársai végzik el,

- a regisztrációs eljárás biztonságát további közreműködők is segítik (pl. közjegyzők),
- az eljárást minden 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 Központi Regisztrációs Egység munkatársai végzik. A tanúsítványkérelmet a Központi Regisztrációs Egység adminisztrátorai felelősek kezelni, miután azonosították az alanyt a kapcsolódó tanúsítványfajta által meghatározott követelményeknek megfelelően.

A regisztráció és kibocsátás fő lépései a következők:

- az Igénylő regisztrálja magát a Szolgáltató Internetes oldalán vagy egyéb módon tanúsítványigénylést juttat el a Szolgáltatóhoz, melynek során elfogadja az Általános Szerződési Feltételeket (ld. 1.5 alfejezet); ehhez kapcsolódóan eljuttatja a szükséges személyazonosító, illetve szervezetazonosító dokumentumok másolatát a Szolgáltatóhoz vagy személyesen bemutatja azokat a Szolgáltató regisztrációs munkatársai előtt,
- a Szolgáltató fogadja a kérelmet, illetve ellenőrzi annak szabályosságát,
- a Szolgáltató azonosítja az Igénylő természetes személyt, és közhiteles nyilvántartásokban ellenőrzi a kérelmező által megadott személyes, illetve szervezeti adatokat,
- a Szolgáltató – amennyiben lehetséges és értelmezett – elektronikus úton ellenőrzi a kérelmező által megadott szervezeti adatokat,
- a Szolgáltató generál kulcspárt az Igénylő számára aláíró eszköz szolgáltatás (bővebben lásd: 1.1.8 pont) keretében,
- az Igénylő vagy a Regisztrációs Egység munkatársa elkészíti Szolgáltatási Szerződést, illetve a Regisztrációs Egység munkatársa előkészíti a további regisztrációhoz szükséges dokumentumokat, és azokat megküldi az Igénylőnek,
- a Szolgáltató egyidejű személyazonosítás elvégzésével átveszi az Alany és – amennyiben értelmezett - a Másodlagos Alany képviselője által aláírt Szolgáltatási Szerződését, valamint – amennyiben értelmezett - a Hozzájáruló és Elfogadó Nyilatkozatot,
- a Szolgáltató összeállítja a kibocsátandó tanúsítványt, azt felfüggeszti, majd a tanúsítványt a hordozóeszközre, illetve a Tanúsítványtárba tölti,
- eszközszolgáltatás esetén a Szolgáltató a hordozóeszközt az Igénylő kezéhez eljuttatja vagy személyesen megjelenve részére átadja, melynek során azonosítja az átvevő Igénylőt,
- a Szolgáltató aktiválja a tanúsítványt,
- a Szolgáltató dokumentálja a regisztrációs lépéseket.

Minősített tanúsítvány kibocsátása esetén a Szolgáltató ellenőrzi, hogy a közölt adatok hiteles regisztrációs szolgáltatótól származnak-e. Egyéb esetekben a Szolgáltató saját regisztrációs munkatársaival végzi a regisztrációt.

A tanúsítványkérelmet a regisztrációs munkatársak felelősek kezelni, miután azonosították az Alanyt a kapcsolódó tanúsítványfajta által meghatározott követelményeknek megfelelően.

A Szolgáltató nyilvántartásba veszi a következőket:

- az ügyfél által megadott cím és/vagy más elérhetőség,
- az Igénylő által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa és maguk a dokumentumok másolatai, amennyiben ehhez az Igénylő előzetesen hozzájárult;,
- a személyazonosító dokumentumok egyedi azonosító adatai, és azonosító számai, illetve a szervezet azonosítására alkalmas kódok, illetve számok,
- a kérelem és az azonosítási dokumentumok – beleértve az Aláíró féllel kötött megállapodást – másolatainak tárolási helyszíne,

- az Aláíró féllel kötött megállapodás esetleges specifikus választásai,
- az ügyfélnek a rá vonatkozó kötelezettségekkel történő egyetértése,
- amennyiben azt a Szolgáltató megköveteli, az ügyfél beleegyezése egy BALE felhasználására vonatkozóan,
- a kérelmet elfogadó egység azonosítója,
- a kérelem életciklusa során az Igénylővel folytatott elektronikus és hagyományos levelezés, kommunikáció (pl. telefon) naplója,
- minden, a tanúsítványok kiadásához kapcsolódó információ.

A Szolgáltató a nyilvántartásokat az ügyféllel közölt időpontig, illetve a jogszabályi előírásoknak megfelelően addig, ameddig a tanúsítványokra jogi eljárások során bizonyítási célból szükség lehet, megőrzi (ld. még 6.5 alfejezet).

4.2.2 Regisztrációs eljárás

Ügyféllel kötött szerződés keretében egyedi eljárás is kiköthető, melynek során az alábbi folyamattól el lehet térni, de az eltérés nem érintheti az eljárás lényegi részét.

Eljárási lépés	Tanúsítványfajta		
	Személyes	Munkatársi	Szervezeti
1. Regisztráció	Magánszemély adatainak (név, lakcím, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Alany a megküldött adatait alátámasztó dokumentumok másolatát megküldi vagy a Szolgáltató ügyfélszolgálatán a regisztrációs munkatársak előtt bemutatja. Végrehajtani jogosult: Központi Regisztrációs Egység.	Szervezeti munkatárs adatainak (név, lakcím, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Alany a megküldött adatait alátámasztó dokumentumok másolatát eljuttatja a Szolgáltatóhoz vagy a Szolgáltató ügyfélszolgálatán a regisztrációs munkatársak előtt bemutatja. Végrehajtani jogosult: és Központi Regisztrációs Egység.	Szervezet adatainak (név, székhely, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Alany a megküldött adatait alátámasztó dokumentumok másolatát eljuttatja a Szolgáltatóhoz vagy a Szolgáltató ügyfélszolgálatán a regisztrációs munkatársak előtt bemutatja. Végrehajtani jogosult: Igénylő munkatárs és Központi Regisztrációs Egység.
2. Kapcsolt regisztráció	Nincs	Szervezet adatainak (név, székhely, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Alany a megküldött adatait alátámasztó dokumentumok másolatát eljuttatja a Szolgáltatóhoz vagy a Szolgáltató ügyfélszolgálatán a regisztrációs munkatársak előtt bemutatja. Végrehajtani jogosult: Igénylő munkatárs és Központi Regisztrációs Egység.	Igénylő természetes személy adatainak (név, lakcím, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Alany a megküldött adatait alátámasztó dokumentumok másolatát eljuttatja a Szolgáltatóhoz vagy a Szolgáltató ügyfélszolgálatán a regisztrációs munkatársak előtt bemutatja. Végrehajtani jogosult: és Központi Regisztrációs Egység.
3. Automatikus visszaigazolások, e-mail cím ellenőrzése, amennyiben az Alany rendelkezik e-mail címmel.	A Szolgáltató automatikus válaszlevélben igazolja vissza a tanúsítvány iránti kérelmet. Az Igénylőnek a visszaigazolásra válaszlevelet kell küldenie. Végrehajtani jogosult: Természetes személy	A Szolgáltató automatikus válaszlevélben igazolja vissza a tanúsítvány iránti kérelmet. Az Igénylőnek a visszaigazolásra válaszlevelet kell küldenie. Végrehajtani jogosult: Igénylő munkatárs	A Szolgáltató automatikus válaszlevélben igazolja vissza a tanúsítvány iránti kérelmet. Az Igénylőnek a visszaigazolásra válaszlevelet kell küldenie. Végrehajtani jogosult: Igénylő munkatárs
4. Természetes személy azonosítása, adatainak ellenőrzése közhiteles nyilvántartásban	Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa		
5. Szervezet azonosítása, adatainak ellenőrzése közhiteles nyilvántartásban	Nincs	Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa	Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa
6. Kulcspár generálása eszközön és kérelem készítése	Végrehajtani jogosult: Természetes személy vagy Központi Regisztrációs Egység	Végrehajtani jogosult: Igénylő munkatárs vagy Központi Regisztrációs Egység	Végrehajtani jogosult: Igénylő vagy Központi Regisztrációs Egység
7. Ügyfélcsomag (PIN boríték, adatlap, számla, tájékoztató, hozzájáruló és elfogadó nyilatkozat, Szolgáltatási Szerződés) összeállítása és megküldése az aláírónak	Végrehajtani jogosult: Központi Regisztrációs Egység		

Eljárási lépés	Tanúsítványfajta		
	Személyes	Munkatársi	Szervezeti
8. Szolgáltatási Szerződés aláírás-hitelesített aláírása a Központi, a Mobil Regisztrációs Egység, vagy közjegyző előtt	Végrehajtani jogosult: Természetes személy	Végrehajtani jogosult: Igénylő munkatárs	Végrehajtani jogosult: Igénylő
9. Személyazonosság ellenőrzése, a személyazonosító igazolványban szereplő fénykép megfeleltetése az Igénylőnek; a személyazonosító igazolványban szereplő aláírás összevetése a Szolgáltatási Szerződésen levővel, Szolgáltató előtti személyes megjelenés során	Végrehajtani jogosult: Alany választása szerint Központi Regisztrációs Egység, Mobil Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Regisztrációs		
10. A Szolgáltatóhoz beérkezett, aláírás hitelesített Szolgáltatási Szerződés, illetve annak kiállításának alapjául használt dokumentumok másolatainak ellenőrzése	Végrehajtani jogosult: Központi Regisztrációs Egység		
11. Tanúsítvány előállítása	Végrehajtani jogosult: Hitelesítő Egység		
12. Tanúsítvány felfüggesztése	Végrehajtani jogosult: Automatikusan vagy a Központi Regisztrációs Egység által		
13. Tanúsítvány hordozó eszközre való letöltése	Végrehajtani jogosult: az igénylő természetes személy Központi Regisztrációs Egység által		
14. Tanúsítvány tanúsítványtárban való közzététele	Végrehajtani jogosult: Automatikusan vagy a Központi Regisztrációs Egység által		
15. Hordozóeszköz eljuttatása az aláíróhoz vagy személyes átvétel	Végrehajtani jogosult: Alany választása szerint Központi Regisztrációs Egység, Mobil Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Regisztrációs- és kézbesítési megbízott		
16. Tanúsítvány (re)aktiválása	Végrehajtani jogosult: Központi Regisztrációs Egység		
17. Dokumentáció	Tanúsítvány adatösszesítő lap, Igénylőlap, közokiratba foglalt,aláírás hitelesített, vagy elektronikus aláírással hitelesített Szolgáltatási Szerződés, Személyes (és szervezeti) dokumentumösszesítő adatlap, Okmánymásolatok, E-mail cím ellenőrzés kinyomtatva vagy egyéb megfelelő módon igazolva (Hozzájáruló és elfogadó nyilatkozat)		

4.2.3 Szolgáltatási Szerződés

Az Alany és a magánkulcs összetartozásának dokumentálására, illetve a kötelező tájékoztatásra a Szolgáltató Szolgáltatási Szerződést alkalmaz. A szerződés feltételeit az ÁSZF[14], jelen Szolgáltatási Szabályzat, illetve az Aláíró elfogadó nyilatkozata (Belépési Nyilatkozat / Szolgáltatási Szerződés) tartalmazza. A Szolgáltató ezen dokumentumokat az Igénylő részére történő elektronikus rendelkezésre bocsátásával az abban foglaltakat magára nézve kötelezőnek fogadja el. A Szolgáltatási Szerződést ezen dokumentumok együttese jelenti. Az Alany részéről feltételeket elfogadó nyilatkozat kapcsán a Központi, a Kihelyezett vagy a Mobil Regisztrációs Egység munkatársai, Regisztrációs és Kézbesítési Megbízott vagy az ügyfél választása szerinti közjegyző aláírás-hitelesítést végeznek, vagy az Alany elektronikus aláírását ellenőrzik. A tanúsítvány kiadásának feltétele ezen szerződés létrejötte. A Szolgáltatási Szerződés akkor lép hatályba, ha az ügyfél a Szolgáltató, vagy annak egyéb regisztrációs egységei előtt személyesen megjelent és azonosítása Szolgáltató által megtörtént.

A Szolgáltató előtti személyes megjelenés és ügyfél azonosítás jogszabályi előírás folytán kötelező, még a tanúsítvány kiadása előtt. Az ügyfél választása szerint ez teljesül:

- a Központi Resztrációs Egység munkatársa előtt, a Szolgáltató székhelyén, vagy
- Mobil regisztráció keretében a Mobil Regisztrációs Adminisztrátor előtt, vagy
- Regisztrációs és Kézbesítési Megbízott előtt, vagy
- Kihelyezett Regisztrációs egység székhelyén.

A Szolgáltató az internetes oldalán, illetve az ügyfél-tájékoztató dokumentumokban közzéteszi, hogy az általa nyújtott szolgáltatások és szolgáltatáscsomagok során kiadott tanúsítványokat milyen módon lehet aláírás-hitelesítve aláírni. A Szolgáltató bizonyos feltételek esetében (pl. a tanúsítvánnyal az egy alkalommal, egyszerre vállalható kötelezettség meghatározott mértéke) kötelezően előírhatja, hogy a Központi vagy Mobil Regisztrációs Egység munkatársai vagy közjegyző előtt aláírás-hitelesített Szolgáltatási Szerződést fogad csak el; illetve meghatározott okirati formát követelhet meg.

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.

A nyilvános kulcs lenyomat karaktereinek átírása:

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

Az elfogadó nyilatkozatot az Igénylő természetes személy vagy a szervezet törvényes, illetve meghatalmazott képviselője írja alá.

4.2.3.1 Elfogadó nyilatkozat minták

A Szolgáltató kérésre megküldi a személyes és munkatársi Közjegyzői Okiratba foglalt vagy aláírás hitelesítésre előkészített elfogadó nyilatkozati mintákat.

4.2.4 A tanúsítványkérelmek jóváhagyásának követelményei

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

- benyújtották a kérelmét a tanúsítvány kibocsátónak,

- az Alany (akinek nevében az Igénylő természetes személy eljár) azonos a kérelemben szereplő alannyal,
- munkatársi tanúsítvány esetén a másodlagos Alany hozzájárult a kibocsátáshoz,
- a kérelemben szereplő adatok ellenőrizhetők és pontosak.

4.2.5 A tanúsítványok tartalma

A tanúsítványok tartalmazzák az alábbiakat:

- a tanúsítvány azonosító kódját,
- a Szolgáltató megnevezését, benne székhelyének ország-azonosítóját,
- azt, hogy a tanúsítvány minősített tanúsítvány,
- a tanúsítvány érvényességi idejének kezdetét és végét (amely nem lehet az érvényesség kezdete időpontnál korábbi); a minősített tanúsítvány érvényességi ideje nem haladja meg a tanúsított aláírás-ellenőrző adathoz kapcsolható aláírás-létrehozó eszközzel összefüggésben meghatározott érvényességi időt, de legfeljebb a kibocsátástól számított két évet,
- minősített tanúsítvány esetében a tanúsítvány vonatkozásában fennálló megőrzési feladatra vonatkozó adatot,
- az Alany nevét
- amennyiben engedélyezett, az álnevét (MHR_Ü és MHR_K hitelesítési rendeknek megfelelő tanúsítványokban nem engedélyezett),
- az Aláírónak külön jogszabályban, illetve a Szabályzatban, illetőleg az Általános Szerződési Feltételekben meghatározott speciális jellemzőit, a tanúsítvány szándékolt felhasználásától függően,
- azt az aláírás-ellenőrző adatot (nyilvános kulcs), amely az Aláíró által birtokolt aláírást készítő adat párjának (magánkulcs) felel meg,
- a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
- az adott tanúsítványt kibocsátó Hitelesítés-szolgáltató elektronikus aláírását.

4.2.6 A tanúsítványok jellemzői

A Szolgáltató által kibocsátott tanúsítványok megfelelnek a következő követelményeknek:

- a tanúsítványazonosító a kibocsátóra nézve egyedi,
- a tanúsítványban foglalt megkülönböztetett név (DN, Distinguished Name) egyedi,
- a kiadott tanúsítványokhoz tartozó kulcsok egyediek, ez alól természetesen kivételt jelent a megújított tanúsítványban szereplő kulcs
- a minősített tanúsítványok megfelelnek a ETSI TS 101 862-ben [8] meghatározott tanúsítványprofiloknak (ld. 8. alfejezet),
- a közigazgatásban használható tanúsítványok megfelelnek a közigazgatásban alkalmazható végfelhasználói tanúsítványok adattartalmára vonatkozó IHM-ajánlásban[21] meghatározott tanúsítványprofiloknak
- a minősített tanúsítványok a Szolgáltató minősített tanúsítvány aláíró kulcsával vannak aláírva,
- a tanúsítványok aláírása ellenőrizhető a tanúsítványban szereplő adatok és a Szolgáltató megfelelő nyilvános kulcsának felhasználásával.

4.2.7 Az Igénylő (Alany) tájékoztatása a kibocsátást megelőzően

A Szolgáltató a tanúsítvány Igénylőjét (Alanyát) magyar nyelven, közérthetően és egyértelműen írásban (a szabályzatok elektronikus publikálásával, és azok az ügyfélszolgálaton nyomtatott formában történő elhelyezésével) tájékoztatja a következőkről:

- a tanúsítványok felhasználásával kapcsolatos alapvető előnyök,
- a szolgáltatás igénybevételének feltételei,
- a szolgáltatási díj,
- az Alany 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, amennyiben a tanúsítvány kibocsátását kérő ezt a Szolgáltatótól szerzi be,
- az Aláíró és az aláírást ellenőrizni kívánó felek felelőssége, kötelezettségei,
- a hitelesítési és kapcsolódó szabályzatok és jogszabályok tartalma, szerepe, elérésének módja,
- a Szolgáltató minősítései,
- a tanúsítvány minősített státusza, ennek joghatásai,
- a tanúsítványok visszavonásának, felfüggesztésének lehetősége,
- a szolgáltatói nyilvános kulcs, valamint annak elérhetősége,
- a panaszok benyújtására, a jogviták rendezésére vonatkozó szabályok,
- a Szolgáltató önkéntes akkreditációs rendszer keretében szerzett esetleges tanúsításai.

Ezen adatoknak külön jogszabályban meghatározott körét az Aláíróval jogviszonyban álló vagy jogviszonyt létesíteni kívánó harmadik személy számára kérésre is hozzáférhetővé teszi a Szolgáltató. Az Aláíró és Érintett Felek figyelmét a Szolgáltató külön felhívja az alábbiakra:

- ha a hitelesítés-szolgáltatási rend nem nyilvános használatra szolgál,
- ha a hitelesítési rend megköveteli egy adott BALE használatát,
- ha a jelen követelményrendszer alapján meghatározott tanúsítvány alaptípusokat érintő előírások szűkítésére, illetve további követelmények támasztására kerül sor.

4.2.8 Tanúsítványkérelmek elutasítása

A Szolgáltató elutasítja a tanúsítványkérelmeket, amennyiben

- a tanúsítványigénylés nem teljes,
- a tanúsítványigénylés nem helyes,
- a jelen Szabályzatban felsorolt feltételek (ld. 4.2.4 pont) teljesülése nem bizonyítható az igényelt tanúsítvány fajtájának előírt módon,
- a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a személy szervezethez tartozása nem egyértelmű,
- a személy és/vagy szervezet kiléte nem állapítható meg minden kétséget kizáróan,
- az Igénylő felhatalmazása a tanúsítvány kibocsátásának kérésére nem egyértelmű,

- az Alany vagy a másodlagos Alany nem járul hozzá másolat készítéséhez az okmányairól, és azokat nem mutatja be személyesen a Szolgáltató regisztrációs egységeinek munkatársai előtt sem.

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

4.2.9 A tanúsítványokra vonatkozó további rendelkezések

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

4.2.9.1 MHR_K

Amennyiben a hatóságot képviselő természetes személy kezdeményezte a tanúsítványigénylést, úgy a Szolgáltató a regisztrációról köteles a meghatalmazást kiállító hatóságot a tanúsítvány kibocsátásának tényéről, valamint a meghatalmazásban foglalt iktatószámról értesíteni.

4.3 A tanúsítványok kibocsátása és hozzáférhetővé tétele

A Regisztrációs és Hitelesítő egységek a 4.2.2 pontban leírt módon feldolgozzák a kérelmet, illetve előállítják a tanúsítványt. Erről az Alany külön értesítést kap. A kész tanúsítvány a Tanúsítványtárba kerül, ahonnan Internetes felületen keresztül Internet böngésző szoftver segítségével is letölthető (ld. még 2.2 alfejezet).

A Szolgáltató regisztrációs egységei a nem teljesített tanúsítványigénylésekről értesítést kapnak a hiba okának megjelölésével hibaüzenet formájában.

4.3.1 A tanúsítvány kibocsátásának időpontja

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

4.3.2 A tanúsítvány érvényessége

A tanúsítványban szereplő nyilvános kulcs magán párja csak a tanúsítványban megjelölt időintervallumban 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 és/vagy a magánkulcsot, illetve a tanúsítványt átvette.

