Titkosító, authentikációs és DV SSL tanúsítvány kibocsátására vonatkozó Szolgáltatási Szabályzat

NETLOCK Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Azonosító szám (OID):	**1.3.6.1.4.1.3555.1.49.20160728**
Jóváhagyás időpontja:	**2016.07.28.**
Hatály kezdőnapja:	**2016.08.02.**
Oldalak száma:	**102,** azaz százkettő
Készítette:	**Varga Viktor,** chief architect
Ellenőrizte:	**dr. Barabás Anett,** hatósági ügyintéző, belső ellenőr
Jóváhagyta:	**Dr. Szűcs Katalin,** cégvezető

OID	Változás leírása	Készítő	Ellenőrző
1.3.6.1.4.1.3555.1.49.20151014	A korábbi DV SSL és általános fokozott tanúsítvány kiadást szabályozó szabályzatok helyett készült egyesített szabályzat. Első változat	NETLOCK Szabályzat Elfogadó Egység (SzEE)	NETLOCK Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.49.20160728	eIDAS szerinti változásoknak megfelelő pontosítások. A szabályzat a Titkosító, authentikációs és DV SSL tanúsítványra vonatkozó szabályokat tartalmazza.	NETLOCK Szabályzat Elfogadó Egység (SzEE)	NETLOCK Szabályzat Elfogadó Egység (SzEE)

1.1 Tartalom

1 Bevezetés

1.1 Áttekintés

Jelen dokumentum a NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaságnak (továbbiakban Szolgáltató) a titkosító, authentikációs és DV SSL tanúsítványokra vonatkozó tanúsítványkiadási és ehhez kapcsolódó szolgáltatásaira vonatkozó gyakorlatát tartalmazó Szolgáltatási Szabályzata (a továbbiakban: Szolgáltatási Szabályzat vagy Szabályzat).

Jelen Szabályzat a részletes eljárási és működési szabályok ismertetése mellett ajánlásokat is megfogalmaz a jelen Szabályzat alapján kibocsátott tanúsítványok kapcsán az Érintett Felek számára.

Szolgáltató jelen Szabályzat alapján az alábbi tanúsítványokat bocsátja ki:

1. Eszközön és szoftveresen (nem eszközön) kibocsátott kliens oldali authentikációs tanúsítvány „B” és „C” hitelesítési osztályban
    a. Személyes authentikációs
    b. Munkatársi authentikációs
    c. Ügyvédi authentikációs
    d. Szervezeti authentikációs
2. Eszközön és szoftveresen (nem eszközön) kibocsátott titkosító tanúsítványok „B” és „C” hitelesítési osztályban
    a. Személyes titkosító
    b. Munkatársi titkosító
    c. Ügyvédi titkosító
    d. Szervezeti titkosító
3. DV SSL tanúsítvány

Arra vonatkozóan, hogy az adott hitelesítési osztályra vonatkozó tanúsítványok aktuálisan igényelhetőek-e, a Szolgáltató a weboldalán tesz közzé tájékoztatást.

1.1.1 A Szabványok és előírások

A Szolgáltatási Szabályzat a *NETLOCK hitelesítési rend nem minősített tanúsítványokra* (röviden: Hitelesítési rend) dokumentum szerkezetét követve az RFC 3647 [12.] szabvány alapján készült, az abban foglalt elvárásoknak való megfelelés módját ismerteti.

A Szabályzat és felhasználja az ETSI 102 042 [14.], az ETSI EN 319 401 [16.], ETSI EN 319 411 [17.], ETSI EN 319 412 [18.]-[21.], valamint az x.509 [11.] szabvány ajánlásait, valamint megfelel a CAB Forum Baseline Requirements Guide aktuális változata által előírtaknak.

A Szolgáltató által használt és alkalmazott jogszabályok, szabványok és előírások a 9.15 pontban kerültek részletezésre.

1.1.2 A Szolgáltató

A jelen Szabályzatban Szolgáltatónak nevezett entitás a NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság.

A Szolgáltató adatai:

Név:	**NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság**
Rövidített név:	NETLOCK Kft.

Név:	**NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság**
Székhely:	1101 Budapest, Expo tér 5-7.
Postázási cím:	1439 Budapest, Pf. 663
Cégjegyzékszám:	01-09-563961
Adószám:	12201521-2-42
Telefonszám:	(1) 437-6655
Fax:	(1) 700-2828
Weboldal:	netlock.hu
E-mail:	info@netlock.hu
Ügyfélfogadás/Nyitvatartás	A Szolgáltató honlapján feltüntetett helyen és időintervallumban

Önkéntes akkreditáció, egyéb minősítések:

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

1.2 A dokumentum neve és azonosítás

Lásd a dokumentum fedlapját.

1.2.1 Hitelesítési Rendek

A Szolgáltató a Hitelesítési Rend 1.2.1 fejezetében meghatározott OID azonosítókat, mint szabványos hitelesítési rend azonosítót, azonosítókat tünteti fel a végfelhasználói tanúsítványok CP (Certificate Policy) mezőjében.

1.2.2 Dokumentum revíziók

Lásd a 2. oldalon kezdődő Revíziók pontban foglaltakat.

1.3 A PKI szereplők

A kibocsátott tanúsítványok alkalmazó közössége a Szolgáltató, a vele szerződéses kapcsolatban álló regisztrációs és egyéb közreműködő szervezetek, a tanúsítványok Igénylői, Végfelhasználói, az Előfizetők és az Érintett Felek.

1.3.1 A Szolgáltató és a hitelesítő egység

A Hitelesítő Egység a Szolgáltató tanúsítványokat kibocsátó egysége. Szolgáltató az alábbi Hitelesítő Egységeket használja:

- a végfelhasználói tanúsítványokat hitelesítő Köztes Hitelesítő Egység, valamint
- legfelső szintű Gyökér Hitelesítő Egység

amelyek hierarchiába szervezetten működnek. A Szolgáltató olyan, Alárendelt Elektronikus Aláírással Kapcsolatos Szolgáltatást is hitelesíthet, amely során a szolgáltató entitás a saját nevében, de oly módon nyújt tanúsítványkibocsátási vagy időbélyegzési szolgáltatást, hogy arra a Szolgáltató jelentős befolyással bír. Az Alárendelt Elektronikus Kapcsolatos Szolgáltatásról a Szolgáltató weboldalán tesz közzé tájékoztatást.

1.3.2 Regisztrációs Egység

A Szolgáltató Központi Regisztrációs Szervezetet, Mobil Regisztrációs Munkatársakat, Kihelyezett Regisztrációs Szervezetet, valamint Regisztrációs- és Kézbesítési Megbízottakat alkalmaz, amelyek feladata a kezdeti regisztráció és a tanúsítvány kibocsátásával kapcsolatos egyéb tevékenységekben való részvétel.

Alapesetben a Központi Regisztrációs Egység feladata a tanúsítványban szereplő Alany(ok) és – amennyiben értelmezett - az Igénylő kezdeti azonosítása (okmányok begyűjtése), adatainak ellenőrzése – amennyiben lehetséges – közhiteles nyilvántartásban, kibocsátás során elektronikus kérelem-feldolgozási tevékenység, eljárási lépések koordinálása, dokumentálás, s további tanúsítvány kezelési feladatok, többek között az Ügyfelekkel való kapcsolattartás. Egyes esetekben a kezdeti azonosításhoz szükséges okmányok begyűjtését a Központi Regisztrációs egység felügyelete és irányítása alatt álló Mobil Regisztrációs Munkatársak, valamint a Kihelyezett Regisztrációs Egység munkatársai végzik. Az ügyfélszolgálati teendőket, valamint az Ügyfelekkel való elsődleges kapcsolattartást a Szolgáltató külön erre a feladatra alkalmazott vevőszolgálati (ügyfélszolgálati) munkatársai végzik. Az ügyfélszolgálati munkatársak a Központi Regisztrációs Egységen belül alkotnak önálló csoportot, elérhetőségeiket Szolgáltató a weboldalán teszi közzé.

A fentieken túl a Központi Regisztrációs Egység a regisztrációs eljárás egészének helyességét és szabályzatoknak való megfelelését ellenőrzi. A Központi Regisztrációs Egység munkatársainak felelőssége a tanúsítvánnyal kapcsolatos végső döntések meghozatala és a tanúsítvány kibocsátása is. A Központi Regisztrációs Egységen belül a Szolgáltató megkülönböztet regisztrációs- és tanúsítványkibocsátó munkakört.

A Szolgáltatási Szerződés aláírására (részletesen lásd 3.2 pont) és/vagy az eszközátadásra az ügyfél választása alapján az alábbiak valamelyike szerint kerül sor:

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

Amennyiben az Ügyfél rendelkezik aláíró vagy bélyegző tanúsítvánnyal, lehetőség van arra, hogy a Szolgáltatási Szerződést az ügyfél a 4.2.1 pont szerinti elektronikus aláírással vagy bélyegzővel ellátva jutassa el a Szolgáltatónak.

A regisztrációs munkatársak, valamint a Regisztrációs és Kézbesítési Megbízottak a tanúsítványkibocsátás során, személyes megjelenés mellett felhasználói adatellenőrzést végeznek, amely tevékenységüket a mindenkor hatályos jogszabályi követelményeknek - így különösen a vonatkozó törvénynek 101[6.] - megfelelően végzik. Az ügyfél választása szerint ők végzik az eszközátadást is, amennyiben az ügyfél nem jelent meg érte a Központi Regisztrációs Egység előtt.

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

1.3.3 Előfizető, Végfelhasználó és Igénylő

1.3.3.1 Előfizető

Azon szerződéses partner, aki a szolgáltatási díjak fizetését vállalja. Az Előfizetőre vonatkozó jogok és kötelezettségek a Szolgáltató által közzétett mindenkor hatályos ÁSZF-ben [8.] elkülönülten is megjelennek. Az Előfizető

- lehet a tanúsítvány Alanyaként megjelölt természetes vagy jogi személy/egyéb szervezet;
- megegyezhet az Igénylővel;
- megegyezhet a Végfelhasználóval;
- és megegyezhet Ügyféllel is.

1.3.3.2 Végfelhasználó

Az a természetes személy, aki a tanúsítványban szereplő nyilvános kulcs magánkulcs párja felett rendelkezik (kizárólagosan használja vagy a használatáért felelős).

1.3.3.3 Igénylő

A tanúsítvány igénylésében, állapotváltoztatásában, megújításában stb. eljáró, egyes esetekben a Szolgáltatói Szerződést is aláíró természetes személy, aki lehet:

- a tanúsítvány Alanyaként megjelölt természetes személy;
- a tanúsítvány Alanyaként megjelölt jogi személy/egyéb szervezet képviselője vagy meghatalmazottja;
- a tanúsítvány Alanyaként megjelölt domain név vagy trademark természetes személy tulajdonosa, illetve jogi személy/egyéb szervezet tulajdonos esetén annak képviselője vagy meghatalmazottja, illetve a domain név fölött kontrollal rendelkező személy.

1.3.3.4 Ügyfél

Az Ügyfél a Szolgáltatóval szerződést kötő személy. Ügyfél lehet a tanúsítványban Alanyként megjelölt természetes vagy jogi személy/egyéb szervezet, illetve a tanúsítvány Igénylője vagy Előfizetője.

1.3.3.5 Érintett Fél

Azon természetes vagy jogi személy, aki/amely valamely jelen Szabályzatban meghatározott szolgáltatást igénybe veszi. A szolgáltatás igénybe vétele különösen, de nem kizárólagosan az alábbiakat jelenti:

- az igényelt tanúsítvány hitelesítése céljából a Szolgáltató által kibocsátott tanúsítványhoz fordul;
- a nem minősített authentikációs, illetve titkosító tanúsítvány érvényességének ellenőrzéséhez a Szolgáltató által karbantartott nyilvántartásokat és szabályzatokat ellenőrzi.

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

1.4 Tanúsítványok alkalmazhatósága

1.4.1 Megfelelő tanúsítványfelhasználás

A Szolgáltató által az LCP [22.], NCP [23.] és NCP+ [24.] hitelesítési rendek alapján kibocsátott végfelhasználói tanúsítványok az Extended Key Usage mező értékétől függően (clientAuth) autentikáció ellenőrzésére, továbbá a Key Usage mező értékétől függően (keyEncipherment, digitalSignature) titkosításra és autentikáció ellenőrzésére. Az DVCP [25.] hitelesítési rend megfelelő végfelhasználói tanúsítványok webszerverek azonosítására használhatók.

A Szolgáltató által kibocsátott szolgáltatói tanúsítványok a végfelhasználói és köztes szolgáltatói tanúsítványok ellenőrzésére használhatók fel.

A tanúsítványokhoz tartozó kulcsok felhasználása tekintetében lásd a 6.1.7. A kulcshasználat célja fejezetet.

Az egyes tanúsítványfajtáknak megfelelő konkrét korlátozásokat lásd még a tanúsítványfajtáknál, illetve a tanúsítványfajtákhoz tartozó profiloknál (lásd 7 fejezet).

1.4.2 Tiltott tanúsítványfelhasználás

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

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

1.5 Szabályzat adminisztráció

A Szolgáltató szabályzatainak karbantartását a Szabályzat Elfogadó Egység végzi. A szabályzatokkal és szerződésekkel kapcsolatos kérdésekkel és észrevételekkel a Regisztrációs Egységek, a Szolgáltató ügyfélszolgálata, vagy közvetlenül a Szabályzat Elfogadó Egység kereshető meg az info@netlock.hu e-mail címen (ld. még 9.12 pont).

1.6 Fogalmak és rövidítések

1.6.1 Fogalmak

- **Alany:** lásd Tanúsítvány alany
- **AIA:CAI (Authority Information Access:Certificate Authority Issuers):** Az adott tanúsítvány kiadói tanúsítványára vonatkozó elérhetőséget (URL) tartalmazó tanúsítványmező.
- **Állapotváltozás:** Az az eljárás/művelet, amelynek eredményeképpen a tanúsítvány állapota (érvényes, felfüggesztett) megváltozik és új értéket vesz fel (érvényes, felfüggesztett, visszavont).
- **Átvevő:** A végfelhasználó valamely kulcsát vagy eszközét (pl. Ügyféleszköz) Szolgáltatótól (személyesen, hagyományos vagy elektronikus kézbesítés útján) átvevő személy, aki az lehet, aki az adott tanúsítvány esetében Igénylő lehet.
- **Biztonságos zóna**: olyan (logikailag vagy fizikailag) védett terület, amely védi a titkosságát, integritását és elérhetőségét a Szolgáltató által használt rendszereknek.
- **Common Name (CN):** Az Igénylő tanúsítványban szereplő, szokásos megnevezéséből képzett neve. DV SSL tanúsítványok esetén az Igénylő által megadott 1 db domain nevet tartalmaz.
- **CRL – Certificate Revocation List:** Lásd Tanúsítvány visszavonási lista
- **Distinguished Name (DN):** A tanúsítványban szereplő, szokásos megnevezéséből, lakóhely vagy székhely szerinti város, ország megnevezéséből, valamint e-mail címéből képzett egyedi neve.
- **DV (vagy automata) SSL tanúsítvány:** olyan, szerverek számára kibocsátott SSL tanúsítvány, melynél kizárólag a domain feletti felügyeleti képesség kerül ellenőrzésre.
- **Előfizető**: lásd az 1.3.3 pontban foglaltakat.
- **Igénylő**: lásd az 1.3.3.3 pontban foglaltakat.
- **Érintett Fél**: lásd az 1.3.3.5 pontban foglaltakat.
- **FQDN (Fully Qualified Domain Name):** Olyan domain név, amely a nevet DNS szerveren keresztül lekérdezve publikus, mindenki számára elérhető hálózati IP címre oldja fel.
- **Hitelesítő egység**: lásd 1.3.1 pontban foglaltakat.
- **Kihelyezett Regisztrációs Egység**: olyan, a Szolgáltatóval szerződéses jogviszonyban álló személy és/vagy szervezet, mely feladata, hogy a Szolgáltató munkáját segítse a tanúsítványkibocsátáshoz szükséges dokumentumok összegyűjtésében, ellássa a tanúsítvány kibocsátásával kapcsolatos koordinációs feladatokat, valamint – adott esetben – részt vegyen az ügyféllel való kapcsolattartásban.
- **Kritikus szolgáltatások**: A Szolgáltató tanúsítvány- és kulcselőállítással, az Ügyfelek eszközzel való ellátásával és a visszavonáskezeléssel kapcsolatos szolgáltatásai.
- **Kulcscsere**: Az a folyamat, amikor a Szolgáltató egy már regisztrált Ügyfele részére annak egy már létező tanúsítványát alapul véve bocsát ki új tanúsítványt és magánkulcsot. Az új tanúsítványban a tanúsítvány sorszámán, a kibocsátás dátumán és az érvényesség kezdetén kívül csak a nyilvános kulcs változik meg.
- **Kulcsletét szolgáltatás**: A Szolgáltató által nyújtott olyan szolgáltatás, amely a Végfelhasználó magánkulcsának megőrzését és annak végfelhasználó számára történő átadását biztosítja (arra az

esetre, ha a végfelhasználó kulcs elveszne, megsemmisülne vagy más okból használhatatlanná válna).

