Minősített Hitelesítés Szolgáltatás Szolgáltatási Szabályzat

NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Nyilvántartási szám (OID): ---------- **1.3.6.1.4.1.3555.1.15.030317**

A Szabályzat hatályának kezdőnapja: ---------- **2003. március 31.**

Oldalak száma: ---------- **90, azaz kilencven**

Jóváhagyta: ---------- **Rózsahegyi Zsolt** ügyvezető

Jóváhagyás dátuma: ---------- **2003. 03. 15.**

Jóváhagyom: ……..

PH.

Hivatkozások

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

- [1] 2001. évi XXXV. Törvény az elektronikus aláírásról
- [2] 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről
- [3] 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- [4] Minősített tanúsítványtípus minták minősített Hitelesítés-szolgáltatók számára, 1.2 verzió
- [5] ISO 3166 English Country Names and Code Elements
- [6] FIPS PUB 140-1 (1994. január 11): "Kriptográfiai modulok biztonsági követelményei"
- [7] ETSI TS 101 456 Minősített tanúsítványokat kibocsátó Hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények
- [8] ETSI TS 101 862 Minősített tanúsítványprofil
- [9] RFC 2459 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány- és tanúsítvány visszavonási lista profil)
- [10] RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer)
- [11] RFC 3039 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítványprofil)
- [12] International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány-keretrendszer”
- [13] Általános Szerződési Feltételek (ÁSZF) – NetLock
- [14] MATT (Minősített alap tanúsítványtípus minősített Hitelesítés-szolgáltatók számára)
- [15] IETF PKIX RFC 2527 (Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework; Chokhani & Ford 1999)
- [16] RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- [17] ETSI TS 101861 v1.1.1 (2001-08)Time Stamping Profile
- [18] MATT + BALE (Minősített alap tanúsítványtípus biztonságos aláírás létrehozó eszköz támogatásával minősített Hitelesítés-szolgáltatók számára)

– Fogalmak

- **Alany:** A tanúsítvány alany (Subject) mezőjében megadott adatokkal meghatározott természetes személy, aki a tanúsítványban szereplő nyilvános kulcs párját jelentő magánkulcs felett rendelkezik.
- **Aláírás-ellenőrző adat**: Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.
- **Aláírás-létrehozó adat**: Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az Aláíró az elektronikus aláírás létrehozásához használ.
- **Aláírás-létrehozó eszköz**: Szoftver vagy hardver, melynek segítségével az Aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
- **Aláíró:** Lásd: Alany.
- **Személyes tanúsítvány:** Természetes személyek számára kibocsátott, kizárólag elektronikus aláírás előállítására használható tanúsítvány.
- **Munkatársi tanúsítvány:** Olyan személyes tanúsítvány melyben az abban szereplő természetes személyt a másodlagos alany saját magához tartozónak ismeri el.
- **Általános Szerződési Feltételek (ÁSZF):** A Szolgáltató szolgáltatásainak, tanúsítványainak igénybevételéhez szükséges feltételeket, illetve egyéb szerződési feltételeket leíró dokumentum.
- **Alkalmazó Közösség**: A PKI rendszert alkalmazó, működtető entitások összessége.
- **Biztonságos aláírás-létrehozó eszköz (BALE):** A [1] Törvény 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.
- **Challenge-response:** Azonosítási módszer, amely egy elektronikus kérdésre megfelelő válaszinformációt várva azonosítja a felhasználót.
- **Common Name:** Az Alany tanúsítványban szereplő, szokásos megnevezéséből képzett neve.
- **Distinguished Name (DN):** A tanúsítványban szereplő, szokásos megnevezéséből, lakóhely vagy székhely szerinti város, ország megnevezéséből, valamint e-mail címéből képzett egyedi neve. Az egyedi név komponensei személyes és munkatársi tanúsítvány esetén eltérhetnek.
- **Domain név**: Virtuális tartomány név.
- **Elektronikus aláírás:** Elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.
- **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.

- **Eszköz Szolgáltató (ESz):** Az a személy vagy szervezet aki/amely a [1] Törvény 6. § (1) bekezdésének c) pontja értelmében meghatározott, elektronikus aláíráshoz kapcsolódó aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése szolgáltatást végez.
- **Felügyelet:** Hírközlési Felügyelet, a Hitelesítés-szolgáltatók felügyeleti szerve.
- **Fizikailag biztosított terület:** Olyan helyiség, amely ésszerű határok mellett képes megvédeni a benne elhelyezett eszközöket az elemi károktól, illetve a szándékos illetéktelen hozzáféréstől.
- **Folyamatosan elérhető szolgáltatás:** Az év 365 napján a nap 24 órájában elérhető szolgáltatást jelent a Szolgáltató szabályzataiban meghatározott rendelkezésre állási időkkel.
- **Fokozott biztonságú elektronikus aláírás**: Elektronikus aláírás, amely megfelel a következő követelményeknek:
  - alkalmas az Aláíró azonosítására és egyedülállóan hozzá köthető,
  - olyan eszközzel hozták létre, amely kizárólag az Aláíró befolyása alatt áll,
  - a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető.
- **Hash:** Ld. Lenyomat.
- **Hitelesítő Egységek:** A végfelhasználói tanúsítványokat létrehozó egységek a Szolgáltatónál.
- **Hitelesítés-szolgáltatás**: Olyan tevékenység, melyet a Szolgáltató végez. A hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványokhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a Tanúsítvány Visszavonási Listát, továbbá időbélyegzés-szolgáltatást, illetve aláírás-létrehozó adat aláírás-létrehozó eszközön való elhelyezést végez.
- **Hitelesítés-szolgáltató (HSZ):** A NetLock Kft., amely a hitelesítés-szolgáltatást végzi.
- **Hozzáférések:** Egy adott számítógépes hálózat vagy annak egyes elemei elérésére vonatkozó szabályok összessége.
- **Host név:** A technikai eszközök azonosítására használt, hálózati eszközök számára értelmezhető egyedi elnevezés.
- **Időbélyegzés Szolgáltató (ISZ):** Az Időbélyegzés Szolgáltató az elektronikus dokumentumhoz időbélyegzőt kapcsol. A minősített időbélyegzőre a minősített tanúsítványra vonatkozó rendelkezéseket kell megfelelően alkalmazni.
- **Késedelem nélküli cselekedet:** A mindenkori technikai feltételek által megengedett lehető leggyorsabb intézkedést jelenti.
- **Kompromittálódás:** Biztonsági sérülés.
- **Közhiteles cégnyilvántartás:** a cégjegyzékbõl, valamint a cégjegyzékben szereplõ adat, jog vagy tény (a továbbiakban együtt: adat) igazolására szolgáló mellékletekbõl, illetve egyéb olyan okiratokból áll, melyeknek benyújtására a céget – a forgalom biztonsága, valamint a hitelezõi érdekek védelme céljából – törvény kötelezi (a továbbiakban együtt: cégiratok). Cégnyilvántartási és Céginformációs Szolgáltat, Megyei és Fõvárosi Bíróság, mint Cégbíróság.
- (**Kriptográfiai**) **Kulcs**: Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.

- **Lenyomat (Hash):** Egy adott elektronikus jelcsoportból egyirányú függvényként működő lenyomatképző algoritmussal készített, a forrás jelcsoportra egyedileg jellemző adat.
- **Magánkulcs védelme:** Mindazon tevékenységek összessége, melyek célja a magánkulcs megfelelő védelme, a magánkulcs teljes élettartama során annak generálásától, annak megsemmisítéséig, a hozzá tartozó tanúsítvány státuszától függetlenül.
- **Másolati példány:** Magán- vagy jogi személyt azonosító eredeti okmányról készült másolat.
- **Másodlagos alany:** Az jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amely a munkatársi tanúsítvány alanyával együttesen szerepel a tanúsítványban és aki az alanyt saját magához tartozónak ismeri el.
- **Munkatárs:** A természetes személyek azon köre, amelyeket egy adott szervezet saját magához tartozóként ismer el.
- **NetLock Minősített Hitelesítés-szolgáltatás:** M osztályú (minősített) tanúsítványok kibocsátása.
- **NetLock Minősített Időbélyeg Szolgáltatás:** Minősített időbélyeg kibocsátása elektronikus dokumentumokra.
- **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 (PKI):** 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).
- **Szabályzatért Felelős Egység:** A jelen és kapcsolódó szabályzatok kialakításáért, elfogadásáért és adminisztrációjáért felelős szolgáltatói egység.
- **Szolgáltatási Szabályzat**: A [1] törvény 2. § (20) alapján a Szolgáltató hitelesítési tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum (ld. 1.1.1).
- **Szolgáltatási szerződés:** Elsődlegesen az ÁSZF és a Szolgáltatási Szabályzat elfogadását jelző, aláírt dokumentum.
- **Tanúsítvány**: A Szolgáltató által kibocsátott elektronikus igazolás, amely az aláírás-ellenőrző adatot a tanúsítvány alanyához kapcsolja.
- **Tanúsítványfajta**: Jelen Szabályzat két megjelenési formáját ismeri: a személyest és a munkatársit.
- **Tanúsítványállapot-nyilvántartás**: A legközelebb kibocsátásra kerülő Tanúsítvány Visszavonási Lista tartalmához kapcsolt online 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 tanúsítványok megbízhatósága szerinti megkülönböztetés. A kibocsátást megelőző ellenőrző lépések biztonságosságának jelzése (M: minősített, A, B, C: fokozott biztonságú). Jelen Szabályzat kizárólag az „M”, azaz minősített osztályra vonatkozik, emellett azonban a Szolgáltató nyújt fokozott biztonságú szolgáltatásokat is, melyekre külön szabályzatok vonatkoznak.
- **Tanúsítványtípus**: Azon szabályok összessége, amelyek megmutatják adott tanúsítványok alkalmazhatóságát egy bizonyos közösségre, illetve alkalmazások olyan csoportjára, ahol azonosak a biztonsági követelmények.
- **Tanúsítvány Visszavonási Lista (CRL)**: Valamely okból visszavont, azaz érvénytelenített, illetve felfüggesztett, azaz ideiglenesen érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a Szolgáltató bocsát ki.
- **Törvény**: A 2001. évi XXXV. törvény az elektronikus aláírásról és annak végrehajtási rendeletei.
- **Ügyfélmenü:** A Szolgáltató Internetes oldalain online 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.

Tartalomjegyzék

1 BEVEZETÉS 14

1.1 Áttekintés 14
1.1.1 A Szabályzat 15
1.1.2 A Szabályzat hatálya 15
1.1.3 A Szolgáltató 15
1.1.4 Szolgáltatások 16
1.1.5 Szabványok és előírások 16
1.1.6 Tanúsítványfajták 17
1.1.7 Időbélyegzés-szolgáltatás 18
1.1.8 Aláíró eszköz szolgáltatás 18

1.2 Azonosítás 19

1.3 Közösség és alkalmazhatóság 20
1.3.1 Szabályzatért Felelős Egység 20
1.3.2 Regisztrációs egységek 20
1.3.3 Hitelesítő egységek 21
1.3.4 Végfelhasználók 21
1.3.5 Érintett fél 22
1.3.6 Alkalmazhatóság 22

1.4 Kapcsolattartás 23

2 ÁLTALÁNOS RENDELKEZÉSEK 24

2.1 Kötelezettségek 24
2.1.1 A Szolgáltató kötelezettségei 24
2.1.2 A végfelhasználó kötelezettségei 26
2.1.3 Az Érintett Fél kötelezettségei 28

2.2 Felelősség 29
2.2.1 A Szolgáltató általános felelőssége 29
2.2.2 A végfelhasználó felelőssége 29
2.2.3 Az Érintett Fél felelőssége 29

2.3 Pénzügyi felelősség 29
2.3.1 A Szolgáltató pénzügyi felelőssége 29

2.4 Értelmezés és érvényesítés 30
2.4.1 Irányadó jog 30
2.4.2 A rendelkezések különválaszthatósága 30

2.4.3 A rendelkezések jogfolytonossága 30
2.4.4 A rendelkezések kiterjesztése 31
2.4.5 Vitás kérdések megoldására vonatkozó eljárások 31

2.5 Díjak 31
2.5.1 Egyéb szolgáltatásokra vonatkozó díjak 31
2.5.2 Visszatérítési elvek 32

2.6 Közzététel és tanúsítványtár 32
2.6.1 A Szolgáltató információ közzététele 32
2.6.2 A közzététel gyakorisága 33
2.6.3 Hozzáférés ellenőrzések 34
2.6.4 Tanúsítványtárak 34

2.7 A megfelelőség vizsgálata 35
2.7.1 A megfelelőség vizsgálatának gyakorisága 35
2.7.2 Az átvizsgáló egységek megnevezése 35
2.7.3 Az átvizsgáló egységek és a vizsgált fél kapcsolata 35
2.7.4 A vizsgálat által érintett területek 36
2.7.5 Hiányosságok esetén végrehajtandó tevékenységek 36
2.7.6 Az eredményekről való tájékoztatás 36

2.8 Bizalmasság, adatvédelem 36
2.8.1 Bizalmasan kezelendő információ típusok 37
2.8.2 Nem bizalmasnak tekintett információ típusok 37
2.8.3 Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése 37
2.8.4 Információszolgáltatás hatósági szervek részére 37
2.8.5 Információszolgáltatás polgári peres eljárás keretében 38
2.8.6 Egyéb információszolgáltatás 38
2.8.7 Az alany kérésére történő felfedés 38
2.8.8 Egyéb információ harmadik félnek történő átadása 38

2.9 Szellemi tulajdonjogok 38

3 AZONOSÍTÁS ÉS HITELESÍTÉS 39

3.1 Kezdeti regisztrálás 39
3.1.1 Névtípusok 39
3.1.2 Különböző elnevezési formák értelmezési szabályai 39
3.1.3 A nevek egyedisége 40
3.1.4 Eljárások a nevekre vonatkozó vitás kérdések megoldására 40
3.1.5 Védjegyek elismerése, hitelesítése és szerepe 40
3.1.6 A magánkulcs birtoklásának bizonyítási módszere 40
3.1.7 Személyazonosság hitelesítése 41

3.1.8 Szervezeti azonosság hitelesítése 41

3.2 Érvényes tanúsítvány megújítása 41
3.2.1 Végfelhasználói tanúsítványok 41
3.2.2 Szolgáltatói tanúsítványok 42

3.3 Érvénytelen tanúsítvány megújítása 42

3.4 Visszavonási kérelem 42

4 MŰKÖDÉSRE VONATKOZÓ KÖVETELMÉNYEK 43

4.1 Tanúsítványigénylés 43
4.1.1 Igénylés feltételei 43

4.2 Tanúsítvány-kibocsátás 43
4.2.1 Általános regisztrációs szabályok 43
4.2.2 Regisztrációs eljárás 45
4.2.3 Szolgáltatási szerződés 46
4.2.4 A tanúsítványkérelmek jóváhagyásának követelményei 46
4.2.5 A tanúsítványok tartalma 47
4.2.6 A tanúsítványok jellemzői 47
4.2.7 Az igénylő (alany) tájékoztatása a kibocsátást megelőzően 47
4.2.8 A tanúsítványok kibocsátása és hozzáférhetővé tétele 48
4.2.9 Tanúsítványkérelmek elutasítása 48
4.2.10 Kibocsátott tanúsítványok 49
4.2.11 A tanúsítványokra vonatkozó további rendelkezések 49