4.4.2 A tanúsítványigénylő nyilatkozata

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

- ismeri, érti és elfogadja jelen és kapcsolódó szabályzatokat,
- a tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályoknak és törvényi előírásoknak megfelelően használja,
- minden adat, amit a Szolgáltatónak a tanúsítvány kiadásának céljából átadott, a valóságnak megfelel, és azok átadása önkéntes volt,
- amennyiben a hitelesítési rend lehetővé teszi az álnév használatát, a választott álnév mások jogait nem sérti,
- a tanúsítványban szereplő minden adat a tudomásával és egyetértésével került a tanúsítványba,
- a tanúsítvány érvényességét befolyásoló tényekről, valamint az igénylés során megadott személyes és szervezeti adatok megváltozása esetén haladéktalanul értesíti a Szolgáltatót,
- tisztában van azzal, hogy a magánkulcs védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége, s ezzel kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
- minden aláírás az elfogadott és érvényes (nem felfüggesztett, visszavont vagy lejárt) tanúsítványba foglalt nyilvános kulcs magán párjával készül,
- minden egyes elektronikus aláírást, amely a tanúsítványban szereplő nyilvános kulcs magán párjával készült, a saját aláírásának ismeri el,
- jogosulatlan személy nem férhet hozzá magánkulcsához,
- ismeri az elektronikus aláírás megfelelő használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,
- tudomása van arról, hogy a minősített elektronikus aláírással, illetve a minősített tanúsítványon alapuló fokozott biztonságú aláírással ellátott elektronikus okiratok a teljes bizonyító erejű 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; hacsak erről külön írásbeli szerződésben a Szolgáltatóval meg nem egyezett,
- amennyiben az Alany beleegyezett a tanúsítvány nyilvánosságra hozatalába, felhatalmazza a Szolgáltatót a tanúsítvány közzétételével, és saját vagy más nyilvános tanúsítványgyűjtő helyeken történő elhelyezésével.

4.4.3 Tanúsítvány közzététele

A Szolgáltató csak abban az esetben teszi közzé a kiadott tanúsítványt, ha a tanúsítvány előfizetője, illetve Alanya ehhez előzetesen hozzájárult.

4.5 A kulcspár és a tanúsítvány használata

4.5.1 Az Alanyok számára szóló előírások

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

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

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

a) magánkulcsát és tanúsítványát csak a hitelesítés-szolgáltatóval szerződésben rögzített korlátozásnak megfelelően használhatja,

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

4.5.1.1 Elektronikus aláírás készítése

Az elektronikusan aláírt dokumentum előállításának folyamatáért elsősorban az Aláíró a felelős. Az Aláíró 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 ha a tanúsítványban feltüntetésre került, a másodlagos Alany felel.

4.5.1.2 Magánkulcs megőrzése

Az elektronikus aláírás csak akkor biztonságos, ha a magánkulcs az Aláírón kívül soha, senki más számára nem hozzáférhető. A kulcsot jelszóval kódoltan és hardvervédelemmel kell ellátni: ezen feltételeket a BALE eszköz teljesíti. A kulcs elvesztéséből, véletlen vagy szándékos nyilvánosságra hozatalából eredő károkért az Aláíró felelős. A kulcs kompromittálódását az előírt módon a Szolgáltatónál be kell jelenteni. A szabályosan bejelentett letiltási kérelem után a jelen Szabályzat 4.9.1 pontjában meghatározott módon felel a felmerült károkért az Aláíró, a másodlagos Alany, illetve a Szolgáltató.

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:

- a Szolgáltató az Általános Szerződési Feltételek és a Szabályzat nyilvánosságra hozatalával,
- az Aláíró a Szolgáltatási Szerződés aláírásával, a tanúsítványkérelem benyújtásával, illetve a tanúsítvány elfogadásával,
- az Érintett Fél az aláírás ellenőrzéséhez szükséges tanúsítvány, illetve az aláírt dokumentum elfogadásával.

4.5.2 Az Érintett Felek számára szóló ajánlások

Nem érvényes elektronikus aláírás esetén, melynek ellenőrzéséhez jelen szabályzat tartalmaz ajánlásokat az elfogadásból eredő minden kár és kockázat az Érintett Felet terheli (lásd még 10.5.4 és 10.6.3 pont).

4.6 Tanúsítvány megújítása

4.6.1 Végfelhasználói tanúsítványok

4.6.1.1 Egyszerűsített megújítás

A végfelhasználói tanúsítványok megújítására a kezdeti ellenőrzési lépések ismételt lefolytatása nélkül kizárólag a jelen pontban leírt módon van lehetőség, egy alkalommal, a megújítást megelőzően alkalmazott érvényességi idő megadásával.

Az alábbi eljárás alkalmazása a feltételek teljesítése esetén sem jelent kötelezettséget az Alany számára, csupán lehetőséget.

4.6.1.1.1 Általános feltételek

A tanúsítvány-megújítás általános feltételei:

- a tanúsítvány korábban nem volt megújítva;
- az Alany korábbiakban tanúsított nyilvános kulcsának kriptográfiai biztonsága még megfelelő az új tanúsítvány tervezett élettartamára, és nincs utalás arra vonatkozóan, hogy az Aláíró magánkulcsa kompromittálódott (hitelét vesztette).
- az Alany, illetve a másodlagos Alany tanúsítványba foglalt adatai, valamint az ezeket igazoló azonosító dokumentumai érvényesek és az abban foglalt adatok nem változtak a tanúsítvány-igénylés óta;
- a tanúsítvány érvényessége még nem járt le;
- a tanúsítvány nem szerepel a visszavonási listán.

4.6.1.1.2 Rendkívüli tanúsítvány-megújítás

A fentieken túl a Szolgáltató – fenntartva a jogot a Szolgáltató internetes oldalán feltüntetett mindenkori külön eljárási díj kivetésére – biztosíthatja a korábban még meg nem újított tanúsítvány egyszerűsített módon történő megújítását abban az esetben, ha az Alany, illetve a másodlagos Alany kiléte, illetve adatai változatlanok maradtak.

4.6.1.1.3 A tanúsítvány-megújítási eljárás

A megújítás során az Alany az Ügyfélmenüből letölthető, az Alany adatait tartalmazó Szolgáltatási Szerződést (Belépési Nyilatkozatot) és – a Szolgáltató erre vonatkozó előírása esetén - a kibocsátáskor megadott adatainak változatlanságáról szóló nyilatkozatot tartalmazó dokumentumot a még érvényes kulcspárja segítségével elektronikusan aláírja és ezeket elektronikus úton eljuttatja a Szolgáltatónak. Ha az Alanynak, illetve a másodlagos Alanynak az adatok változatlanságáról szóló nyilatkozatban feltüntetett adatai a 4.6.1.1.2-as pontban meghatározott mértékben megváltoztak, úgy a nyilatkozatban jelezni kell a megváltozott adatokat és csatolni kell mellékletként a változott adatok igazolását.

Az adatok változatlanságáról szóló nyilatkozatot kinyomtatva és aláírva, a Szolgáltatási Szerződést kinyomtatva és a tanúsítványra vonatkozó előírásnak (lásd 0 pont) megfelelő módon aláírás-hitelesítve kell visszajuttatni a Szolgálathoz, ha az Alany nem rendelkezik érvényes aláíró tanúsítvánnyal, vagy nem áll módjában elektronikusan aláírással ellátni az Ügyfélmenüből letölthető, az Alany adatait tartalmazó Szolgáltatási Szerződést (Belépési Nyilatkozatot) és a kibocsátáskor megadott adatainak változatlanságáról szóló nyilatkozatot tartalmazó dokumentumot.

A Szolgáltató a beérkezett dokumentumok alapján közhiteles, elektronikus nyilvántartásokban ellenőrzi, hogy az Alany és a másodlagos Alany azonosságának igazolására használt információ még mindig érvényes. Amennyiben a Szolgáltató a közhiteles nyilvántartásokban történő ellenőrzés során a kibocsátáskor megadott adatok változását észleli, az egyszerűsített tanúsítvány-megújítási kérelmet elutasítja, illetve fenntartja a jogot az újbóli, ezennel már a valóságnak megfelelő adatokat tartalmazó megújítási kérelem teljesítése esetén az internetes oldalán feltüntetett mindenkori különeljárási díj felszámítására.

Amennyiben a Szolgáltató bármely feltétele, illetve kikötése megváltozott, a változásról a Szolgáltató a tanúsítvány megújítása során tájékoztatja az Alanyt, illetve a másodlagos Alanyt.

A tanúsítvány-megújítás során a Szolgáltató garantálja a feldolgozás biztonságát a tanúsítvány-helyettesítési támadás ellen.

4.6.1.2 Megújítás új igénylés beadásával

Az alábbi esetekben megújításra nincs lehetőség egyszerűsített megújításra és új tanúsítvány-igénylés (lásd 4.2.2 pont) beadása szükséges:

- az Alany körülményei nem felelnek meg az egyszerűsített eljárásban (lásd 4.6.1.1 pont) támasztott feltételeknek;
- az Alanynak, illetve a másodlagos Alanynak az adatok változatlanságáról szóló nyilatkozatban feltüntetett adatai nem egyeznek meg a közhiteles nyilvántartások adataival; ez esetben .a Szolgáltató fenntartja a jogot az újbóli, ezennel már a valóságnak megfelelő adatokat tartalmazó megújítási kérelem teljesítése esetén az internetes oldalán feltüntetett mindenkori különeljárási díj felszámítására.

4.6.1.3 MHR_Ü, MHR_K

A tanúsítvány megújítására a 4.6.1.1.1, 4.6.1.1.3 és 4.6.1.2 pontok irányadóak.

4.6.2 Szolgáltatói tanúsítványok

A Szolgáltató saját tanúsítványait legfeljebb egy alkalommal, alkalmanként a megújítást megelőzően alkalmazott érvényességi idő megadásával újítja meg.

4.7 Kulcscsere

A kulcscsere az a folyamat, amelynek során a Szolgáltató úgy bocsát ki egy megújított tanúsítványt, hogy abban az eredeti tanúsítvány Alanyra vonatkozó adatai közül csak a nyilvános kulcs kerül lecserélésre.

Kulcscsere esetére a Szolgáltató nem állapít meg külön eljárási szabályokat (lásd 3.3 pont). Amennyiben a tanúsítványban szereplő nyilvános kulcsot le kell cserélni, azt a Szolgáltató új tanúsítvány-igénylési kérelemként kezeli.

4.8 Tanúsítvány módosítása

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

Tanúsítvány módosítására a Szolgáltató nem állapít meg külön eljárási szabályokat. Amennyiben a tanúsítványban szereplő adatok – a nyilvános kulcs kivételével – lecserélése szükségessé válik, azt a Szolgáltató új tanúsítvány-igénylési kérelemként kezeli.

4.9 Tanúsítvány felfüggesztése és visszavonása

4.9.1 Általános rendelkezések

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

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

A visszavont, illetve felfüggesztett tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. Amennyiben van rá lehetőség, a visszavont tanúsítványhoz tartozó

magánkulcsot a visszavonást követően azonnal meg kell semmisíteni (ld. még 4.11 pont). A felfüggesztett, visszavont vagy lejárt tanúsítványokban szereplő nyilvános kulcsokat kizárólag addig lehet aláírás ellenőrzésre használni, amíg azok kriptográfiai biztonsága megfelelő.

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

- a visszavonási/felfüggesztési kérelem Szolgáltatóhoz történő megérkezéséig az Általános Szerződési Feltételeknek és jelen szabályzatnak megfelelően az Alany, illetve a másodlagos Alany felelős a felmerülő károkért,
- a visszavonási és felfüggesztési kérelem, Szolgáltató általi befogadását követően a nyilvánosságra hozatalig a Szolgáltató felelős a felmerülő károkért,
- az érvénytelen állapot tanúsítványtárban való megjelenése után az Érintett Fél felelős a felmerülő károkért.

4.9.2 A visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásához a következő körülmények vezetnek:

- végfelhasználói vagy szolgáltatói magánkulcs kompromittálódása, vagy a kompromittálódás gyanúja,
- a tanúsítvány Alanyának (Alany vagy másodlagos Alany) kérelme,
- a tanúsítvány használatának visszautasítása hibás tanúsítvány miatt,
- a Szolgáltató tudomására jutott tény, vagy megalapozott vélelem a regisztrációs adatok valótlanságáról,
- a tanúsítványban foglalt adatok megváltozása,
- a tanúsítvány felfüggesztési idejének lejárata,
- az Alany és a másodlagos Alany kötelezettségeinek be nem tartása,
- rosszhiszemű felhasználás, ,
- a Felügyelet bíróság vagy más hatóság erre vonatkozó jogerős és végrehajtható határozata,
- a felhasználói szerződés megszűnése,
- a hitelesítési szolgáltatás 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 és Felfüggesztést kérheti
Végfelhasználói személyes aláíró tanúsítvány	Alany, Szolgáltató, Felügyelet
Végfelhasználói munkatársi aláíró tanúsítvány	Alany, Másodlagos Alany, Szolgáltató, Felügyelet
Végfelhasználói szervezeti aláíró tanúsítvány	Alany, Szolgáltató, Felügyelet
Szolgáltatói tanúsítványok	Szolgáltató, Felügyelet

4.9.4 Visszavonási kérelemre vonatkozó eljárás

Végfelhasználói tanúsítvány visszavonása egy visszavonási kérelem Szolgáltató számára történő benyújtásával kezdeményezhető. A visszavonási kérelem benyújtható:

Ügyfélszolgálati időben:

- személyesen, a Szolgáltató székhelyén, a Központi Regisztrációs Egységnél,

Ügyfélszolgálati időben és azon kívül:

- telefonon, a Szolgáltató ügyeleti rendszerén keresztül, folyamatosan, 0-24 órában
- a Szolgáltatónak küldött e-mailben, illetve faxon,
- a Szolgáltató székhelyére küldött levélben.

A visszavonási kérelemnek legalább a következő adatokat kell tartalmaznia:

- a tanúsítvány sorszáma vagy egyedi neve,
- a visszavonást kérő megnevezése,
- a visszavonást kérő elérhetősége,
- a visszavonást kérő kapcsolata a tanúsítvány Alanyával,
- a visszavonás oka,

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

A visszavonási eljárás során a Szolgáltató Központi Regisztrációs Egysége ellenőrzi a visszavonási kérelemben szereplő adatokat, a kérelmező személyazonosságát, a kérelem előterjesztésére való jogosultságot, a kérelemben foglalt indokok (ld. 4.9.2 pont) valóságalapját, illetve visszavonásra való alkalmasságát. A kérelemre vonatkozó fenti adatokat a Szolgáltató 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 Szolgáltató a tanúsítvány visszavonását megtagadja.

Helyes és hiteles kérelem esetén a Szolgáltató további mérlegelés nélkül intézkedik a tanúsítvány visszavonása érdekében: a visszavonási kérelmek azonnal végrehajtásra kerülnek, a tanúsítvány visszavont státusza bekerül a tanúsítványtárba (ún. tanúsítványállapot-adatbázisba), ezzel lehetővé téve a valós idejű visszavonási állapot ellenőrzést.

Szolgáltató minden végrehajtott és visszautasított állapotváltoztatási kérelemről e-mailben értesíti az Alanyt (a tanúsítványtárban szereplő e-mail címen), illetve a másodlagos Alanyt, valamint a visszavonás kérelmezőjét. A visszavonási állapotváltoztatásnál az értesítést telefonon, regisztrációnál megadott számon is megkísérli a Szolgáltató.

4.9.5 Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási lépések – figyelemmel az alábbiakban foglaltakra - a lehetséges legkisebb késlekedéssel követik egymást.

- A faxon, e-mailben, illetve postai úton érkezett visszavonási kérelmeket a Szolgáltató folyamatosan fogadja, feldolgozásukat azonban munkaidőben végzi, a munkaidőn túl érkezett kérelmeket a következő munkanapon bírálja el.
- A telefonon, illetve az Ügyfélmenün keresztül érkezett visszavonási kérelmeket a Szolgáltató folyamatosan fogadja és haladéktalanul megkezdi azok feldolgozását, a feldolgozás nem függ a Szolgáltató ügyfélszolgálati idejétől.
- A feldolgozás megkezdése és a tanúsítvány státuszváltásról való döntést követően Szolgáltató a tanúsítványállapot-adatbázist szükség esetén késedelem nélkül frissíti.

Az emberi beavatkozást Igénylő visszavonási kérelmek feldolgozásának ideje legfeljebb 3 óra. Amennyiben ezen időszak alatt a Szolgáltató önhibáján kívül nem képes a visszavonási vagy felfüggesztési kérelem jogszerűségéről – a benyújtó személy jogosultságáról vagy a visszavonást indokoló tény valóságalapjáról - megbizonyosodni, úgy a továbbiakban – ellenkező tény tudomására

jutásáig – a visszavonási kérelmet illetéktelen személytől származónak tekinti, és a visszavonási vagy felfüggesztési folyamatot eredménytelenként lezárja.

A visszavont tanúsítvány státusza azonnal bekerül a tanúsítványtárba (ún. tanúsítványállapot-adatbázisba), ezzel lehetővé téve a valós idejű visszavonási állapot ellenőrzést. A tanúsítványállapot-változást követő legkésőbb 1 órán belül új visszavonási lista kiadására is sor kerül, mely ugyancsak tartalmazza a tanúsítvány megváltozott státuszát.

4.9.6 Visszavonásra vonatkozó egyéb szabályok

A visszavonási kérés és válasz üzeneteket a Szolgáltató védi a visszajátszáson alapuló támadások ellen.

A Szolgáltató rendszerei ésszerű határokon belül képesek üzemzavar vagy katasztrófa esetén is minden kibocsátott tanúsítvány visszavonására.

A minősített tanúsítvány aláíró, az infrastrukturális és az időbélyegzéshez használt kulcsokhoz tartozó tanúsítványok visszavonása kettős ellenőrzés mellett történik.

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

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

4.9.7 A felfüggesztés körülményei

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

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

4.9.8 Felfüggesztés kérelmezése

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

4.9.9 Felfüggesztési kérelemre vonatkozó eljárás

A felfüggesztési kérelem a visszavonási kérelemhez hasonlóan (lásd előzőekben) nyújtható be Szolgáltatóhoz, továbbá a felfüggesztés esetében lehetőség van automata felfüggesztési rendszer igénybe vételére is. Harmadik fél által történő beadás esetén Szolgáltató a rendelkezésére álló eszközökkel meggyőződik a személy kilétéről, a felfüggesztési kérelem jogosságáról. A felfüggesztési kérelmet a visszavonási kérelemmel megegyező módon dolgozza fel Szolgáltató, ha azonban az automata felfüggesztési rendszer útján történik a felfüggesztés akkor, annak jogosult használata esetén a kérelemre vonatkozó 4.9.4. pontban részletezett adatokat a Szolgáltató egyéb módon nem vizsgálja.

Automatikus felfüggesztés esetén a felfüggesztés automatikusan, Szolgáltatói humán közreműködés nélkül hajtódik végre. Az automata felfüggesztési rendszer használatával beadott kérelmeket azonnal teljesíti.

Az automatikus, humán beavatkozást nem Igénylő felfüggesztési kérelem feldolgozása nem függ a Szolgáltató ügyfélszolgálati idejétől, a rendszer jogosult használatával történt bejelentéseket a Szolgáltató azonnal, mérlegelés nélkül végrehajtja. Az automatikus rendszerben indított kérelmek bejelentése és a valamint a tanúsítvány státuszának tanúsítványállapot-adatbázisba való bekerülése között normál üzemmenet esetén nem telik el több, mint 5 perc; rendkívüli üzemeltetési helyzet esetére az 6.7.4 pontban vállalt határidő az irányadó.

4.9.10 A felfüggesztés időtartamára vonatkozó korlátozások

Érvényes tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 5 munkanapig. Ez alól a kibocsátás során a Szolgáltató általi technikai felfüggesztés időtartama jelent kivételt, mely során a tanúsítvány legfeljebb 30 naptári napig lehet felfüggesztett állapotban. Ezen technikai felfüggesztésre csak egy alkalommal kerülhet sor és a tanúsítvány kibocsátásától annak aktiválásáig tart. Minden egyéb esetben a felfüggesztés ideje legfeljebb 5 munkanap lehet. A tanúsítvány visszavonásáról, illetve újbóli érvényesre állításáról Szolgáltatónak a lehető leghamarabb intézkednie kell. A felfüggesztett állapot kezdő időpontja a felfüggesztési kérelem elfogadásától számítandó. Ha ez idő alatt a visszavonáshoz vezető körülmények gyanúja cáfolatot nem nyer, Szolgáltató a tanúsítványt visszavonja.

A Szolgáltató honlapján keresztül kezdeményezett automatikus tanúsítvány felfüggesztés annak sikeres kezdeményezése időpontjától számított 5 munkanapig lehet felfüggesztett állapotban, ezen idő elteltét követően a tanúsítvány automatikusan visszavonásra kerül.

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

4.9.10.1 Újraérvényesítés módja

A tanúsítvány újbóli érvénybe helyezését az Alany és – adott esetben - a másodlagos Alany kérelmezheti a visszavonásra vonatkozó eljárási rend szerinti módon és az ott minimálisan előírt adatok megküldése révén.

4.9.11 Kulcskompromittálódás esetére vonatkozó speciális követelmények

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

4.10 Tanúsítvány-állapot információk közzététele

4.10.1 Tanúsítvány Visszavonási Lista (CRL)

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

- A Szolgáltató a CRL listán jelöli annak érvényességi idejét. CRL egy előző CRL érvényességi ideje alatt is kibocsátható. Amennyiben egy időben több érvényes CRL is létezik, a legutolsó az irányadó.
- A CRL tartalmazhatja a tanúsítvány visszavonásának okát.
- A Szolgáltató a visszavont tanúsítványok listáját a crl1.netlock.hu, crl2.netlock.hu és crl3.netlock.hu internet címeken (URL) publikálja.
- A Szolgáltató feltüntetheti a tanúsítványokban az internet címeket (URL) is, amelyeken keresztül elérhető a visszavont tanúsítványok listája (a feltüntetés a CDP mezőben történik), egyes címek elérhetetlensége esetén a soron következő elérhetőt kell használni.
- 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 elfogadása az Érintett Fél önhibájának minősül, így az ebből adódó kárért felel.

- A Szolgáltató az egyes CRL-eket a kapcsolódó egyéb adatok megőrzési idejével megegyező ideig őrzi meg (ld. 6.5.2 pont).

A visszavonási listán azon visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre, amelyek érvényességi ideje még nem járt le. Ezen kívül Szolgáltató kibocsáthat olyan visszavonási listákat, melyeken az összes visszavont tanúsítvány (érvényességi idejüktől függetlenül), illetve a kibocsátás pillanatában felfüggesztett tanúsítványok kerülnek feltüntetésre.