- **Magánkulcs:** Amennyiben a Szolgáltató jelen Szabályzatban erre vonatkozóan kifejezett rendelkezést nem tesz, magánkulcs alatt az aláíró tanúsítvány esetén az elektronikus aláírást létrehozásához használt adatot, bélyegző tanúsítvány esetén az elektronikus bélyegzőt létrehozásához használt adatot, SSL és kódaláíró tanúsítvány esetén a titkos (privát) kulcsot egyaránt kell érteni.
- **Nyilvános kulcs:** Amennyiben a Szolgáltató jelen Szabályzatban erre vonatkozóan kifejezett rendelkezést nem tesz, nyilvános kulcs alatt az aláíró és bélyegző tanúsítvány esetén az érvényesítési adatot, SSL és kódaláíró tanúsítvány esetén a publikus kulcsot egyaránt érteni kell.
- **OCSP (On-line Certificate Status Protokoll):** Valós idejű, online tanúsítvány állapot szolgáltatás. Az adott szolgáltatás keretében kibocsátott összes tanúsítvány aktuális visszavonási állapota (státusza) lekérdezhető. A lekérdezés azonnali, hiteles választ ad egy tanúsítvány állapotáról.
- **Object Identifier (OID):** objektumok azonosítására használt, hierarchizált rendszer alapján definiált számsor.
- **Qualified Government Information Source (QGIS): Közigazgatási szerv által vezetett közhiteles nyilvántartás.**

  Olyan kormányzati adatbázis tekinthető QGIS-nek, amelyet egy hiteles kormányzati szerv tart fent és amelynek adatközlési kötelezettsége törvényben előírt, illetve ahol a hamis adatközlést a törvény bünteti.(Közigazgatási szerv tanúsítványigénylése esetén nem tiltja a kormányzati források felhasználását az, hogy az adat forrása maga a kormányzat.)
- **Qualified Tax Information Source (QTIS):** Olyan nyilvántartás, amit az állami Adóhatóság vezet, azaz egy olyan QGIS, amely kifejezetten az ügyfél vagy a megrendelő pénzügyi adatait, adózásával kapcsolatos információit tartalmazza.
- **Qualified Independent Information Source (QIIS):** Olyan független, rendszeresen frissített, nyilvánosan elérhető információs adatbázis, amely megbízható forrásnak tekinthető.

  Egy adatbázis akkor tekinthető független rendszernek, ha a CA ellenőrizte, hogy:

  - az adatbázist piaci szereplők használják, de nem a CA hozta létre
  - az adatbázis fenntartó legalább évente frissíti az adatot

  A CA nem használhatja az adatbázist, ha ismert, hogy az adattartalma:

  - önbevallásos
  - nem kerül ellenőrzésre a QIIS által

  CA-k és kapcsolódó szervezetei által készített adatbázisok csak akkor használhatók, ha létrehozásukban a CA nem érintett.
- **Regisztrációs Egység:** lásd 1.3.2 pont.
- **SSL (Secure Socket Layer):** olyan technológia, amely a webhelyek és a böngészők közti kommunikáció és adatcsere során egy titkosított csatornát használ.
- **SSL Tanúsítvány:** lásd weboldal hitelesítő tanúsítvány
- **Szolgáltató:** A NETLOCK Kft, amely tevékenységi körében nem minősített nem aláíró tanúsítványkibocsátási tevékenységet és ehhez kapcsolódó egyéb szolgáltatásokat biztosít.
- **Szolgáltatási Szabályzat**: Lásd 1.1.1 pontban foglaltakat.
- **Szolgáltatási Szerződés**: a Szolgáltató és a szolgáltatási ügyfél között létrejött szerződés, amely a jelen Szabályzat szerinti szolgáltatás nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza.

- **Szolgáltatói Partner**: Olyan természetes vagy jogi személy/egyéb szervezet, amelyek a Szolgáltatóval való megállapodás alapján a Szolgáltatás nyújtásában részt vesznek, vagy saját Szolgáltatást nyújtanak.
- **Szolgáltatói rendszer**: Szolgáltató szolgáltatásnyújtást végző rendszereinek együttese.
- **Szolgáltatói tanúsítvány**: Szolgáltató azon tanúsítványa, amelyeket a jelen Szabályzat szerinti szolgáltatás nyújtás érdekében használ.
- **Tanúsítvány**: A Szolgáltató által kibocsátott elektronikus igazolás, amely a nyilvános kulcsot a tanúsítvány Igénylőhöz kapcsolja.
- **Tanúsítvány alany:** a tanúsítványban a Szolgáltató által igazolt azonosságú vagy tulajdonságú személy.

  Az Alany a tanúsítvány „Subject" mezőjében feltüntetésre kerülő természetes/jogi személy vagy egyéb szervezet vagy általuk birtokolt trademark, illetve eszköz/rendszer azonosítója (pl. domain név) vagy más elnevezése. Személyes tanúsítvány esetén az Alany megegyezik a „Subject/CN" mezőben szereplő természetes személlyel, munkatársi tanúsítvány esetén az Alany egyrészt a „Subject/CN" mezőben szereplő természetes személy, másrészt az „Subject/O" mezőben szereplő jogi személy/szervezet – ebben az esetben a Szolgáltató az Alany elnevezést a CN és az O mezőre egyaránt érti. DV SSL tanúsítvány esetén a „Subject/CN" a domain nevet tartalmazza.
- **Tanúsítványaktiválás:** Felfüggesztett tanúsítvány érvényes állapotúra váltása. Az aktiválás során a Szolgáltató megbizonyosodik arról, hogy a tanúsítvány, illetve az Ügyféleszköz a Végfelhasználó birtokában van.
- **Tanúsítvány felfüggesztése:** Az a folyamat, amelyben a Szolgáltató egy még érvényes Tanúsítvány érvényességét átmenetileg megszünteti az eredetileg tervezett érvényességi idő vége előtt. A tanúsítvány felfüggesztés egy átmeneti állapot, a felfüggesztett Tanúsítvány visszavonható, vagy a Tanúsítvány eredeti érvényességi idejében újra érvényessé tehető. A felfüggesztés időtartama 30 naptári nap.
- **Tanúsítványigénylés:** Az a folyamat, amikor Igénylő tanúsítványt igényel, azaz a tanúsítvány kibocsátásához szükséges adatokat megadja és a Szolgáltató az adatok ellenőrzését követően a tanúsítványt kibocsátja.
- **Tanúsítvány kibocsátása:** tanúsítvány átadása az Ügyfélnek, valamint a Szolgáltató nyilvántartásában a tanúsítvány elérhetővé tétele az Ügyfél hozzájárulása esetén.
- **Tanúsítványtár:** Szolgáltató által üzemeltetett nyilvános adatbázis, amelyen keresztül lekérdezhetők a Szolgáltatói, és a Szolgáltató által kiadott nyilvános végfelhasználói tanúsítványok, és a tanúsítvány érvényességi állapota.
- **Tanúsítvány-visszavonás:** Az a folyamat, amelyben a Szolgáltató – saját hatáskörében eljárva vagy külön erre vonatkozó igény esetén – a tanúsítvány érvényességét megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány-visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont tanúsítvány a visszavonás időpontjában érvényességét veszti, státusza pedig semmilyen körülmények között nem állítható vissza.
- **Tanúsítvány-visszavonási lista:** A Szolgáltató által készített hiteles lista, amely a valamely okból visszavont, azaz érvénytelenített, illetve felfüggesztett, azaz ideiglenesen érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet meghatározott időközökkel a Szolgáltató bocsát ki.
- **Tanúsítványmegújítás:** Az a folyamat, amikor a Szolgáltató ugyanarra a nyilvános kulcsra egy új tanúsítványt állít ki egy új érvényességi időszakra. A tanúsítvány Alanya nem változik.
- **Tanúsítványmódosítás:** Az a folyamat, amikor a Szolgáltató egy új Tanúsítványt bocsát ki egy korábban kibocsátott Tanúsítványa alapján, az abban szereplő nyilvános kulccsal, de megváltozott Alany adatokkal.

- **Ügyfél:** Lásd 1.3.3.4 pontban foglaltakat.
- **Ügyféleszköz:** Olyan biztonságos kriptográfiai eszköz, amely az Végfelhasználó magánkulcsát tartalmazza, azt védi a kompromittálódás ellen, s a kulccsal kriptográfiai műveleteket végez az Végfelhasználó számára. Adott esetben megegyezik az elektronikus aláírást létrehozó eszközzel.
- **Ügyfélmenü:** A Szolgáltató ügyfelei számára a tanúsítványokkal és hozzájuk kapcsolódó szolgáltatásokkal kapcsolatos különböző igénylések elvégzésére illetve a folyamatban lévő igénylések állapotának megtekintésére biztosított a Szolgáltató internetes oldalán keresztül elérhető egyedi felület, melybe egyedi felhasználónév és jelszó megadásával lehet belépni (ügyfélmenü regisztrációt követően).
- **Ügyélmenü regisztráció:** Az a folyamat, melynek során egy természetes személy adatai megadását követően létrehozza a Szolgáltató rendszerében saját ügyfélmenüjét és a hozzá tartozó egyedi felhasználónév és jelszó párost (lásd 4.1.2 pontban foglaltakat).
- **Végfelhasználó:** Lásd a 1.3.3.2 pontban foglaltakat.
- **Végfelhasználói tanúsítvány:** Az Előfizetők tanúsítványát és kulcsát jelöli, megkülönböztetve a Szolgáltató saját tanúsítványaitól és kulcsaitól.

1.6.2 Rövidítések

Lásd 9.1.4 pontban foglaltakat.

2 Közzététel és tanúsítványtár

2.1 Szabályzatok, egyéb információk közzététele

2.1.1 Közzétételi és tájékoztatási elvek

2.1.1.1 A szabályzatban nem tárgyalt elemek

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

2.1.1.2 A Szabályzat közzététele

Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját, lehetőség szerint annak tervezett hatályba lépését megelőzően közzéteszi honlapján (lásd 1.1.2 pont). A Szolgáltató alkalmanként ezt megelőzően is tájékoztathatja a PKI szereplőket a tervezett változtatásairól.

2.1.1.3 Észrevételek kezelése

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

2.1.2 Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus PDF formátumban hozza nyilvánosságra Internetes oldalain keresztül (ld. 1.1.2 pont). Itt a dokumentumok aktuális verziója mellett megtalálhatóak azok korábban érvényben lévő változatai és a jövőbeli tervezetei is.

2.1.3 Rendkívüli információk közzététele

A Szolgáltató a következő eseményekről honlapján hirdetményt tesz közzé:

- új szolgáltatás beindítása,
- valamely szolgáltatás tervezett beszüntetése vagy tartós (7 naptári napot meghaladó) szüneteltetése,
- tevékenységének befejezése (lásd 5.8.1 pont),
- rendkívüli üzemeltetési helyzetről tájékoztatás,
- kiadói tanúsítványainak állapotinformációi.

2.2 A tanúsítványokra vonatkozó információk közzététele

A Szolgáltató az egyes tanúsítványok nyilvánosságra hozatala kapcsán a következő eljárást követi:

- A Szolgáltató a szolgáltatói tanúsítványokat legkésőbb a szolgáltatás megindításakor teszi közzé Internetes honlapján (1.1.2 pont)
- A Szolgáltató a végfelhasználói tanúsítványokat a kibocsátást és – amennyiben értelmezett, az aktiválást - követően haladéktalanul megjeleníti a nyilvános tanúsítványtárban az Ügyfél hozzájárulása esetén.
- Alárendelt Hitelesítés Szolgáltatás esetén a vonatkozó Szolgáltatási Utasításban, illetőleg Szolgáltatási Szabályzat kiegészítésben a fentiektől el lehet térni.

A Szolgáltató a tanúsítványokkal kapcsolatos állapotinformációkat a következő módszerekkel teszi közzé:

- A Szolgáltató által kibocsátott végfelhasználói tanúsítványokkal, valamint a szolgáltatói tanúsítványokkal kapcsolatos állapotinformációk az online tanúsítványállapot-szolgáltatás (OCSP szolgáltatás) keretén belül az állapotváltozást követően azonnal elérhetőek.
- A tanúsítványok állapotára vonatkozó információk tanúsítványvisszavonási listákon (CRL) is megjelennek.
- A Szolgáltató nyilvános tanúsítványtárában a mindenkor érvényes végfelhasználói tanúsítványok elérhetők abban az esetben, ha tanúsítványtárban való megjelenítéshez az Ügyfél hozzájárult.
- A Végfelhasználó az Ügyfélmenübe való bejelentkezéskor a mindenkori tanúsítványai aktuális állapotára vonatkozó információkat elérheti.

A tanúsítvány használatára és kikötésére vonatkozó szabályok a 1.4 pont részletezi.

SSL tesztelési célokra a Szolgáltató weboldalakat tart fent visszavont, lejárt és érvényes tanúsítványokkal.

2.3 A közzététel időpontja és gyakorisága

2.3.1 Kikötések és feltételek közzétételi gyakorisága

Jelen Szabályzattal kapcsolatos új verziók közzététele a 9.12 alfejezetben ismertetett eljárásoknak megfelelően történik.

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

2.3.2 Rendkívüli információk közzétételi gyakorisága

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

2.4 Tanúsítványtár elérésének szabályai

2.4.1 Hozzáférés ellenőrzések

A Szolgáltató által közzétett kikötések és feltételek, rendkívüli információk, tanúsítványok és állapotinformációk nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közlő közegek sajátosságainak megfelelően. A tanúsítványok és állapotinformációk elérése kapcsán az Érintett Felek részére a Szolgáltató által kibocsátott tanúsítványok, illetve időpont hitelesítésének ellenőrzésére jelen Szabályzat tartalmaz ajánlásokat.

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

2.4.2 Tanúsítványtárak

A Szolgáltató az Érintett Felek számára a rendelkezésére álló legpontosabb adatokat biztosítja a lehetőségeknek, vállalásoknak megfelelően leghamarabb, és ennek érdekében nyilvános Tanúsítványtárat üzemeltet az Internet címén (lásd 1.1.2 pont), kivéve DV SSL tanúsítvány esetén, ahol nyilvános tanúsítványtár nem elérhető.

A tanúsítványtárban a Szolgáltató által kiadott tanúsítványok találhatók. A Szolgáltató emellett a weboldalán keresztül elérhetővé teszi az alábbi információkat: visszavont tanúsítványok listái, eljárásrendek, szerződéses feltételek és más dokumentumok (pl. meghatalmazás minta).

A Szolgáltató tanúsítványtára szabványos HTTP, illetve HTTPS protokollokkal érhető el az ott megvalósított lekérdezési műveletekkel. A tanúsítványtár többszintű keresési lehetőséget biztosít a tárolt adatok eléréséhez.

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

A Szolgáltató a kibocsátott tanúsítványok nyilvántartása, a visszavonási nyilvántartások, valamint visszavonási állapot-közzététel legalább 99%-os rendelkezésre állását biztosítja, egyúttal az eseti szolgáltatás kiesések nem haladják meg a 24 órás időtartamot.

2.4.3 Online szolgáltatások hozzáférése

Az online szolgáltatások (AIA:CAI, CRL, OCSP) nem rendelkeznek hozzáférési korlátozással, szabadon hozzáférhetők, de a túlzott használat esetén szolgáltatásvédelmi okokból adott kérések egy határ átlépése esetére korlátozhatók, a korlátozások feltételei közzétételre kerülnek a Szolgáltató weboldalán.

3 Azonosítás és hitelesítés

A Szolgáltató a tanúsítvány kibocsátás előtt az alábbi azonosítási és ellenőrzési lépéseket/módokat hajtja végre/alkalmazza.