4.3 Tanúsítványelfogadás 50
4.3.1 A tanúsítvány elfogadása 50
4.3.2 A tanúsítványigénylő nyilatkozata 50

4.4 A tanúsítványok használata 51
4.4.1 Alkalmazás 51
4.4.2 Elektronikus aláírás készítése 51
4.4.3 Magánkulcs megőrzése 51
4.4.4 Érvényes elektronikus aláírás következményei 51
4.4.5 Eljárás az elektronikus aláírás ellenőrzésekor fellépő hibáknál 52

4.5 Tanúsítvány felfüggesztése és visszavonása 52
4.5.1 Általános rendelkezések 52
4.5.2 A visszavonás körülményei 52
4.5.3 Visszavonás kérelmezése 53
4.5.4 Visszavonási kérelemre vonatkozó eljárás 53

4.5.5 Visszavonási kérelemre vonatkozó türelmi idő 54
4.5.6 Visszavonásra vonatkozó egyéb szabályok 54
4.5.7 A felfüggesztés körülményei 54
4.5.8 Felfüggesztés kérelmezése 55
4.5.9 Felfüggesztési kérelemre vonatkozó eljárás 55
4.5.10 A felfüggesztés időtartamára vonatkozó korlátozások 55
4.5.11 Tanúsítvány Visszavonási Lista (CRL) 55
4.5.12 Valós idejű visszavonási állapot ellenőrzés elérhetősége 56
4.5.13 Valós idejű visszavonás ellenőrzési követelmények 56
4.5.14 A visszavonási információ közzétételének egyéb formái 56
4.5.15 A visszavonási információ egyéb formáinak ellenőrzési követelményei 56
4.5.16 Kulcskompromittálódás esetére vonatkozó speciális követelmények 57

4.6 Általános biztonsági rendelkezések 57

4.7 Biztonsági felülvizsgálati eljárások 57

4.8 A biztonsági naplózás folyamatai 58
4.8.1 A tárolt események típusai 58
4.8.2 A napló állomány feldolgozásának gyakorisága 59
4.8.3 A napló állomány megőrzési időtartama 59
4.8.4 A napló állomány védelme 59
4.8.5 A napló állomány mentési folyamatai 59
4.8.6 A napló gyűjtési rendszere 59
4.8.7 Az eseményeket kiváltó alanyok értesítése 59
4.8.8 Sebezhetőség felmérése 59

4.9 Adatok archiválása 60
4.9.1 A tárolt események típusai 60
4.9.2 Az archívum megőrzési időtartama 60
4.9.3 Az archívum védelme és hozzáférési szabályok 60
4.9.4 Az archívum mentési folyamatai 61
4.9.5 A rekordok időbélyegzésére vonatkozó követelmények 61
4.9.6 Az archívum gyűjtési rendszere 61
4.9.7 Archív információ hozzáférését és ellenőrzését végző eljárások 61
4.9.8 Kulcsok archiválása 61
4.9.9 Egyéb archiválási rendelkezések 61

4.10 Kulcscsere 61

4.11 Helyreállítás kompromittálódás és katasztrófa esetén 62
4.11.1 Sérült számítási erőforrások, szoftverek és/vagy adatok 62
4.11.2 Egy szolgáltatói egység nyilvános kulcsának visszavonása 62
4.11.3 Egy szolgáltatói egység kulcsának kompromittálódása 62

4.11.4 Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően 63

4.12 A Hitelesítés-szolgáltató leállítása 63
4.12.1 Szolgáltatás megszűntetése 63
4.12.2 Regisztrációs pont megszűnése 64

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK 65

5.1 Fizikai óvintézkedések 65
5.1.1 Fizikai hozzáférés 65
5.1.2 Áramellátás 66
5.1.3 EMC védelem 66
5.1.4 Légkondicionálás 67
5.1.5 Beázás és elárasztódás veszélyeztetettsége 67
5.1.6 Tűzmegelőzés és tűzvédelem 67
5.1.7 Adathordozók tárolása 67
5.1.8 Selejt kezelése, megsemmisítése 67
5.1.9 Fizikailag elkülönítetten őrzött mentési példányok 67

5.2 Eljárásbeli óvintézkedések 68
5.2.1 Bizalmi munkakörök 68
5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok 69
5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés 70

5.3 Személyzetre vonatkozó óvintézkedések 70
5.3.1 Személyi kontroll 70
5.3.2 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények 71
5.3.3 Biztonsági háttér ellenőrzésekre vonatkozó eljárások 71
5.3.4 Képzési követelmények 71
5.3.5 Továbbképzési gyakoriságok és követelmények 72
5.3.6 Munkabeosztás körforgásának gyakorisága és sorrendje 72
5.3.7 A felhatalmazás nélküli tevékenységek büntető következményei 72
5.3.8 A szerződéses munkavállalókra vonatkozó követelmények 72
5.3.9 A személyzet számára biztosított dokumentációk 72

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK 73

6.1 Kulcspár előállítás és telepítés 73
6.1.1 Kulcspár előállítás 73
6.1.2 A szolgáltatói kulcsokra vonatkozó általános szabályok 74
6.1.3 Alkalmazott eszközök 75
6.1.4 Magánkulcs eljuttatása az alanyhoz 75

6.1.5 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz 75
6.1.6 A szolgáltatói nyilvános kulcs közzététele 75
6.1.7 Kulcsméretek 75
6.1.8 A nyilvános kulcs paraméterek generálása 76
6.1.9 A paraméterek megfelelőségének ellenőrzése 76

6.2 A magánkulcsok védelme 76
6.2.1 Magánkulcs letétbe helyezése 76
6.2.2 Magánkulcs mentése 76
6.2.3 Magánkulcs archiválása 77

6.3 A kulcspár gondozásának egyéb szempontjai 77
6.3.1 Egyéb kulcskezelési rendelkezések 77
6.3.2 Nyilvános kulcs archiválása 77
6.3.3 A nyilvános és magánkulcsok használatának periódusa 77

6.4 Aktivizáló adatok 78
6.4.1 Aktivizáló adatok előállítása és telepítése 78
6.4.2 Az aktivizáló adatok védelme 78
6.4.3 Az aktivizáló adatok egyéb szempontjai 78

6.5 Számítógép-biztonsági óvintézkedések 78
6.5.1 Speciális számítógép-biztonsági műszaki követelmények 78
6.5.2 Informatikai biztonsági osztályozás 79

6.6 Életciklusra vonatkozó műszaki óvintézkedések 79
6.6.1 Rendszerfejlesztési óvintézkedések 79
6.6.2 Biztonságkezelési óvintézkedések 79
6.6.3 Az életciklusra vonatkozó biztonság osztályozása 79

6.7 Hálózatbiztonsági óvintézkedések 80

6.8 A kriptográfiai modul ellenőrzése 80

6.9 Időforrás és időszinkronizáció 80
6.9.1 Időforrás megnevezése 80
6.9.2 Időforrás pontossága 80
6.9.3 Alkalmazott eszközök 81

7 TANÚSÍTVÁNY, - VISSZAVONÁSI LISTA ÉS IDŐBÉLYEG PROFILOK 82

7.1 Tanúsítványprofilok 82
7.1.1 Személyes tanúsítvány profilja 82
7.1.2 Munkatársi tanúsítvány profilja 83

7.1.3 Szolgáltatói (időbélyegző) tanúsítvány profilja 84
7.1.4 Szolgáltatói (tanúsítvány- és CRL-aláíró) tanúsítvány profilja 85

7.2 Tanúsítvány visszavonási lista profil 85
7.2.1 CRL kiterjesztések 85

7.3 Időbélyeg-profil 86

8 LEÍRÁS ADMINISZTRÁCIÓ 87

8.1 Leírás változtatási eljárások 87
8.1.1 Szabályzat változtatási eljárások 87
8.1.2 A Szabályzatért Felelős Egység összetétele 87
8.1.3 A Szabályzatért Felelős Egység működése 88
8.1.4 Értesítés nélkül változtatható elemek 88
8.1.5 Értesítéssel változtatható elemek 88
8.1.6 Szabályzati objektumazonosítót vagy mutatót változtató módosítások 88

8.2 Közzétételi és tájékoztatási elvek 88
8.2.1 A szabályzatban nem tárgyalt elemek 88
8.2.2 A Szabályzat közzététele 89
8.2.3 Észrevételek kezelése 89
8.2.4 Panaszkezelési szabályok 89

8.3 Szolgáltatási Szabályzat jóváhagyási eljárások 90

1 Bevezetés

1.1 Áttekintés

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

A NetLock Kft. az elektronikus kommunikáció hitelességét és bizalmasságát biztosító elektronikus igazolványok (tanúsítványok) kiadását, az ehhez kapcsolódó publikus adatbázisok, illetve infrastruktúra karbantartását és üzemeltetését végzi. A hitelesítés-szolgáltatói tevékenység mellett kiemelt terület a 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 kompatíbilis egységek) telepítése és folyamatos támogatása.

A NetLock Kft. mint Hitelesítés-szolgáltató A (Közjegyzői), B (Üzleti), C (Expressz) és M (Minősített) osztályban kínál különböző tanúsítványfajtákat. A tanúsítványfajták elsősorban a kibocsátandó tanúsítványban szereplő entitások és egyéb adatok ellenőrzésének szigorában különböznek. Az A, B, C osztályú tanúsítványokhoz – mint fokozott biztonságú tanúsítványokkal aláírt elektronikus dokumentumokhoz – az írásbeliség, míg az M osztályban kibocsátott tanúsítványokhoz – mint minősített tanúsítványokkal aláírt elektronikus dokumentumokhoz – a teljes bizonyító erejű magánokiratok jogkövetkezményeit fűzi az elektronikus aláírásról szóló 2001. évi XXXV. törvény (a továbbiakban: [1] Törvény).

Jelen Szabályzat kizárólag az M, azaz minősített szabályokat tartalmazza.

A tanúsítványok csak abban az esetben nyújtanak biztonságot, ha a hozzájuk tartozó magánkulcshoz kizárólag a tanúsítvány alanya férhet hozzá. A tanúsítványhitelesítés mellett a NetLock Kft. időbélyegzés-szolgáltatást is végez, illetve elektronikus aláírást létrehozó adat elektronikus aláírást létrehozó eszközön való elhelyezését is szolgáltatja. Az időbélyegzés-szolgáltatás keretében a Hitelesítés-szolgáltató a számára megküldött elektronikus dokumentumon időbélyeget helyez el, amely bizonyítja egy adott dokumentum egy meghatározott időpontban való létezését.

A NetLock Kft. jelen szolgáltatási szabályzat hatályba lépésekor az egyetlen olyan hitelesítés-szolgáltató, amely a piaci magán és szervezeti szereplők számára is nyújt tanúsítvány- és időbélyegzés-hitelesítési szolgáltatást. A folyamatos magas színvonalú szolgáltatás érdekében ISO 9001:2000-es szabványnak megfelelő minőségbiztosítási rendszert üzemeltet, amelyet külső, független szakértő évente több alkalommal is ellenőriz.

A NetLock Kft. tevékenysége megfelel a Hitelesítés-szolgáltatókkal szemben támasztott nemzetközi követelményeknek, ezt az Ernst & Young Kft. által kiadott WEB TRUST nemzetközi audit záródokumentum igazolja. A NetLock Kft. szerepel minden Microsoft termék hitelesítés-szolgáltatói listáján világszerte. Szolgáltatásaiért viszontbiztosítással rendelkező biztosító társaság vállal felelősséget.

1.1.1 A Szabályzat

Jelen Szolgáltatási Szabályzat a Szolgáltató minősített tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazza.

A Szabályzat célja, hogy összefogja azokat a szabályzatokat és információkat, amelyeket a Szolgáltatóval valamilyen módon kapcsolatba kerülőknek (elsősorban a végfelhasználóknak és érintett feleknek) tudni érdemes. Mint ilyen, a Szolgáltató működésének átláthatóságát biztosítja, és lehetővé teszi a felhasználók számára, hogy megállapítsák, hogy a Szolgáltató gyakorlatai, illetve adott tanúsítványfajtája mennyiben felel meg elvárásaiknak. A Szabályzat ellenőrzésével a tanúsítvány elfogadóinak egyértelműen meg kell tudni állapítani a tanúsítvány kezelésének módját, az általa garantált biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat.

A tanúsítványok végfelhasználóinak tevékenységére vonatkozóan a jelen Szabályzattól és Szolgáltatótól független egyéb szabályzatok is élhetnek előírásokkal. Amennyiben e szabályzatok bármely vonatkozásban ellentmondással vagy eltérő kikötéssel élnének, jelen Szabályzat előírásai tekinthetők magasabb szintűnek és így irányadónak.

A jelen Szabályzat tartalmára és felépítésére az RFC 2527 [15] dokumentum, illetve a Minősített tanúsítványtípus minták minősített Hitelesítés-szolgáltatók számára [4] adott útmutatót, amelyek struktúráját a Szabályzat követi.

1.1.2 A Szabályzat hatálya

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

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

A Szabályzat személyi hatálya a teljes Közösség (ld. 1.3 alfejezet) minden egyes tagjára, jogi és természetes személyekre egyaránt kiterjed.

1.1.3 A Szolgáltató

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

A Hírközlési Felügyelet (HIF) 2001. október 27-én vette nyilvántartásba a Szolgáltatót fokozott biztonságú szolgáltatóként. HIF regisztrációs szám: FA 6133-5/2001.

A Hírközlési Felügyelet (HIF) 2003. március 19-én vette nyilvántartásba a Szolgáltatót minősített szolgáltatóként. HIF 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)

1.1.4 Szolgáltatások

A Szolgáltató fő tevékenységi köre a hitelesítés-szolgáltatás. Ezen kívül a hitelesítés-szolgáltatáshoz kötődő fejlesztési és tanácsadási tevékenységgel is foglalkozik, és a biztonságos aláíró eszközzel kapcsolatos kereskedelmi és megszemélyesítési feladatokat is ellát. A Szolgáltató hitelesítés-szolgáltatása a következő elemekből áll:

- Regisztrációs szolgáltatás
- Tanúsítványlétrehozási szolgáltatás
- Aláíró eszköz szolgáltatás
- Egyedi név szolgáltatás
- Tanúsítványszétosztási szolgáltatás
- Tanúsítványarchiválási szolgáltatás
- Adattárolási szolgáltatás
- Állapotinformációs szolgáltatás
- Tanúsítványmegújítási szolgáltatás
- Visszavonás kezelési szolgáltatás
- Időbélyegzés-szolgáltatás

1.1.5 Szabványok és előírások

1.1.5.1 Szolgáltatási Szabályzat

A Szabályzat a [10] szabványa alapján készült, a MATT + BALE–nek [18] megfelelően. A Szabályzat tartalmi vonatkozásokban eleget tesz az [1], [2] és [3] hazai jogszabályok előírásainak és ajánlásainak, és felhasználja a [7] műszaki specifikáció, valamint a [12] ajánlásait.

1.1.5.2 Lenyomatképző algoritmusazonosítók

- 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 }

1.1.5.3 Kriptográfiai algoritmusazonosítók

- 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 }

1.1.5.4 Tanúsítvány kiterjesztés algoritmusazonosítók

- KeyUsage OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 15 }
- 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 }
- QcCompliance OID ::= { ITU-T(0) ITU-T Identified Organization(4) ETSI(0) 1862 1 1 }
- QcLimitValue OID ::= { ITU-T(0) ITU-T Identified Organization(4) ETSI(0) 1862 1 2 }
- QcRetentionPeriod OID ::= { ITU-T(0) ITU-T Identified Organization(4) ETSI(0) 1862 1 3 }

1.1.5.5 Alkalmazott formátumok

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

1.1.6 Tanúsítványfajták

A Szolgáltató által támogatott, végfelhasználói tanúsítványfajták összefoglaló táblázata. A tanúsítványfajtákhoz tartozó profilok részletes leírását a 7. fejezet tartalmazza.