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

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

A visszavonási listák mindig tartalmazzák a következő lista kibocsátásnak idejét, melyet megelőzve is kibocsáthat Szolgáltató új listát. A listák érvényességi ideje legfeljebb 24 óra.

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

Szolgáltató gyökértanúsítványait biztonsági okokból off-line módon tárolja, biztonságos - zárt – zónában. Gyökértanúsítványok esetén ezért a CRL kiadás sűrűsége és a lista érvényessége a többi rendszertől eltér. Ezen CRL listák kibocsátása között sem telhet el több mint 30 nap. Mivel azonban az automata rendszerek által vizsgált tanúsítványok esetén az aláírást hitelesítő teljes tanúsítványláncolat ellenőrzése így hosszabb időt vehet igénybe, ezért Szolgáltató fenntartja magának a lehetőséget arra, hogy - a gyökértanúsítvány által kibocsátott tanúsítványokra - delegált CRL aláíró tanúsítványt bocsásson ki, illetve azonnali OCSP válasszal tegye lehetővé a tanúsítványláncolat ellenőrzését.

4.10.1.1 MHR_Ü, MHR_K

A fenti szabályok az alábbi eltéréssel alkalmazandóak:

- A Szolgáltató a tanúsítványokban feltüntetheti az OCSP szolgáltatás internetes elérhetőségeit (URL).

4.10.2 Az ajánlott CRL ellenőrzés 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.

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

4.10.3 Valós idejű visszavonási állapot ellenőrzés elérhetősége

A Szolgáltató valós idejű visszavonási állapot-szolgáltatásokat is nyújt, melyet egyrészt a tanúsítványállapot-nyilvántartáson keresztül, másrészt az OCSP szolgáltatás segítségével érhető el.

A tanúsítványállapot-nyilvántartás a Szolgáltató tanúsítványtárán keresztül érhető el.

A Szolgáltató a tanúsítványállapot-adatbázisa lekérdezéséhez támogatja az OCSP (Online Certificate Status Protocol,[19]) protokollt. Az OCSP szolgáltatás elérhető a kiadóhoz tartozó OCSP válaszadó internet címén, valamint a tanúsítványtárban közzétett egyéb címeken. Az aktuális OCSP válaszadó tanúsítványok és a rájuk vonatkozó visszavonási listák a Szolgáltató tanúsítványtárában érhetőek el.

A Szolgáltató feltüntetheti a tanúsítványokban az internet címeket (URL) is, amelyeken keresztül elérhető a a valós idejű visszavonási állapot ellenőrzés (a tanúsítvány AIA:OCSP mezőjében kerül feltüntetésre), a címek közül egyik elérhetetlensége esetén a következő elérhetőt kell használni.

4.10.4 Valós idejű visszavonás ellenőrzési követelmények

A tanúsítványállapot-adatbázis bárki számára hozzáférhető, kereshető a Szolgáltató tanúsítványtárán keresztül. Az adatbázisban mindig a keresett tanúsítvány aktuális állapota található.

Az OCSP válaszokat aláíró tanúsítványok profilját a 8.1 pont tartalmazza. Az OCSP szolgáltatás által kiadott, elektronikusan aláírt válaszokat az Érintett Félnek ellenőriznie kell, melynek lépéseit a 10.5.4 pont tartalmazza. Az érvénytelennek bizonyult OCSP válaszokat elfogadni nem szabad, ez esetben a tanúsítványállapot-adatbázis adataira, illetve a visszavonási listákra kell támaszkodni.

A valós idejű visszavonás szolgáltatások hozzáférési díjait a 10.1 pont tartalmazza.

4.10.5 A visszavonási információ közzétételének egyéb formái

A visszavonási hirdetmények csak a Szolgáltató tanúsítványtárában és annak biztonsági másolatában, illetve két másik tárban érhetők el. A Szolgáltató saját szolgáltatói tanúsítványának állapotváltozásáról, egy országos terjesztésű napilapban hirdetést tesz közzé.

4.11 Tanúsítvány-előfizetés vége

A Szolgáltató által kiadott tanúsítványok érvényességi ideje és az adott tanúsítvány előfizetési ideje összekapcsolódik, vagyis az előfizetési idő megegyezik a tanúsítványban feltüntetett érvényességgel. Mindez nem zárja ki természetesen, hogy a Szolgáltató – kivételesen, egyedileg meghatározott esetben – a tanúsítványok díjaira vonatkozóan különböző fizetési kedvezményeket határozzon meg (pl. részletfizetés, kedvezmény stb.).

Amennyiben az Alany még a tanúsítványban feltüntetett érvényességi idő lejárta előtt kívánja lemondani az előfizetést, úgy a tanúsítvány visszavonására vonatkozó szabályok az irányadóak (lásd 4.9 pont). A visszavonással egy időben a Szolgáltatási Szerződés megszűnik.

Ha az tanúsítvány érvényességének lejártakor az Alany a Szolgáltató előírásai szerint (lásd 4.6.1 pont) nem újítja meg a tanúsítványt, a Szolgáltatási Szerződés automatikusan megszűnik.

4.12 Kulcs letétbe helyezése és visszaállítása

Szolgáltató nem nyújt minősített magánkulcs letéti szolgáltatást, illetve az Alany aláíró minősített magánkulcsát semmilyen más módon nem tárolja el vagy menti.

A Szolgáltató a saját, szolgáltatói magánkulcsait elmentve is tárolja.

5 Működésre vonatkozó követelmények - időbélyegzés

A Szolgáltató minősített időbélyeg-szolgáltatást jelen szabályzat előírásai alapján nyújt. Jelen pontban nem szabályozott kérdésekre a tanúsítvány szolgáltatásnál leírtakat értelemszerűen kell alkalmazni.

5.1 Időbélyeg-szolgáltatás igénylése

Minősített időbélyeg-szolgáltatást természetes személy, vagy szervezet egyaránt igényelhet, személyesen a Szolgáltató székhelyén (Ld:1.5), telefonon, e-mail-ben, faxon, levélben.

Az igénybevételre két módon kerülhet sor:

- a Szolgáltatóval történő eseti megállapodás, vagy
- a Szolgáltató által nyújtott ajánlatok, csomagok elfogadott megrendelése keretében.

Az igénylés Szolgáltatóhoz való beérkezésétől számított 15 napon belül a Szolgáltató felveszi a kapcsolatot az Igénylővel, s az ajánlatot elfogadja, az Igénylőt felszólítja hiánypótlásra, pontosításra.

A Szolgáltató döntése szerint az ajánlatot visszautasítja, amennyiben az Igénylő a hiánypótlási, pontosítási felszólításnak 15 napon belül nem tesz eleget, a Szolgáltatóval szemben a Szolgáltatás korábbi igénybevételéből eredően díjtartozása van, vagy amennyiben a szolgáltatás nyújtásával más ügyfelek kiszolgálása veszélybe kerül.

5.2 Az időbélyeg- szolgáltatás teljesítése

Szolgáltató az RFC3161 [17]szabványon alapuló időbélyeg kérelmeket fogad és időbélyeg válaszokat ad. Az időbélyeg kérelmek előállításához illetve az időbélyeg válaszok fogadásához, ellenőrzéséhez szükséges programokkal, program modulokkal, infrastruktúrával a Felhasználónak kell rendelkeznie.

A Szolgáltató időbélyegzés-szolgáltatás nyújtása során biztosítja, hogy az időbélyeg válasz – az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve – ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott. Az időbélyegzés szolgáltatás során a Szolgáltató - a technológia jellegéből adódóan - nem ismeri meg az időbélyeggel ellátott dokumentum tartalmát, csak az abból képzett lenyomatot.

Az általános paraméterű időbélyeg-szolgáltatás nyilvános interneten, a Szolgáltató által adott egyedi URL címen keresztül érhető el. Szolgáltató speciális szolgáltatásokat is nyújt, vállalásokat tesz (pl. rendelkezésre állási vállalások, mennyiségi garanciák, speciális szolgáltatás elérési módok és profilok), az általános paraméterű szolgáltatástól való eltérés feltételeit azonban külön megállapodásban kell rögzíteni.

Az időbélyeg-szolgáltatás keretében adott időbélyegek száma az egyedi szerződésben foglaltak, illetve az adott csomagban megjelölt mennyiség. Amennyiben az ügyfél ennél többet kíván igénybe venni ezen többlet időbélyeg mennyiséget a Szolgáltató kiszolgálhatja, de kötelezettsége csak akkor keletkezik, ha

- egyedi megállapodás esetében, azt szerződésbe foglalják,
- csomag esetében, akkor ha az ügyfél kiegészítő csomagot írásban igényelte és azt a Szolgáltató visszaigazolta. Az aktuális kiegészítő csomagokról a Szolgáltató honlapján (lásd:1.5) tájékozódhat.

Felhasználó vállalja, hogy az időbélyegzés szolgáltatáshoz hozzáférést más személyeknek vagy szervezeteknek semmilyen formában sem közvetve, sem közvetlenül nem enged. Felhasználó vállalja a szolgáltatási díjak megfizetését, valamint elfogadja, hogy a szolgáltatás díjának megfizetését nem tagadhatja meg arra való hivatkozással, hogy érdekkörébe tartozó területen és eszközökön keresztül jogosulatlan személy vette igénybe a jelen szerződés tárgyát képező szolgáltatást. Felhasználó vállalja továbbá, hogy amennyiben a kiválasztott időbélyeg csomag(ok)ban meghatározott időbélyeg

mennyiségnél több időbélyeget vesz igénybe, úgy azon időbélyeg díjcsomag ellenértékét is köteles megfizetni, amelyet az adott hónapban ténylegesen igénybevett.

5.3 Minősített Időbélyeg-szolgáltatás joghatása

Az [1] Törvény alapján, amennyiben az időbélyegzést olyan szolgáltató végezte, amely az időbélyegzéskor e szolgáltatás tekintetében a szolgáltatók nyilvántartásában minősítettként szerepelt és az időbélyegző ellenőrzésének eredményéből más nem következik, az ellenkező bizonyításáig vélelmezni kell, hogy a dokumentumban foglalt adatok az időbélyegző elhelyezése óta változatlan formában léteztek.

6 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A kockázatok csökkentése érdekében Szolgáltató az általa biztosított szolgáltatásokhoz szükséges hardver, szoftver, illetve egyéb eszközeit két, fizikailag egymástól elkülönült helyszínen, egy elsődleges és egy másodlagos helyszínen (second site) tárolja. A két helyszín biztonsági előírására vonatkozó szabályok egyenszilárdságúak, az esetleges eltérések a megfelelő pontoknál feltüntetésre kerültek. Ezen túlmenően a Szolgáltató több helyszínen alárendelt elektronikus aláírással kapcsolatos szolgáltatást nyújt – ezen szolgáltatások pontos helyszínei, illetve a szolgáltatásokra vonatkozó nyilvános szabályzatok megtalálhatóak a Szolgáltató honlapján.

A regisztrációs és hitelesítő egységek 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.

Az egységek adatállományairól biztonsági mentések készülnek (ld. 6.5 alfejezet). A mentéseket a Szolgáltató a 6.5.2 pontban meghatározott ideig megőrzi.

Az alábbi szolgáltatásokat biztosító rendszerek ellenállnak az egyszeres meghibásodásnak: tanúsítvány kibocsátás, visszavonás kezelés, visszavonási állapot-közzététel. E szolgáltatások minősített tanúsítványok esetén legalább 99,9%-os rendelkezésre állással elérhetők, egyúttal az eseti szolgáltatás kiesések nem haladják meg a 3 órás időtartamot (lásd még 6.7.4 pont).

A biztonsági szabályokra vonatkozó rendelkezéseket a nem nyilvános Biztonsági Szabályzat tartalmazza.

A folyamatos, magas színvonalú biztonságos szolgáltatás fenntartására a Szolgáltató ISO 27001 (korábban BS 7799-2:2002 elnevezésű) szabványnak megfelelő információbiztonsági irányítási rendszert alkalmaz, amelyet független külső és belső auditorok vizsgálnak folyamatosan, továbbá ISO 9001 szabvány szerinti minőségirányítási rendszert üzemeltet.

6.1 Fizikai óvintézkedések

A fizikai óvintézkedések célja a Szolgáltató bizalmas információira és fizikai körleteire irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a Szolgáltató rendszerében. A biztosított védelem arányban áll a Szolgáltató által végzett kockázatelemzésben megállapított kockázatokkal.

6.1.1 A telephely elhelyezése és szerkezeti felépítése

A Szolgáltató védett számítógép termében valósítják meg a leginkább veszélyeztetett szolgáltatásokat. Ezt a számítógéptermet speciálisan erre a célra tervezték és alakították ki, és tervezésénél sok különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés, beléptetés ellenőrzése és felügyelete, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, stb.) egységes érvényesítésére került sor. Illetéktelen személyek nehezen juthatnak be, a biztonsági őrség viszont rövid idő alatt meg tudja közelíteni riasztás esetén. A biztonsági körletnek nincs ablaka, a bejárati ajtókon kívül csak a különösen erős fal bontásával lehetne behatolni ide.

6.1.2 A Second Site elhelyezése és szerkezeti felépítése

A Szolgáltató másodlagos helyszíne egy védett számítógép teremben található szerver széfben található. Ezt a másodlagos helyszínt speciálisan erre a célra tervezték és alakították ki, és tervezésénél sok különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés, beléptetés ellenőrzése és felügyelete, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, stb.) egységes érvényesítésére került sor. Illetéktelen személyek nehezen juthatnak be, a biztonsági őrség viszont rövid idő alatt meg tudja közelíteni riasztás esetén. A biztonsági körletnek (szerverszéf) nincs ablaka, az ajtókon kívül csak az erős fal bontásával lehetne behatolni ide.

6.1.3 Fizikai hozzáférés

A területek pontos paramétereit, illetve a belépni jogosultak listáját a mindenkori belső operációs dokumentumok tartalmazzák. A bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és kísérettel léphetnek be. A belépések biometrikus azonosításra épülő beléptető rendszeren (kivéve másodlagos helyszín) keresztül történnek a belépések naplózásával. A helyiség kétszerezett (redundáns) klíma-, automata tűzoltó, továbbá illetéktelen behatolást jelző (riasztó) berendezéssel van ellátva. Az eszközök többszörösen túlbiztosított elektromos energiaellátással rendelkeznek. A biztonsági körletet beléptető zsilipét 24 órás videó kamerás megfigyelő rendszer is védi.

A másodlagos helyszín beléptetési rendszere biometrikus beléptető automatizmussal nem rendelkezik, de az egyenszilárdság megőrzésére, a másodlagos helyszínt biztonságát állandó élőerős védelem biztosítja.

6.1.4 Áramellátás és légkondicionálás

6.1.4.1 Áramellátás

A Szolgáltató védett számítógép termének zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében. Ez a következő – egységes tervezéssel megalapozott, a vonatkozó szabványoknak megfelelő – védelmi megoldások együttműködésével biztosított:

- szünetmentes energiaellátás,
- zárlati leoldásra szelektív áramkörök,
- villamos zavar, villám és túlfeszültség védelem.

A szünetmentes energiaellátást biztosító rendszer felépítése a következő:

- dízel gépes áramfejlesztő,
- lokális akkumulátoros szünetmentes tápegység,
- redundáns tápválasztó.

Az alkalmazott üzemmód pedig az alábbi:

- az üzemi táp kimaradása vagy csökkenése esetén a rendszer átkapcsol a tartalék tápra,
- ezalatt a rendszer elindítja az áramfejlesztőt,
- amikor az üzemi táp ismét használható (5 percen keresztül folyamatosan), akkor a rendszer visszatér rá.

Zárlati leoldásra szelektív áramkörök segítségével a gépteremben több egymástól független működésű rendszer lett kialakítva a folyamatos üzemeltetés támogatására. Az elosztó hálózat úgy lett megtervezve, hogy egy eszközcsoport zárlata esetén csak a zárlatot okozó eszközcsoport legyen áramtalanítva, a többi hibátlan eszközcsoport üzemben maradjon.

6.1.4.2 EMC védelem

A villamos zavar, villám és túlfeszültség védelem szempontjából a gépterem nagy értékű, kritikus szolgáltatásokat biztosító berendezései védve vannak a különböző vezetett és sugárzott villamos zavarok, villámok miatt bekövetkező túlfeszültség hatásai ellen. A rendszert külön mechanizmusok védik a villámok által keltett elektromágneses impulzusok (EMI) hatása ellen. A védelem alapfogalmait az MSZ IEC 1312-1, nem kötelező szabvány írja le.

Az üzemeltetett berendezések a sugárzott elektromágneses zavarás elleni védelem (ezt az elektromágneses összeférhetőségnek (EMC) nevezett tulajdonságot az MSZ IEC 1000-1-1 szabvány tárgyalja részletesen) mindkét elvárását teljesítik:

- egyrészt védettek az üzemelési környezetükben jelen levő hatások ellen,
- másrészt nem bocsátanak ki olyan zavaró elektromágneses jeleket, amely a környezetükben üzemelő többi berendezés működését zavarhatná.

Az üzemeltetett berendezéseket a gépterem elektromágneses zavarvédelme továbbá védi az elektromágneses kisugárzással történő kompromittálódás (lehallgatás) ellen.

6.1.4.3 Légkondicionálás

A Szolgáltató biztosítja a géptermek épülettől független légkondicionálását. A védett számítógéptermek üzemi hűtésigényének kiszolgálását ipari klímaberendezések biztosítják. A folyamatos üzemvitelt egy második (tartalék) klímaberendezés is támogatja, mely szükség esetén működésbe lép. A klímaberendezések elhelyezésének módja biztosítja, hogy azok karbantartása ne okozzon zavart a gépterem működésében.

6.1.5 Beázás és elárasztódás veszélyeztetettsége

A biztonsági körletek kialakítása során külön szempont volt az elárasztódás veszélyének minimalizálása. A védett számítógép teremben a fenti biztonságot tovább növeli az álpadló alkalmazása.

6.1.6 Tűzmegelőzés és tűzvédelem

A géptermet befogadó épületben központilag kiépített tűzvédelmi rendszer működik. Az egész épület építési engedélyének tűzvédelmi fejezetét az illetékes tűzoltó parancsnokság jóváhagyta.

A biztonsági körlet utólagos kialakítása során, járulékos tűzvédelmi rendszert építettek ki (melynek fő elemei: füstérzékelő- és tűzjelző rendszer, tűzeseti vezérlések, automatikus oltórendszer), melyet az illetékes tűzoltó parancsnokság engedélyezett.

6.1.7 Adathordozók tárolása

Az adathordozók biztonságos tárolására biztonsági körlet, illetve egy bérelt banki széf szolgál.

6.1.8 Selejt kezelése, megsemmisítése

A biztonsági körletben a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat, csak tartalmuk többszörös visszaállíthatatlan törlése után használják fel nem minősített adatok tárolására (a folyamat pontos leírását a Biztonsági Szabályzat tartalmazza). A feleslegessé vált, bizalmas minősítésű adatokat tartalmazott és megfelelően nem törölhető adathordozókat fizikailag megsemmisítik:

- a papíralapú dokumentumokat zúzógéppel felaprítják,
- a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprítják,
- egyéb más mágneses adathordozókat, demagnetizálás után összetörik,
- egyéb más adathordozókat összetörik.

6.1.9 Fizikailag elkülönítetten őrzött mentési példányok

A szolgáltatásra nagy hatással lévő úgynevezett kritikus adatokat két helyen (bérelt banki széfben is) tárolják.

6.2 Eljárásbeli óvintézkedések

Az eljárásbeli óvintézkedések célja, hogy a bizalmi munkakörök kijelölésével és elkülönítésével, az egyes munkakörök felelősségének dokumentálásával, az egyes feladatokhoz szükséges személyzeti létszámok, valamint az egyes munkakörökben elvárt azonosítás és hitelesítés meghatározásával kiegészítse, egyúttal fokozza a fizikai és személyzetre vonatkozó óvintézkedések hatásosságát.

A Szolgáltató azon egységei, amelyek tanúsítvány előállítással és visszavonás kezeléssel foglalkoznak, olyan dokumentált szervezeti struktúrával rendelkeznek, amely védi a műveletek semlegességét.

6.2.1 Bizalmi munkakörök

A Szolgáltató biztonság politikája a következő bizalmi munkaköröket határozza meg az alábbi felelősségkörökkel:

Megnevezés	Rövid leírás
Biztonsági Tisztviselő	A szolgáltatás biztonságáért általánosan felelős személy, aki tanúsítványok előállítását, kibocsátását, felfüggesztését és visszavonását nem végzi.
Rendszeradminisztrátor	Az informatikai rendszer telepítését, konfigurálását, karbantartását a regisztráció, a tanúsítványok előállítása, az aláírás-létrehozó eszközök szolgáltatása és a tanúsítványok visszavonása, felfüggesztése céljából végző személy.
Rendszerüzemeltető	Az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.
Rendszervizsgáló	A szolgáltató naplózott, illetve archivált adatállományát kezelővizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy
Informatikai vezető	Szolgáltató informatikai rendszeréért általánosan felelős vezető
Regisztrációs adminisztrátor	A végfelhasználói tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

A Szolgáltató **informatikai vezetője**:

- felügyeli a Szolgáltató informatikai rendszert érintő folyamatait,
- koordinálja a rendszer üzemeltetésével foglalkozó munkatársak tevékenységét,
- koordinálja Szolgáltató szoftverfejlesztési tevékenységét,
- a Változáskezelési Szabályzat rendelkezéseinek megfelelően elbírálja a hatáskörébe sorolt változási kérelmeket,

A Szolgáltatóval munkaviszonyban álló, változó helyszínen dolgozó **biztonsági tisztviselő** általánosan (a hitelesítő egységekre, a regisztrációs egységre, valamint az összes külső regisztrációs munkatársra nézve egyaránt) felel:

- a különböző biztonsági óvintézkedések kidolgozásáért,
- a különböző biztonsági óvintézkedések rendszeres felülvizsgálatáért, a szükségessé váló módosítások kezdeményezéséért,
- a biztonsági óvintézkedések érvényre jutásáért, betartatásáért,
- az informatikai rendszerek biztonsági szintjének megőrzéséért (rendszeres auditok szervezésével, támogatásával).