3.1 Elnevezések

A tanúsítványokban található mezők és tartalmuk a következő:

Szabványos megnevezés OID	Ellenőrzési lehetőségek
Subject mező	
CN id-at-commonName 2.5.4.3	**Személyes vagy munkatársi titkosító, illetve authentikációs tanúsítvány esetén a személy teljes nevét tartalmazza, az adatforrásban szereplő formában.** A személynév ellenőrzésére szolgálhat: ● A Nytv. [1.] szerint személyazonosításra alkalmas igazolvány ● Közhiteles nyilvántartással történő összevetés
CN id-at-commonName 2.5.4.3	**Szervezeti igénylő esetén a Szervezet teljes vagy rövidített neve vagy DBA vagy Tradename vagy Termékazonosító és sorszám** **Szervezetnév feltüntetése esetén ellenőrzési források:** ● Hiteles cégkivonat, alapító okirat vagy ezekkel egyenértékű okirat, mely a szervezet létezését igazolja; ● Az ellenőrizendő szervezet hiteles iratai alapján. Cégnyilvántartás Közhiteles cégnyilvántartás alapján. A nyilvántartásban szereplő rövidített vagy idegen nyelvű név is szerepeltethető. **Trademark esetén az ellenőrzési forrás:** ● Hivatalos védjegy nyilvántartás Amennyiben a védjegyet az igénylő jogosult használni, akkor használható védjegy a commonName mezőben. **DBA esetén** Tartalma lehet: 1. Cégformát nem tartalmazó cégnév Az ellenőrzött cégnév hosszú vagy rövid neve szerepelhet benne, a cégforma (Kft, Bt. stb.) megjelölése nélkül. Ellenőrzése során a Szervezet nevére vonatkozó ellenőrzések a mérvadók (lásd korábban) 2. Domain név Amennyiben domain nevet kíván használni az elnevezésben. Az ellenőrzési lépések a domain nevekre vonatkozó lépések. (lásd később).
CN id-at-commonName 2.5.4.3	**DV SSL tanúsítvány esetén a szerver FQDN DNS neve** A commonName csak egy DNS bejegyzést tartalmazhat. Az ellenőrzési lépések a domain nevekre vonatkozó lépések.

Szabványos megnevezés OID	Ellenőrzési lehetőségek
	A SAN/DNSName mezőben ugyanazon tartalomnak kell szerepelnie.
SN Id-at-surname 2.5.4.4	**Vezetéknév** *A mező csak akkor szerepelhet, ha a tanúsítvány alanya természetes személy.* Ez esetben tartalma a Személy teljes nevének felbontása, és annak vezetéknév szakasza. A felbontást a vonatkozó MELASZ ajánlás alapján lehet elvégezni.
id-at-givenName 2.5.4.42	**Keresztnév** *A mező csak akkor szerepelhet, ha a tanúsítvány alanya természetes személy.* Ez esetben tartalma a Személy teljes nevének felbontása, és annak keresztnév (keresztnevek) szakasza. A felbontást a vonatkozó MELASZ ajánlás alapján lehet elvégezni.
id-at-serialNumber 2.5.4.5	Alany globálisan egyedi sorozatszáma.
id-at-countryName 2.5.4.6	Székhely vagy lakhely szerinti ország Az igazolvány (személy) hiteles szervezetazonosító dokumentum (szervezet) és/vagy (köz-)hiteles nyilvántartás (mindkettő) által igazolt teljes név.
L id-at-localityName 2.5.4.7	Székhely vagy lakhely szerinti város Az igazolvány (személy) hiteles szervezetazonosító dokumentum (szervezet) és/vagy (köz-)hiteles nyilvántartás (mindkettő) által igazolt település.
id-at-stateOrProvinceName 2.5.4.8	Székhely vagy lakhely szerinti megye, vagy állam Az igazolvány (személy) hiteles szervezetazonosító dokumentum (szervezet) és/vagy (köz-)hiteles nyilvántartás (mindkettő) által igazolt megye vagy állam.
id-at-organizationName 2.5.4.10	**Szervezet teljes vagy rövidített neve** **Szervezet név feltüntetése esetén ellenőrzési források:** ● Hiteles cégkivonat, alapító okirat vagy ezekkel egyenértékű okirat, mely a szervezet létezését igazolja; ● Az ellenőrizendő szervezet hiteles iratai alapján. ● Cégnyilvántartás Közhiteles cégnyilvántartás alapján. A nyilvántartásban szereplő rövidített vagy idegen nyelvű név is szerepeltethető.
id-at-organizationalUnitName 2.5.4.11	**Szervezeten belüli létező és ellenőrizhető szervezeti egység neve** A tanúsítványba foglaláshoz a szervezetnek igazolnia kell az egység létezését.
organizationIdentifier 2.5.4.97	**Szervezet nyilvántartásban szereplő azonosítója** A szervezet nyilvántartásban szereplő adóazonosító száma, az ETSI EN 319 411-1 által meghatározott szemantikus formában.
Id-at-title 2.5.4.12	**Személy beosztása vagy titulusa** Csak munkatársi tanúsítvány esetén szerepelhet.

Szabványos megnevezés OID	Ellenőrzési lehetőségek
subject/EMAIL	A CN-ben megadott entitáshoz igazoltan tartozó email cím; megismétlésre kerül a SubjectAlternateName mezőben
SAN mező	
SAN SubjectAlternateName:DNSName	Egy vagy több domain nevet tartalmaz, ha a CN DNS bejegyzést tartalmaz, itt meg kell ismételni.
SAN SubjectAlternateName:emailaddress	Az Ügyfél email címét tartalmazza, tartalma egyezik a Subject/EMAIL mező tartalmával, szerver tanúsítvány esetén nem szerepel
SAN SubjectAlternateName:otherIdentifier	A Szolgáltató egyedi azonosítója, mely az RFC4043 szerinti permanens azonosítót tartalmazza

3.1.1 Névtípusok

Szolgáltató a tanúsítványok Subject mezőinek képzése esetén az RFC 5280 szabványnak megfelelően az X.500 distinguished name előírásait követi. Ez alapján a Szolgáltató ötfajta névtípust különböztet meg a végfelhasználói tanúsítványok esetén:

- természetes személyre,
- jogi személyre,
- természetes és jogi személyre együttesen és
- DV SSL-re.

A DV SSL tanúsítványra vonatkozó névtípusok leírását lásd a jelen Szabályzat 7 fejezetében.

Természetes és jogi személyre együttesen vonatkozó névtípus esetén a szervezetazonosító (O, organizationIdentifier) az Előfizető jogi személyt, az Alany azonosító (CN, Common Name) pedig a Természetes személyt azonosítja.

3.1.2 A nevek értelmezhetősége

Természetes személyek számára kibocsátott tanúsítvány *Subject* mezője a következő adatot tartalmazza:

- countryName (Országkód);
- givenName és surName vagy pseudonym (Vezeték és Családnév)
- commonName (Név)

Pseudonym alkalmazása esetén a givenName és surName mezők nem kerülnek feltüntetésre.

Jogi személyek/egyéb szervezetek számára kibocsátott tanúsítvány *Subject* mezője a következő adatot tartalmazza:

- countryName (Országkód);
- commonName (Név)

A Subject mezőre vonatkozó részletes leírást a 3.1 tartalmazza.

A tanúsítványban szereplő természetes és jogi személy/egyéb szervezet nevét a Szolgáltató a – lehetőség szerint - közhiteles nyilvántartásban, annak hiányában hivatalos azonosító dokumentumban, illetve az alapító okiratban szereplő írásmóddal azonos módon tünteti fel.

Amennyiben a tanúsítvány Alanyaként jogi személy/egyéb szervezet kerül feltüntetésre (természetes személy helyett), akkor a tanúsítványban kötelezően szerepel az *organizationIdentifier* mező, amely a jogi személy/egyéb szervezet egyedi azonosítóját tartalmazza. Amennyiben a nem természetes személy Alany a természetes személy Alany mellett szerepel, akkor az *organizationIdentifier* mező feltüntetése opcionális. A mezőben egy hivatalos nemzeti vagy más azonosító rendszerben kapott egyedi azonosító szerepelhet kötött formátumban az alábbiak szerint:

1. Ha a szervezet rendelkezik adószámmal, akkor a VAT előtag, majd a szervezetet bejegyző ország kódja, kötőjel, és az szervezet adószáma változatlan formában. Magyar szervezet esetén a „VATHU-„ előtagot követheti belföldi vagy közösségi adószám változatlan formában.
2. Ha előző pont nem alkalmazható, akkor Cégjegyzékszám kerül feltüntetésre "NTRHU-" előtagot követve.
3. Ha előző pontok nem alkalmazhatók, akkor nemzeti bejegyzett séma alapján "XX:HU" értékkel, amelyben az „XX” a nemzeti vagy EU-s azonosítási séma két karakteres jelölése.
4. Ha előző pontok nem alkalmazhatók, akkor más egyedi hivatalos azonosító kerül alkalmazásra
5. Ha egyik említett azonosító sem áll rendelkezésre, az alapító okirat azonosítója és az alapító jogszabály megnevezése is kerülhet ide.

Más országok azonosítórendszerei esetében a Szolgáltató az ISO 3166 szerinti országkódokat alkalmazza.

Amennyiben *Subject/Serialnumber* mező tartalma egy hivatalos (okmány alapján ellenőrzött) nemzeti azonosító, akkor annak kötelező formátuma: <REF>HU-<igazolványszám>, ahol a <REF> helyére három karakter kerül a következők szerint:

1. "PAS" útlevélszám esetében (pl. PASHU-AE123456)
2. "IDC" személyi igazolvány vagy jogosítvány számának esetén (pl. IDCHU-123456AB (személyi ig. szám) vagy IDCHU-AB123456 (vezetői engedély))
3. "PNO" személyi szám esetén (használata NEM JAVASOLT)
4. "TIN" adóazonosító jel esetében (pl. TINHU-1234567890)

Egyedi azonosítórendszerek esetén a <REF> helyére „XX:” formátumú karaktersorozat kerül, amelyben az „XX” a nemzeti vagy EU-s azonosítási séma két karakteres jelölése (pl. EI:HU-200007292386 vagy AT:EU-BH16251).

Amennyiben a további serialnumber mező nem a fenti igazolványok alapján kerül kitöltésre, formai előírás nincs, kivéve a külön tárgyalt eseteket.

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

- A tanúsítványban az adatok speciális és vezérlő karakterek nélkül szerepelnek.
- A nevek alapértelmezetten tanúsítványban az alábbiak szerint kerülnek feltüntetésre: a személyazonosság igazolására a Nytv. [1.] szerint elfogadott hatósági igazolványban foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve a CN, SN és GN mezőkben (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév, GN = Keresztnév vagy keresztnevek), az UTF-8 kódolást használva. A nevek egyes egységeit szóköz választja el. Ezen szabályoktól a Szolgáltató kivételesen eltérhet, amennyiben a Common Name, Organization és Organization Unit mezőkre vonatkozó karakterszámbeli korlátok nem teszik lehetővé az ilyen formában történő teljes adatrögzítést.
- DV SSL tanúsítványban a „CN” mező nem lehet üres: vagy legalább egy FQDN domain nevet tartalmaz, vagy nem szerepel a tanúsítványban. A CN mező tartalmazhat * tagot.
- A tanúsítványban kivételesen, egyedileg meghatározott esetben, a vonatkozó szabványok szerinti meghatározott maximális karakterszámot meghaladó elnevezések esetén rövidítés használata lehetséges.
- A tanúsítványban a „CN” mező nem üres.
- A tanúsítvány SN és GN mezőjének feltüntetése természetes személy Alany esetén kötelező.
- A „Title” mezőben az Alany beosztása szerepel, amennyiben lehetséges annak feltűntetése, egyéb esetben nem kerül feltüntetésre.

- A „State” mezőben az ország, a megye, vagy megyei jogú város neve kerülhet feltüntetésre.
- Munkatársi tanúsítványokban az „Organization” mezőben szerepel a jogi személy/egyéb szervezet, valamint az „Organization-unit” mezőben szerepelhet a jogi személy/egyéb szervezeten belüli szervezeti egység.
- A „Locality” mezőben feltüntethető az Alany lakcím szerinti vagy munkatársi és szervezeti tanúsítványokban a tanúsítványban feltüntetésre kerülő jogi személy/egyéb szervezet székhely, telephely szerinti városa.
- A tanúsítvány „SubjectAltname” mezőjében szereplő elektronikus levelezési cím struktúrája megfelel az RFC 822 előírásainak.
- DV SSL tanúsítvány esetén
    - a „SubjectAltname” (SAN) mezője nem lehet üres: vagy ki van töltve, vagy nem szerepel a tanúsítványban. Ha kitöltött, akkor legalább egy FQDN domain nevet tartalmaz.
    - a „SubjectAltname” (SAN) mező tartalmazhat * tagot.
    - a „SubjectAltname” (SAN) mezője a kérelmezett FQDN mellett tartalmazhat „www” előtaggal kiegészített FQDN-t, amennyiben a kérelmezett FQDN nem tartalmazott „www” előtagot.
    - a CN mező és a SubjectAltname” (SAN) mező első FQDN tagjának egyeznie kell, amennyiben mindkettő megtalálható a tanúsítványban.
    - a public suffix teljes tartományra nem adható ki * tanúsítvány.
    - A domain nevek dNSName formátumban kerülnek tárolásra.

3.1.3 A különböző elnevezési formák értelmezési szabályai

A Szolgáltató által kibocsátott tanúsítványoknak nem célja, hogy az Alanyként megjelölt természetes személyek, jogi személyek, illetve egyéb szervezetek számára digitális igazolványként funkcionáljon, illetve hogy személyüket kizárólag a tanúsítványban feltüntetett adatok alapján azonosítani lehessen.

A munkatársi tanúsítvány önmagában képviseleti jogosultságot nem igazol.

Az azonosítók értelmezése érdekében Érintett Feleknek a jelen Szabályzatban leírtak alapján kell eljárniuk (lásd különösen a 7.1.5 pont). Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett Félnek segítségre van szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot.

A Szolgáltató az Alany(ok) adatairól többlettájékoztatást – a tanúsítványban feltüntetett adatok értelmezését segítő információn kívül – csak az erre vonatkozó felhatalmazás alapján ad ki.

3.1.3.1 Kibocsátó azonosító

A kibocsátó azonosító úgy értelmezendő, hogy a tanúsítványt a Szolgáltató adta ki egy adott köztes/gyökér tanúsítvány segítségével.

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

3.1.3.2 Alanyazonosító

A *Subject mező* Alany azonosítója úgy értelmezendő, hogy a tanúsítvány alanya a *Common Name* nevű természetes személy, jogi személy, egyéb szervezet vagy domain. Munkatársi tanúsítvány esetén megállapítható, hogy az adott természetes személy mely *Organization* nevű szervezettel és adott esetben az O*rganization-unit* szervezeti egységhez tartozik.

A természetes személy lakóhelye, illetve a szervezet székhelye vagy telephelye a *Country* (ország), a *State* (ország/megye) és a *Locality* (település) mezők szerinti helyen található. Az Alany e-mail címe az igényléskor megadott *E-mail* cím. Amennyiben feltüntetésre kerül, a *Title* mező tartalmazza az Alany Organization mezőben lévő szervezetben betöltött beosztását.

Az Alanyazonosító mezőnek célja, hogy a tanúsítvány Alanyát, munkatársi tanúsítvány esetén a szervezetet is azonosítani lehessen. Munkatársi tanúsítvány esetén az Alany(ok) együttes megjelenítése a tanúsítványban azt jelenti, hogy a tanúsítvány O mezőjében foglalt jogi személy/szervezet hozzájárult a természetes személy és a jogi személy/szervezet Alanyként való feltüntetéséhez.

3.1.4 A nevek egyedisége

A Szolgáltató az általa kibocsátott authentikációs és titkosító tanúsítvány esetében a tanúsítványok Alanyait (Subject mező) egymástól egyértelműen megkülönbözteti. Ennek érdekében a Szolgáltató minden személynek egy egyedi alanyazonosítót (OID alapú permanentID) ad, melyet a tanúsítvány Subject/Serialnumber mezőjében tüntet fel. Ez az azonosító egyedi szinten azonosítja a tanúsítványban szereplő természetes vagy jogi személyt. Egy Alanynak lehet több azonosítója, viszont ezt az azonosítót soha nem kaphatja meg más Alany.

A fentiek mellett a Szolgáltató egy további Subject/Serialnumber mezőben más egyedi azonosítót is feltüntethet (pl. személyazonosító igazolvány szám, hatósági kártya azonosítója stb.).

DV SSL tanúsítvány esetén az OID alapú permanentID nem értelmezett.

3.1.5 Védjegyek azonosítása, ellenőrzése és szerepe

Szolgáltató a tanúsítványban védjegyet is feltüntethet az Ügyfél birtokában/tulajdonában lévő DBA, trademark, terméknév vagy termékazonosító alapján. Ezen adatok a tanúsítvány Subject/CN és/vagy a SubjectAltName/dirname mezőben kerülhetnek feltüntetésre.