Fajta	Alany	Engedélyezett alkalmazások	Tiltott alkalmazások	Osztály	Felelősség biztosítás maximum összege	Joghatás
Személyes aláíró	Természetes személy	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybani, értékbeni stb.) megszegése	Minősített	50 M forint	Teljes bizonyító erejű magánokirat
Munkatársi aláíró	Természetes személy, szervezet munkatársaként	Elektronikus aláírás készítése	Bármilyen korlátozás (földrajzi, tárgybani, értékbeni stb.) megszegése	Minősített	50 M forint	Teljes bizonyító erejű magánokirat

Az egyes tanúsítványfajták nemcsak az azonosítás (a tanúsítvány és a benne megnevezett személyek közötti megfeleltethetőség) szintjében térnek el, hanem a Szolgáltató egyéb adminisztratív, algoritmikus, informatikai és fizikai biztonsági faktorokat is arányosan másképpen kezel velük kapcsolatban.

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 időbélyegzés-szolgáltatás igénybevétele a Szolgáltatóval történő eseti megállapodás alapján lehetséges.

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 vagy jogi személy, szervezet	Azonos a minősített aláírásával.

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 időpecsételt dokumentum tartalmát, csak az abból képzett lenyomatot.

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.

Az aláírás-létrehozó eszköznek szerepelnie kell a [3] Rendelet alapján kijelölt tanúsító szervezetek által kibocsátott listán.

Aláíró eszköz szolgáltatás biztosítása során a Szolgáltató:

- az aláíró kulcsokat a minősített elektronikus aláírások céljaira alkalmas algoritmus felhasználásával generálja,
- 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,
- gondoskodik arról, hogy az általa generált, akár az Aláíró által hozott magán aláíró kulcsokról, semmilyen másolat nem kerül 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,
- biztosítja, hogy az aláírás-létrehozó eszköz a szándék szerinti, hitelesített Aláíróhoz kerül,
- aláíró eszköz biztosítása esetén az aktivizáló adatokat az aláírás-létrehozó eszköztől elkülönítve juttatja el az Aláíróhoz,
- gondoskodik róla, hogy a saját munkavállalói ne élhessenek vissza az aláírás-létrehozó eszközzel a következőképpen:
- az aláírás-létrehozó eszköz előkészítése és továbbítása során alkalmazza a biztonsági eljárásokat,
- az aláírás-létrehozó adat csak az átadás után lesz érvényes.

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 megsemmisíti.

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, illetve -ellenőrző eszközöknek nem szabad az aláírandó elektronikus dokumentumot módosítaniuk, illetőleg az aláírás folyamatában lehetővé kell tenniük ezen dokumentum megjelenítését az Aláíró számára.

1.2 Azonosítás

Jelen dokumentum:

- Teljes neve: NetLock Hitelesítés-szolgáltató Minősített Hitelesítés Szolgáltatás Szolgáltatási Szabályzata
- Rövid neve: Minősített Szolgáltatási Szabályzat
- Verziószáma: 1.3.6.1.4.1.3555.1.15.030317

A Szabályzat hivatalos és aktuális verziója Szolgáltató elektronikus aláírásával ellátva, megtalálható és letölthető Szolgáltató Internetes oldalairól: www.netlock.hu (ld. még 2.6.1 pont).

A Szabályzat alapján a Szolgáltató a következő tanúsítványtípusnak való megfelelést vállalja:

- [MATT + BALE]: Nyilvános körben kibocsátott minősített alap tanúsítványtípus biztonságos aláírás létrehozó eszköz támogatásával [18], OID: 1.3.6.1.4.1.3555.1.14.030317

1.3 Közösség és alkalmazhatóság

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

A Szolgáltató által kibocsátott „M" osztályú tanúsítvány teljesíti a MATT + BALE-ban [18] meghatározott feltételeket, így minősített tanúsítványnak számít.

1.3.1 Szabályzatért Felelős Egység

A Szabályzatért Felelős Egység a Közösség elektronikus hitelesítéssel, illetve hitelesítés-szolgáltatásra vonatkozó szabályozási tevékenységéért felelős egysége. Az Egység a szabályzatok kezelésével kapcsolatos feladatokat is ellátja. A Szabályzatért Felelős Egység adatai:

Név:	*Szabályzatért Felelős Egység*
Egység:	*NetLock Kft.*
Cím:	*1023 Budapest, Zsigmond tér 10.*
Telefon:	*(1) 345-2255*
Fax:	*(1) 345-2250*
Internetcím:	*www.netlock.hu*
E-mail:	*info@netlock.hu*

1.3.2 Regisztrációs egységek

A Szolgáltató saját szervezetén belül központi regisztrációs egységeket, valamint partnerein keresztül regisztrációs pontokat működtet, amelyek feladata a kezdeti regisztráció és a tanúsítvány kibocsátásával kapcsolatos egyéb tevékenységek elvégzése. A központi regisztrációs egységek feladata a további tanúsítvány kezelési feladatok, többek között a felhasználókkal való kapcsolattartás, az ügyfélszolgálati teendők ellátása.

A Szolgáltató külföldön nem tart fenn képviseleti vagy ügyfélszolgálati irodákat.

1.3.2.1 Minősített („M" osztályú) Regisztrációs Egység

A Szolgáltató minősített szolgáltatásai végző regisztrációs egysége. A Minősített Regisztrációs Egység egy központi egységből és több regisztrációs pontból áll. A regisztrációs pontok a minősített eljárási rend („M" osztály) szerint történő minősített tanúsítvány kibocsátás során a felhasználói adatellenőrzést, a regisztráció helyességének és szabályzatoknak való megfelelésének ellenőrzését, valamint a kibocsátás során történő elektronikus kérelem-feldolgozási tevékenységet végzik. A központi egység koordinációs szerepet játszik, a tényleges regisztrációs tevékenységet a regisztrációs pontokat jelentő közjegyzők végzik. A központi egység munkatársainak felelőssége a tanúsítvánnyal kapcsolatos végső döntések meghozatala is.

A Szolgáltató a végfelhasználói minősített tanúsítványok regisztrációs teendőinek ellátására (elsősorban a kezdeti regisztráció feladatának elvégzésére) a Magyar Országos Közjegyzői Kamarával (MOKK) működik együtt. A MOKK-tag közjegyzők a Szolgáltató számára országos regisztrációs hálózatot jelentenek Magyarországon. A Szolgáltató a későbbiekben egyéb egységekkel is szerződést köthet „M" regisztrációs szolgáltatások elvégzésére.

A Szolgáltató külföldön nem tart fenn „M" regisztrációs irodákat.

Név:	*„M" Regisztrációs Egység*
Egység:	*NetLock Kft.*
Cím:	*1023 Budapest, Zsigmond tér 10.*
Telefon:	*(1) 345-2255*
Fax:	*(1) 345-2250*
Internetcím:	*www.netlock.hu*
E-mail:	*info@netlock.hu*

1.3.3 Hitelesítő egységek

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

1.3.3.1 Minősített („M" osztályú) Hitelesítő Egység

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

Név:	*„M" Hitelesítő Egység*
Egység:	*NetLock Kft.*
Cím:	*1023 Budapest, Zsigmond tér 10.*
Telefon:	*(1) 345-2255*
Fax:	*(1) 345-2250*
Internetcím:	*www.netlock.hu*
E-mail:	*info@netlock.hu*

1.3.4 Végfelhasználók

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

A Szolgáltató a következő entitások részére bocsát ki minősített (M osztályú) tanúsítványokat:

- természetes személyek.

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.

1.3.5 Érintett fél

Az Érintett Fél a Közösség azon tagja, aki az elektronikus aláírás, illetve időpont hitelesítése céljából a Szolgáltató által kibocsátott tanúsítványhoz, illetve időbélyegzőhöz fordul, illetőleg ezen tanúsítvány, illetve időbélyegző érvényességének ellenőrzéséhez a Szolgáltató által karbantartott nyilvántartásokat és szabályzatokat ellenőrzi. A Szolgáltató az Érintett Féllel elsősorban a tanúsítványtáron keresztül tart kapcsolatot.

1.3.6 Alkalmazhatóság

1.3.6.1 Engedélyezett alkalmazási lehetőségek

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

A Szolgáltatói aláíró tanúsítványok tanúsítványhitelesítésre, illetve CRL listák hitelesítésére használhatók. A Szolgáltatói időbélyeg tanúsítványok időbélyegek kibocsátására használhatók fel.

1.3.6.2 Korlátozott alkalmazási lehetőségek

A Szolgáltató a jelen Szolgáltatási Szabályzatban leírt felhasználási feltételekkel korlátozza a kibocsátott tanúsítványok felhasználhatóságát. 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 (7. fejezet).

1.3.6.3 Tiltott alkalmazási lehetőségek

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

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

A szolgáltatói aláíró tanúsítványok csak tanúsítványhitelesítésre, illetve CRL listák hitelesítésére használhatók, egyéb más szolgáltatás nyújtásához történő alkalmazása tilos. A szolgáltatói időbélyeg tanúsítványok csak időbélyegzés során használhatók fel, egyéb más szolgáltatás nyújtásához történő alkalmazása tilos.

1.4 Kapcsolattartás

A Szolgáltató adatai:

- Név: NetLock Hálózatbiztonsági és Informatikai Szolgáltató Korlátolt Felelősségű Társaság
- Székhely: 1023 Budapest, Zsigmond tér 10.
- Telefonszám: (1) 345-2255
- Telefax szám: (1) 345-2250
- Internetcím: http:// www.netlock.hu
- Központi e-mail cím: info@netlock.hu
- Ügyfélfogadás: munkanapokon 9–17 óráig
- Panaszkezelési szabályok, illetékes fogyasztóvédelmi felügyelőség: Lásd 8.2.4 pont.

A szolgáltatással kapcsolatos kérdésekkel, problémákkal a végfelhasználók a regisztrációs egységekhez fordulhatnak szóban vagy írásban. A Szolgáltató az Interneten információs szolgáltatást működtet.

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

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

2 Általános rendelkezések

2.1 Kötelezettségek

2.1.1 A Szolgáltató kötelezettségei

2.1.1.1 Szolgáltató általános kötelezettségei

A Szolgáltató kötelessége:

1. a hitelesítő és regisztrációs egységek és a tanúsítványtár felügyelete, üzemeltetése,
2. a szolgáltatásainak a hatályos jogi szabályozással, jelen szabályzattal és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban való nyújtása,
3. a magas színvonalú és biztonságos szolgáltatások folyamatos biztosítása,
4. 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.

2.1.1.2 A Szolgáltatói egységek közös kötelezettségei

A Szolgáltatóhoz tartozó szervezetek, regisztrációs és hitelesítő egységek kötelessége:

1. a Közösség elektronikus hitelesítéssel kapcsolatos tevékenységeinek, alapelveinek meghatározása, ezek alapján a működést részletesen tárgyaló szabályzatok készítése és rendszeres felülvizsgálata,
2. megfelelő szakmai végzettséggel rendelkező, a folyamatos, szabályzatokban előírt működés biztosításához elégséges számú kezelőszemélyzet biztosítása,
3. a szabályzatokban előírt PKI folyamatok elvégzésére alkalmas, megfelelően beállított szoftver és hardver infrastruktúra biztosítása, a szükséges változtatások megtétele,
4. az infrastruktúra működtetéséért, javításáért és karbantartásáért felelős személyzet munkájának és szakmai felkészültségének folyamatos ellenőrzése, a szükséges változtatások megtétele,
5. az előző pontokban előírt infrastruktúra folyamatos, biztonságos üzemeltetése, hibajavítása és az infrastruktúrába tartozó eszközökre előírt szabványos karbantartás elvégzése,
6. Üzleti Folytonossági Terv készítése, alkalmazása,
7. 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,
8. 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,

9. a logikai és fizikai védelmet megteremtő eszközök megfelelő üzemeltetése, az informatikai, fizikai, adminisztrációs és üzleti biztonság megteremtése és fenntartása.
10. szabad hozzáférés biztosítása a Szabályzat Adminisztrátor részére a felügyelendő dokumentumokhoz, továbbá a megfelelő körülmények biztosítása számára a belső ügyviteli folyamatok azok helyszínén való ellenőrzéséhez.

2.1.1.3 A Regisztrációs Egységek közös kötelezettségei

A Regisztrációs Egységek kötelessége:

1. úgy működni, hogy semmilyen módon ne sértsék a szolgáltatás biztonságát,
2. tevékenységüket saját maguk ellátni,
3. az igénylő (alany) tanúsítványra vonatkozó kérelmeinek (kibocsátás, megújítás, felfüggesztés, visszavonás) kezelése,
4. az ügyféladatok összegyűjtése, ellenőrzése és döntés meghozatala azok valódiságára vonatkozóan,
5. a nem nyilvános ügyféladatok megfelelő szintű védelme,
6. az alany (és az igénylő) és a Közösség többi tagjának értesítése a tanúsítvány kibocsátásáról és a tanúsítvánnyal végzett műveletekről,
7. a tanúsítványnak az alany számára elérhetővé tétele,
8. a belépés lehetővé tétele a Szabályzatért Felelős Egység számára a szolgáltatás területére.

2.1.1.3.1 Minősített („M” osztályú) Regisztrációs Pont

1. a személyazonosságot és az egyéb adatok valódiságát igazoló okmányoknak és az ügyfél szolgáltatási szerződésének közjegyzői okiratba foglalása,
2. a közokiratba foglaláshoz szükséges adatok ellenőrzésére használt iratok másolatának a Szolgáltatónál működő központi egységhez való eljuttatása,

Az „M” Regisztrációs Pontok a közjegyzők tevékenységét szabályozó 1991. évi XLI. törvény rendelkezései alapján látják el feladatukat.

2.1.1.3.2 Minősített („M” osztályú) Központi Regisztrációs Egység

1. a hitelesítés ellenőrzése,
2. a tanúsítvány- és visszavonási kérelem nyilvántartásba vétele és a kérelem elbírálása, továbbítása.

2.1.1.4 A hitelesítő egységek közös kötelezettségei

A hitelesítő egységek kötelessége:

1. szabványos X509 tanúsítvány kibocsátása, megújítása, felfüggesztése, reaktiválása, visszavonása a Regisztrációs Egységek által küldött erre vonatkozó kérelem esetén,

2. tanúsítvány felfüggesztésének vagy visszavonásának publikálása CRL-en,
3. saját tanúsítványának nyilvánosságra hozatala,
4. saját magánkulcsának teljes körű védelme, a kulcs dedikált kriptográfiai hardver modulban történő tárolásával,
5. 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.

2.1.1.5 A Szabályzatért Felelős Egység kötelezettségei

A Szabályzatért Felelős Egység kötelessége:

1. a felügyelendő dokumentumok, továbbá a belső ügyviteli folyamatok azok helyszínén való ellenőrzése és a Szolgáltató vezetésének tájékoztatása a megfigyelésekről,
2. a Szolgáltatóhoz érkező szabályzatokkal kapcsolatos észrevételek és javaslatok fogadása,
3. a szabályzatok aktualizálásának előkészítése, egyeztetése és végrehajtása,
4. a minősített tanúsítványtípusok specifikálása, jóváhagyása és karbantartása.