Ők hajtják végre a rendszeradminisztrátorok rendszerhez való hozzáférésének kezelését is, ami magában foglalja az alábbiakat:

- profil felvétele,
- jogosultságok beállítása,
- kezdeti jelszó meghatározása,
- a távozó, illetve munkakört váltó rendszeradminisztrátorok hozzáférési jogainak azonnali megszüntetése.

A Szolgáltatóval munkaviszonyban álló **rendszeradminisztrátorok**:

- telepítik, konfigurálják és karbantartják a hitelesítő egység védett számítógép termében üzemeltetett megbízható rendszert,
- beállítják a fenti megbízható rendszer kezdeti hálózati konfigurációját,
- kezelik a hitelesítő egység állományába tartozó rendszerüzemeltetők vonatkozásában a rendszerhez való hozzáféréseket (profil felvétele, jogosultságok beállítása, módosítása, kezdeti jelszó meghatározása, a távozó, illetve munkakört váltó rendszerüzemeltetők hozzáférési jogainak azonnali megszüntetése),
- letöltik és installálják a felügyeletük alatt üzemeltetett operációs rendszerre és adatbázisra kiadott biztonsági javítócsomagokat, ezen keresztül gondoskodnak az informatika biztonsági szint folyamatos megőrzéséről,
- rendszeres időnként ellenőrzik (víruskereső programok futtatásával, az engedélyezett és a ténylegesen telepített szoftverek egybevetésével) a hitelesítő egység védett géptermében üzemeltetett informatikai rendszerének és információinak a sértetlenségét,
- gondoskodnak a rendszerüzemeltetők által végzett rendszermentések, illetve a regisztrációs egység rendszermentés másolatainak biztonságos tárolásáról,
- gondoskodnak a rendszermentésekről készített, elkülönítetten őrzendő másolati példányok szállításáról.

A Szolgáltatóval munkaviszonyban álló **rendszerüzemeltetők** folyamatosan üzemeltetik a védett számítógépteremben működő megbízható rendszert, melynek során:

- időszakosan rendszermentéseket végeznek,
- naponta egyszer archiválják az előállított tanúsítványokat és visszavonási listákat,
- szükség esetén (a rendszermentések alapján) helyreállításokat hajtanak végre.

A Szolgáltatóval munkaviszonyban álló **rendszervizsgáló**:

- ellenőrzi (áttekinti) és karbantartja (archiválja és törli) a Szolgáltató védett számítógép-termében működő megbízható rendszer biztonsági naplóit,
- szükség esetén az általa készített archívumokban keresést végez.

A Szolgáltatóval munkaviszonyban álló **regisztrációs felelős**:

- a regisztrációs adminisztrátorok tevékenységét irányító személy,
- a végfelhasználói tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

A bizalmi munkakörök között a biztonságos feladatvégzést akadályozó, illetve a jogszabályokban tiltott személyi átfedések nincsenek. Valamennyi fent megnevezett bizalmi munkakört részletes munkaköri leírások dokumentálják. A Szolgáltatónál a bizalmi munkakört betöltő személyek szakirányú felsőfokú végzettséggel és gyakorlattal rendelkeznek. A bizalmi munkakörökbe az ügyvezető nevezi ki a Szolgáltató munkatársait, a biztonsági alapellenőrzés sikeres befejezése után.

6.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

A Szolgáltatónál az alábbi kettős felügyeletet Igénylő munkafolyamatok vannak:

Két bizalmi munkakört betöltő személy együttes jelenléte (és előzetes, sikeres hitelesítése) szükséges az alábbi funkciók kiváltásához:

- a Szolgáltató első saját kulcsának generálása (ld. 7.1 pont),
- a Szolgáltató későbbi saját kulcsgenerálása,
- a Szolgáltató magán aláíró kulcsának biztonsági mentése (klónozása) (ld. 7.2.3 pont),
- a Szolgáltató magán aláíró kulcsának visszaállítása,
- a Szolgáltató magán aláíró kulcsának (és annak összes másodpéldányának) megsemmisítése,
- minden tanúsítvány-kibocsátást megelőző regisztrációs feladatok (ld. 4.2.2 pont).

6.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

A Szolgáltató valamennyi, bizalmi munkakört betöltő munkatársának a zárt körletbe való belépéskor az azonosítását és hitelesítését biometrikus azonosító rendszer végzi (kivéve a másodlagos helyszín, ahol biometrikus azonosítás nincs, bővebben lásd a 6.1.3 pontban foglaltakat), amely a rendszerekhez való hozzáférésnél egyéb, rendszerenként különböző védelemmel egészül ki. Sikeres hitelesítés nélkül a zárt körletbe való bejutás, illetve rendszerhozzáférés nem lehetséges, így egyetlen, biztonság szempontból kritikus tevékenység sem végezhető el.

6.2.4 Változáskezelés

A Szolgáltató a szolgáltatási folyamatokban és az azt kiszolgáló informatikai szolgáltatásokban bekövetkező módosítások, változások biztonságos végrehajtása érdekében szabályozott és dokumentált változáskezelési eljárást alkalmaz.

6.3 Személyzetre vonatkozó óvintézkedések

A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a lehetőségekkel való visszaélés kockázatának csökkentése.

Ennek érdekében a Szolgáltató a személyi biztonsággal már a felvételi szakaszban foglakozik, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Ennek érdekében a Szolgáltató a Biztonsági Szabályzatának részeként pontosan és részletesen kidolgozott, folyamatosan karbantartott Személyzeti Politikával rendelkezik. A Szolgáltató személyzeti politikájában meghatározott ideiglenes és állandó szerepköröket és felelősségeket a megfelelő munkaleírásokban dokumentálja, amelyek tartalmazzák:

- a szerepkörök információkezelési lehetőségei és a különböző hitelesítési folyamatokra való hatásai alapján felmérhető kockázati besorolását,
- a szükséges szakismereti és tapasztalati követelményeket,
- a munkakörrel és a munkatárs feladataival összefüggő tevékenységek leírását, a felelősségek körét és mértékét, továbbá a kapcsolódó munkakörök megnevezését.

A Szolgáltató munkavállalói mindaddig nem tölthetnek be bizalmi munkakört, amíg a személyükkel kapcsolatos ellenőrzések végrehajtása és a szükséges nyilatkozatok megtétele meg nem történt, és a megfelelő képzésben és tapasztalatszerzésben részt nem vettek.

A Szolgáltató vezető tisztségviselői, vezető beosztású munkatársai, bizalmi munkaköröket betöltő munkatársai (felelős munkatársak) függetlenek minden olyan kereskedelmi, pénzügyi és egyéb hatástól, ami hátrányosan befolyásolhatja a Szolgáltató által nyújtott szolgáltatások iránti bizalmat.

6.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A hitelesítő egység, a regisztrációs egység minden bizalmi munkakörére jelölt személynek (emberi megbízhatósága és szakmai alkalmassága ellenőrzése céljából) kezdeti ellenőrzésen (biztonsági alapellenőrzésen) kell keresztülmennie.

A biztonsági alapellenőrzés során az ellenőrzést végző szakemberek: az életrajzban megadott adatokat (életrajzi elemek, referenciák, szakmai előmenetel, stb.) ellenőrzik. Ennek során:

- a képzettségre vonatkozó adatokat egybevetik a jelölt által benyújtandó bizonyítványokkal, diplomákkal,
- a gyakorlati tapasztalatra vonatkozó állításokat személyes referenciákon keresztül, publikációkra alapozva, illetve egyéb úton igazolják.

Az ügyfél regisztráció területén dolgozó munkatársak ismerik a forgalomban lévő hatósági, illetve azonos funkciójú dokumentumokat, azok fajtáit, ismertetőjegyeit, képesek az átadott iratok valódiságának, érvényességének megállapítására.

6.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások

Valamennyi bizalmi munkakört betöltő munkatársnak a biztonsági alapellenőrzésen túl időszakos biztonsági ellenőrzéseken kell átesniük.

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a „magas biztonsági kockázat” minősítést kapja.

Az időszakos biztonsági ellenőrzésre évente kerül sor

- az informatikai vezető,
- a biztonsági tisztviselők,
- a rendszeradminisztrátorok,
- a rendszerüzemeltetők,
- regisztrációs felelősök
- rendszervizsgáló

esetében egyaránt.

Az ellenőrzés során vizsgálják a munkatárs erkölcsi bizonyítványát és olyan körülményeket, melyek kockázati tényezőt jelentenek. E mellett figyelembe veszik a közvetlen vezetők véleményét is.

6.3.3 Képzési követelmények

A hitelesítő egység, a Központi Regisztrációs Egység területén dolgozó valamennyi munkatárs felvételét követően, a saját munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt. Ennek keretében minden munkatárs egy egységes informatika biztonsági alapkiképzésben is részesül. Ennek a képzési formának a fő célja az egész hitelesítés-szolgáltatásra vonatkozó, egységes biztonságpolitika megismerése, megértése, az ezen alapuló aktuális eljárások és követelmények megismerése és a későbbi helyes alkalmazása érdekében. További részletek a személyzeti politikában találhatók.

6.3.4 Továbbképzési gyakoriságok és követelmények

Abban az esetben, amikor a hitelesítés-szolgáltatásban jelentős változás következik be, valamennyi munkatárs a szükséges felépítésű és szintű moduláris továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat. További részletek a személyzeti politikában találhatók.

6.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között nem valósul meg.

6.3.6 A felhatalmazás nélküli tevékenységek büntető következményei

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

6.3.7 A szerződéses munkavállalókra vonatkozó követelmények

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

6.3.8 A személyzet számára biztosított dokumentációk

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

6.4 A biztonsági naplózás folyamatai

Szolgáltató hitelesítési rendszere a jogszabályi követelményeknek megfelelő, széleskörű naplózási tevékenységet folytat a tanúsítványokra vonatkozó műveletek és az ezek során felhasznált adatok megőrzése érdekében. A napló tartalmazza a bejegyzés pontos idejét, a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét. A Szolgáltató a naplókban feltüntetett időt olyan gyakorisággal szinkronizálja a Szabályzatban megjelölt referencia időforráshoz (ld. 7.8.2 pont), hogy a saját idő és a valódi idő közti eltérés ne haladja meg az 1 másodpercet. Az esetleges ennél nagyobb eltérések szintén naplózásra kerülnek.

A Szolgáltató egyéb rendszerei szintén naplóznak. E naplózások tulajdonságai az adott alkalmazások függvényei. A naplózások elemei elkülönülten keletkeznek a különböző modulokban. A több komponensből álló rendszer miatt a napló állományok nem egy helyen keletkeznek, de feldolgozásuk egy központi helyen történik.

Operatív szinten az egyes rendszerek üzemeltetési leírásai szabályozzák a napló adatok kezelését.

6.4.1 A tárolt események típusai

Az alkalmazott PKI rendszer minden jogszabályban előírt eseményt és hibát regisztrál, amely a rendszer üzemeltetése, visszakereshetősége és adminisztrációja szempontjából kritikus.

Különösen az alábbi fő eseménytípus csoportok kerülnek naplózásra:

- rendszertevékenységek (indítás, leállítás, verziófrissítés, újraindexelés, újrakulcsolás, saját kulcsok és tanúsítványok kezelése, stb.),
- mentési tevékenységek (teljes mentés, különbségi mentés, mentés ellenőrzés, stb.),
- naplózási tevékenységek (naplózási funkció elindítása és leállítása, naplózási paraméterek megváltoztatása, a naplózás tárolási hibája miatt végzett tevékenységek, stb.)
- CRL tevékenységek (kiadás, kombinált kiadás, visszavonás, felfüggesztés, stb.),
- felhasználói események (tanúsítványkiadás, regisztráció, visszavonás, kulcsvisszaállítás, a biztonságos aláírás-létrehozó eszközök készítésével és átadásával kapcsolatos események, stb.),
- adminisztratív események (adminisztrátor ki-, belépés, felhasználó visszaállítás, stb.),
- adatbázis események,
- címtár események,
- operációs rendszer események,
- hibák.

A naplózott események időbélyegzővel ellátott bejegyzésként kerülnek napló állományba. A Szolgáltató a napló minden bejegyzését elektronikus aláírás és biztonsági másolat és mentés alkalmazásával védi a módosítástól, illetéktelen hozzáféréstől, megsemmisítéstől, a napló bejegyzéseinek törlésétől, a bejegyzések sorrendjének bármilyen módon történő megváltoztatásától.

A naplóban a Szolgáltató biztosítja a naplóbeli események között az esemény típusa és/vagy a felhasználó személye szerinti keresést. A naplóbejegyzések szöveges formátumban jelenítődnek meg.

6.4.2 A napló állomány feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása napi rendszerességgel megtörténik. Szolgáltató hálózati védelmi rendszerei riasztási funkciókkal is el vannak látva az erőforrásokhoz történő jogosulatlan hozzáférés észlelésének jelzésére. Ilyen riasztási esetekben a naplóbejegyzések soron kívül átvizsgálásra kerülnek. Rendellenességek észleléskor, reklamációkor vagy egyéb megkeresések kapcsán is sor kerülhet a napló adatok rendkívüli átvizsgálására.

6.4.3 A napló állomány megőrzési időtartama

A napló állományok keletkezésük helyén tárolódnak, illetve archiválásra kerülnek (ld. 6.5.4 pont), és a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg a velük kapcsolatban felmerült és bejelentett jogvita jogerős lezárásáig megőrződnek.

6.4.4 A napló állomány védelme

Szolgáltató hitelesítési rendszerének naplóbejegyzései a Szolgáltató elektronikus aláírásával ellátva, a törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A napló állományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében Szolgáltató gondoskodik az adatok bizalmas tárolásáról. A napló állományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán szükségük van. Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi.

6.4.5 A napló állomány mentési folyamatai

A naplóállományok rendszeresen mentésre kerülnek (ld. 6.5.4 pont) rejtjelezett és aláírt formában.

6.4.6 A napló gyűjtési rendszere

A naplóbejegyzéseket az alkalmazások automatikusan gyűjtik és tárolják a napló állományokban. A mentett médiákat Szolgáltató napi rendszerességgel begyűjti. A médiákat Szolgáltató saját munkatársai szállítják a megőrzési helyre.

6.4.7 Az eseményeket kiváltó Alanyok értesítése

A naplóbejegyzéseket kiváltó személyeket, egységeket és alkalmazásokat Szolgáltató nem értesíti, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában közreműködőknek a Szolgáltatóval fennálló szerződéses viszony, vagy jogszabály rendelkezése esetén kötelessége a Szolgáltatóval való együttműködés.

6.4.8 Sebezhetőség felmérése

A naplóbejegyzések feldolgozása során Szolgáltató a naplózott események alapján a sebezhetőségre vonatkozó felméréseket végez. A napi rendszerességgel végzett feldolgozáson túl Szolgáltató szakemberei havonta áttekintik a rendkívüli eseményeket és ezek alapján a sebezhetőségre vonatkozó elemzéseket végeznek. Ezen elemzések alapján a Szolgáltató lépéseket tesz a rendszer biztonságának javítására.

6.5 Adatok archiválása

Szolgáltató informatikai rendszerének biztonsági és egyéb általános naplózási folyamatait ugyanazon rendszerek végzik, ugyanazon módszerek segítségével. Jelen fejezetben csak a Szolgáltató ettől eltérő papír alapú és egyéb speciális archiválási rendszerét ismertetjük.

6.5.1 A tárolt események típusai

A Szolgáltató regisztrációs egységei valamennyi regisztrációs eljárás során keletkező iratot tárolják. Így tárolásra kerül:

- a Szolgáltatóhoz benyújtott valamennyi elektronikus illetve papír alapú kérelem (tanúsítvány kibocsátás, megújítás, visszavonás, stb.);
- az Igénylő hozzájárulása esetén a személyes és szervezeti identitásának igazolására bemutatott valamennyi dokumentum másolata;
- a Szolgáltató és az Alany, illetve a másodlagos Alany között megkötött valamennyi vonatkozó megállapodás (ideértve a tanúsítvány közzétételéhez történő hozzájárulást is);
- a kérelmet elfogadó regisztrációs ügyintéző azonosítója;
- a küldő regisztrációs szervezet neve.

A Szolgáltató továbbá megőrzi a tanúsítványokkal kapcsolatos elektronikus információkat – beleértve az, azok előállításával összefüggőket is – és az ahhoz kapcsolódó személyes adatokat.

6.5.2 Az archívum megőrzési időtartama

Szolgáltató a tanúsítványokkal kapcsolatos elektronikus információkat és az ahhoz kapcsolódó személyes adatokat – amennyiben a Törvény szigorúbb követelményt nem támaszt - legalább a tanúsítvány érvényességének lejártától számított tíz évig, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi, valamint ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható. E megőrzési kötelezettségnek Szolgáltató minősített archiválási szolgáltató igénybevételével is eleget tehet.

6.5.3 Az archívum védelme és hozzáférési szabályok

A Szolgáltató az archivált adatállományt legalább fokozott biztonságú elektronikus aláírás és időbélyeg elhelyezésével hitelesíti, védi a módosítástól, illetve biztosítja azt, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá. Az archívum nem tartalmaz védelem nélkül kritikus biztonsági paramétereket. A Szolgáltató a tanúsítványokra vonatkozó archivált adatok titkosságát és integritását fenntartja.

Az archivált adatokhoz a Szolgáltató vezető tisztségviselői és a Szolgáltató auditorai férnek hozzá. A Szolgáltató biztosítja, hogy az adatok az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

6.5.4 Az archívum mentési folyamatai

Az adatok mentése naponta – legalább 1 példányban - történik. Ezen kívül heti, havi mentésekre és hosszú távú archiválásokra kerül sor. A mentést hordozó médiát a Szolgáltató biztonságos környezetben tárolja.

6.5.5 A rekordok időbélyegzésére vonatkozó követelmények

Lásd a 6.4.1 pontot.

6.5.6 Az archívum gyűjtési rendszere

A külső regisztráció során keletkezett iratokat a regisztrációt végző szervezetek bizalmasan tárolják és őrzik. Az elektronikus másolati példányban is létező iratok elektronikus üzenet formájában kerülnek a Szolgáltató központi adattárba.

6.5.7 Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés az Alanynak, illetve a másodlagos Alanynak a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.4 pont szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és a hozzáférést naplózza.

6.5.8 Egyéb archiválási rendelkezések

Az archívumban esemény típus szerinti keresést lehet végrehajtani.

Az archiválásra vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat tartalmazza.

6.6 Biztonsági rendelkezések

A Szolgáltató biztonsági műveleteit az üzemi műveletektől elkülöníti. A Szolgáltató biztonsági műveleteivel kapcsolatos felelősségek:

- üzemeltetési eljárások és felelősségek,
- biztonsági rendszerek tervezése és elfogadása,
- káros szoftver elleni védelem,
- rendszeradminisztráció,
- hálózatkezelés,
- audit napló, eseményelemzések és nyomon követések,
- adathordozók kezelése és biztonsága,
- adat és szoftver javítása, cseréje.

A Szolgáltató elvégzi a biztonsági követelmények elemzését, minden egyes rendszerfejlesztési vagy bővítési folyamat tervezési és követelmény specifikálási eljárás során.

A Szolgáltató rendszeres ellenőrzésekkel biztosítja, hogy a személyi azonosító eszközök (chipkártyák stb.) elvesztését, esetleges sérülését, kompromittálódását minél hamarabb felfedezze (nyilvántartások vezetése).

6.6.1 Biztonsági felülvizsgálati eljárások

A Szolgáltató a tanúsítványok kiadásával, megújításával, felfüggesztésével, továbbá visszavonásával kapcsolatos összes eseményt felülvizsgáltatja. A felülvizsgált események tételes felsorolását a Biztonsági Szabályzat tartalmazza.

A Szolgáltató szúrópróbaszerű esemény felülvizsgálatot havonta többször, általános felülvizsgálatot félévente, illetve rendkívüli üzemeltetési helyzetet követően hajt végre.

Szolgáltató a felülvizsgálatról készült feljegyzéseket a felülvizsgálattól számított 10 évig megőrzi.

A felülvizsgálati naplókhoz a Szolgáltató vezető tisztségviselői férhetnek hozzá, a hozzáférés naplózásával. Az elektronikus feljegyzéseket a Szolgáltató elektronikusan aláírja.

A feljegyzésekre vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat tartalmazza.

6.7 Helyreállítás kompromittálódás és katasztrófa esetén

6.7.1 Incidens- és kompromittálódás-kezelési eljárások

A Szolgáltató a folyamatos működés biztosítása, illetve a vészhelyzetek minél gyorsabb elhárítása érdekében Üzleti Folytonossági Tervvel (ÜFT) rendelkezik, amely tartalmaz katasztrófa helyreállítási tervet is. Az ÜFT olyan eljárásokat tartalmaz, amelyek leírják a megbízható üzemmenet mielőbbi helyreállításának leggyorsabb módját. A Szolgáltató ellenőrzések végrehajtásával rendszeresen teszteli a biztonsági előírások hiánytalan technikai és személyi végrehajtását.

A Szolgáltató mentésekkel biztosítja, hogy szükség esetén az informatikai rendszer egészét helyre tudja állítani. A mentéseket a Szolgáltató védi a módosítások, illetve az ellen, hogy jogosulatlan személyek a mentett adatállományhoz hozzáférhessenek.

A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását megelőzi.

Rendkívüli üzemeltetési helyzet bekövetkezése esetén a Szolgáltató haladéktalanul értesíti a Felügyeletet a rendkívüli üzemelési helyzet bekövetkezéséről, annak hatásáról, várható időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről. Ezenfelül közvetlenül értesíti mindazon személyeket, akiket a rendkívüli üzemeltetési helyzet érint, illetve tájékoztatást tesz közzé az interneten (lásd 2.3.2 pont).