A Szolgáltató a tanúsítvány kibocsátását megelőzően meggyőződik arról, hogy az Ügyfél jogosan birtokolja a nevet és az azonosítós, és az nem megtévesztő (amennyiben értelmezett). Az ellenőrzést a Szolgáltató hivatalos dokumentum vagy egyéb megbízható adatforrás alapján végzi.

Az Ügyfél részéről egy védjegy megszerzése nem tekinthető olyan eseménynek, amely szükségszerűen a tanúsítvány megújítását eredményezi. A tanúsítványigényléssel és elfogadással az Ügyfél kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik személy jogait. Szolgáltatónak nem kötelessége a védjegyek jogos használatának az ellenőrzése.

3.2 Kezdeti azonosítás

Amennyiben a Szolgáltató még nem ellenőrizte vagy a korábbi ellenőrzése már nem igazolja hitelt érdemlően a tanúsítvány Alanyát/Alanyait, Igénylőit, akkor az alábbiak szerint részletezett kezdeti azonosítási eljárással ellenőriznie kell az Igénylő személyazonosságát, valamint az Alany(ok) azon adatait, amelyeket a tanúsítványban fel kíván tüntetni, illetve amelyeket a tanúsítványról el kíván tárolni.

DV SSL tanúsítvány kibocsátása esetén a Szolgáltató kizárólag a domain feletti felügyeleti képességet ellenőrzi (lásd 3.2.2.3 pont).

Amennyiben a Szolgáltató a titkosító, illetve authentikációs tanúsítvány kibocsátásával egyidejűleg a *NETLOCK Szolgáltatási Szabályzat nem minősített tanúsítványokra* szabályzat szerinti azonosítási feladatokat is elvégezte, akkor a Szolgáltató jelen Szabályzat szerinti azonosítási feladat nem végez.

Az ellenőrzés lehet teljeskörű (pl. amennyiben az érintett személy még nem ismert Szolgáltató számára) vagy részleges (amennyiben az érintett egyes adatai szorulnak csak újbóli megerősítésre, pl. egyes dokumentumok érvényességének lejárata miatt). Amennyiben az Előfizető/Igénylő rendelkezik a Szolgáltató vagy nem a Szolgáltató által kibocsátott érvényes aláíró vagy bélyegző tanúsítvánnyal, akkor a kezdeti ellenőrzésnél a Szolgáltató a lentebb meghatározott módon jár el.

A Szolgáltató jelen dokumentumában és belső eljárásrendjében határozza meg a részletes eljárást, amely alapján kiadja az Ügyfél számára a tanúsítványát.

A Szolgáltató a titkosító, illetve authentikációs tanúsítványba foglalandó adatokat ellenőrizi, így különösen az Alany (természetes és/vagy jogi személy/szervezet) adatait, a személyazonosság megállapításához használt azonosító adatok valódiságát és a Szolgáltató erre irányuló döntése estén a közhiteles vagy más

központi nyilvántartásban foglalt adatokkal való megegyezőségét, az Igénylő eljárási jogosultságát, a tanúsítványba foglalandó képviseleti jog meglétét, a tanúsítványba foglalandó szervezeti egység létezését, a tanúsítványba foglalandó szabályozott szakma megnevezése esetén az annak gyakorlására való jogosultságot.

A tanúsítvány Alanyának ellenőrzése a különböző hitelesítési osztályok esetében az alábbiak szerint valósul meg:

- "C" hitelesítési osztály esetén:
  (1) "C" osztályú ellenőrzés során a szükséges személy- és szervezetazonosító dokumentumokat, valamint az aláírt Szolgáltatási Szerződést (lásd 4.2.1 pont) elegendő másolatban eljuttatni a Szolgáltatóhoz. A másolatok ellenőrzése során meg kell győződni arról, hogy minden dokumentum hiánytalanul megérkezett-e és olvasható-e. Ha valamelyik dokumentum hiányzik vagy valamelyik lap olvashatatlan, azt a Szolgáltató újra bekéri.
  (2) Abban az esetben, ha az Igénylő/Végfelhasználó a Szolgáltató által kibocsátott érvényes aláíró tanúsítvánnyal/bélyegzővel rendelkezik, a Szolgáltató dokumentumok ismételt benyújtását alapesetben nem kéri.
  (3) Abban az esetben, ha Igénylő/Végfelhasználó nem a Szolgáltató által kibocsátott, de a Szolgáltató által elfogadott (lásd 4.2.1 pont) érvényes aláíró tanúsítvánnyal/bélyegzővel rendelkezik, a Szolgáltató mindig egyedileg mérlegeli, hogy milyen azonosító dokumentum(ok) benyújtását kéri.
- "B" hitelesítési osztály esetén:
  (1) "B" osztályú ellenőrzés során a szükséges személyazonosító dokumentumokat eredetiben kell bemutatni a Szolgáltató Központi Regisztrációs Szervezet, a Mobil Regisztrációs Munkatársak, a Kihelyezett Regisztrációs Szervezetet, vagy Regisztrációs- és Kézbesítési Megbízott munkatársaknak. Ezen túlmenően a Szolgáltató kérheti a szervezetazonosító dokumentumok eredetiben történő bemutatását is. A Szolgáltatási Szerződést a Szolgáltató képviselője előtt személyesen kell aláírnia (lásd 4.2.1 pont) a tanúsítvány Igénylőjének vagy Előfizetőnek.
  (2) Az ügyfél a személyes megjelenés helyett választhatja azt is, hogy közjegyző előtt írja alá a Szolgáltatási Szerződést (ún. aláíráshitelesítés). Ebben az esetben a közjegyző előtt aláírt Szolgáltatási Szerződés eredeti példányát kell eljuttatnia a Szolgáltatóhoz, csatolva – amennyiben értelmezett - a szervezet azonosítására szolgáló eredeti dokumentumokat. Ebben az esetben a tanúsítvány kibocsátását/aktiválását megelőzően még szükséges a Regisztrációs és Kézbesítési megbízottal való találkozás is.
  (3) Amennyiben a Szolgáltató személyes jelenléttel egyenértékű egyéb azonosítási módszert is elfogad, arról honlapján tesz részletes tájékoztatást közzé.
  (4) Amennyiben a Szolgáltató biztosítja a személyes megjelenésre vonatkozóan az eIDAS **Hiba! A hivatkozási forrás nem található.** 24. cikk (1) b) pontja alapján távoli elektronikus azonosító eszköz használatát, akkor arról honlapján tesz részletes tájékoztatást közzé.
  (5) Abban az esetben, ha az Igénylő/Végfelhasználó a Szolgáltató által kibocsátott érvényes aláíró tanúsítvánnyal/bélyegzővel rendelkezik, a Szolgáltató dokumentumok ismételt benyújtását alapesetben nem kéri.
  (6) Abban az esetben, ha az Igénylő/Végfelhasználó nem a Szolgáltató által kibocsátott, de a Szolgáltató által elfogadott (lásd 4.2.1 pont) érvényes aláíró tanúsítvánnyal/bélyegzővel rendelkezik, a Szolgáltató mindig egyedileg mérlegeli, hogy milyen azonosító dokumentumok benyújtását kéri.

A tanúsítvány Alanyának ellenőrzése során, az Alany típusától függően a Szolgáltató az alábbi ellenőrzési módszert követi:

- Természetes személy Alany esetén
  (1) Személyes jelenlét alapján vagy azzal egyenértékű azonosítás esetén, amennyiben természetes személy alany a Nytv. [1.] hatálya alá tartozik, akkor Nytv. [1.] szerinti

személyazonosság igazolására alkalmas hatósági igazolvány alapján. Ebben az esetben a Szolgáltató a hatósági igazolvány érvényességét és az igazolványban foglalt adatok egyezését a megfelelő közhiteles hatósági nyilvántartásban is ellenőrizheti.

(2) Személyes jelenlét alapján vagy azzal egyenértékű azonosítás esetén, amennyiben természetes személy alany a Nytv. [1.] hatálya alá nem tartozik, akkor elsősorban a Szmtv. [2.] szerinti úti okmány alapján.

(3) Személyes jelenlét alapján vagy azzal egyenértékű azonosítás esetén, amennyiben természetes személy alany a Nytv. [1.] hatálya alá nem tartozik és a személyazonosság ellenőrzésére Magyarország területén kívül kerül sor, továbbá a természetes személy alany úti okmánnyal nem rendelkezik, a Szolgáltató a személyazonosság ellenőrzését csak olyan megbízható okmányok vagy más iratok alapján végzi, amely esetén a Szolgáltató igazolni tudja, hogy a megbízható okmány vagy más irat a Harmtv. [3.] törvényben meghatározott személyazonosság megállapításában és ellenőrzésében foglaltakkal azonos fokú bizonyosságot ad.

(4) Amennyiben a személyazonosság ellenőrzésére (2) vagy (3) bekezdés szerint került sor, akkor a Szolgáltató az okmány vagy más irat érvényességét (hitelességét), valamint az abban használt adatok és a rájuk vonatkozó központi nyilvántartás egyezőségét is ellenőrizheti. Ha ilyen nyilvántartás nem érhető el, a Szolgáltató számára nem hozzáférhető vagy a hozzáférés és ellenőrzés költsége aránytalanul magas, a Szolgáltató ezt a tényt rögzíti, és az egyéb rendelkezésére álló bizonyítékok alapján dönt arról, hogy az adott tanúsítványt az Igénylő részére kibocsátja-e.

- Nem természetes személy Alany esetén

(1) Ha a tanúsítvány alanya nem természetes személy, a Szolgáltató legalább az Alany tanúsítványba foglalt teljes nevét és egyedi azonosító adatát ellenőrzi.

(2) Ha a tanúsítvány alanya Magyarországon bejegyzett szervezet, a Szolgáltató ezen adatok valódiságát és hatályosságát közhiteles nyilvántartásban is ellenőrizheti, vagy ha ilyen közhiteles nyilvántartás nincsen, a bejegyzést igazoló közokirat alapján ellenőrzi.

(3) Ha a tanúsítvány alany nevében a Szolgáltató előtt képviselő jár el, vagy a tanúsítvány teljes vagy részleges képviseleti jogot vagy ekként is értelmezhető jogviszonyt is tartalmaz (a továbbiakban együtt: képviseleti jog), a Szolgáltató köteles a tanúsítvány kibocsátása előtt a képviseleti jog fennállásáról és annak a tanúsítványból kiolvasható tartalmáról jogszabály, közhiteles nyilvántartás, létesítő okirat vagy ezek hiányában meghatalmazás alapján meggyőződni és az ellenőrzés eredményét rögzíteni.

A Szolgáltatónak az adatok ellenőrzésére használt információkat (mint pl. dokumentumok típusa, azonosítószáma, érvényességi ideje), valamint az Előfizető eléréséhez szükséges adatokat (pl. postacím, telefonszám, e-mail cím) megőrzi az 5.5 pont szerint. A Szolgáltató egyéb, az Ügyfél és Igénylő azonosításához és a kapcsolattartáshoz nem szükséges információkat nem tárol.

A szolgáltatás igénybevevője Szolgáltató vagy annak munkatársa, Szolgáltatói partnere is lehet.

3.2.1 A magánkulcs birtoklásának igazolása

Amennyiben a Szolgáltató állítja elő az Ügyfél számára a kulcspárt, a Szolgáltató nem igényel bizonyítékot arra, hogy az Alany rendelkezik a hitelesítendő nyilvános kulcs magánkulcs párjával.

Amennyiben az Igénylő állítja elő a kulcspárt, úgy a Szolgáltató gondoskodik mindazon technikai és műszaki eljárás alkalmazásáról, melynek révén megbizonyosodhat arról, hogy az Igénylő ténylegesen birtokolja a nyilvános kulcshoz tartozó magánkulcsot. Ennek igazolása történhet egyebek mellett az Ügyfél által generált PKCS#10, SPKAC vagy önaláírt tanúsítványon alapuló igényléssel és annak Szolgáltató felé átadásával.

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

3.2.2 Szervezeti azonosság ellenőrzése

3.2.2.1 Általános szabályok

Amennyiben a tanúsítványban egy jogi személy/egyéb szervezet kerül feltüntetésre (akár a CN, az O vagy OU vagy más mezőkben), akkor a Szolgáltató a 3.2 pontban leírtak alapján jár el. Ebben az esetben az Igénylőnek minden esetben rendelkeznie kell a jogi személy nevében való eljárási jogosultsággal (képviseleti jog vagy képviselő általi felhatalmazás útján). A képviseleti jogot a Szolgáltató hiteles okmánnyal vagy megbízható adatbázisban való megtekintéssel is ellenőrzheti.

Amennyiben az ellenőrizendő szervezet adatai közhiteles nyilvántartásban nem elérhetők, akkor a Szolgáltató más megbízható, rendszeresen frissített adatbázist is használhat vagy a szervezet székhelyét is felkeresheti. A cím ellenőrzésére bankkivonat, közműszámla, hivatalos adózási okmány vagy más dokumentum is felhasználható.

3.2.2.2 Eszköz, rendszer vagy termék esetére vonatkozó speciális szabályok

Amennyiben a tanúsítvány Alanyaként egy eszköz, rendszer vagy termék neve, illetve azonosítója vagy DBA / Védjegy vagy más egyedi elnevezés kerül feltüntetésre (önállóan vagy egy természetes vagy jogi személy mellett), akkor a 3.2-ben írtakon túl meg kell győződni arról, hogy az Ügyfél jogosan birtokolja a nevet és/vagy azonosítót, s az nem megtévesztő (amennyiben ezek értelmezhetőek). Az ellenőrzésnek hivatalos dokumentumon, megbízható adatforráson, az azonosítót kezelő hivatalos szervvel való egyeztetésen vagy más megbízható adatforráson kell alapulnia, amely igazolja a névhasználat jogosságát.

Ilyen esetben, amennyiben az Alany adataként ország is megnevezésre kerül, s a mögötte álló természetes vagy jogi személy nem ismert, akkor a szolgáltatónak az országot az eszközhöz tartozó domain név szerint kell ellenőriznie.

3.2.2.3 Domain névre vonatkozó speciális szabályok

DV SSL tanúsítvány esetén a Szolgáltató kizárólag a domain feletti kontrollt ellenőrzi. A domain feletti felügyeleti képesség (kontroll) ellenőrzése a domaint kiszolgáló szerverhez, vagy a domain DNS TXT rekordjához való hozzáférés ellenőrzését jelenti. DV SSL tanúsítvány wildcard/UCC karaktert nem tartalmazhat.

A Szolgáltató belső domain neves tanúsítvány nem ad ki.

3.2.2.4 Munkatársi tanúsítványra vonatkozó speciális szabályok

Ha a Végfelhasználó tanúsítványával kifejezetten jelezni kívánja, hogy ő egy adott szervezethez tartozik, akkor a személyazonosítás során fel kell mutatnia az adott szervezet képviseletére jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást vagy Hozzájáruló és Elfogadó Nyilatkozat (HEF) arra, hogy a szervezet képviseletében a tanúsítványt használja. Be kell mutatni a szervezet képviseletére jogosult aláírási címpéldányát vagy aláírás mintáját, valamint a Szolgáltató erre vonatkozó kérése esetén a szervezet azonosságát igazoló, közhiteles nyilvántartás által kiadott igazolást.

Az ügyintézést elősegítendő a Szolgáltató weboldaláról (1.1.2) letölthető az igényléshez szükséges meghatalmazás-minta.

Az Igénylő a weboldalon feltüntetett, az igénylés időpontjában érvényes árlista szerint díj ellenében kérheti, hogy az adott szervezet azonosságát hitelesítő, közhiteles nyilvántartásból származó, hiteles kivonatot a Szolgáltató kérje le.

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

3.2.3 Természetes személy azonosságának hitelesítése

A tanúsítvány Igénylője minden esetben ellenőrzésre kerül. Amennyiben a tanúsítvány Igénylője megegyezik a tanúsítvány Alanyával, további személyazonosság ellenőrzésre nincs szükség. Amennyiben az Igénylő nem egyezik meg az Alannyal, a tanúsítványban Alanyként megjelölt entitás (személy-) azonosságának ellenőrzése is szükséges.

Amennyiben a tanúsítványban Alanyként a természetes személy mellett egy jogi személy/egyéb szervezet is feltüntetésre kerül, akkor a jogi személy/egyéb szervezet képviselőjének hiteles igazolása szükséges a természetes személy szerepeltetéséhez (3.2.2 pont).