2.1.1.6 A tanúsítványtár kötelezettségei és vele kapcsolatos tevékenységek

A Tanúsítványtár kötelessége az üzemeltetés során:

1. a Tanúsítványtár nyilvános, minden Érintett Fél számára elérhető módon való üzemeltetése a Szolgáltató Internetes oldalán (ld. 1.4 alfejezet),
2. a Szolgáltató saját tanúsítványainak, a Szolgáltató által kibocsátott tanúsítványok, CRL listák, aktuális és korábbi szabályzatok (NetLock ÁSZF, Szolgáltatási Szabályzat és Tanúsítványtípusok) késedelem nélküli közzététele,
3. a szabályzatok során minimum Adobe Acrobat elektronikus könyv és Microsoft Word dokumentum formátumban közzétenni,
4. bizalmas információkat, nem nyilvános adatokat a Tanúsítványtárban meg nem jeleníteni,
5. a Tanúsítványtárat minimum 99,9 %-os rendelkezésre állással működtetni, ezt a mutatót is figyelembe véve elérhetővé tenni az év valamennyi napján, 0–24 óráig,
6. a rendelkezésre állást a Szolgáltató az Üzleti Folytonossági Tervben rögzített, a szokásostól eltérő üzletmenet elhárítására kidolgozott eljárások végrehajtásával biztosítani,
7. a Tanúsítványtárhoz írási jogosultságot csak a Szolgáltatónak biztosítani.

2.1.2 A végfelhasználó kötelezettségei

A végfelhasználó általános kötelessége:

1. megismerni és betartani az Általános Szerződési Feltételeket és a jelen Szabályzatot,

2. igényeinek megfelelő tanúsítványtípust választani minősített tanúsítvány igénylése előtt,
3. igényeinek és a kiválasztott tanúsítványtípusnak megfelelő tanúsítványfajtát kiválasztani,
4. a feltételeknek és szabályzatoknak megfelelően eljárni a szolgáltatások felhasználása során, beleértve a tanúsítvány és magánkulcs igénylését és alkalmazását,
5. hozzájárulni a szolgáltatás biztonságához, elsősorban korrekt adatszolgáltatáson keresztül, valamint a nyilvános kulcsú infrastruktúra tudatos és felelősségteljes alkalmazásával,
6. esetleges jogvita kezdetéről és jogerős lezárásáról haladéktalanul tájékoztatni a Szolgáltatót,
7. az aláírással vagy az így aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt – külön jogszabályban, illetve a Szabályzatban meghatározott – rendellenességről tájékoztatni a Szolgáltatót,
8. betartani a tanúsítványban jelzett esetleges korlátozásokat.

A végfelhasználó kötelessége saját kulcs kezelése során:

9. a magánkulcsát biztonságos módon generálni, tárolni, kezelni,
10. a kulcspárt és tanúsítványát rendeltetésszerűen használni,
11. magánkulcsát a hozzá tartozó tanúsítvány lejárta után megsemmisíteni,
12. amennyiben magánkulcsa kompromittálódásának lehetősége fennáll, a lehető leghamarabb tanúsítványának visszavonását, illetve felfüggesztését kérni a Szolgáltatótól.

A végfelhasználó kötelessége a tanúsítványának kezelése során:

13. 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 bemutatásával alátámasztani,
14. az azonosításához szükséges személyazonosító adatokról, más személy (szervezet) képviseletében történő aláírásra jogosító elektronikus aláírás esetén a képviseletre, illetőleg aláírásra jogosult személy személyazonosító adatairól, valamint a cégadatokról és mindezek változásáról tájékoztatni a Szolgáltatót,
15. 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,
16. 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,
17. a regisztrált adatainak a kibocsátott tanúsítványának érvényességi ideje alatt történő megváltozásáról késedelem nélkül a Szolgáltatót tájékoztatni,
18. olyan eljárásokat követni és alkalmazásokat használni, amelyek támogatják a Szolgáltató által kibocsátott tanúsítványok helyes kezelését,
19. a tanúsítvány első felhasználása előtt ellenőrizni a tanúsítványban feltüntetett adatainak helyességét és amennyiben azok nem felelnek meg a valóságnak, akkor a tanúsítvány visszavonását kérni.

20. 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 alany, illetve a másodlagos alany közokirat-hamisítás bűntettét valósítja meg a Btk. 274. §.-a értelmében.

2.1.3 Az Érintett Fél kötelezettségei

Az Érintett Fél köteles:

1. olyan eljárásokat, alkalmazásokat használni, amelyek támogatják a Szolgáltató által kibocsátott tanúsítványok helyes kezelését,
2. elektronikus aláírás elfogadásakor a rendelkezésre álló módszerekkel meggyőződni az aláírás és a tanúsítvány érvényességéről, elfogadhatóságáról, továbbá minden egyéb tevékenységet megtenni annak érdekében, hogy az elektronikus aláírás 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 listák áttanulmányozásával.

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 vissza kell utasítania az elektronikus aláírás elfogadását, ha bármely ellenőrzési lépés eredményéből az elektronikus aláírás, a tanúsítvány vagy azok alkalmazásának érvénytelenségére, jogszerűtlenségére, jelen és kapcsolódó szabályzatokba ütköző voltára utaló következtetés vonható le.

2.2 Felelősség

2.2.1 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.

2.2.1.1 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.

2.2.2 A végfelhasználó felelőssége

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

2.2.3 Az Érintett Fél felelőssége

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

2.3 Pénzügyi felelősség

2.3.1 A Szolgáltató pénzügyi felelőssége

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 a Törvény [1] alábbi szakaszaiban foglaltakat 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, de maximum 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.

2.3.1.1 A Szolgáltató pénzügyi felelősségének korlátozása

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

2.4 Értelmezés és érvényesítés

2.4.1 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi (ld. [1] Törvény, [2] Irányelv, [3] Rendelet). A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők.

2.4.2 A rendelkezések különválaszthatósága

Bármely rendelkezés hatályon kívül kerülése nem befolyásolja a többi rendelkezés hatályát.

2.4.3 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.

2.4.4 A rendelkezések kiterjesztése

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

2.4.5 Vitás kérdések megoldására vonatkozó eljárások

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

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. 8.2.4 pont).

2.5 Díjak

A mindenkor érvényes szolgáltatások díjait a Szolgáltató saját Internetes oldalán (ld. 1.4 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: gyorsasági felár 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 szabványos azonosítási rendelkezésekben rögzített feltételeknek. Egyéb esetekben a Szolgáltató egyedi díjszabást alkalmazhat.

A Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF 8. pontja tartalmazza.

2.5.1 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) egyedi díjszabást alkalmazhat.

A Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF 8. pontja tartalmazza.

2.5.2 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 kérvényt 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 megjelölt bankszámlaszámra 20 naptári napon belül visszautalja.

A tanúsítvány kibocsátását, illetve megújítását követően az alany/igénylő kizárólag csak a Szolgáltató bizonyított szerződés- vagy kötelezettségszegése esetén jogosult díjvisszafizetésre. Nem tartozik a visszatérítési okok közé a kibocsátott tanúsítványhoz tartozó magánkulcs bármely okból történő megsemmisülése.

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

2.6 Közzététel és tanúsítványtár

2.6.1 A Szolgáltató információ közzététele

2.6.1.1 Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában (Microsoft Word és Adobe Acrobat formátumokban) hozza nyilvánosságra Internetes oldalain keresztül (ld. 1.4 alfejezet). Itt a dokumentumok aktuális verziója mellett megtalálhatóak azok korábban érvényben lévő változatai is.

2.6.1.2 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 4.12 alfejezet),

- rendkívüli üzemeltetési helyzetről tájékoztatás,

2.6.1.3 Tanúsítványok nyilvánosságra hozatala

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

- saját szolgáltatói tanúsítványát közzéteszi tanúsítványtárában, valamint Internetes honlapján keresztül (ld. 1.4 alfejezet),
- minden hitelesítő egység tanúsítványát közzéteszi tanúsítványtárában, valamint Internetes honlapján keresztül.

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat a következő módszerekkel teszi közzé:

- az alany és az érintett felek részére a nyilvános tanúsítványtárában.

2.6.1.4 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,

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 (igénylő) nem járult hozzá.

2.6.2 A közzététel gyakorisága

2.6.2.1 Kikötések és feltételek közzétételi gyakorisága

Jelen Szabályzattal kapcsolatos új verziók közzététele a 8.1 alfejezetben ismertetett eljárásoknak megfelelően történik.

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

2.6.2.2 Rendkívüli információk közzétételi gyakorisága

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

2.6.2.3 Tanúsítványok nyilvánosságra hozatalának gyakorisága

A Szolgáltató az egyes 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. 1.4 alfejezet) 10 munkanapon belül jelenik meg,
- a Szolgáltató a végfelhasználói tanúsítványokat a kibocsátást követően, a regisztrációs eljárás részeként átadja az alany (igénylő) részére,
- a Szolgáltató a végfelhasználói tanúsítványokat a tanúsítványtárában az előállítást követően 10 munkanapon belül teszi közzé.

2.6.2.4 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

A Szolgáltató az általa működtetett hitelesítő egységek és felhasználók tanúsítványával kapcsolatos állapotinformációkat a 4.5.11.1 pontban tárgyalt gyakorisággal teszi közzé.

2.6.3 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 a Szabályzat kikötéseinek és feltételeinek elfogadását jelenti.

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

2.6.4 Tanúsítványtárak

A Szolgáltató az Érintett Felek számára a rendelkezésére álló legpontosabb adatokat biztosítja a lehetőségeknek, vállalásoknak megfelelően leghamarabb, és ennek érdekében nyilvános Tanúsítványtárat üzemeltet.

A Szolgáltató tanúsítványtára szabványos LDAP és HTTP protokollokkal érhető el a Szolgáltató Internetes oldalain keresztül (ld. 1.4 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 (ld. Folyamatosan elérhető szolgáltatás). A Szolgáltató a tervezett karbantartásokat munkaidőn kívüli időszakokra ütemezi, és ezekről a karbantartás megelőzően 24 órával értesítést tesz közzé honlapján ([3] 14. §).

2.7 A megfelelőség vizsgálata

Szolgáltató szolgáltatásának következő elemeinek megfelelőségét vizsgálja, vizsgáltatja:

- a minősített 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 minősített tanúsítványok kezeléshez használt módszereit, eljárásait.

2.7.1 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 3 alkalommal, belső ellenőrzés keretében, illetve legalább évente, szakhatósági eljárás keretében is,
- a magas színvonalú szolgáltatást biztosító ISO 9001:2000-es minőségbiztosítási rendszer ellenőrzésére évente 3 alkalommal.

2.7.2 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 [3] Rendelet előírásainak megfelelően kerül sor,
- a minősített tanúsítványok kezeléshez használt módszerek, eljárások ellenőrzését hatósági eljárás keretében a Hírközlési Felügyelet,
- a Hitelesítés-Szolgáltatókkal szemben támasztott nemzetközi követelményeknek való megfelelést a nemzetközi auditor cég (a Szabályzat kibocsátásakor az Ernst&Young Tanácsadó Kft.),
- az ISO 9001:2000-es minőségbiztosítási rendszer működtetését legalább évente akkreditált ISO tanúsító szervezet (a Szabályzat kibocsátásakor a Moody Nemzetközi Kft.).

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 Szabályzatért Felelős Egység vizsgálja saját munkarendje szerint.

2.7.3 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 biztosítja. A Nyilatkozatot a Szolgáltató Személyzeti Politikája tartalmazza.

2.7.4 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 tanúsítványtípusainak 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).

2.7.5 Hiányosságok esetén végrehajtandó tevékenységek

A Szabályzatért Felelős Egység a jogszabályi előírásoknak ellentmondó működés esetén a szolgáltatói tevékenységeket szabályozó belső eljárásrendek és szabályzatok megváltoztatásával, illetőleg a változás végrehajtásához szükséges rendszer implementáció végrehajtatásával intézkedik. A változások bejelentésre kerülnek a felügyeleti szerv, illetve a Közösség felé.

2.7.6 Az eredményekről való tájékoztatás

A Szolgáltató a vizsgálatok végeredményét saját honlapján közzéteszi. Ez nem vonatkozik a vizsgálatok során feltárt, az eljárás végeredményét nem befolyásoló hiányosságokra és részeredményekre.

A minősítési eljárás pozitív eredményéről a külvilágot a HÍF a minősített szolgáltatók nyilvántartásán keresztül is tájékoztatja.

A vizsgálat eredményéről és a megtett intézkedésekről a Szabályzatért Felelős Egység beszámol a Szolgáltató vezető tisztségviselőjének.

2.8 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 elsődleges célja a hitelesítés-szolgáltatási tevékenység regisztrációs feladatainak ellátása. A Szolgáltató az adatokat a törvények által előírt eseteken kívül kizárólag a főtevékenység hatékonyságának funkcionális támogatásához, illetve a belső statisztikákhoz 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 és 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 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 2.1.2 pontban megfogalmazott kötelezettségek szerint értesítik), valamint ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.

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

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

2.8.1 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.

2.8.2 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.

2.8.3 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 4.5 alfejezet).

2.8.4 Információszolgáltatás hatósági szervek részére

A [1] Törvény 11.§ 2., 3. és 4. bekezdésében foglalt esetekben és formában az érintett személyazonosságát igazoló adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíti, az adatátadásról a hitelesítés-szolgáltató az Aláírót a [1] Törvény értelmében nem tájékoztatja.

2.8.5 Információszolgáltatás polgári peres eljárás keretében

A hitelesítés-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.

2.8.6 Egyéb információszolgáltatás

Álnév használata minősített tanúsítványok esetén nem megengedett.

2.8.7 Az alany kérésére történő felfedés

A Szolgáltató az alany, illetve másodlagos alany meghatalmazása alapján tár fel bizalmas felhasználói információkat harmadik fél részére.

2.8.8 Egyéb információ harmadik félnek történő átadása

Egyéb információ harmadik félnek történő átadására sor kerülhet 30 napja lejárt díjtartozás esetén végrehajtás 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.

2.9 Szellemi tulajdonjogok

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.

3 Azonosítás és hitelesítés

3.1 Kezdeti regisztrálás

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:

- az azonosító mezők karaktertípusa: UTF8String,
- a tanúsítványban az adatok ékezetek, speciális és vezérlő karakterek nélkül szerepelnek,
- a nevek egyes egységeit egy szóköz választhatja el,
- a tanúsítványban a név („Common Name") mező nem üres,
- álnevek jelzése nem megengedett,
- a „State" mezőben a megye vagy megyei jogú város neve kerül feltüntetésre vagy a mező üresen marad,
- a tanúsítvány alany lakóhelyének, székhelyének ország megjelölésénél esetén a Szolgáltató az ISO 3166 [5] szabványban meghatározott kétkarakteres országkódot alkalmazza.

3.1.2 Különböző elnevezési formák értelmezési szabályai

A Szolgáltató által kibocsátott tanúsítványoknak nem célja, hogy az alanyként megjelölt természetes személyek számára digitális személyi igazolványként funkcionáljon, illetve, hogy személyüket a tanúsítványban feltüntetett adatok alapján azonosítani lehessen.

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 közvetlen is felveheti a kapcsolatot. A Szolgáltató ilyen esetben 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. 2.8.7 pont).

3.1.2.1 Kibocsátó azonosító

A kibocsátó azonosítója úgy értelmezendő, hogy a tanúsítványt a NetLock Kft. mint Hitelesítés-szolgáltató hitelesítő egysége adta ki (székhely, elérhetőség: ld. 1.4 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.

3.1.2.2 Alanyazonosító

Az alany azonosítója úgy értelmezendő, hogy a tanúsítvány alanya a *Common Name* nevű természetes személy, aki az *Organization* nevű szervezet *Organizational unit* nevű egységéhez tartozik. Amennyiben a szervezet gazdasági társaság, akkor ez az egység típusából látszódik.

A természetes személy nevei (családi, elő- és utóneve) olyan sorrendben szerepelnek a *Common Name* mezőben, ahogyan azok a személyazonosságát igazoló okmányban.