6.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltató megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik, a hardver- és szoftver meghibásodások, valamint az adatsérülések minimalizálása érdekében. A szolgáltatások helyreállíthatóságát Szolgáltató háttérszerződései és saját tartalékeszközei garantálják, amelyek az 6.7.4 pontban vállalt időn belül bármely kieső kritikus eszköz pótlására képesek. Szolgáltató rendszeres mentései és tranzakció naplózása biztosítja az adatok visszaállíthatóságát valamely adattároló eszköz kiesésének esetére. Ez a rendszer a legrosszabb esetben az előző napi adatok helyreállítására képes.

Szolgáltató katasztrófa elhárítási terve eseményjelentési előírásokkal rendelkezik valamennyi eszköze meghibásodása, illetve rendellenes működése tekintetében (ezek egy része automatizált, más része a kezelőszemélyzet felelőssége). A jelentéseket szakértő személyzet értékeli ki és válaszadás eljárásokat foganatosítva minimalizálja az esetleges károkat és szolgáltatás kieséseket.

6.7.3 Egy szolgáltatói egység kulcsának kompromittálódása

Szolgáltató katasztrófa elhárítási terve a szolgáltatói magánkulcsok kompromittálódása esetére akciótervvel rendelkezik (ld. Üzleti Folytonossági Terv). Az akcióterv a szolgáltatói nyilvános kulcs visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik az ez által érintett valamennyi fél értesítéséről (a 2.1 ponttól függetlenül, de arra tekintettel), megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet, valamint a kompromittálódott kulccsal kiadott tanúsítványokat visszavonja.

6.7.4 Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően

Természeti vagy más katasztrófát követően, illetve a Szolgáltató berendezéseinek meghibásodása esetén Szolgáltató a következő szolgáltatások legfeljebb 3 órán belüli elindítását vállalja:

- visszavonáskezelés-szolgáltatás,
- visszavonási állapot közzététele szolgáltatás.

Minden egyéb szolgáltatás elindítását Szolgáltató 5 munkanapon belül vállalja.

6.8 A Szolgáltató leállítása

6.8.1 Szolgáltatás megszűntetése

Amennyiben a Szolgáltató tevékenységét tervezetten megszűnteti vagy tartósan szünetelteteti, a tevékenység leállását megelőzően legalább az alábbi eljárásokat hajtja végre:

a) A tevékenység befejezését legalább 60 nappal megelőzően értesíti az általa kibocsátott és még vissza nem vont tanúsítványokban Aláíróként megjelölt személyeket, a Felügyeletet, megjelölve azt a - vele azonos besorolású – szervezetet, amely legkésőbb a tevékenység befejezésekor átveszi a visszavonási állapot közlési nyilvántartásokat, valamint a regisztrációs információ és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket a Szolgáltató számára előírt vagy általa vállalt időtartamra (lásd 10.3 pont).
b) A szolgáltatás megszűnése előtt 30 nappal értesítést tesz közzé Internetes oldalain (ld. 1.5 alfejezet), e-mail címmel rendelkező ügyfelei számára a szolgáltatás befejezéséről elektronikus levélben értesítőt küld.
c) A Szolgáltató a tevékenység befejezését legalább 20 nappal megelőzően az általa kibocsátott, és még vissza nem vont tanúsítványokat visszavonja.
d) A Szolgáltatóval szerződéses kapcsolatban álló, a tanúsítvány kibocsátásban résztvevő, összes vállalkozással, regisztrációs szervezettel korábban megkötött szerződés alapján fennálló kezelési jogokat, illetve felhatalmazást visszavonja, valamennyi regisztrációs szervezetet felhívja a náluk tárolt adatok átadására.
e) A regisztrációs információk, és az eseménynapló archívumok megőrzése érdekében, időbélyegzővel ellátott teljes körű mentést hajt végre. A mentésnek tartalmaznia kell a tanúsítványokkal kapcsolatos korábbi változások adatait, a tanúsítványok helyzetére, esetleges felfüggesztésére, illetve visszavonására vonatkozó adatokat, valamint a tanúsítvány kibocsátásra vonatkozó Szolgáltatói szabályzatokat és az aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását. A mentett adatállományokat a Szolgáltató védi jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását, valamint az adatoknak megőrzési időn belüli, jogosultak számára való hozzáférhetőségét és értelmezhetőségét.
f) Saját magánkulcsait megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat visszavonja, és erről egy országos terjesztésű napilapban hirdetést tesz közzé.
g) A Szolgáltató a tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is eleget tesz.
h) A Szolgáltató új tanúsítványokat a megszűnés bejelentése után nem bocsát ki.

Ha a Szolgáltató ellen felszámolási vagy végelszámolási eljárás indult, haladéktalanul tájékoztatja a Felügyeletet e tényről, megnevezve az eljárást lefolytató szervezetet.

A Szolgáltató rendelkezik a leállási követelmények teljesítésével kapcsolatos költségek fedezetével. A leálláshoz kapcsolódó kötelezettségek teljesítését 25.000.000 Ft-os bankgarancia szavatolja.

A Szolgáltató annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak, azokat a szolgáltató által fogadóképes médián és formátumban helyezi el vagy biztosítja a szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, melyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

6.8.2 Regisztrációs pont megszűnése

A Szolgáltató a lehetőségeknek megfelelően folyamatosan törekszik arra, hogy az esetlegesen kieső Regisztrációs Pontokat újakkal pótolja, s regisztrációs szolgáltatásának személyes elérhetőségét országosan fenntartsa. Valamely regisztrációs pont megszűnése esetén a Szolgáltató biztosítja a regisztrációs ponton tárolt adatok begyűjtését, illetve a vele kötött szerződéstől és az adatkezelés céljától függően felhívja a Regisztrációs Pontot az adatkezelés megszüntetésére.

7 Műszaki biztonsági óvintézkedések

A Szolgáltató megbízható, biztonságtechnikailag értékelt és ellenőrzött termékekből álló informatikai rendszert használ szolgáltatásai nyújtásához.

A kulcskezelési rendelkezések az alábbi kulcsokat különböztetik meg:

Szolgáltatói magánkulcsok:

- minősített tanúsítványokat, CRL és OCSP válaszokat aláíró magánkulcs,
- egyéb tanúsítványokat, CRL és OCSP válaszokat aláíró magánkulcs,
- időbélyegző magánkulcs,
- infrastrukturális és kontrollkulcsok,
- viszontazonosítási válasz aláíró kulcs.

Szolgáltatói nyilvános kulcsok:

- a szolgáltatói magánkulcsok nyilvános párjai.

Végfelhasználói magánkulcsok:

- végfelhasználó magánkulcsa, amelyet saját maga hozott létre,
- végfelhasználó magánkulcsa, amelyet számára a Szolgáltató hozott létre.

Végfelhasználói nyilvános kulcsok:

- a végfelhasználói magánkulcsok nyilvános párja.

7.1 Kulcspár előállítás és telepítés

7.1.1 Kulcspár előállítás

		Végfelhasználói kulcspár	**Szolgáltatói kulcspárok**
Kulcsgenerálás és installáció	Kulcsgenerálás, tárolás	A kulcsgenerálást a végfelhasználó saját maga vagy aláíró eszköz szolgáltatás keretében a Szolgáltató végzi. Kulcsgenerálás és –tárolás végfelhasználók részére BALE-n vagy egyéb informatikai eszközön történhet. Szolgáltató aláírás-létrehozó adat generálására BALE-t vagy a jogszabályi előírásoknak megfelelően tanúsított informatikai eszközt használhat.	Szolgáltató a saját tanúsítvány aláíró és egyéb infrastrukturális kulcspárjait biztonságos módon generálja és tárolja. A kulcsgenerálás a Szolgáltató kizárólagos feladata és felelőssége. A magánkulcsokat a Szolgáltató nem bocsátja ki nyíltan.
	Kulcs méretek	A végfelhasználóknak legalább a mindenkor hatályos iránymutatást tartalmazó felügyeleti határozatban [31] előírt hosszúságú kulccsal kell rendelkezniük.	A szolgáltatói kulcspárok hossza megfelel a kibocsátáskor hatályos iránymutatást tartalmazó felügyeleti határozatban [31] előírt hosszúságnak.
	Kulcs felhasználási célok	A Szolgáltató vagy végfelhasználó aláíró kulcspárt generál.	- minősített tanúsítvány és CRL válaszok aláírása; - egyéb tanúsítvány, CRL és OCSP válaszok aláírása, - időbélyegző aláírása, - infrastrukturális és kontrollkulcsok, - viszontazonosítási válasz aláírására használt kulcsok.
Magánkulcs védelme	Magánkulcs több-személyes kontrollja	A Szolgáltató több-személyes kontrollt vagy ennek megfelelő technikai védelmet biztosít a magánkulcsok generálásakor és kezelésekor.	A Szolgáltató legalább kétszemélyes kontrollt alkalmaz a magánkulcsok esetében.
	Magánkulcs letét	Szolgáltató nem nyújt minősített magánkulcs letéti szolgáltatást.	Szolgáltató nem nyújt minősített magánkulcs letéti szolgáltatást.

		Végfelhasználói kulcspár	Szolgáltatói kulcspárok
	Magánkulcs mentése	Minősített magánkulcsot a Szolgáltató nem ment.	Magánkulcsait a Szolgáltató menti.
	Magánkulcs aktiválása	A magánkulcsok aktiválását az Alany kezdeményezi.	A Szolgáltató 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 a magánkulcsát az érvényességi idő lejárta után megsemmisíteni.	A Szolgáltató magánkulcsait és azok minden előfordulását az érvényesség lejáratakor a Szolgáltató megsemmisíti.
Egyéb tevékenységek	Nyilvános kulcs archiválása	A végfelhasználói nyilvános kulcsokat a Szolgáltató a jogszabályokban meghatározott ideig archív formában megőrzi (ld. 4.8.4. pont).	A szolgáltatói nyilvános kulcsokat a Szolgáltató a jogszabályokban meghatározott ideig archív formában megőrzi (ld. 4.8.4. pont).
	Kulcsok felhasználási ideje	A végfelhasználói magánkulcs felhasználási ideje megegyezik a hozzá tartozó tanúsítvány érvényességi idejével, de maximálisan 2, a tanúsítvány meghosszabbítása esetén 4 év. A nyilvános kulcs a kriptográfiai biztonságáig érvényes.	A szolgáltatói magánkulcs felhasználási ideje megegyezik a hozzá tartozó tanúsítvány érvényességi idejével. A nyilvános kulcs a kriptográfiai biztonságáig érvényes.

A Szolgáltató valamennyi szolgáltatói kulcspárát saját maga 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 szolgáltatói kulcspár, bármely okból történő megsemmisítése válik szükségessé, úgy az az eszköz tanúsítványában előírt módon két személyes kontroll mellett történik.

7.1.1.1 Alkalmazott eszközök

Aláíró eszközök	Hardware és firmware specifikáció	Kulcskezeléshez közvetlenül használt szoftverek specifikációja
Minősített Hitelesítő Egység	ProtectServer Gold (hardware verzió: B2, firmware verzió: 2.03.00) ProtectServer Orange (korábbi nevén CSA 8000 Adapter), hardver verzió: G verzió, Cprov förmver verzió: 1.10 Luna PCI 3000 V3.0 /Hardver verzió: VBD-04-0100, förmver verzió: 4.7.1(3000)/ kriptográfiai modul Luna PCI-e 3000 SFF V3.0 /Hardver verzió: VBD-04-0102, förmver verzió: 4.7.1(3000)/ kriptográfiai modul	ProtectServer Gold (hardver verzió: B2, firmware verzió: 2.03.00) drivere, ProtectServer Orange (korábbi nevén CSA 8000) Cprov förmver verzió: 1.10 drivere, PKCS11 interfész, tanúsított NCA NetLock tanúsítványkiadó rendszer. Luna kriptogáfiai modulok driverei
Végfelhasználói eszköz	IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4, applet IDOneClassIC v1.0 embedded, P5CT072VOP-en, ID-One Cosmo v7.0.1-n kártya IAS ECC 1.0.1 alkalmazással (applet version 1121), NXP P5CC081 V1A (Standard) komponenssel Gemalto MultiApp ID Citizen 72k intelligens kártya: S3CC91C mikrochip, MultiApp v1.1 Java Card platform és IAS Classic v.3.0 elektronikus aláíró alkalmazás SafeNet eToken (Smartcard or USB token), 9.1-es Verzió, Athena IDProtect/OS755 Java Card kártya, Atmel AT90SC25672RCT-USB Microcontrolleren, IDSign applet beágyazással IAS Classic v3 alkalmazás Java Card platformon P5CC081V1A chippel, MultiApp ID V2.1 nyílt szabvány szerint, szűrővel ellátott MPH117 v2.2 ProtectServer Orange (korábbi nevén CSA 8000 Adapter), hardver verzió: G verzió, Cprov förmver verzió: 1.10	ProtectServer Orange (korábbi nevén CSA 8000 Adapter), hardver verzió: G verzió, Cprov förmver verzió: 1.10 Oberthur eszközökhöz driverek Gemalto eszközökhöz driverek SafeNet eszközök driverei

A Szolgáltató által alkalmazott eszközökhöz közvetetten felhasználásra kerülhetnek más, tanúsított szoftverekben is, mint a Mokka, az NCA rendszer, az Archer és az e-Szigno termékek.

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.

7.1.2 Magánkulcs eljuttatása az Alanyhoz

Mivel a Szolgáltató valamennyi kulcspárja helyben generálódik (ld. 7.1.1 pont), azokat nem kell sehová továbbítani.

A végfelhasználók aláíró magánkulcsát nem kell továbbítani, ha azt az alany saját maga állítja elő. Amennyiben a Szolgáltató aláíró eszköz-szolgáltatás keretében generálta a végfelhasználói kulcspárt, akkor az eszközt biztonságos módon közvetlenül juttatja el az alanyhoz és adja át annak.

7.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A Szolgáltató valamennyi nyilvános kulcsáról saját maga készít tanúsítványt.

A végfelhasználók nyilvános kulcsát a már sikeresen regisztrált alany (ld. 4.2.2 pont) védett csatornán küldi meg a regisztrációs egységnek, amely – miután sikeresen ellenőrizte, hogy az alany által megküldött nyilvános kulcsnak megfelelő magánkulccsal valóban rendelkezik-e az alany – szintén védett csatornán továbbítja a hitelesítő egységnek.

Eszközszolgáltatás esetén a kulcspárt a Szolgáltató helyben generálja, így nincs szükség a nyilvános kulcs továbbítására.

7.1.4 A szolgáltatói nyilvános kulcs közzététele

A Szolgáltató a hitelesítő egység által aláírt tanúsítványait saját tanúsítványtárában, illetve ügyfélszolgálatán teszi mindenki számára elérhetővé.

7.1.5 Kulcsméretek

Lásd 7.1.1 pont.

7.1.6 A nyilvános kulcs paraméterek generálása és megfelelőségük ellenőrzése

A nyilvános kulcs paraméterek megfelelnek az előírásoknak (ld. a Felügyelet irányadó határozatai, [31]), és előállításuk során a megfelelő szabványok, algoritmusok kerültek alkalmazásra.

7.1.6.1 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.

Ezeken felül a tanúsító szervezetek évente felülvizsgálják, 3 évente újra tanúsítják az eszközöket.

7.1.7 A kulcs használat célja (az X.509 v3 kulcshasználati mezők tartalmának megfelelően)

A Szolgáltatónak a tanúsítványok aláírásához használt magánkulcsát, ezeken kívül, csak a tanúsítvány visszavonási lista (CRL) aláírására szabad felhasználnia.

A Szolgáltatónak csak olyan minősített aláírásra használható aláíró tanúsítványt bocsáthat ki, melyekre teljesül, hogy az aláíró tanúsítvány kulcshasználati mezője kritikus, és a mezőben kizárólag a "NonRepudiation" bit van „true” értékre beállítva.

7.2 A magánkulcsok védelme

7.2.1 A szolgáltatói kulcsokra vonatkozó általános szabályok

A szolgáltatói kulcsokra az alábbi szabályok vonatkoznak:

- a kulcsok létrehozása, tárolása, mentése, helyreállítása, megsemmisítése fizikailag biztonságos környezetben, kettős személyi ellenőrzés mellett valósul meg,
- a minősített hitelesítő egység kulcsai FIPS 140, Level 3 tanúsítvánnyal rendelkező kriptográfiai modulban kerülnek előállításra, tárolásra,
- a kulcsokat kizárólag az arra felhatalmazottak használhatják, a létrehozás céljának megfelelő funkcióra,
- a Szolgáltató rendszerei saját szolgáltatói kulcsaik használata előtt meggyőződnek arról, hogy az ezen kulcsokhoz kapcsolódó tanúsítványok érvényesek,
- a Szolgáltató tanúsítvány és CRL aláíró kulcsai különböznek minden más funkcióra szolgáló kulcstól,
- a szolgáltatói kulcsfrissítés out-of-band cserével történik,
- a szolgáltatói 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 exportálásakor a Szolgáltató gondoskodik a kulcs védelméről,
- élettartamuk végén a kulcsokat a Szolgáltató olyan módon semmisíti meg, hogy az aláíró kulcsok ne legyenek visszanyerhetőek,
- azokat a rendszereket, melyek kriptográfiai hardver eszközön kívül dolgoznak fel kriptográfiai szempontból érzékeny információt (magán- vagy titkos kulcsokat) a Szolgáltató védi az elektromágneses kisugárzással történő kompromittálódás ellen (ld. 6.1.4.2 pont).

7.2.2 Magánkulcs letétbe helyezése

A szolgáltatói és végfelhasználói magánkulcsot nem lehet letétbe helyeztetni.

7.2.3 Magánkulcs mentése

A Szolgáltatónál a következő magánkulcsok kerülnek mentésre (illetve duplikálásra, klónozásra):

- a hitelesítő egység aláíró magánkulcsa,
- időbélyeg-válaszokat aláíró magánkulcs.

A mentés során a 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.

7.2.4 Magánkulcs archiválása

A Szolgáltató sem az aláíró magánkulcsát, sem a minősített végfelhasználói magánkulcsokat nem archiválja.

7.3 A kulcspár gondozásának egyéb szempontjai

7.3.1 Egyéb kulcskezelési rendelkezések

Minősített eszközszolgáltatásnál, ha a kulcspár előállítása a BALE eszközön kívül történik, a kulcspárt előállító kriptográfiai eszköz tanúsítvánnyal igazoltan megfelel az alábbi szabványok, szabványjellegű dokumentumok legalább egyikének: a) FIPS 140, 3-as szint, b) CEN HSM – PP.

A Szolgáltató a szolgáltatások nyújtásához használt elektronikus aláírási termékeit elkülönítetten kezeli és működteti az egyéb tevékenységeihez használt termékektől. A hitelesítés-szolgáltatáshoz alkalmazott termékek körén belül elkülönítve kezeli a minősített szolgáltatások nyújtásához használt elektronikus aláírási termékeit a nem minősített szolgáltatásokhoz használt elektronikus aláírási termékektől.

A Szolgáltató a szolgáltatások nyújtásához használt valamennyi elektronikus aláírási terméket kockázatelemzések alapján biztonsági osztályokba sorolja, és ezekről nyilvántartást vezet.

A még tanúsítvánnyal el nem látott nyilvános kulcsokat a Szolgáltató fizikailag biztosított környezetben tárolja.

7.3.2 Nyilvános kulcs archiválása

A regisztrációs egység minden a Szolgáltató által előállított tanúsítványt archivál, az alábbi időszakra:

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

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

A Szolgáltató az Aláíró magánkulcsát nem archiválja. (Lásd 7.2.4 pont.)

7.3.3 A nyilvános és magánkulcsok használatának periódusa

Szolgáltatói tanúsítványok és a bennük foglalt nyilvános kulcsok magán párjai:

- minősített tanúsítvány és CRL aláíró magánkulcs: legfeljebb 20 év
- minősített időbélyegző magánkulcs: legfeljebb 20 év

A végfelhasználói aláíró kulcsokhoz tartozó tanúsítványoknak és a bennük foglalt nyilvános kulcsok magán párjainak érvényességi ideje maximálisan 2, a tanúsítvány meghosszabbítása esetén 4 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.

7.4 Aktivizáló adatok

7.4.1 Aktivizáló adatok előállítása és telepítése

A Szolgáltató a biztonságos aláírás-létrehozó eszközhöz tartozó aktivizáló adatokat (PIN kód) biztonságos módon, az eszközöktől elkülönítetten állítja elő. A PIN kód beállítása a biztonságos aláírás-létrehozó eszköz tanúsítója által előírt módon történik. A további pontos szabályok az Alany érdekében nem nyilvánosak.

7.4.2 Az aktivizáló adatok védelme

A Szolgáltató a biztonságos aláírás-létrehozó eszközhöz tartozó aktivizáló adatokat (PIN kód) csak abból a célból rögzíti, hogy azt a szolgáltatást igénybe vevő személy számára – másolat megőrzése nélkül – átadhassa.

7.4.3 Az aktivizáló adatok egyéb szempontjai

A Szolgáltató a biztonságos aláírás-létrehozó eszközhöz tartozó aktivizáló adatot (PIN kód) a biztonságos aláírás-létrehozó eszköztől elkülönítve juttatja el az Alanyhoz. Kivételt jelent ez alól a személyes átadás, ahol az aláírás létrehozó eszköz és az azt aktivizáló adat egyszerre is átadásra kerülhet, a bizalmassági követelményeknek való megfelelés fenntartása mellett.