Az eljárásban részt vevő természetes személyek azonosságát „C" osztály esetén a Szolgáltató dokumentummásolatok, míg „B" osztály esetén személyes megjelenés vagy azzal egyenértékű azonosítás esetén személyazonosító okmány fényképe alapján is ellenőrzi (bővebben lásd 3.2 pont). A személyazonosításra alkalmas hivatalos igazolványban szereplő fénykép alapján a természetes személynek egyértelműen felismerhetőnek kell lennie, a dokumentumon szereplő aláírásának meg kell egyeznie a Szolgáltatási Szerződésen tett aláírásával. Amennyiben kétség merül fel a fénykép vagy az aláírás megfeleltethetősége kapcsán, a Szolgáltató megtagadja a tanúsítványkiadási kérelem teljesítését.

Az Ügyfél, Igénylő és Átvevő által biztosított adatok valódiságát a Szolgáltatási Szerződés (kézi vagy elektronikus) aláírásakor aláírásukkal el kell ismerniük. Az elfogadott elektronikus aláírások körét a Szolgáltató korlátozhatja (lásd 4.2.1).

A regisztráció támogatására az Alany/Igénylő hozzájárulásával a személyazonosító dokumentumokról másolat készülhet, melyek archiválásra kerülnek

3.2.4 Nem ellenőrzött személyes adat

A Szolgáltató által kibocsátott tanúsítványban csak olyan alany adatok szerepelnek, amelyeket a Szolgáltató ellenőrzött, vagy amelyek valódiságáról az Előfizető/Igénylő előzetesen írásban, büntetőjogi felelősségének tudatában nyilatkozott. Amennyiben a Szolgáltató nem tudta/tudott teljes körűen meggyőződni az adatok valódiságáról és helyességéről, a tanúsítványkibocsátást megtagadja.

3.2.5 Jogok, felhatalmazások ellenőrzése

Amennyiben Előfizető nem a saját nevében jár el Szolgáltató előtt (pl. Igénylőként vagy Átvevőként), hanem meghatalmazotton keresztül, akkor Szolgáltatónak minden esetben egyértelműen azonosítania kell a meghatalmazott személyét (lásd 3.2.3) és ellenőriznie kell az Előfizető nevében történő eljárási jogosultságát a Szolgáltató előtt, az adott eljárás (pl. tanúsítványigénylés, felfüggesztés, aktiválás és visszavonás) kapcsán. Jogi személy/egyéb szervezet nevében csak a képviseletre jogosult adhat meghatalmazást képviseletre.

A meghatalmazás hitelességét (lásd 3.2.2) és érvényességét ellenőrizni szükséges. Meghatározott időre adott meghatalmazások esetén minden felhasználás esetén ellenőrizni kell a lejárati időpont meg nem haladását, valamint (jogi személyek/egyéb szervezetek esetén) a meghatalmazó képviseleti jogának fennállását.

3.2.6 Együttműködési képességre vonatkozó követelmények

A Szolgáltató a szolgáltatás nyújtása során együttműködhet más Szolgáltatókkal, akik magukra kötelező érvényűnek ismerik el a Hitelesítési rendbe foglalt követelményeket.

A Szolgáltató közzétesz minden kereszthitelesített tanúsítványt, amely Alanyaként vagy kibocsátójaként szerepel.

3.3 Azonosítás és hitelesítés kulcscsere kérelem esetén

Kulcscsere csak a Szolgáltatási Szerződés időtartama alatt kérhető. A kulcscserével kapcsolatos eljárás részletei a 4.7 fejezetben olvashatók.

Új kulcsot tartalmazó tanúsítvány kibocsátására kizárólag az új tanúsítvány igénylésének folyamata keretében kerülhet sor. DV SSL tanúsítvány esetén a kulcscsere nem értelmezett.

3.3.1 Azonosítás és hitelesítés érvényes tanúsítvány esetén

Kulcscsere kérelmek benyújtására a következő lehetőségeket biztosítja a Szolgáltató:

- papíralapú Szolgáltatási Szerződés kézi aláírásával személyesen a Szolgáltató ügyfélszolgálati irodájában, a Szolgáltató Mobil Regisztrációs munkatársai vagy valamely külső Regisztrációs Szervezet regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;
- Szolgáltatási Szerződés elektronikus aláírásával ellátva e-mailben vagy egyéb elektronikus dokumentum útján;
- a Tanúsítvány felfüggesztési vagy visszavonási folyamata során;
- papíralapú Szolgáltatási Szerződés kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

Személyes kérelem benyújtása esetén a kérelmező azonosítása a 3.2.3 fejezetben leírtak szerint történik.

A Szolgáltató lehetőséget biztosít az Ügyfélnek arra, hogy amennyiben a kulcscserére azért van szükség, mert a tanúsítványhoz tartozó magánkulcs kompromittálódott, akkor az Igénylő ezt a Tanúsítvány felfüggesztési vagy visszavonási eljárás keretében (lásd 4.9 pont) jelezze. Ebben az esetben az Alany a felfüggesztési illetve visszavonási eljárás keretében kerül azonosításra, ennek részleteit a 4.9 pont tartalmazza.

A papíralapon, postai úton történő kulcscsere kérelem benyújtása esetében az Igénylő azonosítása és az Igény megerősítése benyújtását követően, személyesen találkozás során történik.

3.3.2 Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Kulcscsere kérelmeket – kizárólag a Szolgáltatási Szerződés érvényessége alatt – visszavont vagy felfüggesztett tanúsítványokhoz is elfogad a Szolgáltató. A kérelmet benyújtó személy azonossága ugyanúgy kerül ellenőrzésre, mint a még érvényes Tanúsítványhoz történő kulcscsere kérelem esetében (lásd: 3.3.1 pont), azzal a különbséggel, hogy az ott felsorolt lehetőségek közül nem mindegyiket tudja igénybe venni az Ügyfél.

3.4 Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási igénylés esetén

Szolgáltató tanúsítványvisszavonási és -felfüggesztési szolgáltatásokat egyaránt nyújt. A Szolgáltató visszavonás, illetve felfüggesztés esetén a visszavonással, illetve felfüggesztéssel érintett tanúsítvánnyal aláírt kérelmet nem fogadja el. A visszavonási-, illetve felfüggesztési igény benyújtóját (lásd 4.9.2 pont) a Szolgáltató legalább egy kódszóval (adott esetben az ügyfélmenüben korábban megadott kérdés-válasszal), vagy felhasználóneve és jelszava megadásával azonosítja. Amennyiben ezen azonosítás nem vezet eredményre, a Szolgáltató a személyes azonosító adatok megadásával is azonosíthatja az Igénylőt.

DV SSL tanúsítvány esetén a felfüggesztés nem értelmezett.

4 Tanúsítvány életciklus követelmények

A tanúsítvány életciklusa a tanúsítvány kiadásától annak lejártáig vagy visszavonásáig terjed. Ezen időtartamban van lehetőség a tanúsítvány felfüggesztésére (kivéve DV SSL), (újra) aktiválásra (kivéve DV SSL tanúsítvány), illetve amennyiben adott Szolgáltatás keretében elérhető, a tanúsítvány módosítására (kivéve DV SSL) vagy a hozzá tartozó kulcsok cseréjére (kivéve DV SSL), továbbá a kulcsletét (kivéve DV SSL), és kulcshelyreállítás (kivéve DV SSL), szolgáltatás igénybevételére.

4.1 Tanúsítványigénylés

Minden új kliens oldali authentikációs és titkosító végfelhasználói tanúsítvány kibocsátásához az Igénylő által a Szolgáltató Regisztrációs Egységéhez (lásd: 1.3.2 pont) előzőleg eljuttatott Tanúsítványigénylés szükséges. Tanúsítványigénylés kezdeményezéséhez az Igénylőnek egy alkalommal Ügyfélmenü regisztrációt kell végeznie, hogy létrejöjjön saját Ügyfélmenüje. Tanúsítványigénylés az Ügyfélmenüben kezdeményezhető, kivéve az ÁSZF-ben [8.] meghatározott szolgáltatáscsomagok megrendelése esetén, mely esetben a csomag elektronikus megrendelő űrlapjának kitöltése és elküldése tekinthető az Ügyfélmenü regisztráció és a tanúsítványigénylés kezdeményezésének. Ebben az esetben a megrendelő űrlapon megadott adatok alapján Szolgáltató Központi Regisztrációs Egysége végzi el Igénylő számára az Ügyfélmenü regisztrációt és rögzíti a tanúsítványigényléshez szükséges adatokat. A tanúsítványigénylés állapotát Igénylő az Ügyfélmenüben nyomon kísérheti.

Ügyfélmenüt minden esetben természetes személy hozhat létre. Amennyiben a tanúsítványban (pl. authentikációs) a természetes személy mellett egyéb adat – jogi személy/egyéb szervezet stb. – feltüntetésre kerül, akkor ezen Szervezetregisztrációt az Ügyfélmenü hozzáféréssel rendelkező természetes személy hozhat létre, az Ügyfélmenübe saját felhasználó nevével és jelszavával bejelentkezve.

Az Ügyfélmenü regisztráció és a tanúsítványigénylés fent leírt módjaitól Ügyféllel történő külön megállapodás alapján Szolgáltató eltérhet (pl. tömeges tanúsítványigénylés esetén).

A tanúsítványigénylési folyamat során a Szolgáltató az Ügyfélmenü regisztrációkor és a tanúsítványigénylés során megadott adatok alapján elkészíti és elektronikus formában eljuttatja Igénylőhöz az igényelt tanúsítvány kiadására vonatkozó Szolgáltatási Szerződést és - amennyiben a tanúsítvány alanyaként jogi személy/egyéb szervezet is feltüntetésre kerül és amennyiben értelmezett - a szerződés mellékletét képző nyilatkozatot. A Szolgáltatási szerződést az Igénylőnek és - amennyiben van - a szerződés mellékletét képző nyilatkozatot a jogi személy/egyéb szervezet képviselőjének/meghatalmazottjának a 4.2.1 pontban foglaltak szerint kell aláírnia. A tanúsítványigénylés a Szolgáltatási Szerződés érvényes aláírásával tekinthető teljesnek és hitelesnek. A Szolgáltatási Szerződés tartalmazza az Igénylő és Előfizető nyilatkozatát arra vonatkozóan, hogy a kötelezettségeiket megismerték és azok betartását vállalják. A Szolgáltató a Szolgáltatási Szerződést nem írja külön alá, a Szolgáltatási Szerződés elfogadását a tanúsítványkibocsátással jelzi.

DV SSL tanúsítvány esetén külön Szolgáltatási Szerződés aláírására nem kerül sor, a szerződéses feltételek elfogadása az Ügyfél által a rendelés folyamata során történik.

A megfelelően aláírt és a Szolgáltató által elfogadott Szolgáltatási Szerződést (amennyiben értelmezett), valamint a szerződés alapján kibocsátott tanúsítvány kiadásával összefüggő adatokat a Hitelesítési Rendnek megfelelően a tanúsítvány érvényességének végétől számított 10 (tíz) évig, vagy jogvita esetén a jogvita jogerős lezárásáig őrzi meg a Szolgáltató az 5.5 fejezetben foglaltak szerint.

A jelen Szolgáltatási Szabályzatban megadott feltételekkel és módon kizárólag a jelen Szolgáltatási szabályzatban meghatározott tanúsítványok igényelhetők. A Szolgáltató netlock.hu címen elérhető nyilvános weboldalán közérthető írásos tájékoztatást nyújt:

- a tanúsítványok alkalmazhatóságáról (lásd 1.4 pontban foglaltakat);
- a szolgáltatással kapcsolatos üzleti és jogi tudnivalókról (lásd 9 fejezetben foglaltakat);
- a Szolgáltatási Szerződés megkötésének feltételeiről;
- a felek jogairól és kötelezettségeiről;

- a Szolgáltató Általános Szerződési Feltételeinek (ÁSZF) [8.] a Tanúsítványkibocsátási szolgáltatásra vonatkozó részeiről;
- a magánkulcs használatával kapcsolatosan szükséges biztonsági intézkedésekről;
- az Ügyféleszköz használatáról, amennyiben az Igénylő ezt a Szolgáltatótól szerzi be.

A Szolgáltatási Szerződés megkötését követően a weboldalon közzétett mindenkor hatályos Szolgáltatási Szabályzatot vagy annak egyértelmű azonosítóját a Szolgáltató eljuttatja Igénylő részére e-mailben, mely a vonatkozó jogi szabályozás [5.] értelmében tartós adathordozónak minősül.

4.1.1 Ki nyújthat be tanúsítványigénylést?

Tanúsítványigénylést olyan természetes személyek nyújthatnak be a Szolgáltató Regisztrációs egységének, akik rendelkeznek Ügyfélmenü regisztrációval, beleértve a DV SSL igénylésére vonatkozó regisztrációt is. A Szolgáltató honlapján feltüntetésre került szolgáltatáscsomagok megrendelése esetén a tanúsítványigénylés kezdeményezhető előzetes Ügyfélmenü regisztráció nélkül is.

Szolgáltató kockázatlistát kezelhet azon személyekről, akik esetében a tanúsítványigényléssel kapcsolatos kockázatokat tart nyilván, valamint külső adatforrásokat is felhasználhat kockázatértékeléshez. Szolgáltató a kockázatértékelés alapján visszautasíthatja a tanúsítványigényléseket.

Az igényelt végfelhasználói tanúsítványok Alanyának tartalma (tanúsítványprofil) szerint az egyes tanúsítványokat az alábbi szereplők igényelhetik:

TANÚSÍTVÁNY PROFIL	IGÉNYLŐ
SZEMÉLYES (7.1 pont, 2 alpont)	A tanúsítvány Alanyaként megjelölt természetes személy saját maga részére
MUNKATÁRSI (7.1 pont, 3 alpont)	A tanúsítvány Alanyaként megjelölt - természetes személy saját maga részére, megjelölve, hogy egy adott jogi személyhez/egyéb szervezethez tartozik - A jogi személy/egyéb szervezet képviselője, megjelölve a természetes személyt, akinek részére kéri a tanúsítványt.
ÜGYVÉDI (7.1 pont, 4 alpont)	A tanúsítvány Alanyaként megjelölt természetes személy saját maga részére, amennyiben rendelkezik a NETLOCK Minősített Szolgáltatási Szabályzat szerinti érvényes minősített ügyvédi aláíró tanúsítvánnyal vagy igénylésük párhuzamosan zajlik.
DV SSL (7.1 pont, 5 alpont)	A tanúsítvány Alanyaként megjelölt domain név felett kontrollal rendelkező természetes személy.

4.1.2 Az igénylés folyamata és a résztvevők felelőssége

Tanúsítványigénylést a 4.1 pontban részletezett személyek az alábbi módokon nyújthatnak be:

- a Szolgáltató weblapján keresztül elérhető Ügyfélmenübe bejelentkezve
- authentikációs és titkosító tanúsítvány esetén elektronikus megrendelő űrlap kitöltésével és elküldésével
- a Szolgáltató és az Előfizető előzetes megállapodása alapján egyéb módon (pl. papír alapú nyomtatvány, adatösszesítő űrlap stb. kitöltésével), kivéve DV SSL esetén.

A tanúsítványigénylést megelőző Ügyfélmenü regisztráció és a tanúsítványigénylési eljárás részben automatizált folyamatok, részben pedig humán beavatkozással zajlanak. Az ezek során az Igénylő

részéről megtenni szükséges lépéseket részletesen a Szolgáltató weboldaláról letölthető útmutatók tartalmazzák.

Authentikációs és titkosító tanúsítvány esetén a természetes személy Ügyfélmenü regisztrációja során az alábbi adatokat rögzíti és megőrzi informatikai rendszerében a Szolgáltató:

- név (kötelező);
- ország (kötelező);
- város (kötelező);
- utca, házszám (opcionális);
- irányítószám (opcionális);
- telefon/fax (kötelező)
- email cím (kötelező);
- bejelentkező név (kötelező);
- jelszó (kötelező);
- azonosító kérdés és válasz (opcionális);
- jelszó emlékeztető (opcionális).

Authentikációs és titkosító tanúsítvány esetén, amennyiben a tanúsítványban jogi személy/egyéb szervezet is feltüntetésre kerül, az Ügyfélmenü regisztráció során a Szolgáltató informatikai rendszerében az alábbi adatokat rögzíti és őrzi meg:

- szervezet neve (kötelező);
- ország (kötelező);
- város (kötelező);
- utca, házszám (opcionális);
- irányítószám (opcionális);
- telefon/fax (opcionális);
- email cím (kötelező);

DV SSL tanúsítvány esetén a Szolgáltató informatikai rendszerében az alábbi adatokat rögzíti és őrzi meg:

- az ügyfél által megadott e-mail cím (kötelező)
- adószám (kötelező)
- számlázási név (kötelező)
- irányítószám (kötelező)
- Város (kötelező)
- Utca, házszám, épület, emelet, ajtó (kötelező)
- kapcsolattartó neve (kötelező)
- e-mail címe (kötelező)
- telefonszám (opcionális)
- számlázási mód (kötelező)

Tanúsítványigénylés az igényelt tanúsítványprofil szerint az alábbi adatok benyújtásával kezdeményezhető.