A természetes személy lakóhelye, illetve a szervezet székhelye vagy telephelye a *Country* ország, *State* megye, *Locality* településén található. Az alany e-mail címe az igénylő egységgel összefüggésben *E-mail*.

Az alanyazonosító mezőnek célja, hogy a tanúsítvány alanyát (a felhasználó egységen belül) azonosítani lehessen. Az alany és a felhasználó egység együttes megjelenítése a tanúsítványban azt jelenti, hogy az igénylő hozzájárult az alany és az egység nevének együttes feltüntetéséhez. A két fél közti viszony mikéntjére (munkavállalói, tagsági, támogatói, szimpatizánsi, ügyféli, partneri, stb.) vonatkozóan információt semmilyen formában nem fejez ki.

3.1.3 A nevek egyedisége

A Szolgáltató a kibocsátott összes tanúsítvány esetében a tanúsítványok alanyait egymástól egyértelműen megkülönbözteti a tanúsítványban rögzített összes személyes adatuk (név, lakóhely ország, lakóhely város, e-mail cím, ha van) segítségével (egyedi név). A tanúsítvány alany egyediségét az „egyedi” vagy „megkülönböztető” név alkalmazása biztosítja.

3.1.4 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.

3.1.6 A magánkulcs birtoklásának bizonyítási módszere

Az aláíró eszköz szolgáltatás esetében a Központi Regisztrációs Egység míg hitelesítés szolgáltatás esetében a Regisztrációs Pontok állítják elő az alany számára a kulcspárt, így a Szolgáltató nem igényel

bizonyítékot igényel arról, hogy az alany rendelkezik a hitelesítendő nyilvános kulcs magánkulcs párjával. A Szolgáltató – attól függetlenül, hogy a kulcspárt ki generálta – ellenőrzi, hogy a nyilvános kulcs korábban nem került-e kiosztásra más alany számára.

3.1.7 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 Közjegyzői Okiratba foglalt szolgáltatási szerződésen tett aláírásával.

A Regisztrációs Pontokon bemutatott és a közokirat kiállításának alapjául szolgáló eredeti dokumentumokról fénymásolatot készül, melyet a közokirattal együtt a Regisztrációs Pont megküld a Központi Regisztrációs Egységnek, amely ezen másolatban beérkezett dokumentumok alapján adatlapokat tölt ki. A másolatok archiválásra kerülnek.

3.1.8 Szervezeti azonosság hitelesítése

A Szolgáltató által kibocsátott munkatársi tanúsítványban feltüntetésre kerül a felhasználó szervezet (másodlagos alany) és opcionálisan annak egy szervezeti egységének a neve.

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

A Regisztrációs Pontokon bemutatott és a közokirat kiállításának alapjául szolgáló eredeti dokumentumokról fénymásolatot készül, melyet a közokirattal együtt a Regisztrációs Pont megküld a Központi Regisztrációs Egységnek, amely ezen másolatban beérkezett dokumentumok alapján adatlapokat tölt ki. A másolatok archiválásra kerülnek.

3.2 Érvényes tanúsítvány megújítása

3.2.1 Végfelhasználói tanúsítványok

A Szolgáltató lehetőséget biztosít a felhasználók részére a tanúsítvány lejártát megelőző 30 napos időszakban arra, hogy a tanúsítványt kulcscsere nélkül megújítsák. A megújításra csak abban az esetben van lehetőség, ha még érvényesek azok dokumentumok, amelyek alapján a tanúsítvány kibocsátásra került és az azokban foglalt adatok nem változtak.

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

A Szolgáltató ellenőrzi, hogy az ügyfél azonosságának igazolására használt információ még mindig érvényes. A tanúsítványmegújítási kérelemben az alanynak, illetve a másodlagos alanynak együttesen nyilatkozni kell arról, hogy a kezdeti regisztrációkor megadott adataik, különös tekintettel a tanúsítványban megjelenő adatokra továbbra is érvényesek. A kérelmet az alanynak saját (még érvényes)

magánkulcsával kell aláírnia. A kérelem mintája a Szolgáltató honlapján elérhető. Az ügyfélnek a meghosszabbítási kérelem során nyilatkoznia kell arról, hogy a tanúsítvány-kérelem során közölt adatok továbbra is érvényesek.

A Szolgáltató csak akkor bocsát ki új tanúsítványt az Aláíró korábbiakban tanúsított nyilvános kulcsának felhasználásával, ha annak kriptográfiai biztonsága még megfelelő az új tanúsítvány tervezett élettartamára, és nincs utalás arra vonatkozóan, hogy az Aláíró magánkulcsa kompromittálódott (hitelét vesztette).

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

Amennyiben bármilyen az ügyféllel, illetve az Aláíróval kapcsolatos információ megváltozott, azt a Szolgáltató az új tanúsítvány kibocsátásnál alkalmazott módszernek megfelelően nyilvántartásba veszi, és új tanúsítványt bocsát ki.

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.

3.2.2 Szolgáltatói tanúsítványok

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

3.3 Érvénytelen tanúsítvány megújítása

A Szolgáltató az érvénytelen tanúsítványok megújításának elektronikus üzenetváltáson alapuló, személyes megjelenést nem igénylő megvalósítását nem teszi lehetővé.

Ha az alanynak a tanúsítvány visszavonása után új tanúsítványra van szüksége, akkor új tanúsítványt kell igényelnie (ld. 4.1 alfejezet). Amennyiben az alany a visszavont tanúsítványban szereplő névre (alanyazonosítóra) igényt tart, akkor az arra való további jogosultságát igazolnia kell a Szolgáltatónál.

3.4 Visszavonási kérelem

Szolgáltató tanúsítvány visszavonási és -felfüggesztési szolgáltatásokat egyaránt nyújt. Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait a 4.5.4 pont tárgyalja.

4 Működésre vonatkozó követelmények

4.1 Tanúsítványigénylés

4.1.1 Igénylés feltételei

A Szolgáltatónál tanúsítvány hitelesítésének igényével csak a Szolgáltató rendszerében regisztrált természetes személy élhet.

A regisztráció során a szolgáltatott adatok önkéntesek, és írásbeli kérés alapján – tanúsítvány egyidejű visszavonása mellett – a regisztrációs adatbázisból a Szolgáltató törli ezeket.

Kizárólag a jelen Szabályzatban megadott fajtájú és profilú tanúsítványok igényelhetők.

Az igénylő köteles a tanúsítvány ellenértékét egy évre előre, a mindenkori díjtáblázatban fogalt tanúsítvány havi díjak alapján a tanúsítvány kibocsátását megelőzően, postai csekken vagy átutalással a Szolgáltató számlájára befizetni. A számlán történt befizetés jóváírását megelőzően a tanúsítvány kibocsátásáról a Szolgáltató saját hatáskörén belül dönt.

A tanúsítványmegújítás kérelmezését lásd a 3.2 alfejezetben.

4.2 Tanúsítvány-kibocsátás

Végfelhasználói tanúsítványok kibocsátására a tanúsítványigénylési eljárás lefolytatását követően kerül sor. A tanúsítvány elkészítésére az új tanúsítványigénylés során a kérelemben megadott, a Közjegyzői Okiratba foglalt 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.

Teszt tanúsítványok kiadásához az igénylőnek érvényes elektronikus levelezési címmel kell rendelkeznie. A Szolgáltató a megadott elektronikus levelezési címre továbbít utasításokat, 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 Szolgáltató Regisztrációs Egységének munkatársai végzik el,
- az eljárást minden tanúsítványigénylés esetében teljes egészében le kell folytatni,
- az eljárás részben automatizált, elektronikus rendszereken keresztül zajló, részben humán beavatkozással végzett folyamat.

A regisztráció és kibocsátás fő lépései a következők:

- az igénylő regisztrálja magát a Szolgáltató Internetes oldalán vagy más módon tanúsítvány igénylést juttat el a Szolgáltatóhoz (ld. 1.4 alfejezet),
- az igénylő a Regisztrációs Pontokon kulcspárt generál vagy a Szolgáltató generál kulcspárt az igénylő számára az aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatás keretében.
- a Szolgáltató fogadja a kérelmet, ellenőrzi annak szabályosságát, illetve kriptográfiai megfelelőségét, valamint meggyőződik a magánkulcs birtoklásáról,
- a Szolgáltató azonosítja az igénylő természetes személyt vagy munkatársát amennyiben az adott kérelem esetén ezek bármelyikére szükség van,
- a Regisztrációs Pont előállítja a Közjegyzői Okiratba foglalt szolgáltatási szerződését, előkészíti a további regisztrációhoz szükséges dokumentumokat,
- a Szolgáltató átveszi a Közjegyzői Okiratba foglalt szolgáltatási szerződését,
- a Szolgáltató megvizsgálja a Közjegyzői Okiratba foglalt szolgáltatási szerződést és annak kiállításának alapjául szolgáló az entitásazonosító dokumentumokat,
- a Szolgáltató összeveti a kérelem adatait az entitás adataival,
- a Szolgáltató összeállítja a kibocsátandó tanúsítványt,
- a Szolgáltató dokumentálja a regisztrációs lépéseket,
- a Szolgáltató kibocsátja a tanúsítványt az ellenőrzések pozitív lezárása esetén.

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

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

A Szolgáltató nyilvántartásba veszi a következőket:

- az ügyfél által megadott cím, vagy más elérhetőség,
- az igénylő által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa és maguk a dokumentumok,
- az azonosítási dokumentumok egyedi azonosító adatainak, számainak, illetve azok kombinációinak rekordja,
- 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,
- az igénylővel folytatott elektronikus és hagyományos levelezés 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 4.9 alfejezet).

4.2.2 Regisztrációs eljárás

Eljárási lépés	Tanúsítványfajta	
	Személyes	**Munkatársi**
1. Regisztráció	Magánszemély adatainak (név, lakcím, telefon, fax, e-mail cím) elektronikus regisztrációja. Végrehajtani jogosult: Természetes személy vagy Központi Regisztrációs Egység, ha a regisztráció nem ügyfélmenü létrehozásával történt	Szervezeti munkatárs adatainak (név, lakcím, telefon, fax, e-mail cím) elektronikus regisztrációja. Végrehajtani jogosult: Igénylő munkatárs vagy Központi Regisztrációs Egység, ha a regisztráció nem ügyfélmenü létrehozásával történt
2. Kapcsolt regisztráció	Nincs	Szervezet adatainak (név, székhely, telefon, fax, e-mail cím) elektronikus regisztrációja. Végrehajtani jogosult: Igénylő munkatárs vagy Központi Regisztrációs Egység, ha a regisztráció nem ügyfélmenü létrehozásával történt
3. Kulcspár generálása eszközön és kérelem készítése	Hitelesítés szolgáltatás esetén végrehajtani jogosult: Természetes személy Közjegyző előtt Eszközszolgáltatás esetén végrehajtani jogosult: Központi Regisztrációs Egység	Hitelesítés szolgáltatás esetén végrehajtani jogosult: Igénylő munkatárs Eszközszolgáltatás esetén végrehajtani jogosult: Központi Regisztrációs Egység
4. 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
5. PIN boríték és adatlap összeállítása és megküldése az aláírónak	Hitelesítés szolgáltatás esetén nem értelmezett. Eszközszolgáltatás esetén végrehajtani jogosult: Központi Regisztrációs Egység	
6. Természetes személy azonosítása	Végrehajtani jogosult: Regisztrációs pontként működő Közjegyző	
7. Szervezet azonosítása	Nincs	Végrehajtani jogosult: Regisztrációs pontként működő Közjegyző
8. Kitöltött hozzájáruló és elfogadó nyilatkozat ellenőrzése és Szolgáltatónak való megküldése	Nincs	Végrehajtani jogosult: Regisztrációs pontként működő Közjegyző
9. Közjegyzői Okiratba foglalt szolgáltatási szerződés elkészítése és Szolgáltatónak való megküldése a kiállítás alapjául szolgáló dokumentumok másolataival együtt	Végrehajtani jogosult: Regisztrációs pontként működő Közjegyző	
10. A Szolgáltatóhoz beérkezett Közjegyzői Okiratba foglalt szolgáltatási szerződés illetve annak kiállításának alapjául használt dokumentumok másolatainak ellenőrzése	Végrehajtani jogosult: Központi Regisztrációs Egység	
11. Tanúsítvány előállítása és a tanúsítványtárban való közzététele	Végrehajtani jogosult: Hitelesítő Egység	
12. Tanúsítvány felfüggesztése és (re)aktiválása	Hitelesítés szolgáltatás esetén nem értelmezett. Végrehajtani jogosult: Központi Regisztrációs Egység	
13. Tanúsítvány hordozó eszközre való letöltése	Eszközszolgáltatás esetén nem értelmezett. Végrehajtani jogosult: Alany	

14. Hordozóeszköz eljuttatása az aláíróhoz	Hitelesítés szolgáltatás esetén nem értelmezett. Eszközszolgáltatás esetén végrehajtani jogosult: Központi Regisztrációs Egység
15. Dokumentáció	Tanúsítvány adatösszesítő lap, Kérelem, Közjegyzői Okiratba foglalt szolgáltatási szerződés, Személyes (és szervezeti) dokumentumösszesítő adatlap, Okmánymásolatok, E-mail cím ellenőrzés kinyomtatva (Hozzájáruló és elfogadó nyilatkozat)

4.2.3 Szolgáltatási szerződés

A természetes személy és a magánkulcs összetartozásának dokumentálására, illetve a kötelező tájékoztatásra a Szolgáltató szolgáltatási szerződést alkalmaz, amelyet a Regisztrációs Pontokként működő közjegyzők közokiratba foglalnak. A tanúsítvány kiadásának feltétele ennek az elfogadó nyilatkozatnak az aláírása.

A nyilatkozat legalább a következőket tartalmazza:

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

A nyilatkozatot az igénylő természetes személy írja alá. A nyilatkozatot a Regisztrációs Pontként működő közjegyzők az előzetesen számukra megküldött minták alapján készítik el.

A nyilvános kulcs lenyomat karaktereinek átírása:

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

4.2.3.1 Szolgáltatási szerződés minták

A Szolgáltató honlapján megtalálható a személyes és munkatársi Közjegyzői Okiratba foglalt szolgáltatási szerződés mintákat.

4.2.4 A tanúsítványkérelmek jóváhagyásának követelményei

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

- az benyújtották a kérelmét a tanúsítvány kibocsátónak,
- a természetes személy (akinek nevében az igénylő eljár) azonos a kérelemben szereplő alannyal,
- az igénylő birtokában van a kérelemben szereplő nyilvános kulcs titkos párja,
- a kérelemben szereplő adatok ellenőrizhetők és pontosak.

4.2.5 A tanúsítványok tartalma

A tanúsítványok tartalmazzák az alábbiakat:

- a tanúsítvány azonosító kódját,
- a Hitelesítés-szolgáltató megnevezését, benne székhelyének ország-azonosítóját,
- azt, hogy a tanúsítvány minősített tanúsítvány,
- a tanúsítvány érvényességi idejének kezdetét (amely nem lehet a kibocsátási időpontnál korábbi) és az érvényesség végét (amely nem lehet az érvényesség kezdete időpontnál korábbi, illetve a maximálisan 1 éves érvényességi időtartam által meghatározott időpontnál későbbi); 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 Aláíró nevét,
- az Aláírónak külön jogszabályban, illetve a Szabályzatban, illetőleg az Általános Szerződési Feltételekben meghatározott speciális jellemzőit, a tanúsítvány szándékolt felhasználásától függően,
- más személy (szervezet) képviseletére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minőségét és a képviselt személy (szervezet) adatait,
- 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 egyedi,
- a kiadott tanúsítványokhoz tartozó kulcsok egyediek,
- a minősített tanúsítványok megfelelnek a ETSI TS 101 862-ben [8] meghatározott tanúsítványprofiloknak (ld. 7.1 alfejezet),
- 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, az ügyfélszolgálaton nyomtatott formában történő elhelyezésével) tájékoztatja a következőkről:

- a tanúsítványok felhasználásával kapcsolatos alapvető előnyök,

- a szolgáltatás igénybevételének feltételei,
- a szolgáltatási díj,
- az ügyfél 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 következményei,
- a tanúsítványok visszavonásának, felfüggesztésének lehetősége,
- a szolgáltatói nyilvános kulcs, valamint annak elérhetősége,
- a panaszok benyújtására, a jogviták rendezésére vonatkozó szabályok,
- az a tény, hogy létezik önkéntes minősítési rendszer.