7.5 Számítógép-biztonsági óvintézkedések

A Szolgáltató a következő számítógép-biztonsági óvintézkedéseket alkalmazza:

- megköveteli, hogy az informatikai rendszerek és alkatrészek szállítói olyan dokumentációkat biztosítsanak, melyek érthetővé teszik a megbízható rendszerek helyes és biztonságos működtetését, a rendszerhibák kockázatának minimalizálását biztosító telepítését, a vírusokkal és kártékony szoftverekkel szembeni védelmet a rendszerek és az általuk feldolgozott információk sértetlenségének fenntartása érdekében,
- megköveteli a szolgáltatási rendszerek szállítóitól a következők átadását: telepítési útmutató, rendszeradminisztrációs útmutató, üzemeltetési útmutató,
- az egyes rendszerek kezelése során hozzáférési szinteket, hozzáférési jelszavakat alkalmaz,
- az audit napló állományokat napi, heti és havi, valamint éves gyakorisággal ellenőrzi.

Az ide vonatkozó részletes rendelkezéseket az 6.6 6.4 és az 6.1 alfejezet, valamint a Biztonsági Szabályzat tartalmazza.

7.5.1 Speciális számítógép-biztonsági műszaki követelmények

Az **alkalmazások** által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a rendszerüzemeltetői hozzáférések és tevékenységek rögzítése),
- kommunikáció (a hitelesítő egység és a Központi Regisztrációs Egység közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása a kriptográfiai hardver modulok megfelelő funkcióinak aktivizálásával),

- a felhasználói adatok védelme (a hozzáférés ellenőrzési szabályok érvényre juttatása az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják, a maradvány információ védelmének támogatása),
- azonosítás és hitelesítés (a rendszerüzemeltetők azonosítása, hitelesítése, az alkalmazások által biztosított funkciók elérésének sikeres hitelesítéshez kötése).

A **kriptográfiai hardver modulok** által megvalósított biztonsági funkciók az alábbiak:

- kriptográfiai támogatás (kriptográfiai kulcsok generálása, védelme és megsemmisítése; bizalmasságot, sértetlenséget, hitelességet és letagadhatatlanságot biztosító kriptográfiai eljárások megvalósítása),
- a felhasználói adatok védelme (a saját hozzáférés ellenőrzési szabályok érvényre juttatása),
- azonosítás és hitelesítés (a saját felhasználók /biztonsági tisztviselők vagy rendszerüzemeltetők azonosítása, hitelesítése, a saját funkciók elérésének sikeres hitelesítéshez kötése),
- biztonságkezelés (saját biztonsági szerepkörök kezelése, a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
- a biztonsági funkciók megbízható védelme (saját működés biztonsági tesztelése, biztonságos állapot megőrzése hiba esetén, a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása),
- megbízható út/csatorna (megbízható útvonal kiépítése a magát hitelesítő felhasználóval, mely alkalmas az átvitt adatok illetéktelen felfedésének és módosításának megakadályozására).

Az informatikai biztonsági intézkedéseket részletesen a Szolgáltató Biztonsági Szabályzata tartalmazza.

7.5.2 Informatikai biztonsági osztályozás

Az ide vonatkozó rendelkezéseket a Szolgáltató belső használatú Kockázatkezelési Szabályzata tartalmazza.

7.6 Életciklusra vonatkozó műszaki óvintézkedések

7.6.1 Rendszerfejlesztési óvintézkedések

A Szolgáltató által fejlesztett rendszerek esetében sor kerül az esetleges kockázatok felmérésére és elemzésére.

A Szolgáltató a maga által fejlesztett szoftverek esetében változáskezelési eljárást alkalmaz a kibocsátásokra, a módosításokra, és a sürgős szoftver javításokra. A változáskezelési eljárás lehetőség szerint az üzembehelyezés előtt lezajlik. Ez alól kivételt képezhetnek a sürgős javítások, melyek esetében a dokumentálás utólagos elvégzésére is van lehetőség, amennyiben a szoftverjavítás késedelmes üzembe helyezése a Szolgáltató működését érdemben veszélyezteti, illetve jelentős anyagi vagy erkölcsi kárt okozna.

Az ide vonatkozó rendelkezéseket részletesen a Szolgáltató belső használatú Szoftverfejlesztési Szabályzata és Informatikai Változáskezelési Szabályzata tartalmazza.

7.6.2 Biztonságkezelési óvintézkedések

A Szolgáltató kockázatelemzést végez az üzleti kockázatainak felmérésére, széleskörűen figyelembe véve a szolgáltatásokat, adatokat, eszközöket, információkat fenyegető veszélyforrásokat. A kockázatelemzés eredménye alapján határozza meg a szükséges biztonsági követelményeket és a működési eljárásokat.

A Szolgáltató különös figyelmet fordít a biztonságra a beszerzések során is: a kulcsfontosságú rendszereinek szállítói a Beszerzési Szabályzat szabályai szerint értékelt beszállítók, illetőleg a beszerzett eszközök értékelt eszközök. Kiválasztásuk gondos mérlegelés alapján történt, a beruházás

megtörténte után a kapcsolat hosszabb távú. Az eszközök gyártói számos referenciával és megbízható háttérrel rendelkező szervezetek. Ezen szabályok biztosítják, hogy Szolgáltató eszközeihez szükség esetén megkapja a szükséges támogatást, illetve meghibásodás esetén a szállítóval szembeni jótállási, szavatossági igények érvényesíthetők legyenek.

A felhasznált, beépített eszközök nagyrészt a kereskedelmi forgalomban könnyen beszerezhetők, így azok pótlása számos forrásból, viszonylag gyorsan megoldható.

7.6.3 Az életciklusra vonatkozó biztonság osztályozása

Az alkalmazott biztonsági eljárások, módszerek értékelését független szakértő vizsgálja. A folyamatos, magas színvonalú biztonságos szolgáltatás fenntartására a Szolgáltató ISO 27001 (korábban BS 7799-2:2002 elnevezésű) szabványnak megfelelő információbiztonsági irányítási rendszert is alkalmaz, amelyet ugyancsak független külső és belső auditorok vizsgálnak.

A szükséges biztonsági értékelést független auditor vizsgálja.

7.7 Hálózatbiztonsági óvintézkedések

A Szolgáltató saját hálózatát a nyílt hálózatokról tűzfal szerverekkel választja le. Az ide vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat és az Üzletmenet Folytonossági- és Katasztrófa Terv tartalmazza.

A **tűzfal** és a **behatolás detektáló** által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a hálózati kommunikáció naplózása, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),
- a felhasználói adatok védelme (az információ áramlás ellenőrzési szabályok érvényre juttatása /szűrés, a tiltott információ áramlás megakadályozása, megfigyelése),
- azonosítás és hitelesítés (a saját felhasználók /hálózati adminisztrátorok/ azonosítása, hitelesítése, a saját funkciók elérésének sikeres hitelesítéshez kötése),
- a biztonsági funkciók megbízható védelme (az információ áramlás ellenőrzés megkerülhetetlenségének biztosítása).

7.8 A kriptográfiai modul ellenőrzése

Szolgáltató a jelen Szabályzat vonatkozó részében megadott szintű minősítéssel rendelkező kriptográfiai modulokat alkalmaz. Az ide vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat és az Üzleti Folytonossági Terv tartalmazza.

7.8.1 Időforrás és időszinkronizáció

A Szolgáltató megbízható rendszereinek belső órája szabványos időforráshoz van szinkronizálva.

A Szolgáltató a csatlakoztatott időforrást szolgáltató berendezések esetében a beérkező időadatok sérthetetlenségét, illetve módosíthatatlanságát biztosítja.

A rendszeridő szinkronitásának kiesését a Szolgáltató a szinkron eltérés észlelésének időpontjában az eltérés mértékének megjelölésével naplózza, illetve időszinkron kieséskor OCSP válaszadás, CRL- és tanúsítvány kibocsátás, valamint időbélyegzés-szolgáltatást nem végez.

7.8.2 Az időforrások megnevezése

A Szolgáltató több független UTC forrási rendszert és azok jeleit venni képes eszközöket alkalmaz az időforrás üzembiztonsága érdekében:

- időforrás GPS: GPS műholdas navigációs rendszer által szolgáltatott referenciaidő,
- időforrás DCF: németországi referenciaidő,
- időforrás PRS: ACTS kompatibilis nemzeti időszolgáltatókhoz szinkronizált, nagy pontosságú, rubídium oszcillátor alapú, független helyi időforrás,
- időforrás NTP: minimum 4 stratum 1 szintű, interneten elérhető NTP szerver.

7.8.3 Időforrás pontossága

A megbízható rendszerek minden időponttal kapcsolatos szolgáltatáshoz használt óráját a Szolgáltató szinkronizálja az ún. koordinált, egységes időforrással (UTC - Universal Time Co-ordinated) minősített időbélyegzés esetén legalább 0,1 másodperces, egyéb hitelesítés-szolgáltatáshoz kapcsolódó tevékenység esetén legalább egy másodperces pontossággal. A Szolgáltató által alkalmazott időforrás pontossága maximum néhány ezred másodperc eltérés az UTC-hez képest.

Szolgáltató biztosítja az egyedi külső időforrások szinkronból kiesése, vagy elérhetetlensége esetére a rendszereinek megbízható időforrással való kapcsolatát.

Az időszinkronizációt a Szolgáltató az elfogadott referencia időhöz képest minimum naponta 64 alkalommal elvégzi, amennyiben a szinkronitási követelmény teljesítéséhez ez szükséges, a napi időszinkronizációk számát növeli.

7.8.4 Alkalmazott eszközök

Időszinkronizációs eszközök	Időszinkronizációs forrás
HOPF 6039 GPS típusú vevő	GPS műholdas navigációs rendszer (időforrás GPS)
HOPF 6039 DCF típusú vevő	németországi referenciaidő (időforrás DCF)
PRS10 rubídium oszcillátor	ACTS kompatibilis nemzeti időszolgáltatók (időforrás PRS)
NTP szerver	4 külső időforrás (időforrás NTP)

8 Tanúsítvány, -visszavonási lista és időbélyeg profilok

8.1 Tanúsítványprofilok

A Szolgáltató az X.509 [10] ajánlásnak megfelelő tanúsítványokat bocsát ki.

8.1.1 Személyes végfelhasználói tanúsítványok profiljainak állandó elemei

Mező	Tartalom
Common Name	Az Alany neve a személyazonosító igazolványában szereplő írásmódon Álnév használatát megengedő tanúsítványtípus esetén “ALNEV„ előtét, vagy a „(*)” karakter illetve az elfogadott álnév. Pseudonym mező használata esetén a szabályzatban meghatározott adattartalom
Organization	a mező nincs megjelenítve vagy „—„
Organization Unit	a mező nincs megjelenítve vagy „—„
Country	Lakóhely szerinti ország kódja ISO 3166 [5] szerint MHR_Ü: HU
Locality	Lakcím szerinti város
State	Nem megjelenített / „—„ vagy lakcím szerinti megye (MHR_Ü)
Title	Beosztás vagy a mező nincs megjelenítve
E-mail	Az Alany e-mail címe vagy a mező nincs megjelenítve / „—„ MHR_Ü: Az Alany e-mail címe
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	cA = FALSE (kritikus kiterjesztes)
KeyUsage	NonRepudiation (kritikus kiterjesztes)
qcStatements	qcCompliance (kritikus kiterjesztes)
További kiterjesztések	A profildefiníciókat tartalmazó dokumentumok [20], [24] részletezik
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	Kibocsátó adatai
Signature	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)

8.1.2 Munkatársi végfelhasználói tanúsítványok profiljainak állandó elemei

Mező	Tartalom
Common Name	Az Alany neve a személyazonosító igazolványában szereplő írásmódon Álnév használatát megengedő tanúsítványtípus esetén “ALNEV„ előtét, , vagy a „(*)” karakter, illetve az elfogadott álnév Pseudonym mező használata esetén a szabályzatban meghatározott adattartalom
Organization	Szervezet(ek), azaz a másodlagos Alany(ok) neve MHR_K: közigazgatási szerv
Organization Unit	Szervezeti egység(ek) neve(i) vagy a mező nincs megjelenítve vagy „—„ MHR_K szervezeti egység
Country	Székhely szerinti ország kódja ISO 3166 [5] szerint MHR_K: HU
Locality	Székhely szerinti város
State	a mező nincs megjelenítve vagy „—„vagy székhely szerinti megye (MHR_K)
Title	Beosztás vagy a mező nincs megjelenítve vagy „—„
E-mail	Az Alany e-mail címe vagy a mező nincs megjelenítve vagy „—„ MHR_K: Az Alany e-mail címe
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Basic Constraints	cA = FALSE (kritikus kiterjesztes)
KeyUsage	NonRepudiation (kritikus kiterjesztes)
qcStatements	qcCompliance (kritikus kiterjesztes)
További kiterjesztések	A profildefiníciókat tartalmazó dokumentumok [20], [24] részletezik

Mező	Tartalom
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	Kibocsátó adatai
Signature	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)

8.2 Szolgáltatói tanúsítványok profilja

8.2.1 Szolgáltatói (tanúsítvány- és visszavonási lista aláíró) főtanúsítvány profilja

Mező	Tartalom
Common Name	A szolgáltató fő tanúsítványának az egyedi elnevezése (zárójelben angol elnevezése)
Organization	NetLock Kft.
Organization Unit	Tanusitvanykiadok vagy Tanúsítványkiadók (zárójelben angol elnevezése)
Country	HU
Locality	Budapest
State	a mező nincs megjelenítve vagy „—„
E-mail	a mező nincs megjelenítve vagy „—„
Public Key	Szolgáltatói tanúsítvány nyilvános kulcsa
Basic Constraints	cA = TRUE, Path Length = 4 (kritikus kiterjesztes)
KeyUsage	Certificate Signing, CRL Signing (kritikus kiterjesztes)
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	Kibocsátó adatai
Signature	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)

8.2.2 Szolgáltatói (tanúsítvány- és visszavonási lista aláíró) kiadói tanúsítvány profilja

Mező	Tartalom
Common Name	A tanúsítvány nevében szerepelnie kell a „minősített” vagy „minositett” szavaknak (zárójelben angol elnevezése szerepelhet)
Organization	NetLock Halozatbiztonsagi Kft. vagy NetLock Kft.
Organization Unit	Tanusitvanykiadok vagy Tanúsítványkiadók (zárójelben angol elnevezése szerepelhet)
Country	HU
Locality	Budapest
State	a mező nincs megjelenítve vagy „—„
E-mail	info@netlock.hu vagy a mező nincs megjelenítve vagy „—„
Public Key	Szolgáltatói tanúsítvány nyilvános kulcsa
Basic Constraints	cA = TRUE, Path Length = 4 (kritikus kiterjesztes)
KeyUsage	Certificate Signing, CRL Signing (kritikus kiterjesztes)
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	Kibocsátó adatai
Signature	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)

8.2.3 Szolgáltatói (visszavonási lista aláíró) tanúsítvány profilja

Mező	Tartalom

Mező	Tartalom
Common Name	A hozzárendelt kiadóhoz kapcsolódó név
Organization	NetLock Halozatbiztonsagi Kft. vagy NetLock Kft.
Organization Unit	Tanusitvanykiadok vagy Tanúsítványkiadók (zárójelben angol elnevezése szerepelhet)
Country	HU
Locality	Budapest
State	a mező nincs megjelenítve vagy üres
E-mail	info@netlock.hu vagy a mező nincs megjelenítve vagy „—„
Public Key	Szolgáltatói tanúsítvány nyilvános kulcsa
Basic Constraints	cA = FALSE
KeyUsage	CRL Signing (kritikus kiterjesztes)
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	Kibocsátó adatai
Signature	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)

8.2.4 Szolgáltatói (időbélyegző) tanúsítványok profilja

Mező	Tartalom
Common Name	A tanúsítvány nevében szerepelnie kell a „minősített” vagy „minositett” és az „időbélyeg” vagy „idobelyeg” szavaknak
Organization	NetLock Halozatbiztonsagi Kft.
Organization Unit	Tanusitvanykiadok
Country	HU
Public Key	Szolgáltatói tanúsítvány nyilvános kulcsa
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	KGYHSZ (Public Administration Root CA - Hungary)
Signature	sha1RSA

8.2.5 Szolgáltatói (OCSP válasz aláíró) tanúsítványok profilja

Mező	Tartalom
Common Name	NetLock OCSP Kiszolgalo
Organization	NetLock Kft.
Organization Unit	Idobelyeg Szolgaltatok vagy Időbélyeg Szolgáltatók
Country	HU
Locality	Budapest
State	a mező nincs megjelenítve
E-mail	a mező nincs megjelenítve
Public Key	Időbélyegző tanúsítvány nyilvános kulcsa
basic Constraints	cA = FALSE (kritikus kiterjesztes)
keyUsage	NonRepudiation (kritikus kiterjesztes)
extendedKeyUsage	timeStamping (kritikus kiterjesztes)
További kiterjesztések	A profildefiníciókat tartalmazó dokumentumok [20], [24] részletezik
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	Kibocsátó adatai
Signature	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)

8.2.6 Közigazgatási Gyökér Hitelesítés-Szolgáltató által felülhitelesített szolgáltatói (tanúsítvány- és visszavonási lista aláíró) tanúsítvány profilja

Mező	Tartalom
Common Name	A tanúsítvány nevében szerepelnie kell a „minősített” vagy „minositett” és a „közigazgatási” vagy „kozigazgatasi” szavaknak (zárójelben angol elnevezése szerepelhet)
Organization	NetLock Halozatbiztonsagi Kft. vagy NetLock Kft.
Organization Unit	Tanusitvanykiadok vagy Tanúsítványkiadók (zárójelben angol elnevezése szerepelhet)
Country	HU
Public Key	Szolgáltatói tanúsítvány nyilvános kulcsa
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Issuer	KGYHSZ kiadó gyökértanúsítványában megtalálható elnevezés
Signature	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)

A Közigazgatási Gyökér Hitelesítés-szolgáltató által alkalmazott tanúsítványprofil ismertetését a KGYHSZ Hitelesítési Szabályzata [30] tartalmazza.

8.3 Tanúsítvány visszavonási lista profil

A Szolgáltató az x.509 [9] megfelelő visszavonási listákat (CRL) bocsát ki. A Szolgáltató által aktuálisan kibocsátott tanúsítvány visszavonási lista profilokat a Minősített tanúsítvány, -visszavonási lista és időbélyeg profildefiníciók [18] dokumentum tartalmazza és azt a Szolgáltató saját Internetes oldalán (ld. 1.5 alfejezet), a Tanúsítványtárnál megadott publikálási szabályoknak megfelelően közzéteszi.

Mező	Tartalom
Version	V2
Issuer	Kiadónként eltérő, lásd profildefiníciók [18]
Last update	Utolsó kibocsátás dátuma
Next update	Következő kibocsátás dátuma
Signature	Kibocsátó elektronikus aláírása
CRL entry	Az érvénytelenített tanúsítvány sorozatszáma, érvénytelenítés dátuma, időpontja
CRL entry extension	Profildefiníciók [20] dokumentum tartalmazza

8.4 Időbélyeg-profil

A Szolgáltató által nyújtott időbélyegzés szolgáltatás az RFC3161-es szabvány [16], az ETSI TS 101 861 [15] technikai leírás és az Irányelv [2] ajánlásainak figyelembevételével működik. A Szolgáltató által aktuálisan kibocsátott időbélyeg profilokat a Minősített tanúsítvány, -visszavonási lista és időbélyeg profildefiníciók [18] dokumentum tartalmazza és azt a Szolgáltató saját Internetes oldalán (ld. 1.5 alfejezet), a Tanúsítványtárnál megadott publikálási szabályoknak megfelelően közzéteszi.

Mezők, tulajdonságok	Tartalom, értelmezés
Időbélyeg kérelemben engedélyezett hash algoritmus	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)
Időbélyeg kérelemben megnevezhető szabályzati azonosító (OID)	Üresen hagyható vagy a kért szabályzat azonosítója
Időbélyeg kérelemben szereplő véletlen szám (nonce) hossza	Maximum 64 bit
Időbélyeg kérelemben kérhető-e a szolgáltató tanúsítványa (certReq)	Igen
Időbélyeg válaszban szereplő szabályzati azonosító (OID)	A kért szabályzat azonosítója
Az időbélyeg válasznál használt hash algoritmus	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)
Az időbélyeg válasznál használt aláíró algoritmus	Aktuálisan használható kriptográfiai algoritmusok (1.1.5.2, 1.1.5.3)
Kiterjesztések	Profildefiníciók [18] dokumentum tartalmazza
Verzió	V1

Mezők, tulajdonságok	Tartalom, értelmezés
Sorszám mérete	Dinamikus hosszúságú
Sorszám egyedisége	Az időbélyegzőben használt sorszám egyedi a Szolgáltatóra nézve. Ez a tulajdonság ésszerű keretek között fennmarad a szolgáltatás lehetséges megszakadása után is.

9 A megfelelőség vizsgálata

Szolgáltató szolgáltatásának következő elemeinek megfelelőségét vizsgálja, vizsgáltatja:

- a végfelhasználói tanúsítványok aláírására használt biztonságos eszközeit;
- a saját magánkulcsainak tárolására használt kriptográfiai hardver modult;
- az Alanyok számára biztosított biztonságos aláíró eszközöket (pl. intelligens kártyákat);
- a végfelhasználói és szolgáltatói tanúsítványok kezeléshez használt módszereit, eljárásait;
- a közigazgatásban felhasználható tanúsítványokra vonatkozó előírások teljesülését ([4], [5], [19]);
- az ISO 9001 minőségbiztosítási rendszer előírásai szerinti működést;
- az ISO 27001 információbiztonsági irányítási rendszer előírásainak megfelelő működést.