TANÚSÍTVÁNY-PROFIL	BENYÚJTANDÓ ADATOK
SZEMÉLYES (7.1 pont, 2 alpont)	Az Igénylő természetes személy ● személyazonosító igazolványban szereplő családi és utóneve vagy utónevei; ● lakcímet igazoló hatósági igazolványában szereplő lakcíme vagy tartózkodási helye; ● telefon vagy fax száma (nem kötelező); ● saját email címe; ● számlázási adatok.

TANÚSÍTVÁNY-PROFIL	BENYÚJTANDÓ ADATOK
MUNKATÁRSI (7.1 pont, 3 alpont)	Az Igénylő természetes személy ● személyazonosító igazolványban szereplő családi és utóneve vagy utónevei; ● lakcímet igazoló hatósági igazolványában szereplő lakcíme vagy tartózkodási helye; ● telefon vagy fax száma (nem kötelező); ● saját email címe; a tanúsítvány Alanyaként feltüntetésre kerülő jogi személy/egyéb szervezet ● szervezetazonosító dokumentumban szereplő neve; ● szervezetazonosító dokumentumban szereplő székhelyének címe; ● szervezeti egységének megnevezése (nem kötelező megadni); ● adószáma; az Előfizető számlázási adatai.
ÜGYVÉDI (7.1 pont, 4 alpont)	Az Igénylő ügyvéd ● személyazonosító igazolványban szereplő családi és utóneve vagy utónevei; ● lakcímet igazoló hatósági igazolványában szereplő lakcíme vagy tartózkodási helye; ● saját email címe; ● telefon vagy fax száma (nem kötelező); ● Kamarai Azonosító Száma (KASZ); az Igénylő egyéni ügyvéd vagy az Igénylő ügyvéd ügyvédi irodájának ● Magyar Ügyvédi Kamaránál bejegyzett neve; ● Magyar Ügyvédi Kamaránál bejegyzett székhelyének címe; ● Ügyvédi irodán belüli szervezeti egység megnevezése (nem kötelező megadni); az Előfizető számlázási adatai.
DV SSL (7.1 pont, 5 alpont)	● A tanúsítvány Alanyaként feltüntetésre kerülő domain név; ● tanúsítványkérelem fájl (Certificate Signing Request - CSR); ● számlázási adatok.

A Tanúsítvány Alanyaként feltüntetett tartalomtól függetlenül – kivéve DV SSL - az Igénylőnek meg kell adnia

- a tanúsítvány tervezett felhasználási célját,
- az Igénylő típusát (magánszemély, vállalat, kormányzat vagy egyéb),
- valamint a 4.2.1 pontban leírtak szerint hitelesített Szolgáltatási Szerződést át kell adnia a Szolgáltatónak.

Az Ügyfél a Szolgáltatási Szerződés aláírásával – kivéve DV SSL - nyilatkozik az alábbiakról:

- a szerződésben szereplő személyes adatai a valóságnak megfelelőek és azokat önkéntesen adta meg a Szolgáltatónak;
- megismerte, érti és elfogadja a Szolgáltató Általános Szerződési Feltételeit [8.], az igényelt tanúsítványra vonatkozó jelen Szolgáltatási szabályzatot és a NETLOCK Nem Minősített Hitelesítési rendet, melyek elérhetők a Szolgáltató weboldalán;
- a szerződéskötést megelőzően a szerződés megkötéséhez szükséges tájékoztatást megkapta, és a tanúsítványra vonatkozó korlátozásokat (pl. szolgáltatói felelősségvállalás,) megismerte;
- felhatalmazza Szolgáltatót a Szolgáltatási szerződésben megjelölt tanúsítvány kibocsátására.

Az Ügyfél a Szolgáltatási szerződés aláírásával továbbá igazolja, hogy

- hozzájárul az Ügyfélmenü regisztráció és az Igénylés során megadott személyes és szervezeti adatok kezeléséhez;
- kéri a szerződés szerinti nyilvános kulcs hitelesítését és a tanúsítvány nyilvános tanúsítványtárba való felvételét, tárolását és kezelését;

- ismeri a szerződő felek jogait és kötelezettségeit.

Amennyiben a tanúsítvány Alanyaként jogi személy/egyéb szervezet feltüntetésre kerül, a jogi személy/egyéb szervezet képviselőjének vagy meghatalmazottjának mint Előfizetőnek a Szolgáltatási Szerződésben, vagy ha a Szolgáltatási Szerződéshez külön került csatolásra, a Szolgáltatási Szerződéshez tartozó mellékletben kell nyilatkozik az alábbiakról:

- a tanúsítványigénylés tudtával és hozzájárulásával történik;
- meghatalmazza Igénylőt, hogy a tanúsítvány igénylésével, illetve felfüggesztésével, visszavonásával, aktiválásával, megújításával kapcsolatban eljárjon;
- vállalja a szerződés kapcsán felmerülő szolgáltatási díjak megfizetését;
- megismerte, érti és elfogadja az ÁSZF-et [8.], az igényelt tanúsítványra vonatkozó jelen Szolgáltatási szabályzatot és a NETLOCK Nem Minősített Hitelesítési rendet, melyek elérhetők a Szolgáltató weboldalán.

Az Igénylőnek az Igénylésben megadott adatok valódiságát a 3 fejezetben megadott dokumentumokkal és módon kell igazolnia.

A Szolgáltató a kapcsolattartáshoz szükséges adatokat az Ügyfélmenü regisztráció során rögzíti. A tanúsítványigénylések kezeléséért a Szolgáltató Regisztrációs Egységének munkatársai felelősek.

4.2 Tanúsítványigénylések feldolgozása

Az Igénylés beérkezését a Szolgáltató elektronikus úton küldött automatikus válaszlevélben igazolja vissza az Igénylés során megadott email címre. Az automatikus visszaigazolás nem jelenti az Igénylés Szolgáltató általi elfogadását, mindössze arról tájékoztatja Ügyfelet, hogy az Igénylést Szolgáltató kézhez vette és megkezdi annak feldolgozását.

DV SSL tanúsítvány esetén a megrendelés fogadásáról szóló automatikus válaszlevél nem jelenti az Igénylés Szolgáltató általi elfogadását, mindössze arról tájékoztatja az Ügyfelet, hogy a sikeres tanúsítványkibocsátáshoz kapcsolódóan az Ügyfélnek még milyen lépéseket kell megtennie.

A tanúsítványigénylések feldolgozása során az Ügyfélmenü regisztrációkor és a tanúsítványigényléskor vagy a szolgáltatáscsomagra vonatkozó elektronikus megrendelő űrlap kitöltésével megadott személyes és szervezeti adatok ellenőrzését, az Igénylő azonosítását és eljárási jogának ellenőrzését, valamint – az Igénylő erre vonatkozó jelzése esetén - a kulcspár generálását és a Szolgáltatási Szerződés elkészítését a Regisztrációs Egység bizalmi munkatársai végzik.

A Szolgáltató az Igénylés során ellenőrzi a megadott email cím valódiságát is, innen kéri a tanúsítványigénylés megerősítését, valamint utasításokat és információkat továbbít ide, melyek Igénylő általi teljesítése és megismerése elengedhetetlen a tanúsítványigénylési eljárás lefolytatásához.

4.2.1 Azonosítás és hitelesítés

A Szolgáltató a 3 fejezetben írtak szerint ellenőrzi Igénylő személyazonosságát, eljárási jogát, valamint az Igénylésben szereplő adatok megfelelőségét és valódiságát.

Amennyiben az Igénylőt és a tanúsítványigénylésben megadott adatokat Szolgáltató korábban *még nem* ellenőrizte, vagy a legutóbbi ellenőrzést a tanúsítványigényléskor a Szolgáltató már nem tekinti érvényesnek az azonosítás és ellenőrzés a 3.2 pontban foglaltak szerint történik.

Amennyiben az Igénylőt és a tanúsítványigénylésben megadott adatokat Szolgáltató korábban *már ellenőrizte* a 3.2 pontban foglaltak szerint és az ellenőrzést a tanúsítványigényléskor a Szolgáltató még érvényesnek tekinti, az azonosítás és ellenőrzés a 3.3 pontban meghatározottak szerint történik.

A Szolgáltatási Szerződés Ügyfél részéről történő hitelesítése a 3.2 pontban, a tanúsítvány hitelesítési osztályainál részletezett módok valamelyik végezhető el. A Szolgáltatási Szerződés aláírása minden tanúsítványkibocsátást megelőzően szükséges, kivéve DV SSL tanúsítvány. Különösen indokolt esetben, ha a tanúsítványkibocsátás óta nem telt el hosszú idő, az adatok nem változtak, ugyanakkor új tanúsítványkibocsátás jogszabályi vagy egyéb, a szervezet életében bekövetkező változás miatt

szükséges, a Szolgáltató a lentiektől eltérő Szolgáltatási Szerződés hitelesítési módot is előírhat/megállapíthat – ennek tényét és szükségességét a Szolgáltató minden esetben külön jegyzőkönyvvel igazolja.

A Szolgáltatási Szerződést és – amennyiben értelmezett- az ahhoz tartozó mellékletet az alábbiak szerint kell hitelesíteni (papír alapon és elektronikus formában – a lentebb szereplő tanúsítványok elfogadására vonatkozó kitétellel - egyaránt):

- Személyes authentikációs, illetve titkosító tanúsítvány esetén a természetes személy Alanynak,
- Szervezeti authentikációs, illetve titkosító tanúsítvány esetén a szervezet képviselőjének vagy meghatalmazottjának,
- Authentikációs vagy titkosító munkatársi tanúsítvány esetén a tanúsítványban feltüntetésre került természetes személy Alanynak és a szervezet képviselőjének, vagy amennyiben a természetes személy Alany meghatalmazással rendelkezik, akkor csak neki.
- Ügyvédi tanúsítvány esetén a természetes személy ügyvédnek.

Természetes személy Alany esetén a természetes személy nem adhat meghatalmazást másnak a Szolgáltatási Szerződés aláírására.

Amennyiben a Szolgáltatási Szerződés és – amennyiben értelmezett - az ahhoz tartozó melléklet aláírása elektronikusan történik, a Szolgáltató az alábbi aláírásokat és bélyegzőket fogadja el:

- Személyes authentikációs, illetve titkosító tanúsítvány esetén fokozott biztonságú elektronikus aláírással ellátva, melynek tanúsítványát egy az Európai Unió Bizalmi listáján szereplő kiadó adta ki, s melynek Alanya megegyezik az igényelt tanúsítvány Alanyaként feltüntetett személlyel.
- Szervezeti authentikációs és titkosító tanúsítvány igénylése esetén
    - fokozott biztonságú elektronikus bélyegzővel ellátva, melynek tanúsítványát egy az Európai Unió Bizalmi listáján szereplő kiadó adta ki, s melynek Alanya megegyezik az igényelt Tanúsítvány Alanyával; vagy
    - fokozott biztonságú elektronikus aláírással ellátva, melynek tanúsítványát egy az Európai Unió Bizalmi listáján szereplő kiadó adta ki, s melynek Alanyaként mind az igényelt Tanúsítvány Alanyaként feltüntetett jogi személy / egyéb szervezet, mind pedig annak szervezetazonosító dokumentum szerinti képviselője feltüntetésre került.
- munkatársi profilú authentikációs és titkosító tanúsítvány igénylése esetén
    - fokozott biztonságú elektronikus aláírással ellátva, melynek tanúsítványát egy az Európai Unió Bizalmi listáján szereplő kiadó adta ki, s melynek Alanya megegyezik az igényelt Tanúsítvány Alanyaként feltüntetett személlyel; *vagy*
    - fokozott biztonságú elektronikus bélyegzővel ellátva, melynek Tanúsítványát egy az Európai Unió Bizalmi listáján szereplő kiadó adta ki, s melynek Alanya megegyezik az igényelt Tanúsítvány Alanyaként feltüntetett jogi személlyel.

Az elektronikusan hitelesített Szolgáltatási Szerződést és – amennyiben értelmezett - mellékletét hitelesítésük után a kerelmek@netlock.hu címre kell Igénylőnek elküldenie.

A papír alapon saját kézzel aláírt szerződést – „C” hitelesítési osztályú tanúsítvány esetén - digitalizálva szintén a kerelmek@netlock.hu címre kell Igénylőnek elküldenie, vagy személyesen is átadhatja azt a Szolgáltató bizalmi munkatársának a Szolgáltató weboldalán közzétett ügyfélszolgálati helyen és időben, illetve postai úton is eljuttathatja a Szolgáltató 1.1.2 pontban meghatározott postai címére. „B” hitelesítési osztályú tanúsítvány esetén a Szolgáltatási Szerződést 3.2 pontban meghatározott módon lehet hitelesíteni és a Szolgáltató részére visszajuttatni

4.2.2 .Tanúsítványigénylések elfogadása vagy visszautasítása

A Szolgáltató az authentikációs és titkosító tanúsítványokra vonatkozó tanúsítványigénylés feldolgozása során dönt annak elfogadásáról vagy visszautasításáról. A DV SSL tanúsítványok kibocsátása humán közreműködés nélkül történik, amennyiben a DV SSL tanúsítvány kiadásának technikai feltételei fennállnak, illetve az ellenőrzés sikeres volt, akkor az automatikusan kibocsátásra kerül.

A tanúsítványigénylés elfogadásának feltételei authentikációs és titkosító tanúsítvány:

- Igénylő sikeres személyazonosítása;
- a tanúsítvány Alanyaként feltüntetésre kerülő adatok valódiságának ellenőrzése sikeres és az adatok valódiak;
- a Szolgáltatási Szerződés megfelelő aláírása.

Amennyiben a személyazonosítás és az adatok ellenőrzése sikeresen megtörténik, valamint Szolgáltató elfogadja az aláírt Szolgáltatási Szerződést, a tanúsítványigénylés a Szolgáltató által elfogadottnak tekinthető.

Tanúsítványigénylés elfogadása után Szolgáltató haladéktalanul gondoskodik a tanúsítvány kibocsátásáról. A Szolgáltató és az Előfizető erre vonatkozó megállapodását kivéve a díjfizetés az ÁSZF-ben [8.] meghatározott módon a tanúsítvány kibocsátása előtt esedékes. DV SSL tanúsítvány esetén a díjfizetésnek mindig meg kell előznie a tanúsítvány kibocsátását.

Authentikációs és titkosító tanúsítvány esetén, amennyiben az magánkulcs generálása az igénylés, megrendelés vagy szolgáltatói ajánlat alapján Ügyféleszközre történik, a Szolgáltató a kulcsgenerálást követően az Ügyfél részére összeállít egy csomagot, mely tartalmazza

- az Ügyféleszközt és amennyiben használatához szükséges, az Ügyféleszköz-olvasót;
- az Ügyféleszköz első használatbavételéhez szükséges tájékoztatót.

A csomag (Ügyféleszköz) elkészültéről a Szolgáltató az Igényléskor megadott email címen értesíti az Ügyfelet, melyet ezután az Igénylő vagy Átvevő az e-mailben megadott helyen és módon átvehet.

Amennyiben az adatok ellenőrzése - ideértve az email cím ellenőrzését is -, vagy az Igénylő személyazonosítása sikertelen, és ennek oka, hogy az ellenőrzéshez és azonosításhoz a Szolgáltatónak nem áll rendelkezésre minden szükséges adat, vagy a rendelkezésre álló adat nem hiteles, a Szolgáltató Igénylőt hiánypótlásra szólítja fel.

Amennyiben az adatok ellenőrzése - ideértve az email cím ellenőrzését is - vagy az Igénylő személyazonosítása sikertelen, és ennek oka, hogy az Igénylő nem jogosult az adott tanúsítványigénylés beadására és/vagy a hiánypótlás a felszólítást követő 30 naptári napon belül nem történik meg, a Szolgáltató a tanúsítványkérelmet visszautasítja.

További körülmények, melyek a tanúsítványigénylés visszautasítását vagy törlését eredményezhetik:

- a szolgáltatás díjának kiegyenlítése nem történik;
- az Ügyféleszközt az arra jogosult nem veszi át az első értesítést követő 30 napon belül;
- az adatok hitelesítése céljából bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel;
- a tanúsítványban szereplő és/vagy az Igénylő személy és a tanúsítványban szereplő szervezet kapcsolata nem egyértelmű;
- a személy és/vagy szervezet kiléte nem állapítható meg minden kétséget kizáróan;
- az szervezet képviselőjének felhatalmazása a tanúsítvány kibocsátásának kérésére nem egyértelmű;
- az Igénylő személy és a tanúsítványban szereplő szervezet képviselője nem járul hozzá másolat készítéséhez az adatok ellenőrzésére és hitelesítésére bekért dokumentumairól és azokat nem mutatja be személyesen a Szolgáltató bizalmi munkatársainak sem.