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 tanúsítványtípus nem nyilvános használatra szolgál,
- ha tanúsítványtípus 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 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 ügyfél külön értesítést kap. A kész tanúsítvány a Tanúsítványtárba kerül, ahonnan Internetes felületen keresztül Internet böngésző szoftver segítségével letölthető (ld. még 2.6 alfejezet).

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

4.2.9 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.

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.

4.2.10 Kibocsátott tanúsítványok

4.2.10.1 A tanúsítvány kibocsátásának időpontja

A Szolgáltató az Internetcímén (ld. 1.4 alfejezet) elérhető elektronikus adatbázist, úgy nevezett Tanúsítványtárat üzemeltet, amelyben a Szolgáltató által kiadott tanúsítványok, a visszavont tanúsítványok listái, eljárási rendek, szerződési feltételek és más dokumentációk találhatók (ld. még 2.6.4 pont). A tanúsítvány kibocsátásának időpontja az az időpont, amikor a Szolgáltató az aláírt tanúsítványt elérhetővé teszi ebben az Internetcímén elérhető adatbázisában (ld. 1.4 alfejezet).

4.2.10.2 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 Aláíró illetve Érintett Fél felelőssége.

4.2.11 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.

A Szolgáltató nem alkalmaz kereszttanúsítványt.

4.3 Tanúsítványelfogadás

4.3.1 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 Aláíró belép a Szolgáltató Interneten elérhető adatbázisába (ld. 1.4 alfejezet) a tanúsítvány letöltése céljából, vagy egyéb módon letölti tanúsítványát. Ha ez nem történik meg, a magánkulcs és a tanúsítvány az értesítést követő 15. napon automatikusan elfogadottnak tekintendő.

4.3.2 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,
- a tanúsítványban szereplő minden adat a tudomásával és egyetértésével került a tanúsítványba,
- a tanúsítvány érvényességét befolyásoló tényekről 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) tanúsítvány alapján készül,
- minden egyes elektronikus aláírást, amely a tanúsítványban szereplő nyilvános kulcs párjával készült, a saját aláírásának ismeri el,
- jogosulatlan személy nem férhet hozzá magánkulcsához,
- ismeri az elektronikus aláírás megfelelő használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,
- tudomása van arról, hogy a minősített elektronikus aláírással ellátott dokumentumok 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 kiadására használni; hacsak erről külön írásbeli szerződésben a Szolgáltatóval meg nem egyezett,
- felhatalmazza a Szolgáltatót a tanúsítvány nyilvánosságra hozatalával, és saját vagy más nyilvános tanúsítványgyűjtő helyeken történő elhelyezésével.

4.4 A tanúsítványok használata

4.4.1 Alkalmazás

Az aláíró tanúsítványok elektronikus aláírások és ezzel üzenetek 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.

4.4.2 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 Aláíró nem körültekintően jár el, úgy az ebből származó kárért kizárólag ő a felelős.

4.4.3 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. A kulcsot idegen gépre átvinni védelem nélkül nem szabad. 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 Szabályzatban meghatározott visszavonási ideig (ld. 4.5.6 pont) még az Aláírót terheli az összes felelősség.

4.4.4 Érvényes elektronikus aláírás következményei

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

- a Hitelesítés-szolgáltató az Általános Szerződési Feltételek és a Szolgáltatási 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.

4.4.5 Eljárás az elektronikus aláírás ellenőrzésekor fellépő hibáknál

Nem érvényes elektronikus aláírás esetén, vagy ha az ellenőrzés nem a szabályzatok pontjainak megfelelően történt, az aláírás nem tekinthető valódinak és az elfogadásból eredő minden kár és kockázat az Érintett Felet terheli (ld. 2.1.3 és 2.2.3 pont).

4.5 Tanúsítvány felfüggesztése és visszavonása

4.5.1 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 4.5.10 pont).

A visszavont/felfüggesztett tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. A visszavont tanúsítványhoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni (ld. még 4.5.16 pont).

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 megfelelően az alany, illetve a másodlagos alany felelős a felmerülő károkért,
- a visszavonási/felfüggesztési kérelem megérkezésétől a legközelebb kibocsátandó Tanúsítvány Visszavonási Lista megjelenésének a jelen Szabályzat szerint tervezett időpontjáig az alany, illetve a másodlagos alany felelős a felmerülő károkért,
- amennyiben a jelen szabályzat szerint tervezett legközelebbi kibocsátás időpontjában a visszavont tanúsítványok listája nem kerül a Szolgáltató által kibocsátásra, a visszavont tanúsítványok listájának tényleges megjelenéséig a Szolgáltató felel az esetlegesen ezen eseményből fakadó károkért,
- az érvénytelen állapot tanúsítványtárban való megjelenése után az Érintett Fél felelős a felmerülő károkért.

4.5.2 A visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásához a következő körülmények vezetnek:

- végfelhasználói vagy szolgáltatói magánkulcs kompromittálódása,
- a tanúsítvány alanyainak 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,
- a HIF, bíróság vagy más hatóság erre vonatkozó jogerős határozata,
- a felhasználói szerződés megszűnése,
- a hitelesítési szolgáltatás megszűnése.

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

4.5.3 Visszavonás kérelmezése

A visszavonást az alábbi entitások kérelmezhetik:

Tanúsítványok	Visszavonást kérheti
Végfelhasználói tanúsítvány	Alany, (Másodlagos Alany), Szolgáltató, Felügyelet
Szolgáltatói tanúsítványok	Szolgáltató, Felügyelet

4.5.4 Visszavonási kérelemre vonatkozó eljárás

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

- személyesen ügyfélszolgálati időben a Szolgáltató székhelyén, a Központi Regisztrációs Egységnél,
- a Szolgáltatónak küldött e-mailben, 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,
- dátum, aláírás.

A visszavonási eljárás során a Szolgáltató Központi Regisztrációs Egysége ellenőrzi a visszavonási kérelemben szereplő adatokat. Ha az adatok helytelenek, az igénylő kiléte vagy a visszavonásra való jogosultság nem állapítható meg, akkor Szolgáltató a tanúsítvány visszavonását megtagadja. 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.

Helyes és hiteles kérelem esetén a Szolgáltató további mérlegelés nélkül intézkedik a tanúsítvány visszavonása érdekében: a visszavonási kérelmek azonnal végrehajtásra kerülnek, a visszavont tanúsítvány bekerül a következő alkalommal kibocsátott visszavonási listába.

Szolgáltató minden végrehajtott és visszautasított állapotváltoztatási kérelemről telefonon (regisztrációnál megadott számon) és e-mailben értesíti az alanyt (a tanúsítványban szereplő e-mail címen), illetve a másodlagos alanyt, valamint a visszavonás kérelmezőjét.

4.5.5 Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási lépések késedelem nélkül követik egymást. A visszavont tanúsítvány a visszavonás időpontját követő első CRL kiadás időpontjától kerül rá a CRL listára.

A visszavonási és felfüggesztési kérelmeket a Szolgáltató ügyfélszolgálati időben haladéktalanul végrehajtja, és a tanúsítványállapot-adatbázist késedelem nélkül frissíti, ha a kérelem feldolgozása befejeződött. Az ügyfélszolgálati időn kívül a Szolgáltatóhoz érkezett visszavonási és felfüggesztési kérelmekkel kapcsolatos humán beavatkozást igénylő műveletet a Szolgáltató a bejelentéstől számított legközelebbi ügyfélszolgálati napon teljesíti. Egy visszavonási, illetve felfüggesztési kérelem feldolgozása és a Tanúsítvány Visszavonási Listába a változás felvétele között eltelt idő „M” osztályú tanúsítványok esetén nem lépi túl a 24 órát.

4.5.6 Visszavonásra vonatkozó egyéb szabályok

A visszavonás, felfüggesztés 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 és infrastrukturális kulcsokhoz tartozó tanúsítványok visszavonása kettős ellenőrzés mellett történik.

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

4.5.7 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.

4.5.8 Felfüggesztés kérelmezése

A felfüggesztést ugyanazok kérelmezhetik, akik a visszavonást (ld. 4.5.3 pont), kiegészítve olyan harmadik felekkel, akik hitelt érdemlő módon bizonyítani tudják a visszavonáshoz vagy felfüggesztéshez vezető körülmények alapos gyanújának a fennállását.

4.5.9 Felfüggesztési kérelemre vonatkozó eljárás

A felfüggesztési kérelem a visszavonási kérelemhez hasonlóan nyújtható be Szolgáltatóhoz. Harmadik fél által történő beadás esetén Szolgáltató a rendelkezésére álló eszközökkel meggyőződik a személy kilétéről. A felfüggesztési kérelmet a visszavonási kérelemmel megegyező módon dolgozza fel Szolgáltató.

4.5.10 A felfüggesztés időtartamára vonatkozó korlátozások

Tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 5 naptári napig. Ezen belül a tanúsítvány visszavonásáról, illetve újbóli érvényesre állításáról Szolgáltatónak a lehető leghamarabb intézkednie kell. A felfüggesztett állapot kezdő időpontja a felfüggesztési kérelem elfogadása után jelen Szabályzat szerinti legközelebbi Tanúsítvány Visszavonási Lista (CRL) kibocsátásától számítandó. Ha ez idő alatt a visszavonáshoz vezető körülmények gyanúja cáfolatot nem nyer, Szolgáltató a tanúsítványt visszavonja.

4.5.10.1 Újraérvényesítés módja

Amennyiben a felfüggesztést az alany, illetve a másodlagos alany kérelmezte, ugyanő kérelmezheti a tanúsítvány újbóli érvénybe helyezését is ugyanolyan módon, ahogyan a felfüggesztést kérelmezte.

4.5.11 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 tartalmazza a tanúsítvány visszavonásának okát.
- A CRL ellenőrzése kötelező minden Érintett Fél részére az elektronikus aláírás ellenőrzési eljárásának részeként (ld. 2.1.3 pont). A CRL-en szereplő, azaz érvénytelen tanúsítvány elfogadásából keletkező bárminemű kár az Érintett Felet terheli.
- A Szolgáltató az egyes CRL-eket a kapcsolódó egyéb adatok megőrzési idejével megegyező ideig őrzi meg (ld. 4.9.2 pont).

4.5.11.1 A Tanúsítvány Visszavonási Lista kibocsátási gyakorisága

Szolgáltató a tanúsítványok érvényességének ellenőrzésére visszavonási listákat bocsát ki (CRL). 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 felfüggesztett tanúsítványok az újbóli érvényesítés hatására kerülhetnek ki a listából.

A visszavonási lista kibocsátása a Szolgáltató tanúsítványtárába történik. A kibocsátások minősített tanúsítvány esetén legalább 24 óránként követik egymást. Ezen időközönként CRL akkor is kibocsátásra kerül, ha a legutóbbi kibocsátás óta nem történt tanúsítvány visszavonás vagy felfüggesztés.

A visszavonási listák mindig tartalmazzák a következő lista kibocsátásnak idejét, melyet megelőzve is kibocsáthat Szolgáltató új listát.

4.5.11.2 A Tanúsítvány Visszavonási Lista ellenőrzési követelményei

A visszavonási lista ellenőrzése érintett felek részére kötelező a tanúsítványok elfogadását megelőzően. 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.

4.5.12 Valós idejű visszavonási állapot ellenőrzés elérhetősége

A Szolgáltató valós idejű visszavonási állapot-szolgáltatást nem nyújt.

4.5.13 Valós idejű visszavonás ellenőrzési követelmények

A Szolgáltató valós idejű visszavonási állapot-szolgáltatást nem nyújt.

4.5.14 A visszavonási információ közzétételének egyéb formái

A visszavonási hirdetmények csak a Szolgáltató tanúsítványtárán keresztül érhetők el, kivéve a Szolgáltató saját szolgáltatói tanúsítványának állapotváltozásáról egy országos terjesztésű napilapban közzétett hirdetést.

4.5.15 A visszavonási információ egyéb formáinak ellenőrzési követelményei

Nincs ilyen követelmény.

4.5.16 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.

4.6 Általános 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).

4.7 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.

4.8 A biztonsági naplózás folyamatai

Szolgáltató hitelesítési rendszere 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 Sza bályzatban megjelölt referencia időforráshoz (ld. 6.9.1 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.

4.8.1 A tárolt események típusai

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

A fő eseménytípus csoportok, amelyek naplózásra kerülnek:

- rendszertevékenységek (indítás, leállítás, verziófrissítés, újraindexelés, újrakulcsolás stb.),
- mentési tevékenységek (teljes mentés, különbségi mentés, mentés ellenőrzés stb.),
- CRL tevékenységek (kiadás, kombinált kiadás, visszavonás, felfüggesztés stb.),
- felhasználói események (tanúsítványkiadás, regisztráció, visszavonás, kulcsvisszaállítás 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.

A napló állományok ellenőrzése elkülönített szerepkör.

4.8.2 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.

4.8.3 A napló állomány megőrzési időtartama

A napló állományok keletkezésük helyén tárolódnak, illetve archiválásra kerülnek (ld. 4.9.4 pont), és a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg a velük kapcsolatban felmerült és bejelentett jogvita jogerős lezárásáig megőrződnek.

4.8.4 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.

4.8.5 A napló állomány mentési folyamatai

A naplóállományok rendszeresen mentésre kerülnek (ld. 4.9.4 pont) rejtjelezett és aláírt formában.

4.8.6 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.

4.8.7 Az eseményeket kiváltó alanyok értesítése

A naplóbejegyzéseket kiváltó személyeket, egységeket és alkalmazásokat Szolgáltató nem értesíti, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az eseményt kiváltásában közreműködőknek ilyen esetben kötelessége a Szolgáltatóval való együttműködés.

4.8.8 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.

4.9 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.

4.9.1 A tárolt események típusai

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

- a Szolgáltatóhoz benyújtott valamennyi papír alapú kérelem (tanúsítvány kibocsátás, megújítás, visszavonás, stb.),
- az igénylő személyes és szervezeti identitásának igazolására bemutatott valamennyi dokumentum fénymásolata,
- a Szolgáltató és az alany, illetve a másodlagos alany között megkötött valamennyi vonatkozó megállapodás (ideértve a tanúsítvány közzétételéhez történő hozzájárulást is).

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

4.9.2 Az archívum megőrzési időtartama

A Szolgáltató az archivált adatokat az [1] törvény 9. § (7) bekezdésében előírt határidőig (jelen Szabályzat hatálybalépésekor 10 év), az egyéb naplózott adatokat a keletkezésüktől, a Szabályzatot és annak módosításait pedig hatályon kívül helyezésétől számított tíz évig megőrzi. A Szolgáltató ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.