9.1 A megfelelőség vizsgálatának gyakorisága

A különböző vizsgálatokra a jogszabályoknak megfelelően az alábbi gyakorisággal kerül sor:

- az eszközök vizsgálatára a használatba vételt megelőzően egyszer, majd a folyamatos megfelelés ellenőrzéseképpen legalább évente;
- a tanúsítványok kezeléshez használt módszerek, eljárások tanúsítására átfogó helyszíni ellenőrzéssel együtt évente legalább 1 alkalommal, független elektronikus aláírás szakértői ellenőrzés keretében, illetve a szakhatóság döntése szerint, szakhatósági eljárás keretében bármikor;
- a magas színvonalú szolgáltatást biztosító ISO 9001 minőségbiztosítási rendszer ellenőrzésére évente legalább 1 alkalommal, a teljes rendszerre vonatkozóan;
- az információbiztonsági irányítási rendszer ISO 27001 szabványnak való megfelelés ellenőrzése évente legalább 1 alkalommal a teljes rendszerre vonatkozóan;

9.2 Az átvizsgáló egységek megnevezése

A megfelelőségi vizsgálatokat külső szervezetek végzik/végezték:

- a biztonságos aláírás létrehozó eszközök tanúsítását a jogszabályi előírásoknak megfelelő tanúsító szervezet (ld. [1] Törvény 24. §), amelynek kijelölésére a [16] Rendelet előírásainak megfelelően kerül sor;
- a minősített és a közigazgatásban használható minősített tanúsítványok kezeléshez használt módszerek, eljárások ellenőrzését hatósági eljárás keretében a Felügyelet;
- a közigazgatásban használható tanúsítványokra vonatkozó előírásoknak ([4], [5], [19]) való megfelelést a Közigazgatási Gyökér Hitelesítés-szolgáltató;
- a szolgáltatási rendszer jogszabályi követelményeknek való megfelelését, illetve biztonságát legalább évente független szakértő felülvizsgálja. A vizsgálat kiterjed a kontroll rendszerre, a szabályozásra, a szabályok implementációjára és azok monitorozására;
- az ISO 9001 minőségbiztosítási rendszer működtetését legalább évente akkreditált ISO tanúsító szervezet;
- az ISO 27001 információbiztonsági irányítási rendszer működtetését legalább évente akkreditált, külső, független tanúsító szervezet.

A Szolgáltató e külső vizsgálatokon túl saját belső ellenőrzési rendszerrel is rendelkezik, mely rendszeresen vizsgálja a korábbi tanúsításoknak való megfelelőséget, és eltérés esetén megteszi a

szükséges lépéseket. Az egyes szolgáltatói tevékenységek a jogszabályoknak és kapcsolódó szabályzatoknak való megfelelését a Szabályzat Elfogadó Egység vizsgálja saját munkarendje szerint.

9.3 Az átvizsgáló egységek és a vizsgált fél kapcsolata

A Szolgáltatóval kapcsolatban vizsgálatot végző külső szervezetek a Szolgáltatótól függetlenek, és befolyástól mentesen végzik tevékenységüket. A vizsgálatot végző szervezetek nem rendelkeznek tulajdonrésszel vagy érdekeltséggel a Szolgáltatóban, és a Szolgáltató nem tulajdonosa közvetlenül vagy közvetve a vizsgálatot végző szervezeteknek. A szervezetek díjazása nem függ a tanúsítás során végzett tevékenységük megállapításaitól.

A belső függetlenséget a munkatársak esetében a Szolgáltató Függetlenségi Nyilatkozat aláíratásával, valamint a tevékenységi körök elválasztásával biztosítja. A Nyilatkozatot a Szolgáltató Személyzeti Politikája tartalmazza.

9.4 A vizsgálat által érintett területek

A vizsgálatok vizsgáló szervezetenként más és más területekre terjednek ki. A vizsgálatok keretében sor kerül valamennyi a Szolgáltató működésére vonatkozó jogszabályi feltétel teljesítésének ellenőrzésére. A vizsgálatok kiterjednek továbbá a Szolgáltató saját hitelesítés-szolgáltatási rendjeinek és egyéb szabályzatainak való megfelelőség ellenőrzésére is.

A szabályzatoknak való megfelelés vizsgálata során a Szolgáltató teljes tevékenységi köre, illetőleg annak összes belső szabályzata vizsgálatra kerül (így például a Regisztrációs és Hitelesítő Egységek szabályzatai).

9.5 Hiányosságok esetén végrehajtandó tevékenységek

A Szabályzat Elfogadó Egység a jogszabályok illetve szabványok, szokványok és ajánlások előírásainak ellentmondó működés esetén a szolgáltatói tevékenységeket szabályozó belső eljárásrendek és szabályzatok megváltoztatásával, illetőleg a változás végrehajtásához szükséges rendszer implementáció végrehajtatásával intézkedik.

A szolgáltatói tevékenységet lényegesen érintő változások bejelentésre kerülnek a felügyeleti szerv, illetve a Közösség felé.

10 Üzleti és jogi tudnivalók

10.1 Díjak

A mindenkor érvényes szolgáltatások díjait a Szolgáltató saját Internetes oldalán (ld. 1.5 alfejezet), a Tanúsítványtárnál megadott publikálási szabályoknak megfelelően közzéteszi.

A közzétett adatok:

- tanúsítvány kibocsátásának és megújításának díja,
- tanúsítvány hozzáférési, tárolási díj,
- visszavonási adatok hozzáférési díja,
- időbélyegzés díja,
- egyéb, a hitelesítés-szolgáltatáshoz kapcsolódó, különleges díjtételek (pl.: különeljárási díj, stb.).

A tanúsítvány kibocsátásának és megújításának a Szolgáltató mindenkor érvényes díjszabásában közzétett díja abban az esetben érvényes, ha a regisztráció Alanya, illetve másodlagos Alanya eleget tud tenni a Szolgáltató regisztrációs eljárásrendjében meghatározott feltételeknek. A regisztrációs eljárásrendről tájékoztatás a Szolgáltató tanúsítványtárában található, a Központi Regisztrációs Egységtől és ügyfélszolgálattól kérhető (lásd 1.5 pont), valamint a tanúsítványkérés megkezdésekor automatikus tájékoztató is továbbításra kerül. A regisztrációs eljárásrendben meghatározott eseteken kívül (tipikusan külföldi személyazonosítók, elektronikusan nem lekérdezhető szervezeti nyilvántartások ellenőrzésének szükségessége) a Szolgáltató egyedi díjszabást alkalmaz.

A Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF tartalmazza.

10.1.1 Egyéb szolgáltatásokra vonatkozó díjak

A Szolgáltató a kibocsátott tanúsítványok visszavonásáért, felfüggesztéséért és újraérvényesítéséért eljárási díjat számolhat fel az Alany/Igénylő felé, mely tartalmazza a tanúsítvány megváltozott állapotának a tanúsítványtárban visszavonási lista formájában történő közzétételének költségét.

A Szolgáltató az ezt Igénylő ügyfeleinek emelt szintű szolgáltatásokért (pl. közvetlen bérelt vonali hozzáférés, gyorsított kibocsátás) egyedi díjszabást alkalmazhat.

A Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF tartalmazza.

10.1.2 Visszatérítési elvek

Indokolt esetben a Szolgáltató a tanúsítványok kibocsátásához kapcsolódó, meghatározott időszakra vonatkozó egyes díjakat (pl.: tanúsítványtárolási díj) egyedi elbírálás alapján, időarányosan téríti vissza. Az egyszeri díjak visszatérítése teljes összegben történik.

Az Alany, illetve másodlagos Alany a számára kibocsátott tanúsítvány kibocsátási és teljes fenntartási díjának visszatérítésére tipikusan a következő esetekben jogosult:

- a kibocsátott tanúsítvány valamely adata a Szolgáltató hibájából fakadóan nem megfelelő,
- a Szolgáltató egyéb hibát követ el a tanúsítvány kibocsátásakor,
- a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét az Alany tanúsítványának kezelésekor.

A díj visszatérítésére az Alanynak, illetve másodlagos Alanynak a tanúsítvány kibocsátását vagy megújítását követő 30 naptári napon belül a regisztrációs egység központi egységénél kérvényben kell beadnia a Szolgáltató részére. A kérvény pozitív elbírálása esetén a Szolgáltató a tanúsítványt díjmentesen visszavonja és a kibocsátási és teljes fenntartási díjat az Alany/Igénylő számára a kérelemben megjelölt bankszámlaszámra 20 naptári napon belül visszautalja.

A tanúsítvány kibocsátása, illetve megújítása a Szolgáltató általi teljesítésnek tekintendő, így ezt követően az Alany/Igénylő kizárólag csak a Szolgáltató bizonyított szerződés- vagy kötelezettségszegése esetén jogosult díjvisszatérítésre. Nem tartozik a visszatérítési okok közé különösen a kibocsátott tanúsítványhoz tartozó magánkulcs bármely okból történő megsemmisülése.

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

10.2 Pénzügyi felelősség

A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személynek okozott kárért a Polgári Törvénykönyv általános szabályai szerint felel, az Aláíróval szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással vagy időbélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal okozott kárért, ha az [1] Törvényben vagy egyéb jogszabályokban foglalt kötelezettségeit, így különösen az alábbiakat megszegte.

- 7. § (2): megfelelő aláíró eszköz használatának kötelezettsége,
- 9-11. §: tájékoztatási és adatvédelmi kötelezettségek,
- 14. §: tanúsítvány felfüggesztéssel és visszavonással kapcsolatos kötelezettségek.

A Szolgáltató a Törvény 6. § (4), illetve a 9. § (2) bekezdése szerint az alábbiakban meghatározza az egy alkalommal vállalható legmagasabb kötelezettség értéket. Figyelembe véve a Törvény adta lehetőségeket, illetve tekintettel a tanúsítványok kockázat - ár viszonyára, az ezen korlátokat meghaladó ügyletekben kibocsátott és aláírt elektronikus dokumentumból származó követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.

Az egy alkalommal vállalható legmagasabb kötelezettség értéke minősített tanúsítványoknál a tanúsítványban feltüntetett összeg, amennyiben ilyen korlát nem szerepel benne, akkor 50,000,000 magyar forint, azaz ötven millió magyar forint.

A Szolgáltató biztosítója azon bizonyított károkért, amelyek a Szolgáltató felelősségi körében annak saját hibájából vagy mulasztásából keletkeztek, kártérítést fizet a fenti, káreseményenkénti felső határral.

Az egyes tanúsítványok esetén a felelősségbiztosítás egy biztosítási esemény vonatkozásában káreseményenként a fent felsorolt összeghatár ötszörös értékéig biztosít fedezetet az összes károsultnak okozott károkra. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

10.3 Bizalmasság, adatvédelem

A Szolgáltató a birtokába jutott adatokat a hatályos jogszabályi rendelkezésekre figyelemmel tárolja és kezeli. A Szolgáltató a törvényi előírásokon túlmenően saját belső szabályozási rendszerében is rögzített módon mindent megtesz az ügyfelek adatainak biztonságos kezelése érdekében.

Az adatgyűjtések célja a hitelesítés-szolgáltatási tevékenység regisztrációs feladatainak ellátása. A Szolgáltató az adatokat a törvények által előírt eseteken kívül kizárólag a főtevékenység hatékonyságának funkcionális támogatásához (lásd 10.3.8 pont), illetve megfelelő módon anonimizálva a belső statisztikáihoz használja fel.

Szolgáltató a regisztráció során kitöltött regisztrációs adatlap adatait elektronikus formában, a jelen Szabályzatban meghatározott azonosítási eljárások végrehajtása során fénymásolat formájában birtokába jutott adatokat papír alapon illetve elektronikus formában tárolja. Biztonságos fizikai tárolással, illetve logikai védelmi rendszerrel biztosítja az adatok biztonságát, lehetővé téve az adatvesztés, adatsérülés, az adatok helytelen vagy illetéktelen használatának elkerülését.

A Szolgáltató a hatályos jogszabályoknak megfelelően a tanúsítványokkal kapcsolatos elektronikus információkat – beleértve az azok előállításával összefüggőket is – és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejártától számított 10 évig, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős

lezárásáig megőrzi (amennyiben annak kezdetéről és végéről a 10.5.3.1 pontban megfogalmazott kötelezettségek szerint értesítik), valamint ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.

A Szolgáltató biztosítja, hogy honlapján történő információkeresés, illetve az ún. ügyfélmenü használatán kívül eső oldalak tallózása során az ügyfelek névtelenek maradjanak.

A Szolgáltató biztosítja, hogy bármely adat rendelkezésre bocsátása esetén ezen adatokhoz illetéktelen személyek ne férhessenek hozzá.

10.3.1 Bizalmasan kezelendő információ típusok

Alapértelmezésben a felhasználók azon adatai, amelyek a tanúsítványban nem szerepelnek. Bizalmas adatnak számítanak továbbá a Szolgáltató belső eljárásrendjei és a magánkulcsok.

10.3.2 Nem bizalmasnak tekintett információ típusok

Azon regisztrációs adatok, amelyeket a felhasználó engedélye alapján a Szolgáltató nyilvánosként kezel. Nyilvánosak továbbá a tanúsítványtárban elhelyezett tanúsítványok, a szabályzatok, a CRL.

10.3.3 Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése

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

10.3.4 Információszolgáltatás hatósági szervek részére

A Szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint az [1] Törvény 12. §-ának megfelelően egyeztetett adatok tekintetében az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét a Szolgáltató rögzíti, az adatátadásról a Szolgáltató a Törvény rendelkezéseinek értelmében az Aláírót nem tájékoztathatja.

A Szolgáltató a Felügyelet részére az [1] Törvény 8/A §-a alapján hozott határozata alapján felmérések, elemzések és értékelések készítése céljából adatot szolgáltat. A Szolgáltató a Felügyeletnek történő adatszolgáltatás során is biztosítja az adatok bizalmasságát, azok valódiságát és hiánytalanságát.

A Szolgáltató tevékenységének befejezése esetén, amennyiben a tevékenység befejezését követően más, az adott szolgáltatást azonos, vagy magasabb szinten végző szolgáltató nem szerepel a Felügyelet nyilvántartásában a tanúsítvánnyal kapcsolatos adatokat az [1] Törvény 16. §-ának rendelkezéseinek megfelelően a Felügyeletnek adja át.

10.3.4.1 MHR_Ü, MHR_K

A Szolgáltató a közigazgatásban felhasználható tanúsítványok esetében az ügyintéző hatóság elektronikus úton történő megkeresésére viszontazonosítást végez. Ennek során a Szolgáltató összeveti a megadott természetes személyazonosító adatokat az általa kezelt, beazonosított természetes személyazonosító adatokkal, és válaszként megküldi a hatóság részére, hogy a viszontazonosítás során megadott adatok megegyeznek-e az általa kezelt személyazonosító adatokkal.

10.3.5 Információszolgáltatás polgári peres eljárás keretében

A Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során az Aláíró személyazonosságát igazoló adatokat átadhatja az ellenérdekű peres félnek vagy képviselőjének, illetőleg azt közölheti a megkereső bírósággal a 10.3.8 pontban leírtakat is figyelembe véve.

10.3.6 Egyéb információszolgáltatás

A Szolgáltató tevékenységének befejezésekor a tanúsítványokkal kapcsolatos adatokat (így különösen tanúsítványokkal kapcsolatos változások adatai, a tanúsítványok aktuális helyzetéről, visszavonásáról, felfüggesztéséről vezetett nyilvántartásokat) az [1] Törvény 16. §-a alapján más, vele a befejezett szolgáltatás vonatkozásában azonos besorolású hitelesítés-szolgáltatónak adja át. A tevékenység befejezése esetén a Felügyelet részére történő adatszolgáltatás szabályait a 10.3.4 pont tartalmazza.

10.3.7 Az Alany kérésére történő felfedés

A Szolgáltató az Alany, illetve másodlagos Alany meghatalmazása alapján tár fel bizalmas felhasználói információkat harmadik fél részére, melyért a Szolgáltató az internetes oldalán (lásd 1.5 pont) feltüntetett, mindenkor érvényes különeljárási díjat számol fel.

10.3.8 Egyéb információ harmadik félnek történő átadása

Egyéb információ harmadik félnek történő átadására sor kerülhet 30 napja lejárt díjtartozás esetén, annak érvényesítése céljából.

A Szolgáltató átadhat egyéb információt vele szerződéses kapcsolatban álló olyan szervezeteknek, amelyek a Szolgáltató szolgáltatásai kapcsán kibocsátott elektronikus dokumentumok vagy az azokkal hitelesített más elektronikus dokumentumok érvényességének, hatályosságának, alkalmazhatóságának megállapításával kapcsolatos szolgáltatást nyújtanak.

10.4 Szellemi alkotásokhoz fűződő jogok

A szolgáltatási tevékenység során alkalmazott összes név, termék, szabályzat, CRL a Szolgáltató tulajdonát képezi, a szoftver és hardver komponensek a Szolgáltató tulajdonát képezik vagy azokat jogszerűen használja.

10.5 Jogok és kötelezettségek

10.5.1 A hitelesítő egységek közös kötelezettségei

a) szabványos X509 tanúsítvány kibocsátása, megújítása, felfüggesztése, reaktiválása, visszavonása a Központi Regisztrációs Egység által küldött erre vonatkozó kérelem esetén,

b) tanúsítvány felfüggesztésének vagy visszavonásának publikálása CRL-en,

c) saját tanúsítványának nyilvánosságra hozatala,

d) saját magánkulcsának teljes körű védelme, a kulcs dedikált kriptográfiai hardver modulban történő tárolásával,

e) a hitelesítő kulcspár kompromittálódásának feltételezése, a kulcspár sérülése, megsemmisülése esetén az alkalmazó Közösség tagjainak késedelem nélküli értesítése elektronikusan (pl. elektronikus levélben, Internet oldalon közzététellel), illetve out-of-band módon (pl. postai úton, napilapban közzététellel) továbbá a Szabályzatért Felelős Egység bármely tagjának írásban vagy személyesen történő megkeresésével.

10.5.2 A Regisztrációs Egységek közös kötelezettségei

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

b) tevékenységüket saját maguk ellátni,

c) az Igénylő tanúsítványra vonatkozó kérelmeinek (kibocsátás, megújítás, felfüggesztés, visszavonás) kezelése,

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

e) a nem nyilvános ügyféladatok megfelelő szintű védelme,

f) az Igénylő és a Közösség többi tagjának értesítése a tanúsítvány kibocsátásáról és a tanúsítvánnyal végzett műveletekről,

g) a tanúsítványnak az Alany számára elérhetővé tétele,

h) a belépés lehetővé tétele a Szabályzatért Felelős Egység számára a szolgáltatás területére.

10.5.2.1 Külső regisztrációs munkatársak

a) a személyazonosságot és az egyéb adatok valódiságát igazoló okmányoknak ellenőrzése és az ügyfél Szolgáltatási Szerződésének - az igényelt felelősségvállalás mértékétől, illetve egyéb feltételekről függően - aláírás-hitelesítése.

b) az ellenőrzésére használt eredeti iratok másolatának a Szolgáltatónál működő központi egységhez való eljuttatása.

10.5.2.2 Minősített Központi Regisztrációs Egység

a) A külső regisztrációs munkatársak hitelesítésének ellenőrzése

b) a hitelesítés ellenőrzése, melynek alapját a hozzá eljutatott másolati dokumentumok képezik; és az adatok valós idejű, elektronikus közhiteles nyilvántartásban való ellenőrzése.

c) a tanúsítvány- és visszavonási kérelem nyilvántartásba vétele és a kérelem elbírálása, továbbítása.

10.5.3 A végfelhasználó kötelezettségei

10.5.3.1 A végfelhasználó általános kötelessége:

a) megismerni és betartani az Általános Szerződési Feltételeket és a jelen Szabályzatot,

b) igényeinek megfelelő hitelesítési rendet választani minősített tanúsítvány igénylése előtt,

c) igényeinek és a kiválasztott hitelesítési rendnek megfelelő tanúsítványfajtát kiválasztani,

d) választani a Szolgáltató által meghatározott egy alkalommal vállalható legmagasabb összeghatárok közül, amely feltüntetésre kerül a kibocsátott tanúsítványban,

e) jelezni a Szolgáltatónak, ha a tanúsítványt jogszabályban meghatározott ügyintézésre is fel kívánja használni,

f) álnevet tartalmazó tanúsítvány esetén olyan álnevet választani, amely mások jogait nem sérti,

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

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

i) esetleges jogvita kezdetéről és jogerős lezárásáról haladéktalanul tájékoztatni a Szolgáltatót,

j) az aláírással vagy az így aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt – külön jogszabályban, illetve a Szabályzatban meghatározott – rendellenességről tájékoztatni a Szolgáltatót,

k) betartani a tanúsítványban jelzett esetleges korlátozásokat.

10.5.3.2 A végfelhasználó kötelessége saját kulcs kezelése során:

a) a magánkulcsát biztonságos módon tárolni, kezelni,

b) a kulcspárt és tanúsítványát rendeltetésszerűen használni,

c) magánkulcsát a hozzá tartozó tanúsítvány lejárta után megsemmisíteni,

d) amennyiben magánkulcsa kompromittálódásának lehetősége fennáll, a lehető leghamarabb tanúsítványának visszavonását, illetve felfüggesztését kérni a Szolgáltatótól.

10.5.3.3 A végfelhasználó kötelessége a tanúsítványának kezelése során:

a) a tanúsítványkiadáshoz előírt regisztrációs eljárásrend alapján felvett adatainak valódiságát a jelen Szabályzat vonatkozó pontjaiban (ld. 3. fejezet) található eljárások alapján a szükséges okmányok eredetijének, hiteles másolatának továbbá másolatának bemutatásával alátámasztani,

b) az azonosításához szükséges személyazonosító adatokról, munkatársi tanúsítvány esetén a szervezet nevében aláírásra jogosult személy személyazonosító adatairól, valamint a cégadatokról és mindezek változásáról tájékoztatni a Szolgáltatót,

c) a Törvény 2. számú mellékletének *d)* pontja szerinti adatokról (az Aláírónak külön jogszabályban, illetve a Szolgáltatási Szabályzatban, illetőleg az Általános Szerződési Feltételekben meghatározott speciális jellemzői, a tanúsítvány szándékolt felhasználásától függően) és azok változásáról tájékoztatni a Szolgáltatót,

d) a Törvény 2. számú mellékletének *k)* pontja szerinti adatokról (más személy [szervezet] képviseletére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minősége és a képviselt személy [szervezet] adatai) és azok változásáról tájékoztatni a Szolgáltatót,

e) a regisztrált adatainak a kibocsátott tanúsítványának érvényességi ideje alatt történő megváltozásáról késedelem nélkül a Szolgáltatót tájékoztatni,

f) olyan eljárásokat követni és alkalmazásokat használni, amelyek támogatják a Szolgáltató által kibocsátott tanúsítványok helyes kezelését,

g) a tanúsítvány első felhasználása előtt ellenőrizni a tanúsítványban feltüntetett adatainak helyességét és amennyiben azok nem felelnek meg a valóságnak, akkor a tanúsítvány visszavonását kérni.

h) A kötelezettségek értelemszerűen alkalmazandók a tanúsítvány és kulcs érvényességi időszaka alatt, és ha szükséges, akkor azt követően is.