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

A Szolgáltató CAA ellenőrzést nem végez.

Igénylő a tanúsítványigénylés állapotát az Ügyfélmenüben saját regisztrált felhasználónevével és jelszavával bejelentkezve nyomon követheti.

4.2.3 A tanúsítványigénylés feldolgozásának időtartama

A Tanúsítványigénylés akkor tekinthető feldolgozottnak, ha a tanúsítvány kibocsátásra került.

A Szolgáltató authentikációs és titkosító tanúsítvány esetén a tanúsítványigénylés kezdeményezését visszaigazoló automatikus üzenet elküldésétől számított 10 munkanapon belül feldolgozza a tanúsítványigénylést. A Szolgáltató a tanúsítványt a tanúsítványkibocsátásához szükséges feltételek teljesülése esetén alapesetben 3-5 munkanapon belül bocsátja ki.

Hiánypótlási felszólítás esetén a hiánypótlás időtartama nem számít be a tanúsítványigénylés feldolgozásának határidejébe.

DV SSL tanúsítvány esetén a tanúsítványkibocsátás a sikeres igénylést és ellenőrzést, valamint a fizetést követően azonnali.

4.3 Tanúsítvány kibocsátása

Végfelhasználói tanúsítványok kibocsátása

A tanúsítvány kibocsátásának időpontja az az időpont, amikor a Szolgáltató az aláírt tanúsítványt elérhetővé teszi a tanúsítványtárban. A tanúsítványt kizárólag az Igénylés feldolgozása során ellenőrzött adatokkal adhatja ki a Szolgáltató.

A Szolgáltató eljárhat úgy is, hogy a szolgáltatási díj kiegyenlítése előtt – kivéve DV SSL tanúsítvány - előállítja és kibocsátja a tanúsítványt. Ebben az esetben a Szolgáltató meghatározza, hogy mely időpontig kell Ügyfélnek a szolgáltatás díját kiegyenlítenie.

Amennyiben a tanúsítványhoz tartozó nyilvános kulcs magánkulcs párját a Szolgáltató Ügyféleszközre generálta, az Ügyféleszközt tartalmazó csomagot a Szolgáltató kizárólag Igénylőnek vagy Átvevőnek adhatja át.

Ügyféleszközre generált magánkulcs esetén a Végfelhasználónak alapesetben a tanúsítványt rá kell töltenie az Ügyféleszközre a Szolgáltató weboldaláról letölthető útmutató alapján. Ügyféleszköz átvétele esetén a Szolgáltató a tanúsítványt abban az esetben bocsátja ki, amennyiben kétséget kizáróan meggyőződött arról, hogy az Ügyféleszközt az arra jogosult vette át. Az Ügyféleszközön a Szolgáltató Igénylővel történő előzetes megállapodás alapján annak átvétele előtt elhelyezheti a kibocsátott tanúsítványt felfüggesztett állapotban, melyet a csomag átvételét követően Végfelhasználónak haladéktalanul, de legkésőbb a 4.9.13 pontban meghatározott időn belül aktiválnia kell. Az aktiválás során a Szolgáltató megbizonyosodik arról, hogy a Végfelhasználó birtokában van az Ügyféleszköz. A végleges használatbavétel ezt követően történhet meg.

Szolgáltatói tanúsítványok kibocsátása

A szolgáltatói tanúsítványok kiadása (gyökér/köztes kiadói tanúsítvány) a Szolgáltató a Biztonsági Szabályzatában meghatározott módon, kétszemélyes kontroll mellett jegyzőkönyvezetten történik. A szolgáltatói tanúsítványokat a Szolgáltató a 2.2 pontban meghatározott módon is időtartam alatt tesz közzé.

4.3.1 A Szolgáltató tevékenysége a tanúsítvány kibocsátás során

A Szolgáltatási Szerződés aláírását és az ahhoz kapcsolódó ellenőrzések sikeres lezárultát, valamint - a Szolgáltató és az Előfizető erre vonatkozó megállapodását kivéve – a szolgáltatás díjának kiegyenlítését követően a Szolgáltató az informatikai rendszerében a korábban létrehozott tanúsítványigénylés alapján létrehozza, saját szolgáltatói tanúsítványával hitelesíti, majd Végfelhasználó számára elérhetővé teszi a tanúsítványt.

DV SSL tanúsítvány esetén a Szolgáltató a domain feletti kontrollt (lásd 3.2.2.3), valamint a fizetés megtörténtét ellenőrzi. Amennyiben mindkettő sikeres, a tanúsítvány automaikusan kibocsátásra kerül.

A kibocsátás során a Szolgáltató biztosítja a tanúsítványkibocsátás biztonságát, megakadályozva a tanúsítványok hamisíthatóságát.

Amennyiben a magánkulcsot a Szolgáltató generálta Ügyféleszközre, a tanúsítvány kibocsátása előtt a Szolgáltató megbizonyosodik arról is, hogy az Ügyféleszközt az arra jogosult átvette - ennek igazolására az Ügyfélnek átvételi elismervényt kell aláírnia.

Amennyiben a magánkulcsot a Szolgáltató generálta az Ügyféleszközre és az Ügyféleszközre a tanúsítványt is felfüggesztett állapotban feltöltötte, a tanúsítvány aktiválására csak abban az esetben kerülhet sor, amennyiben Szolgáltató megbizonyosodik arról, hogy az Ügyféleszköz a Végfelhasználónál van.

4.3.2 Végfelhasználó értesítése a tanúsítvány kibocsátásáról

A tanúsítvány kibocsátásáról a Szolgáltató a tanúsítványban szereplő e-mail címen értesíti Végfelhasználót.

Végfelhasználó a tanúsítványt a kibocsátásáról értesítő e-mail elküldését követően az Ügyfélmenübe való bejelentkezés után töltheti le és a Szolgáltató weboldaláról letölthető útmutató alapján telepítheti vagy aktiválhatja. Amennyiben a Szolgáltató az Ügyféleszközre a tanúsítványt előzetesen feltöltötte, a tanúsítvány külön telepítésére nincs szükség, viszont aktiválni szükséges a Szolgáltatónak.

4.4 Tanúsítvány elfogadása

Authetnikációs és titkosító tanúsítvány esetén magánkulcs használatba vétele előtt Ügyfélnek kötelessége ellenőrizni a tanúsítványban feltüntetett adatok helyességét. A tanúsítvány adatait a Végfelhasználó az Ügyfélmenübe bejelentkezve tekintheti meg. Amennyiben bármilyen rendellenességet talál, a magánkulcsot nem használhatja fel, hanem kifogását azonnal jeleznie kell a Szolgáltató Ügyfélszolgálata felé vagy intézkednie kell a tanúsítvány visszavonása/felfüggesztése érdekében. DV SSL tanúsítvány esetén az Ügyfélnek kötelessége ellenőrizni a tanúsítványban feltüntetett domain helyességét.

Amennyiben Ügyfél a tanúsítvány kibocsátását követő 5 munkanapon belül nem jelzi a Szolgáltatónak a tanúsítvánnyal kapcsolatos kifogást vagy nem kezdeményezi annak visszavonását vagy felfüggesztését, a tanúsítvány az Ügyfél által automatikusan elfogadottnak tekintendő.

4.4.1 A tanúsítványelfogadás módja

A tanúsítvány és a hozzá tartozó nyilvános kulcshoz tartozó magánkulcs elfogadottnak tekintendő, ha Ügyfél az Ügyféleszközt és a magánkulcsot és/vagy a tanúsítványt átvette és 5 munkanapon belül nem jelzi a Szolgáltatónak a tanúsítvánnyal kapcsolatos kifogást vagy nem kezdeményezi annak visszavonását vagy felfüggesztését.

4.4.2 A tanúsítvány közzététele

A Szolgáltató közzéteszi a kiadott tanúsítványt nyilvános tanúsítványtárában, kivéve, ha a tanúsítvány Igénylője másként nem nyilatkozott. Igénylő ilyen nyilatkozatot a Szolgáltatási Szerződés aláírásakor, vagy a tanúsítványigénylés feldolgozása során e-mailben tehet a Szolgáltató Regisztrációs Egysége felé.

DV SSL tanúsítvány esetén a Szolgáltató nyilvános tanúsítványtárat nem működtet.

4.4.3 További szereplők értesítése a tanúsítvány kibocsátásról

A Szolgáltató a 4.3.2 pontban meghatározottakon túl további szereplőket a tanúsítvány kibocsátásáról külön nem értesít.

4.5 Kulcspár és tanúsítvány alkalmazhatósága

4.5.1 A magánkulcs és a tanúsítvány használata

A Tanúsítvány és a benne szereplő nyilvános kulcshoz tartozó magánkulcs a Tanúsítvány “KeyUsage” és “Extended KeyUsage” mezőjében megadott célokra használható a 7.1 fejezet 12 pontja szerint, az 1.4 fejezetben foglaltakkal is összhangban.

Egyéb megkötések a tanúsítvány használatával kapcsolatban:

- Amennyiben az authentikációs és titkosító tanúsítvány esetén a kulcsgenerálás Ügyféleszközre történt, Végfelhasználó a magánkulcsot kizárólag azon az Ügyféleszközön aktiválhatja és használhatja, melyre a kulcsot generálták.
- Amennyiben a kulcsgenerálás nem Ügyféleszközre történt, Végfelhasználó a magánkulcsot csak saját befolyása alatt álló eszközön aktiválhatja és használhatja.
- A magánkulcs a Végfelhasználó kizárólagos befolyása alatt kell, hogy álljon.
- Lejárt érvényességű, visszavont vagy felfüggesztett állapotú tanúsítvány és kapcsolódó kulcsok használata nem megengedett.
- Amennyiben a Végfelhasználó – nem Ügyféleszközre generált magánkulcs esetén - a magánkulcsról másolatot készít, akkor azt ugyanolyan gondossággal köteles kezelni, mint az eredeti példányt.
- Végfelhasználó azonnal köteles értesíteni a Szolgáltatót, amennyiben az alábbi esetek valamelyike bekövetkezik a tanúsítvány érvényességének vége előtt, és egyúttal köteles azonnal beszünteti a magánkulcs alkalmazását,
    - a magánkulcs elvesztése, ellopása, kompromittálódása
    - a magánkulcs feletti kizárólagos kontroll elvesztése, pl. az aktiválási adat kompromittálódása miatt
    - a tanúsítványban feltüntetett adatok pontatlansága vagy változása
- A végfelhasználói tanúsítványt aláíró szolgáltatói kulcs kompromittálódása esetén a Végfelhasználó azonnal köteles beszünteti a magánkulcs és a tanúsítvány alkalmazását.
- A Végfelhasználó a tanúsítványhoz tartozó magánkulcsot, illetve annak bármilyen másolatát a tanúsítvány érvényessége végén vagy visszavonása esetén visszaállíthatatlan módon törölni köteles.

4.5.2 Az Érintett felek nyilvános kulcs és tanúsítvány használata

A tanúsítvány felhasználása során a Szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az Érintett Felek megfelelő körültekintéssel járjanak el, a Szolgáltató szabályzataiban leírt követelményeknek megfelelően, különös tekintettel az alábbiakra:

- a nyilvános kulcsokat csak olyan felhasználás esetén fogadja el, amelyek összhangban vannak a Tanúsítvány “KeyUsage” és “Extended KeyUsage” mezőinek tartalmával;
- ellenőrizze a tanúsítvány érvényességét, visszavonási és felfüggesztési állapotát;
- vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítványban hivatkozott szabályzatokban szerepel.

Amennyiben az Érintett fél nem a Szolgáltató szabályzataiban leírtaknak megfelelően jár el, az ebből eredő károkért a Szolgáltató nem vállal felelősséget.

4.6 Tanúsítványmegújítás

A végfelhasználói tanúsítványok megújítására a kezdeti ellenőrzési (3.2 pont) lépések ismételt lefolytatása nélkül a jelen pontban leírt módon van lehetőség a megújítást megelőzően alkalmazott érvényességi idő megadásával.

DV SSL tanúsítvány esetén a megújítás nem értelmezett, helyette új tanúsítvány igénylése szükséges.

A megújított tanúsítvány érvényességének intervalluma alapesetben megegyezik az eredeti tanúsítvány érvényességének intervallumával, kivéve, amikor Szolgáltató saját hatáskörben dönt a tanúsítvány oly módon történő megújításáról, mely esetben az érvényesség vége pontosan megegyezik az eredeti tanúsítványban szereplő időponttal (technikai megújítás).

A tanúsítvány lejáratának közeledtéről – DV SSL tanúsítványt kivéve - minden esetben e-mail értesítést küld a Szolgáltató.

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

4.6.1 A tanúsítványmegújítás körülményei

Ügyfél Tanúsítványa megújítását az alábbi feltételek fennállása esetén igényelheti:

- a tanúsítvány érvényes (nem járt le és nincs felfüggesztve vagy visszavonva);
- a tanúsítvány lejárata legfeljebb 31 napon belül esedékes;
- a tanúsítványban szereplő nyilvános kulcs kriptográfiailag még biztonságosnak tekinthető és vélhetően az is marad a megújított tanúsítvány érvényességi ideje alatt is;
- a tanúsítványhoz tartozó magánkulcs nem kompromittálódott.

Szolgáltató a Tanúsítvány lejáratát megelőzően 30 nappal a tanúsítványban szereplő e-mail címre értesítést küld, melyben tájékoztatja Alanyt a tanúsítvány közelgő lejártáról és a tanúsítványmegújítás folyamatáról. A Szolgáltató dönthet úgy, hogy a tanúsítvány lejártát megelőzően többször értesíti az ügyfelet, az első értesítésnek azonban mindig a tanúsítvány lejártát megelőző 30 nappal meg kell történnie.

Szolgáltató saját hatáskörben az alábbi feltételek fennállása esetén kezdeményezheti végfelhasználói tanúsítvány megújítását:

- a tanúsítvány érvényes (nem járt le és nincs felfüggesztve vagy visszavonva);
- a tanúsítványt valamely külső körülmény (pl. jogszabályi vagy szabványkörnyezet változása) miatt az eredeti érvényesség lejárta előtt vissza kell vonni, de a visszavonás még nem történt meg;
- a megújítással és amennyiben szükséges a tanúsítványprofil módosításával biztosítható a tanúsítvány esetleges új feltételeknek való megfelelése;
- a tanúsítványban szereplő nyilvános kulcs kriptográfiailag még biztonságosnak tekinthető és vélhetően az is marad a megújított tanúsítvány érvényességi ideje alatt is.

4.6.2 Ki igényelheti a tanúsítványmegújítást?

A tanúsítványmegújítást az Igénylő az Ügyfélmenüben saját regisztrált felhasználónevével és jelszavával bejelentkezve kezdeményezhet. A megújítási eljárás lépéseit részletesen a Szolgáltató weboldaláról letölthető útmutató tartalmazza.

Igénylőn kívül a tanúsítvány megújítását saját hatáskörben a Szolgáltató is kezdeményezheti, melyről minden esetben értesítenie kell Ügyfelet.

4.6.3 A tanúsítványmegújítási igénylések feldolgozása

A tanúsítványmegújítási igénylés beérkezését a Szolgáltató elektronikus úton küldött automatikus válaszlevélben igazolja vissza a tanúsítványban szereplő email címre. Az automatikus visszaigazolás nem jelenti az Igénylés Szolgáltató általi elfogadását, mindössze arról tájékoztatja Ügyfelet, hogy az Igénylést kézhez vette és megkezdi annak ellenőrzését és feldolgozását.

Az Igénylő azonosítását és a megújítási igény teljességének és hitelességének ellenőrzését a Szolgáltató Regisztrációs Egységének munkatársai végzik. Sikeres azonosítás és a tanúsítványmegújítás feltételeinek (4.6.1 pont) fennállása esetén a Szolgáltató elfogadja a megújítási igényt és haladéktalanul gondoskodik az új Szolgáltatási szerződés elkészítéséről, a megújított tanúsítvány előállításáról, illetve az ÁSZF [8.] szerinti módon a szolgáltatás díjának bekéréséről.

A Szolgáltatási Szerződés aláírására megújítás esetén is szükség van. A Szolgáltatási Szerződést és - amennyiben van - mellékletét ugyanolyan módon kell hitelesíteni és a Szolgáltatóhoz eljuttatni, mint a tanúsítványigénylés esetén (lásd 4.2.1 pont).