4.9.3 Az archívum védelme és hozzáférési szabályok

A Szolgáltató az archivált adatállományt 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 férnek hozzá. A Szolgáltató biztosítja, hogy az adatok az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

4.9.4 Az archívum mentési folyamatai

Az archiválás naponta 1 példányban történik szalagos egységre. Ezen kívül heti, havi és hosszú távú mentésekre kerül sor. A mentést hordozó médiát a Szolgáltató biztonságos környezetben tárolja.

4.9.5 A rekordok időbélyegzésére vonatkozó követelmények

Lásd a 4.8.1 pontot.

4.9.6 Az archívum gyűjtési rendszere

A Regisztrációs Pontokon keletkezett iratokat a Regisztrációs Egységek bizalmasan tárolják és őrzik. Az elektronikus másolati példányban létező iratok elektronikus üzenet formájában kerülnek a Szolgáltató központi adattárba.

4.9.7 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 2.6.3 és 2.6.4 pont szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és a hozzáférést naplózza.

4.9.8 Kulcsok archiválása

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.

4.9.9 Egyéb archiválási rendelkezések

Az archívumban esemény típus szerinti keresést lehet végrehajtani.

Az archiválásra vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat tartalmazza.

4.10 Kulcscsere

Szolgáltató még érvényes tanúsítvány kulcscserével történő megújítását nem támogatja, mert ez új tanúsítvány kibocsátásának minősül.

4.11 Helyreállítás kompromittálódás és katasztrófa esetén

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.

A következő pontokban e katasztrófa elhárítási terv irányelveit foglaljuk össze.

4.11.1 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 a 4.11.4 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.

4.11.2 Egy szolgáltatói egység nyilvános kulcsának visszavonása

A szolgáltatói nyilvános kulcsok visszavonásáról a Szolgáltató a 2.6.1 pontnak megfelelően értesítést tesz közzé.

4.11.3 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 2.6.1 ponttól függetlenül, de arra tekintettel), megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet.

4.11.4 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.

4.12 A Hitelesítés-szolgáltató leállítása

4.12.1 Szolgáltatás megszűntetése

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

- 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.
- A szolgáltatás megszűnése előtt 30 nappal értesítést tesz közzé Internetes oldalain (ld. 1.4 alfejezet), e-mail címmel rendelkező ügyfelei számára a szolgáltatás befejezéséről elektronikus levélben értesítőt küld.
- A Szolgáltató a tevékenység befejezését legalább 20 nappal megelőzően az általa kibocsátott, és még vissza nem vont tanúsítványokat visszavonja.
- A Szolgáltatóval szerződéses kapcsolatban álló, a tanúsítvány kibocsátásban résztvevő, összes vállalkozással, regisztrációs szervezettel korábban megkötött szerződés alapján fennálló kezelési jogokat, illetve felhatalmazást visszavonja.
- A regisztrációs információk, és az eseménynapló archívumok megőrzése érdekében, időbélyegzővel ellátott teljes körű mentést hajt végre.
- Saját magánkulcsait megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat visszavonja, és erről egy országos terjesztésű napilapban hirdetést tesz közzé.
- A Szolgáltató a tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is eleget tesz.
- 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.

4.12.2 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.

5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

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. 4.9 alfejezet). A mentéseket a Szolgáltató a 4.9.2 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 (ld. 4.11.4 pont).

A biztonsági szabályokra vonatkozó rendelkezéseket a Biztonsági Szabályzat tartalmazza.

5.1 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 az Szolgáltató által végzett kockázat elemzésben megállapított kockázatokkal.

5.1.1 Fizikai hozzáférés

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.

A terület pontos paramétereit, illetve a belépni jogosultak listáját a mindenkori belső operációs dokumentumok tartalmazzák. Az ott dolgozó bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és kísérettel léphetnek be. A belépések biometrikus azonosításra épülő beléptető rendszeren 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.

5.1.2 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.

5.1.3 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.

5.1.4 Légkondicionálás

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

5.1.5 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.

5.1.6 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.

5.1.7 Adathordozók tárolása

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

5.1.8 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 lásd a Biztonsági Szabályzatban). 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.

5.1.9 Fizikailag elkülönítetten őrzött mentési példányok

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

5.2 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.

5.2.1 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 kezelő személy.

A Szolgáltatóval munkaviszonyban álló, változó helyszínen dolgozó **biztonsági tisztviselő** általánosan (a hitelesítő egységekre, a regisztrációs egységre, valamint az összes regisztrációs pontra 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:

- folyamatosan üzemeltetik a regisztrációs pontokon működő számítógépes munkaállomásokat,
- időszakosan rendszermentéseket végeznek,
- naponta egyszer archiválják az előállított tanúsítványokat és visszavonási listákat,
- szükség esetén (a rendszermentések alapján) helyreállításokat hajtanak végre.

A Szolgáltató állományába tartozó **rendszervizsgáló**:

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

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.

5.2.2 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. 6.1.2 pont),
- a Szolgáltató későbbi saját kulcsgenerálása,
- a Szolgáltató magán aláíró kulcsának biztonsági mentése (klónozása) (ld. 6.2.2 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).

5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

A Szolgáltató valamennyi bizalmi munkakört betöltő munkatársának (biztonsági tisztviselő, rendszeradminisztrátor, rendszerüzemeltető, valamint rendszervizsgáló) a zárt körletbe való belépéskor az azonosítását és hitelesítését biometrikus azonosító rendszer végzi, amely a rendszerekhez való hozzáférésnél egyéb, rendszerenként különböző védelemmel egészül ki. Sikeres hitelesítés előtt a zárt körletbe való bejutás, illetve rendszerhozzáférés nem lehetséges, így egyetlen biztonság kritikus tevékenység sem végezhető.

5.3 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.

5.3.1 Személyi kontroll

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.

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.

5.3.2 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.

5.3.3 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

- a biztonsági tisztviselők,
- a rendszeradminisztrátorok,
- a rendszerüzemeltetők,
- regisztrációs adminisztrátorok

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.

5.3.4 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 egység biztonságpolitika megismerése, megértése, az ezen alapuló aktuális eljárások és követelmények megismerése és a későbbi helyes alkalmazása érdekében. További részletek a személyzeti politikában találhatók.

5.3.5 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.

5.3.6 Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között nem valósul meg.

5.3.7 A felhatalmazás nélküli tevékenységek büntető következményei

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

5.3.8 A szerződéses munkavállalókra vonatkozó követelmények

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

5.3.9 A személyzet számára biztosított dokumentációk

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

6 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 tanúsítvány és CRL aláíró magánkulcs,
- egyéb tanúsítvány és CRL aláíró magánkulcs,
- időbélyegző magánkulcs,
- infrastrukturális és kontrollkulcsok.

Szolgáltatói nyilvános kulcsok:

- a tanúsítvány és CRL aláíró magánkulcsok nyilvános párja,
- időbélyegző magánkulcsok nyilvános párja.

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.

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

		Végfelhasználói kulcspár	Szolgáltatói kulcspárok
Kulcsgenerálás és installáció	Kulcsgenerálás, tárolás	A kulcsgenerálást eszköz szolgáltatás esetén kizárólag a Szolgáltató végezheti. A kulcsgenerálást hitelesítés-szolgáltatás esetén kizárólag az alany végezheti Kulcstárolás kizárólag BALE-n megengedett.	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 végfelhasználók minimum 1024 bites RSA kulccsal rendelkeznek.	A Szolgáltató legalább 1024 bites RSA kulcsokat generál.
	Kulcs felhasználási célok	A végfelhasználó aláíró kulcspárt generál.	A Szolgáltató aláíró és titkosító kulcspárt generál a Hitelesítő Egységek számára.
Magánkulcs védelme	Magánkulcs több-személyes kontrollja	A Szolgáltató nem alkalmaz több-személyes kontrollt a magánkulcsok esetében.	A Szolgáltató kétszemélyes kontrollt alkalmaz a magánkulcsok esetében.

	Magánkulcs letét	Szolgáltató nem nyújt magánkulcs letéti szolgáltatást.	
	Magánkulcs mentése	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 és szolgáltatói nyilvános kulcsokat a Szolgáltató az elektronikus aláírásról szóló törvényben meghatározott ideig archív formában megőrzi (ld. 4.8.4. pont).	
	Kulcsok felhasználási ideje	A magánkulcs érvényességi ideje megegyezik a hozzá tartozó tanúsítvány érvényességi idejével. A nyilvános kulcs a kriptográfiai biztonságáig érvényes.	

A Szolgáltató valamennyi szolgáltatói kulcspárát saját maga generálja, egy 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 két személyes kontroll mellett történik oly módon, hogy a műveletben résztvevő felek a kriptográfiai hardver modulon lévő pint 0 állapotba állítják majd az eszközt rövid időre eltávolítják az azt meghajtó számítógépből.

6.1.2 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 140-1, Level 3 tanúsítvánnyal rendelkező kriptográfiai modulban kerülnek előállításra, tárolásra,
- minősített hitelesítés-szolgáltatásnál, ha a kulcspár előállítása az aláírás-létrehozó eszközön kívül történik, a kulcspárt előállító kriptográfiai eszköz tanúsítvánnyal igazoltan megfelel az alábbi szabványok, szabványjellegű dokumentumok legalább egyikének: a) FIPS 140-1, 3-as szint, b) CEN HSM – PP, c) CEN SSCD – PP,
- 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. 5.1.3 pont).

6.1.3 Alkalmazott eszközök

Aláíró eszközök	Hardver specifikáció	Szoftver specifikáció
M osztályú Hitelesítő Egység	ERACOM CSA 8000 FIPS 140-1 Level 3 HSM	ERACOM CSA 8000 driverek, PKCS11 interfész, NCA NetLock tanúsítványkiadó rendszer

6.1.4 Magánkulcs eljuttatása az alanyhoz

Mivel a Szolgáltató valamennyi kulcspárja helyben generálódik (ld. 6.1.2 pont), azokat nem kell sehová továbbítani.

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

6.1.5 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.

6.1.6 A szolgáltatói nyilvános kulcs közzététele

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

6.1.7 Kulcsméretek

Lásd 6.1.1 pont.

6.1.8 A nyilvános kulcs paraméterek generálása

A nyilvános kulcs paraméterek megfelelnek az előírásoknak (ld. Irányelv [2] melléklete), és előállításuk során a megfelelő szabványok, algoritmusok kerültek alkalmazásra.

6.1.9 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 modulokat az ezzel megbízott bizalmi munkakört betöltő munkatársak rendszeres időközönként tesztelik.

A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám-generálásukat.

6.2 A magánkulcsok védelme

6.2.1 Magánkulcs letétbe helyezése

A szolgáltatói és végfelhasználói magánkulcsot nem lehet letétbe helyeztetni.

6.2.2 Magánkulcs mentése

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

- a M hitelesítő egység aláíró magánkulcs.

A mentés során a magánkulcsot generáló kriptográfiai hardver modulból egy másik kriptográfiai hardver modulba másolódik át (duplikálódik, klónozódik) 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.

6.2.3 Magánkulcs archiválása

A Szolgáltató magánkulcsokat nem archivál.

6.3 A kulcspár gondozásának egyéb szempontjai

6.3.1 Egyéb kulcskezelési rendelkezések

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.

6.3.2 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).

6.3.3 A nyilvános és magánkulcsok használatának periódusa

Szolgáltatói tanúsítványok és a bennük foglalt nyilvános kulcsok magán párjai:

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

A végfelhasználói aláíró kulcsokhoz tartozó tanúsítványoknak és a bennük foglalt nyilvános kulcsok magán párjainak érvényességi ideje 1 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.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

A pontos szabályok az alany érdekében nem nyilvánosak.

6.4.2 Az aktivizáló adatok védelme

A pontos szabályok az alany érdekében nem nyilvánosak.

6.4.3 Az aktivizáló adatok egyéb szempontjai

A pontos szabályok az alany érdekében nem nyilvánosak.

6.5 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 a 4.6, a 4.8 és az 5.1 alfejezet, valamint a Biztonsági Szabályzat tartalmazza.

6.5.1 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).

6.5.2 Informatikai biztonsági osztályozás

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

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

Az ide vonatkozó rendelkezéseket a Szolgáltató belső használatú Biztonsági Szabályzata és Üzleti Folytonossági Terve tartalmazza.

6.6.2 Biztonságkezelési óvintézkedések

Az alkalmazott eljárásokat, módszereket független szakértő vizsgálta. A folyamatos, magas színvonalú biztonságos szolgáltatás fenntartására a Szolgáltató ISO 9001:2000-es minőségbiztosítási rendszert is alkalmaz, amelyet ugyancsak független külső és belső auditorok vizsgálnak.

6.6.3 Az életciklusra vonatkozó biztonság osztályozása

A szükséges biztonsági értékelést független auditor vizsgálta.

6.7 Hálózatbiztonsági óvintézkedések

A Szolgáltató saját hálózatát a nyílt hálózatokról tűzfal szerverekkel választja le. Az ide vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat és az Üzleti Folytonossági 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).

6.8 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.

6.9 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 CRL- és tanúsítvány kibocsátás, valamint időbélyegzés-szolgáltatást nem végez.

6.9.1 Időforrás megnevezése

A Szolgáltató két független UTC-forrást alkalmaz az időforrás üzembiztonsága érdekében:

- időforrás 1: GPS műholdas navigációs rendszer által szolgáltatott UTC világidő,
- időforrás 2: németországi referenciaidő (UTC).

6.9.2 Időforrás pontossága

A megbízható rendszerek minden időponttal kapcsolatos szolgáltatáshoz használt óráját a Szolgáltató szinkronizálja az ún. koordinált, egységes időforrással (Co-ordinated Universal Time – UTC) 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.

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.