Figyelem!
Nem valós, hamis vagy hamisított adatok közlésével az Igénylő egyes esetekben közokirat-hamisítás bűntettét valósítja meg, amelyért büntetőjogi felelősséggel tartozik.

10.5.4 Ajánlások az Érintett Fél részére

Jelen Szabályzatban az Érintett Fél számára meghatározott tevékenységek ajánlást jelentenek a Szolgáltató részéről, amelyek szükségesek az elektronikus aláírás elfogadása biztonságos végrehajtásához.

A Szolgáltató kizárja a felelősségét, ha az érintett fél az aláírás, tanúsítvány vagy időbélyeg érvényességének és hatályosságának ellenőrzése során - a Szolgáltató hitelesítési rendjében, szolgáltatási szabályzatában lévő ajánlások ellenére - a tőle az adott helyzetben általában elvárható magatartást nem tanúsítja, illetve ha nem a hatályos jogszabályok szerint jár el.

Az Érintett Fél számára az alábbi előírások betartása ajánlott:

a) Meghatározott célokra korlátozva és csak olyan alkalmazásokkal fogad el nyilvános kulcsokat, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat" és „kiterjesztett kulcshasználat" mezőinek tartalmával.

b) Olyan eljárásokat, alkalmazásokat használ, amelyek támogatják a Szolgáltató által kibocsátott tanúsítványok helyes kezelését.

c) Elektronikus aláírás vagy időbélyeg elfogadásakor a rendelkezésre álló módszerekkel meggyőződik az aláírás / időbélyeg és a tanúsítvány érvényességéről, elfogadhatóságáról, továbbá minden egyéb tevékenységet megtesz annak érdekében, hogy az elektronikus aláírás / időbélyeg és tanúsítvány elfogadásáról hozott döntése megalapozott legyen, így:

A. Az elektronikus üzenet, az elektronikus aláírás és a tanúsítvány összetartozása, az üzenet sértetlensége:

- az elektronikusan aláírt adatok pontos kiválasztása az üzenetből,
- az elektronikus aláírás dekódolása a tanúsítványban található nyilvános kulcs segítségével,
- az elektronikus aláírás és az aláírt üzenet összetartozásának és az üzenet sértetlenségének ellenőrzése üzenet lenyomat képzéssel és összehasonlítással.

B. A tanúsítvány jogos és a szabályzatokkal összhangban történő használatának ellenőrzése:

- az üzenet aláírási időpontjának ellenőrzése, lehetőség szerint időbélyeg ellenőrzésével,
- az aláíró kulcs használatára vonatkozó korlátozások ellenőrzése,
- az Aláíró feltételezett vagy jelzett szándéka szerinti értelmezés meghatározása,
- a tanúsítvány egyéb adatainak áttanulmányozása és a korlátok értelmezése.

C. A nyilvános kulcsot tartalmazó tanúsítvány érvényességének vizsgálata:

- a tanúsítvány Alanyára, illetve másodlagos Alanyára vonatkozó adatok megvizsgálása és azok alapján a „Subject" mezőben szereplő entitás(ok) megállapítása,
- a tanúsítvány időbeni érvényességének megállapítása,
- a tanúsítvány státuszának megállapítása a Szolgáltató által a jelen Szabályzat rendelkezései szerint közzétett visszavonási információk áttanulmányozásával, visszavonási szolgáltatások igénybevételével.

D. Hitelesítési lánc ellenőrzése:

- tanúsítványláncok kialakítása és a megfelelő lánc kiválasztása,
- a tanúsítványlánc tagjainak ellenőrzése a Tanúsítványtár alapján a jelen fejezetben megjelölt ellenőrzési lépések megtételével.

Figyelem!

Az Érintett Félnek ajánlott visszautasítania az elektronikus aláírás vagy időbélyeg elfogadását, ha bármely ellenőrzési lépés eredményéből az elektronikus aláírás vagy időbélyeg, a tanúsítvány vagy azok alkalmazásának érvénytelenségére, jogszerűtlenségére, jelen és kapcsolódó szabályzatokba ütköző voltára utaló következtetés vonható le.

Amennyiben ezt nem teszi meg, az érvénytelen, jogszerűtlen, vagy jelen és kapcsolódó Szabályzatba ütköző aláírás vagy időbélyeg elfogadásából eredő károkért maga felel.

10.5.5 Szolgáltató egyéb kötelezettségei

A Szolgáltató általános kötelessége:

a) a hitelesítő és regisztrációs egységek és a tanúsítványtár felügyelete, üzemeltetése;

b) a szolgáltatásainak a hatályos jogi szabályozással, jelen szabályzattal és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban való nyújtása;

c) a magas színvonalú és biztonságos szolgáltatások folyamatos biztosítása;

d) az alvállalkozók feladatainak egyértelműen meghatározása, működésük rendszeres ellenőrzése, a Szolgáltató által előírt eljárások betartásának biztosítása, és az esetlegesen szabályzattól eltérő működés esetén a helytelen működés megszüntetésének előírása és ellenőrzése;

e) Az ügyintéző hatóság által elektronikus úton továbbított viszontazonosítási kérelemben megjelölt ügyfél természetes személyazonosító adatainak és a Szolgáltató által kezelt, az ügyfélre vonatkozó természetes személyazonosító adatainak összevetése és az adatok egyezőségének vagy annak hiányának tényét megküldeni az ügyintéző hatóság részére; ennek kapcsán a Szolgáltató köteles a viszontazonosítási kérelem teljesítése előtt az ügyintéző hatóság aláírását ellenőrizni, ezzel igazolva a kérelem hitelességét.

10.5.5.1 A Szolgáltatói egységek közös kötelezettségei

A Szolgáltatóhoz tartozó szervezetek, regisztrációs és hitelesítő egységek kötelessége:

a) a Közösség elektronikus hitelesítéssel kapcsolatos tevékenységeinek, alapelveinek meghatározása, ezek alapján a működést részletesen tárgyaló szabályzatok készítése és rendszeres felülvizsgálata,

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

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

d) az infrastruktúra működtetéséért, javításáért és karbantartásáért felelős személyzet munkájának és szakmai felkészültségének folyamatos ellenőrzése, a szükséges változtatások megtétele,

e) az előző pontokban előírt infrastruktúra folyamatos, biztonságos üzemeltetése, hibajavítása és az infrastruktúrába tartozó eszközökre előírt szabványos karbantartás elvégzése,

f) Üzleti Folytonossági Terv készítése, alkalmazása,

g) a szabályzatokban előírt módon folytatott tevékenység során keletkező adatok jelen és kapcsolódó szabályzatokban meghatározott kezelésére, tárolására, archiválására alkalmas szoftver és hardver eszközök biztosítása, működtetése, karbantartása,

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

i) a logikai és fizikai védelmet megteremtő eszközök megfelelő üzemeltetése, az informatikai, fizikai, adminisztrációs és üzleti biztonság megteremtése és fenntartása.

j) szabad hozzáférés biztosítása a Szabályzat Adminisztrátor részére a felügyelendő dokumentumokhoz, továbbá a megfelelő körülmények biztosítása számára a belső ügyviteli folyamatok azok helyszínén való ellenőrzéséhez.

10.5.5.2 A Szabályzat Elfogadó Egység kötelezettségei

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

b) a Szolgáltatóhoz érkező szabályzatokkal kapcsolatos észrevételek és javaslatok fogadása,

c) a szabályzatok aktualizálásának előkészítése, egyeztetése és végrehajtása,

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

10.5.5.3 A tanúsítványtár kötelezettségei és vele kapcsolatos tevékenységek

A Tanúsítványtár kötelessége az üzemeltetés során:

a) a Tanúsítványtár nyilvános, minden Érintett Fél számára elérhető módon való üzemeltetése a Szolgáltató Internetes oldalán (ld. 1.5 alfejezet),

b) a Szolgáltató saját tanúsítványainak, a Szolgáltató által kibocsátott tanúsítványok, CRL listák, aktuális és korábbi szabályzatok (NetLock ÁSZF, Szolgáltatási Szabályzat és Hitelesítési Rend) késedelem nélküli közzététele,

c) a szabályzatok során minimum Adobe Acrobat és Microsoft Word dokumentum formátumban közzétenni,

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

e) a Tanúsítványtárat minimum 99,9 %-os rendelkezésre állással működtetni, ezt a mutatót is figyelembe véve elérhetővé tenni az év valamennyi napján, 0–24 óráig; az eseti leállások nem haladhatják meg a 3 órát,

f) a rendelkezésre állást a Szolgáltató az Üzleti Folytonossági Tervben rögzített, a szokásostól eltérő üzletmenet elhárítására kidolgozott eljárások végrehajtásával biztosítani,

g) a Tanúsítványtárhoz írási jogosultságot csak a Szolgáltatónak biztosítani.

10.6 Felelősség

10.6.1 A Szolgáltató általános felelőssége

A Szolgáltató felelős:

- a Szabályzat keretei között végzett szolgáltatói tevékenységekért,
- a szolgáltatásai ellátásához szükséges regisztrációs és hitelesítő egységek működéséért akkor is, ha egyes funkciókat alvállalkozók végeznek.

10.6.1.1 A felelősség korlátai

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy az Aláíró vagy az Érintett Fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályoknak, illetve szolgáltatói szabályzatoknak megfelelően járt el, illetve nem tanúsította a tőle elvárható gondosságot.

Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a saját hibájából, kötelezettségeinek megszegéséből, valamint a neki felróható okokból bekövetkező, bizonyítható károkért tartozik helyt állni (lásd 10.2 pont).

10.6.2 A végfelhasználó felelőssége

Ha végfelhasználó a jelen szabályzat szerinti kötelezettségét megszegte, felel az ebből fakadó károkért.

10.6.3 Az Érintett Fél felelőssége

A Szolgáltató kizárja a felelősségét, ha az érintett fél az aláírás, tanúsítvány vagy időbélyeg érvényességének és hatályosságának ellenőrzése során - a Szolgáltató hitelesítési rendjében, szolgáltatási szabályzatában lévő ajánlások ellenére - a tőle az adott helyzetben általában elvárható magatartást nem tanúsítja, illetve ha nem a hatályos jogszabályok szerint jár el.

10.7 Változtatási eljárás

10.7.1 Szabályzat-változtatási eljárás

A Szolgáltatón belül Szabályzat Elfogadó Egység működik, amely a Szabályzat karbantartásáért felelős. A változtatási igényeket ezen egység gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

A változtatásokat gyűjtve az egység belső nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. Szolgáltató a változásokat kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A Szolgáltató elfogadás előtt megvizsgálja a hitelesítés-szolgáltatási rend formai megfelelését az RFC 3647 [12] szabványnak.

A hitelesítés-szolgáltatási rendek elfogadására vagy esetlegesen a Felügyelet által már nyilvántartásba vett hitelesítés-szolgáltatási rendek közül történő kiválasztására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd egyetértés esetén a Felügyelet nyilvántartásba veszi a Szolgáltató által jóváhagyott és bejelentett hitelesítés-szolgáltatási rendet.

A Szolgáltató jóváhagyás előtt megvizsgálja a Szabályzatot a szolgáltatási szabályzat megfelelőség szempontjából, hogy a Szabályzat tartalmilag és formailag megfelel-e a hitelesítés-szolgáltatási rendeknek.

A Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd bejelentés után a Szabályzatot a Felügyelet nyilvántartásba veszi.

A Szolgáltatási Szabályzat módosított változatai mindig új verziószámmal kerülnek nyilvánosságra. A szabályzatok egymásnak, a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente kétszer történik. A szabályzatok rendkívüli felülvizsgálatára és módosítására a jogszabályi változások esetén kerül sor. A szabályzatok felülvizsgálatát a Szolgáltató a működése során szerzett gyakorlati tapasztalatok alapján is elvégzi.

10.7.2 Szabályzat Elfogadó Egység

10.7.2.1 A Szabályzat Elfogadó Egység összetétele

A Szabályzat Elfogadó Egység a következő összetételű munkacsoportként működik:

- Szabályzat Vezető: a Szabályzat Elfogadó Egység vezetője, feladata az Egység munkájának koordinálása, illetve határozatainak jóváhagyása.
- Szabályzat Adminisztrátor: a Szabályzat Elfogadó 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. Az adminisztrátor hatásköre és felelőssége továbbá a minősített hitelesítés-szolgáltatási rendek specifikálása, jóváhagyatása és karbantartása.

10.7.2.2 A Szabályzat Elfogadó Egységműködése

A Szabályzat Elfogadó Egység 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 Szabályzat Elfogadó Egység tagjainak mindenkor érvényes névsorát a Szabályzat Elfogadó Egység tagjegyzéke tartalmazza. A Szabályzat Elfogadó Egység üléseiről jegyzőkönyv készül.

10.7.3 Értesítés nélkül változtatható elemek

A Szolgáltató jelen Szabályzat módosítását a jogszabályokban erre előírt módosítási eljárás nélkül nem lépteti hatályba.

10.7.4 Értesítéssel változtatható elemek

A Szolgáltató jelen Szabályzat, valamennyi módosítását kizárólag az erre a vonatkozó jogszabályokban előírt eljárásban meghatározott feltételek teljesülése esetén lépteti hatályba. Azon módosítások, melyek a szolgáltatások biztonsági szintjét, felhasználhatóságát nem módosítják (ilyenek tipikusan a helyesírási hibák, formai változtatások, különböző kontaktadatok, Internet címek, telefonszámok) összevontan kerülnek módosításra és ezzel együtt értesítésre. A szolgáltatások biztonsági szintjét, felhasználhatóságát módosító változtatásokra pedig a Szolgáltató a weboldalán közzétett tájékoztatással hívja fel a Közösség figyelmét (lásd 2.1.2 pont).

10.7.5 Szabályzati objektumazonosítót vagy mutatót változtató módosítások

Minden módosítás megváltoztatja a Szabályzat verziószámát és objektumazonosítóját. Azt a módosított szabályzatot, amely csak az újonnan kibocsátásra kerülő tanúsítványokra vonatkozik (de a már kibocsátottakra nem), a Szolgáltató az előző főbb verziótól eltérő Internet címen teszi közzé, így csak az újonnan kibocsátott tanúsítványok mutatói fognak rá hivatkozni, amennyiben a tanúsítványban van ilyen mutató.

10.8 Panaszkezelési szabályok

10.8.1 Panaszok benyújtásának helye

A Szolgáltató (beleértve a regisztrációs egységeket is) tevékenységével kapcsolatos kérdések, kifogások és panaszok benyújtásának helye a Szolgáltató ügyfélszolgálati irodája (ld. 1.5 alfejezet).

10.8.2 Panaszok benyújtásának módja

A panaszokat a Szolgáltató levélben, e-mailben a info@netlock.hu címen, faxon, telefonon és személyesen fogadja (ld. 1.5 alfejezet).

10.8.3 Panaszok kezelésének eljárása

A panasz kézhezvételéről a Szolgáltató az érkeztetést követően 1 munkanapon belül értesíti a beadó felet a megjelölt címen, az ügy kivizsgálásához szükséges idő megjelölésével. A jelzett időn belül, amely lehetőség szerint nem több, mint 10 munkanap, a Szolgáltató a panaszt kivizsgálja, a felmerült hibát a műszakilag indokolt időn belül elhárítja, és mindezen tevékenységekről a bejelentőt írásban tájékoztatja. Ha a választ bejelentő nem fogadja el, egyeztetést kell kezdeményeznie a Szolgáltatóval. Ha a Szolgáltató ezt megtagadja, vagy ha a felek közötti egyeztetés annak megkezdésétől számított 20

munkanapon belül nem vezetne eredményre, akkor a bejelentő jogi útra terelheti az ügyet. A panaszkezelés véghatárideje a fentiek a bejelentéstől számított figyelembevételével 30 nap.

10.8.4 Illetékes fogyasztóvédelmi felügyelőség

Budapest Főváros Kormányhivatal, Fogyasztóvédelmi Felügyelőség, elérhetőségei:

- **Cím**: 1052 Budapest, V. ker. Városház u. 7.
- **Levelezési cím**: 1364 Budapest, Pf. 144.
- **Telefon**: +36 1 328-0185
- **Fax**: +36 1 411-0116
- **E-mail**: fogyved_kmf_budapest@nfh.hu

10.9 Hivatkozott jogszabályok, szabványok és egyéb dokumentumok

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

[1] 2001. évi XXXV. Törvény az elektronikus aláírásról („Törvény")

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

[3] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól és ennek végrehajtási rendeletei

[4] 78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól

[5] Minősített tanúsítványtípus minták minősített Hitelesítés-szolgáltatók számára, 1.2 verzió

[6] ISO 3166 English Country Names and Code Elements

[7] FIPS PUB 140-1 (1994. január 11): "Kriptográfiai modulok biztonsági követelményei"

[8] ETSI TS 101 456 V1.4.3 (2007-05) Minősített tanúsítványokat kibocsátó Hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények

[9] ETSI TS 101 862 Minősített tanúsítványprofil

[10] RFC 5280 (korábban RFC 3280) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány- és tanúsítvány visszavonási lista profil

[11] RFC 3647 (korábban RFC 2527) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer

[12] RFC 3739 Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítványprofil

[13] International Telecommunication Union X.509 "Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány-keretrendszer"

[14] Általános Szerződési Feltételek (ÁSZF) – NetLock

[15] 9/2005. IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

[16] ETSI TS 101 861 v1.3.1 (2006-01) Time Stamping Profile

[17] RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

[18] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható hitelesítési rendekre, Biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített hitelesítési rendek:
- Ügyfelekre vonatkozó hitelesítési rend: 0.2.216.1.100.42.101.1.2.1
- Közigazgatási köztisztviselőkre vonatkozó hitelesítési rend: 0.2.216.1.100.42.101.2.2.1

[19] Minősített tanúsítvány, visszavonási lista és időbélyeg profildefiníciók

[20] ETSI 102 042 v2.1.1 (2009-05) Policy requirements for certification authorities issuing public key certificates

[21] RFC 2560 Online Certificate Status Protocol (OCSP)

[22] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára

[23] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

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

[25] 45/2005 (III. 11.) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

[26] 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

[27] 7/2002 (IV. 26.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

[28] Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési Szabályzat

[29] Aláírás Célú Tanúsítvány Hitelesítési Rend – NetLock Kft.

[30] Általános Időbélyegzési Rend – NetLock Kft.

[31] A Felügyletnek az elektronikus aláírással kapcsolatos szolgáltatások területén alkalmazható kriptográfiai algoritmusokról és paraméterekről szóló mindenkor hatályos határozatai és azok mellékletei, melyek elérhetőek a Felügyelet honlapján (www.nmhh.hu). A Szolgáltató számára megküldött, jelenleg hatályos határozat száma: EF-26838-8/2011.

[32] A Nemzeti Hírközlési Hatóság Hivatalának tájékoztatója a láncolt hitelesítés-szolgáltatásokról és más alárendelt elektronikus aláírással kapcsolatos szolgáltatásokról (2007. május 22.), továbbá, ha egy újabb tájékoztató ezt hatályon kívül helyezi, akkor a felügyeleti tájékoztató mindenkor hatályos változata.

10.10 Értelmezés és érvényesítés

10.10.1 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi (ld. [1] Törvény, [3] Rendelet). A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők.

10.10.2 A rendelkezések különválaszthatósága

Bármely rendelkezés hatályon kívül kerülése vagy bíróság általi semmissé nyilvánítása nem befolyásolja a többi rendelkezés hatályát, érvényességét.

10.10.3 A rendelkezések jogfolytonossága

A visszavonásra és a visszavonási információ kezelésére vonatkozó szabályok abban az esetben is érvényben maradnak (és az archivált adatok megőrződnek), ha a szolgáltatás és ezáltal a Szabályzat megszűnik.

10.10.4 A rendelkezések kiterjesztése

A szolgáltatási tevékenységhez kapcsolódó egyéb szerződések figyelemmel vannak jelen Szabályzat rendelkezéseire is.

10.10.5 Vitás kérdések megoldására vonatkozó eljárások

A Szolgáltató (beleértve a regisztrációs egységeket is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat a info@netlock.hu e-mail címen, valamint a Szolgáltató központi fax számán lehet írott formában bejelenteni (ld. 10.8 pont), illetve telefonon vagy személyesen a Szolgáltató ügyfélszolgálati irodájában (lásd: 1.5).

Bármely vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra terelése előtt a felhasználónak kötelessége, az Érintett Félnek vagy bármely harmadik félnek ajánlott a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően. A felek vitáikat mindenkor megkísérlik békés, tárgyalásos úton rendezni.

Amennyiben a Felek közötti egyeztetés - mely a Szolgáltató a panasz kivizsgálásának eredményeként adott válaszát követi - valamelyik fél által kezdeményezetett egyeztetés napjától számított 20 napon belül nem vezet eredményre, arra az esetre a Felek kölcsönösen alávetik magukat a Kereskedelmi és Iparkamara mellett szervezett Állandó Választottbíróság kizárólagos illetékességének. A Választottbírósági eljárás nyelve a magyar, az eljárásban irányadó jog a mindenkor hatályos magyar anyagi és eljárásjog. Az eljáró bírók száma: 3.