6.9.3 Alkalmazott eszközök

Időszinkronizációs eszközök	Időszinkronizációs forrás
HOPF 6039 GPS típusú vevő	GPS műholdas navigációs rendszer által szolgáltatott UTC világidő
HOPF 6039 DCF típusú vevő	németországi referenciaidő

7 Tanúsítvány, - visszavonási lista és időbélyeg profilok

7.1 Tanúsítványprofilok

A Szolgáltató a [12] ajánlás 2. verziójának megfelelő tanúsítványokat bocsát ki. A Szolgáltató által kibocsátott tanúsítványok alapmezői a következők:

7.1.1 Személyes tanúsítvány profilja

Mező	Tartalom	Kritikus
Common Name	Magánszemély neve	-
Organization	Üres	-
Organization Unit	Üres	-
Country	HU	-
Locality	Lakcím szerinti város	-
State	Megye vagy üres	-
E-mail	Magánszemély e-mail címe	-
Version	V3	-
Serial number	Egyedi sorozatszám érték	-
Signature	Kibocsátó elektronikus aláírása	-
Issuer	CN= NetLock Minositett (Class Q) Tanusitvanykiado/ O= NetLock Halozatbiztonsagi Kft./ OU= Tanusitvanykiadok/ C= HU/ L= Budapest/ ST= / E= info@netlock.hu	-
Validity	Érvényesség kezdete és vége	-
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa	-
Basic Constraints	cA = FALSE	Igen
KeyUsage	nonRepudiation	Igen
Netscape Comment	FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Szolgaltatasi Szabalyzataban leirt eljarasok alapjan keszult. A kibocsatott tanusitvanyhoz tartozo magankulcs a jogszabalyi rendelkezeseknek megfelelo Biztonsagos Alairas Letrehozo Eszkozben (BALE) keszult. A minositett elektronikus alairas joghatas ervenyesulesenek, valamint elfogadasanak feltetele a Minositett Szolgaltatasi Szabalyzatban, az Altalanos Szerzodesi Feltetelekben eloirt ellenorzesi eljaras megtetele. A dokumentumok megtalalhatok a https://www.netlock.hu/docs/ cimen vagy kerhetok az info@netlock.net e-mail cimen. WARNING! This certificate has been issued as a qualified certificate. The corresponding private key has been generated on a Secure Signature Creation Device (SSCD). The issuance and the use of this certificate are subject to the NetLock Qualified CPS available at https://www.netlock.hudocs/ or by e-mail at info@netlock.net.	Nem
Netscape Certificate Type (opcionális)	SSL client, S/MIME client	Nem
QcCompliance	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány a 2001 évi XXXV. Törvény és végrehajtási rendeletei alapján minősített tanúsítvány.	Igen

CertificatePolicies (opcionális)	RFC 2459 [9] szerinti szabályzat azonosító	Igen
QcLimitValue	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány a 2001 évi XXXV. Törvény és végrehajtási rendeletei alapján (MonetaryValue::= érték * $10^{érték}$ HUF) értékhatárig használható.	Igen
QcRetentionPeriod	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány hoz kapcsolódó dokumentációt a 2001 évi XXXV. Törvény és végrehajtási rendeletei, továbbá belső szabályzatainak rendelkezései alapján, a tanúsítvány lejártát követő (QcEuRetentionPeriod::= Integer) évig őrzi meg. A Szolgáltató a dokumentációt a megőrzési időtartam letelte előtt meginduló jogi eljárás eseten az eljárás lezárását követően 10 évig őrzi meg.	Igen

7.1.2 Munkatársi tanúsítvány profilja

Mező	Tartalom	Kritikus
Common Name	Munkatárs neve	-
Organization	Szervezet, azaz a másodlagos alany neve	-
Organization Unit	Szervezeti egység neve	-
Country	HU	-
Locality	Székhely szerinti város	-
State	Megye vagy üres	-
E-mail	Munkatárs e-mail címe	-
Version	V3	-
Serial number	Egyedi sorozatszám érték	-
Signature	Kibocsátó elektronikus aláírása	-
Issuer	CN= NetLock Minositett (Class Q) Tanusitvanykiado/ O= NetLock Halozatbiztonsagi Kft./ OU= Tanusitvanykiadok/ C= HU/ L= Budapest/ ST= / E= info@netlock.hu	-
Validity	Érvényesség kezdete és vége	-
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa	-
Basic Constraints	cA = FALSE	Igen
KeyUsage	nonRepudiation	Igen
Netscape Comment	FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Szolgaltatasi Szabalyzataban leirt eljarasok alapjan keszult. A kibocsatott tanusitvanyhoz tartozo magankulcs a jogszabalyi rendelkezeseknek megfelelo Biztonsagos Alairas Letrehozo Eszkozben (BALE) keszult. A minositett elektronikus alairas joghatas ervenyesulesenek, valamint elfogadasanak feltetele a Minositett Szolgaltatasi Szabalyzatban, az Altalanos Szerzodesi Feltetelekben eloirt ellenorzesi eljaras megtetele. A dokumentumok megtalalhatok a https://www.netlock.hu/docs/ cimen vagy kerhetok az info@netlock.net e-mail cimen. WARNING! This certificate has been issued as a qualified certificate. The corresponding private key has been generated on a Secure Signature Creation Device (SSCD). The issuance and the use of this certificate are subject to the NetLock Qualified CPS available at https://www.netlock.hudocs/ or by e-mail at info@netlock.net.	Nem
Netscape Certificate Type (opcionális)	SSL client, S/MIME client	Nem

QcCompliance	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány a 2001 évi XXXV. Törvény és végrehajtási rendeletei alapján minősített tanúsítvány.	Igen
CertificatePolicies (opcionális)	RFC 2459 [9] szerinti szabályzat azonosító	Igen
QcLimitValue	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány a 2001 évi XXXV. Törvény és végrehajtási rendeletei alapján (MonetaryValue::= (érték) * $10^{\text{érték}}$ HUF) értékhatárig használható.	Igen
QcRetentionPeriod	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány hoz kapcsolódó dokumentációt a 2001 évi XXXV. Törvény és végrehajtási rendeletei, továbbá belső szabályzatainak rendelkezései alapján, a tanúsítvány lejártát követő (QcEuRetentionPeriod::= Integer) évig őrzi meg. A Szolgáltató a dokumentációt a megőrzési időtartam letelte előtt meginduló jogi eljárás eseten az eljárás lezárását követően 10 évig őrzi meg.	Igen

7.1.3 Szolgáltatói (időbélyegző) tanúsítvány profilja

Mező	Tartalom	Kritikus
Common Name	NetLock Minositett Idopecset Szolgaltato	-
Organization	NetLock Halozatbiztonsagi Kft.	-
Organization Unit	Idopecset Szolgaltatok	-
Country	HU	-
Locality	Budapest	-
State	-	-
E-mail	-	-
Version	V3	-
Serial number	- (csak a minősítés megtörténte után értelmezhető)	-
Signature	Kibocsátó elektronikus aláírása	-
Issuer	CN=NetLock Minositett (Class Q) Tanusitvanykiado/ O=NetLock Halozatbiztonsagi Kft./ OU=Tanusitvanykiadok/ C=HU/ L=Budapest/ ST=/ E=info@netlock.hu	-
Validity	- (csak a minősítés megtörténte után értelmezhető)	-
Public Key	Időbélyegző nyilvános kulcsa	-
Basic Constraints	cA = FALSE	Igen
KeyUsage EnhancedKeyUsage	nonRepudiation timeStamping	Igen Igen
QcCompliance	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány a 2001 évi XXXV. Törvény és végrehajtási rendeletei alapján minősített tanúsítvány.	Igen
QcLimitValue	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány a 2001 évi XXXV. Törvény és végrehajtási rendeletei alapján (MonetaryValue::= (érték) * $10^{\text{érték}}$ HUF) értékhatárig használható.	Igen
QcRetentionPeriod	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány hoz kapcsolódó dokumentációt a 2001 évi XXXV. Törvény és végrehajtási rendeletei, továbbá belső szabályzatainak rendelkezései alapján, a tanúsítvány lejártát követő (QcEuRetentionPeriod::= Integer) évig őrzi meg. A Szolgáltató a dokumentációt a megőrzési időtartam letelte előtt meginduló jogi eljárás eseten az eljárás lezárását követően 10 évig őrzi meg.	Igen

7.1.4 Szolgáltatói (tanúsítvány- és CRL-aláíró) tanúsítvány profilja

Mező	Tartalom	Kritikus
Common Name	NetLock Minositett (Class Q) Tanusitvanykiado	-
Organization	NetLock Halozatbiztonsagi Kft.	-
Organization Unit	Tanusitvanykiado	-
Country	HU	-
Locality	Budapest	-
State	Megye vagy üres	-
E-mail	Info@netlock.hu	-
Version	V3	-
Serial number	- (csak a minősítés megtörténte után értelmezhető)	-
Signature	Kibocsátó elektronikus aláírása	-
Issuer	CN= NetLock Minositett (Class Q) Tanusitvanykiado/ O= NetLock Halozatbiztonsagi Kft./ OU= Tanusitvanykiadok/ C= HU/ L= Budapest/ ST= / E= info@netlock.hu	-
Validity	- (csak a minősítés megtörténte után értelmezhető)	-
Public Key	Szolgáltató nyilvános kulcsa	-
Basic Constraints	cA = TRUE, Path Length = 4	Igen
KeyUsage	Certificate Signing, Off-line CRL Signing, CRL Signing	Igen
Netscape Comment	FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Szolgaltatasi Szabalyzataban leirt eljarasok alapjan keszult. A kibocsatott tanusitvanyhoz tartozo magankulcs a jogszabalyi rendelkezeseknek megfelelo Biztonsagos Alairas Letrehozo Eszkozben (BALE) keszult. A minositett elektronikus alairas joghatas ervenyesulesenek, valamint elfogadasanak feltetele a Minositett Szolgaltatasi Szabalyzatban, az Altalanos Szerzodesi Feltetelekben eloirt ellenorzesi eljaras megtetele. A dokumentumok megtalalhatok a https://www.netlock.hu/docs/ cimen vagy kerhetok az info@netlock.net e-mail cimen. WARNING! This certificate has been issued as a qualified certificate. The corresponding private key has been generated on a Secure Signature Creation Device (SSCD). The issuance and the use of this certificate are subject to the NetLock Qualified CPS available at https://www.netlock.hudocs/ or by e-mail at info@netlock.net.	Nem
Netscape Certificate Type (opcionális)	SSL CA, S/MIME CA, ObjectSigning CA	Nem
QcCompliance	A Szolgáltató jelen nyilatkozatában kijelenti, hogy a jelen tanúsítvány a 2001 évi XXXV. Törvény és végrehajtási rendeletei alapján minősített tanúsítvány.	Igen

7.2 Tanúsítvány visszavonási lista profil

A Szolgáltató a [12] ajánlás 2. verziójának megfelelő visszavonási listákat bocsát ki.

7.2.1 CRL kiterjesztések

A Szolgáltató által használt visszavonás bejegyzési kiterjesztések a következők:

Mező	Tartalom	Kritikus
ReasonCode	A visszavonás oka	Nem
Instruction	A felfüggesztett tanúsítvány kezelése	Nem
CRL number	A visszavonási lista egyesével növekvő sorozatszáma	Nem

7.3 Időbélyeg-profil

A NetLock Kft. által nyújtandó időbélyegzés szolgáltatás az RFC3161-es szabvány [16], az ETSI TS 101 [17] technikai leírás és a Irányelv [2] ajánlásainak figyelembevételével működik. A szolgáltatás paraméterei és a fenti szabványok ajánlásai a következők:

Mezők, tulajdonságok	**Tartalom, értelmezés**
Verzió	v1
Időbélyeg kérelemben engedélyezett hash algoritmus	MD5, SHA-1, RIPEMD160
Időbélyeg kérelemben megnevezhető szabályzati azonosító (OID)	Üresen hagyható vagy a Minősített Szolgáltatási Szabályzat azonosítója
Időbélyeg kérelemben szereplő véletlen szám (nonce) hossza	64 bit
Időbélyeg kérelemben kérhető-e a szolgáltató tanúsítványa (certReq)	Igen
"Extension" mező értelmezése	Nem használt
"Accuracy" mező értelmezése	Nem használt
"StatusString" mező értelmezése	Nem használt
"Ordering" mező értelmezése	Szolgáltató nem garantálja
"FailInfo" mező értelmezése	Az időbélyeg válasz tartalmazza
Időbélyeg válaszban szereplő szabályzati azonosító (OID)	Minősített Szolgáltatási Szabályzat azonosítója
Az időbélyeg válasznál használt hash algoritmus	SHA1 vagy RIPEMD160
Az időbélyeg válasznál használt aláíró algoritmus	RSA
Az időbélyeg válasz időfelbontása (genTime)	1 másodperc
Időbélyegző szolgáltatás "UTC max offset" értéke	0,1 másodperc
Támogatott elérési protokoll	HTTP, HTTPS
"Store and forward protocol" alkalmazása	Nem támogatott
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.

8 Leírás adminisztráció

8.1 Leírás változtatási eljárások

8.1.1 Szabályzat változtatási eljárások

A Szolgáltatón belül Szabályzatért Felelős 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 tanúsítványtípus meghatározott követelményeknek való megfelelőségét:
- tartalmi megfelelés a [7] MTT tanúsítványtípusokkal szemben támasztott minimális követelményeknek,
- formai megfelelés a [10] szabványnak.

A tanúsítványtípus elfogadására vagy esetlegesen a HIF által már nyilvántartásba vett tanúsítványtípusok közül történő kiválasztására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd egyetértés esetén a HIF nyilvántartásba veszi a Szolgáltató által jóváhagyott és bejelentett tanúsítványtípust.

A Szolgáltató jóváhagyás előtt megvizsgálja a Szabályzatot a szolgáltatási szabályzat megfelelőség szempontjából:
- a Szabályzat tartalmilag és formailag megfelel a tanúsítványtípusnak.

A Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd bejelentés után a Szabályzat megfelelőségét a HIF is megvizsgálja és értékeli (jóváhagyja vagy módosíttatja) a Szolgáltató minősítési eljárása során.

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.

8.1.2 A Szabályzatért Felelős Egység összetétele

A Szabályzatért Felelős Egység a következő összetételű munkacsoportként működik:

- Szabályzat Vezető: a Szabályzatért Felelős Egység vezetője, feladata az Egység munkájának koordinálása, illetve határozatainak jóváhagyása.
- Szabályzat Adminisztrátor: a Szabályzatért Felelős Egység által felügyelt szabályzatokat alkalmazó Közösség felől a szabályzatok módosítása tekintetében érkező igények feldolgozására,

illetve a szabályzatok módosításának kidolgozására és javaslat formában történő előterjesztésére kijelölt személy. Az adminisztrátor hatásköre és felelőssége továbbá a minősített tanúsítványtípusok specifikálása, jóváhagyatása és karbantartása.

8.1.3 A Szabályzatért Felelős Egység működése

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

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

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

8.1.4 Értesítés nélkül változtatható elemek

Szolgáltató fenntartja a jogot, hogy a Szabályzat nem lényegi elemeit előzetes értesítés és bejelentés nélkül változtassa. Ilyenek lehetnek a helyesírási hibák, formai változtatások, különböző kontaktadatok (Internetcímek, telefonszámok), és egyéb olyan elemek, melyek a tanúsítványok biztonsági szintjét, felhasználhatóságát a legkisebb mértékben sem módosítják.

8.1.5 Értesítéssel változtatható elemek

Minden, a tanúsítványok biztonsági szintjét, felhasználhatóságát módosító változtatás értesítésköteles.

8.1.6 Szabályzati objektumazonosítót vagy mutatót változtató módosítások

Minden jelentős 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 Internetcímen teszi közzé, így csak az újonnan kibocsátott tanúsítványok mutatói fognak rá hivatkozni, amennyiben a tanúsítványban van ilyen mutató.

8.2 Közzétételi és tájékoztatási elvek

8.2.1 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).

8.2.2 A Szabályzat közzététele

Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 45 nappal közzéteszi Internetes oldalán és a hatályba lépést megelőző 30 nappal pedig megküldi a HIF részére. A Szolgáltató alkalmanként ezt megelőzően is tájékoztathatja a Közösséget a tervezett változtatásairól. A jelen szabályzattal kapcsolatos közzéteendőket a 8.1.5 pont határozza meg.

8.2.3 Észrevételek kezelése

A közzétett új szabályzattal kapcsolatos észrevételeket Szolgáltató a hatályba lépést megelőző 35. napig fogadja a info@netlock.hu címen. A Szabályzat észrevételekkel módosított változatát Szolgáltató a hatályba lépést megelőző 30. nap zárja le és teszi ismételten közzé.

8.2.4 Panaszkezelési szabályok

8.2.4.1 Panaszok benyújtásának helye

A Szolgáltató (beleértve a regisztrációs egységeket is) tevékenységével kapcsolatos kérdések, kifogások és panaszok benyújtásának helye a Szolgáltató ügyfélszolgálati irodája (ld. 1.4 alfejezet).

8.2.4.2 Panaszok benyújtásának módja

A panaszokat a Szolgáltató levélben, e-mailben a info@netlock.hu címen, faxon, telefonon és személyesen fogadja (ld. 1.4 alfejezet).

8.2.4.3 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.

8.2.4.4 Illetékes fogyasztóvédelmi felügyelőség

Budapest Főváros Közigazgatási Hivatal Fogyasztóvédelmi Felügyelőség, 1088 Budapest, József krt. 6. Levélcím: 1364 Budapest, Pf. 234., telefon: (1) 459-4918, telefax: (1) 459-4870.

8.3 Szolgáltatási Szabályzat jóváhagyási eljárások

Ld. 8.1 pont