Amennyiben valamely külső körülmény (pl. jogszabályi vagy szabványkörnyezet változása) miatt a Szolgáltató köteles egyes tanúsítványokat visszavonni eredeti érvényességük lejárta előtt, és a visszavonás megtörténte előtt saját hatáskörben kezdeményezi az érintett tanúsítványok megújítását (technikai megújítás), a Szolgáltató a Szolgáltatási Szerződés 4.2.1 pont szerinti hitelesítésétől eltekinthet. A Szolgáltató ebben az esetben is értesíti az Ügyfelet, és csak az Ügyfél erre vonatkozó kifejezett rendelkezése esetén tekint el a megújítástól. Ebben az esetben a Szolgáltató külön jegyzőkönyvet vesz fel a megújítás tényéről, és a megújítással érintett tanúsítvány adatairól.

Megújítás esetén a Szolgáltatási Szerződés aláírásával Igénylő az alábbiakról is nyilatkozik:

- a tanúsítványkibocsátáskor ellenőrzött adatok változatlanságáról;
- arról, hogy az adatok valódiságát a tanúsítványigényléskor igazoló dokumentumok még érvényesek;
- arról, hogy nincs tudomása a tanúsítványban szereplő nyilvános kulcshoz tartozó magánkulcs kompromittálódásáról.

Amennyiben az eredeti tanúsítvány kibocsátása előtt ellenőrzött adatokban a megújítást megelőzően változás történt, a megváltozott adatok ellenőrzését 3.2 pontban foglaltak szerint kell elvégezni. Ebben az esetben a Szolgáltatási Szerződésbe foglalt adatváltozatlansági nyilatkozat csak a meg nem változott adatokra vonatkozik.

A tanúsítványmegújítási igényt Szolgáltató az alábbi körülmények fennállása esetén elutasíthatja:

- a megújítási igény Szolgáltatóhoz való elküldésekor Igénylő nem jelezte, hogy a tanúsítvány kibocsátásakor ellenőrzött adatok változtak;
- Igénylő a megváltozott adatok valódiságát nem igazolja megfelelően a tanúsítvány érvényességének lejártáig;
- a tanúsítványigénylés visszautasítását eredményező bármely a megújításra is alkalmazható körülmény fennállása;
- az Ügyfél a szolgáltatási díjjal elmaradásban van;
- az érintett tanúsítvány nem azonosítható egyértelműen.

Amennyiben a megváltozott adatok ellenőrzése és/vagy az Igénylő személyazonosítása és/vagy eljárási jogának ellenőrzése sikertelen, és ennek oka, hogy az ellenőrzéshez és azonosításhoz a Szolgáltatónak nem áll rendelkezésre minden adat, vagy a rendelkezésre álló adat nem hiteles, a Szolgáltató Igénylőt hiánypótlásra szólítja fel.

Amennyiben az ellenőrzés és azonosítás sikertelen, és ennek oka, hogy az Igénylő nem jogosult az adott Tanúsítványigénylés beadására és/vagy a hiánypótlás a felszólítást követő 30 naptári napon belül nem történik meg, a Szolgáltató a tanúsítványkérelmet visszautasíthatja.

Szolgáltató egyéb indokkal - pl. jogszabályi vagy szabványkörnyezet változása esetén - is megtagadhatja a Tanúsítvány megújítását, amennyiben ezt írásban indokolja.

A megújítási igény visszautasítása esetén Ügyfél új tanúsítvány igénylésével tarthatja fenn a szolgáltatás igénybevételének folytonosságát abban az esetben, ha korábbi tanúsítványra vonatkozó díjtartozás nem áll fenn.

A Szolgáltató a tanúsítványmegújítási igénylést a 4.2.3 pontban meghatározott időtartam alatt dolgozza fel.

Amennyiben a fenti feltételek nem teljesülnek, a késedelemmel egyenlő mértékben növekszik a feldolgozás időtartama. Hiánypótlási felszólítás esetén a hiánypótlás időtartama nem számít be a tanúsítványigénylés feldolgozásának határidejébe.

A megújított tanúsítványt a feltételek fennállása esetén a Szolgáltató az eredeti tanúsítvány érvényességének lejáratát megelőzően, de – a Szolgáltató és az Igénylő/Előfizető erre vonatkozó megállapodását kivéve - legfeljebb 3 munkanappal lejárata előtt bocsájtja ki.

Szolgáltató nem vállal felelősséget azért, ha a megújított tanúsítvány nem kerül kibocsátásra az eredeti tanúsítvány lejárta előtt és ezzel a szolgáltatás folytonossága megszakad, abban az esetben, ha ehhez az Ügyfél mulasztása vagy késedelme vezetett.

4.6.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A Szolgáltatónak megújított tanúsítvány kibocsátása előtt ugyanolyan tájékoztatási kötelezettsége van a kibocsátandó tanúsítvánnyal kapcsolatban, mint az eredeti tanúsítvány kibocsátását megelőzően (4.1 pont). Végfelhasználó (Ügyfél) értesítésére a megújított tanúsítvány kibocsátásáról a 4.3.2 pont rendelkezései alkalmazandók.

4.6.5 A megújított tanúsítvány elfogadása

A megújított tanúsítvány elfogadására a 4.4.1 pont rendelkezései alkalmazandók.

4.6.6 A megújított tanúsítvány közzététele

A megújított tanúsítvány közzétételére a 4.4.2 pontban foglalt rendelkezések az alkalmazandók.

4.6.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A további szereplők értesítésére a 4.4.3 rendelkezései az alkalmazandók.

4.7 Kulcscsere

A Szolgáltató a tanúsítvány érvényességi idején belül történő alkalmazhatósága érdekében Kulcscsere szolgáltatást biztosít. A kulcscserét a Szolgáltató saját hatáskörben is végrehajthatja, valamint az Ügyfél indokolás nélkül is kezdeményezheti.

DV SSL tanúsítvány esetén a kulcscsere nem értelmezett.

A Szolgáltató saját hatáskörében eljárva kezdeményezi a kulcscserét abban az esetben, amennyiben a tanúsítványban szereplő nyilvános kulcs (érvényesítési adat) már nem felel meg a hatályos jogszabályi követelményeknek, az irányadó szabványoknak, vagy rendkívüli helyzetben akkor, ha a Szolgáltató a végfelhasználói tanúsítvány hitelesítésére használt szolgáltatói kulcsot cseréli. A kulcscsere szükségességéről a Szolgáltató az Tanúsítványban vagy a regisztrációban szereplő email címen értesíti Ügyfelet.

A kulcscserére sor kerülhet még érvényes és érvénytelen (pl. kulcskompromittálódás miatt visszavont) tanúsítvány esetén egyaránt. Kulcscsere esetén az Ügyfél nem igényelheti a kulcsokon kívül más adat módosítását, ugyanakkor az Ügyfél nyilvános kulcsa mellett változhatnak egyéb adatok (pl. tanúsítvány sorszám és érvényességi idő, Szolgáltatói adatok, CRL/OCSP elérhetőség).

A végfelhasználói kulcsok cseréjét Szolgáltató új tanúsítványigénylés útján biztosítja, mivel új kulcsok generálása esetén új tanúsítvány kibocsátására is szükség van. Amennyiben Ügyfél, bármilyen okból a tanúsítványához tartozó kulcsokat le kívánja cserélni, ezt az Ügyfélmenübe bejelentkezve új tanúsítványigénylés elküldésével kezdeményezheti a 4.1 pontban meghatározott módon. Amennyiben kulcscsere céljából történik tanúsítványkiadás, a lecserélt kulcshoz tartozó tanúsítványt a Szolgáltató – amennyiben az még érvényes – visszavonja a 4.9 pontban meghatározott módon.

4.7.1 A kulcscsere körülményei

Kulcscsere esetére a Szolgáltató nem állapít meg külön eljárási szabályokat.

4.7.2 Ki igényelheti a kulcscserét?

A kulcscsere igénylésére a 4.6.2 pont rendelkezései alkalmazandók.

4.7.3 A kulcscsere igénylések feldolgozása

Az igények feldolgozására a 4.6.3 pont rendelkezései alkalmazandók azzal a különbséggel, hogy az érintett tanúsítvány érvényessége, illetve a hozzá tartozó magánkulcs kompromittálódás-mentessége nem elvárás (kivéve, ha az igénylés azzal lett aláírva).

Amennyiben a Szolgáltatónak a kulcscsere eljárás során jut tudomására, hogy a kulcs kompromittálódott, akkor azonnal intézkedik a tanúsítvány visszavonásáról, és ennek megfelelően visszautasítja a kulcscsere igénylést.

4.7.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

Az Ügyfél értesítésére a 4.3.2 pont rendelkezései alkalmazandók.

4.7.5 A kulcscserével megújított tanúsítvány elfogadása

A megújított tanúsítvány elfogadására a 4.4.1 pont rendelkezései alkalmazandók.

4.7.6 A kulcscserével megújított tanúsítvány közzététele

A megújított tanúsítvány közzétételére a 4.4.2 pontban foglalt rendelkezések az alkalmazandók.

4.7.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A további szereplők értesítésére a 4.4.3 pont rendelkezései az alkalmazandók.

4.8 Tanúsítványmódosítás

A Szolgáltató a tanúsítványok folyamatos hiteles adattartalma és alkalmazhatósága érdekében tanúsítványmódosítási szolgáltatást nyújt, kivéve DV SSL tanúsítvány esetén, ahol a tanúsítványmódosítás nem értelmezett.

Tanúsítványmódosítást az Ügyfél is kezdeményezheti, valamint azt a Szolgáltató saját hatáskörben is jogosult végrehajtani, amennyiben a végfelhasználói tanúsítvány valamely adatának megváltozásáról tudomást szerez, vagy ha a végfelhasználói tanúsítvány hitelesítésére használt szolgáltatói tanúsítvány megváltozik.

Tanúsítvány módosítására abban az esetben van szükség, ha a tanúsítványba foglalt adatok a tanúsítvány érvényességi idején belül megváltoznak.

Tanúsítvány módosításakor az új tanúsítvány adata a nyilvános kulcs (érvényesítési adat) kivételével megváltozik. Az adatváltozás különösen az alábbiakat jelenti:

- a tanúsítványmódosítást indukáló adatváltozásból eredő módosult adat vagy adatok;
- a tanúsítvány érvényességének kezdete;
- a tanúsítvány sorszáma.

A Tanúsítványmódosítási eljárás keretében kiadott tanúsítvány maximális érvényességi ideje az eredeti érvényességi idővel egyezik meg. Tanúsítványmódosítást Ügyfél az Ügyfélmenübe belépve ugyanúgy kezdeményezhet, mint Tanúsítványmegújítást. (Lásd 4.6 pont)

4.8.1 A tanúsítványmódosítás körülményei

A tanúsítványmódosításra a 4.6.1 pont rendelkezései alkalmazandóak.

4.8.2 Ki igényelheti a tanúsítványmódosítást

A tanúsítványmódosításra a 4.6.2 pont rendelkezései alkalmazandók azzal, hogy a tanúsítványban szereplő Alany adatok változatlan voltáról szóló nyilatkozat nem vonatkozik a megváltozott adatokra.

4.8.3 A tanúsítványmódosítási igénylések feldolgozása

A tanúsítványmódosításra a 4.6.3 pont rendelkezései alkalmazandók azzal, hogy az Alany megváltozott adatai tekintetében a 3.2 fejezet rendelkezései szerinti azonosítási/ellenőrzési eljárást kell lefolytatni.

4.8.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

Az Ügyfél (Végfelhasználó) értesítésére a 4.3.2 pont rendelkezései alkalmazandók.

4.8.5 A módosított tanúsítvány elfogadása

A megújított tanúsítvány elfogadására a 4.4.1 pont rendelkezései alkalmazandók.

4.8.6 A módosított tanúsítvány közzététele

A módosított tanúsítvány közzétételére a 4.4.2 pontban foglalt rendelkezések az alkalmazandók.

4.8.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A további szereplők értesítésére a 4.4.3 pont rendelkezései az alkalmazandók.

4.9 Visszavonás és felfüggesztés

A Szolgáltató az authentikációs és titkosító tanúsítványok érvényességének kezelésére Állapotváltoztatási szolgáltatást (tanúsítvány-visszavonási, -felfüggesztési és tanúsítvány aktiválási) nyújt. DV SSL tanúsítvány esetén a felfüggesztési és aktiválási tevékenység nem értelmezett.

Az Állapotváltozást a Szolgáltató saját hatáskörben is végrehajthatja, valamint azt az Ügyfél, a Bíróság vagy hatóság is kezdeményezheti.

A felfüggesztett és visszavont tanúsítványok érvénytelenek. A felfüggesztett tanúsítvány csak a felfüggesztés időtartama alatt érvénytelen. A felfüggesztés meghatározott időtartamra szól, ezen időszak leteltével a Szolgáltató a tanúsítványt visszavonja, vagy újra aktiválja. A visszavonás véglegesen érvénytelenné teszi a tanúsítványt a visszavonás pillanatától.

4.9.1 A visszavonást és felfüggesztést indukáló körülmények

4.9.1.1 Végfelhasználói tanúsítványok visszavonása vagy felfüggesztése

A Szolgáltató a visszavonásra/felfüggesztésre vonatkozó, nem automata rendszeren keresztül érkezett igényt az igény beérkezését követő legfeljebb 24 órán belül elbírálja, és ennek alapján a tanúsítványt visszavonja vagy felfüggeszti, illetve a visszavonási/felfüggesztési igényt elutasítja.

Az automata rendszeren keresztül történő igénylés esetén a Szolgáltató nem mérlegel, a tanúsítványt azonnali hatállyal visszavonja/felfüggeszti.

A végfelhasználói tanúsítványok visszavonását vagy felfüggesztését az alábbi körülmények indukálhatják:

- Ügyfél szabályos igénylése (Állapotváltoztatási ügyféligény);
- Ügyfél jelzése, hogy az eredeti tanúsítványigénylés nem volt engedélyezett és azt utólag sem engedélyezi;
- az Ügyfél kötelezettségeit nem tartja be;
- a Szolgáltató szabályzataiban és az ÁSZF-ben [8.] meghatározott egyéb körülmény;

- a tanúsítványban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódása;
- a tanúsítványt hitelesítő szolgáltatói magánkulcs kompromittálódása;
- a tanúsítvány módosítása vagy kulcscseréje;
- jogszerűtlen név- vagy adathasználat,
- a tanúsítványban hibásan rögzített adatok vagy az adatok valótlansága, megváltozása, félrevezetésre alkalmassága;
- az Ügyfél nem kérte a tanúsítvány aktiválását a felfüggesztési időn belül;
- a tanúsítvány rosszhiszemű felhasználása;
- bíróság vagy hatóság erre vonatkozó jogerős és végrehajtható határozata;
- a tanúsítvány műszaki jellemzői a mértékadó szakmai ajánlások alapján az elfogadhatónál nagyobb kockázatot jelentenek bármely félnek (pl. kulcshossz ajánlottnál kisebb mérete);
- a Szolgáltatási Szerződés megszegése vagy megszűnése;
- a tanúsítvány nem a vonatkozó szabályzatok szerint lett kibocsátva;
- a szolgáltató tudomására jut, hogy a tanúsítványban szereplő valamely név használatára az Ügyfél nem jogosult;
- a szolgáltató tudomására jut a tanúsítványban feltüntetett képviseleti jogosultság megszűnése;
- amennyiben a tanúsítványra vonatkozó érvényességi információs szolgáltatások fenntartása megszűnik;
- a jelen Szabályzat szerinti szolgáltatás megszűnése, kivéve, ha a Szolgáltató korábban gondoskodott az általa kibocsátott tanúsítványok vonatkozásában a CRL és OCSP szolgáltatások fenntartásáról;
- jogszabály teszi kötelezővé.

A tanúsítványok felfüggesztésének további lehetséges okai:

- a tanúsítvány kiadását követő kezdeti felfüggesztés a szállítás biztonságának növelésére;
- a tanúsítvány visszavonását indukáló bármely körülményre vonatkozó alapos vélelem.

4.9.1.2 A köztes hitelesítő egység tanúsítványának felfüggesztése vagy visszavonása

A Szolgáltató legfeljebb 7 napon belül köteles intézkedni a köztes hitelesítő egység tanúsítványának visszavonásáról az alábbi esetekben:

- a köztes hitelesítő egység szabályos, írásbeli igénylése (Állapotváltoztatási ügyféligény);
- a köztes hitelesítő egység jelzi a Szolgáltatónak, hogy az eredeti tanúsítványigénylés nem volt hiteles és azt utólag sem hitelesíti, illetve engedélyezi;
- a tanúsítványban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódása;
- a tanúsítványt hitelesítő szolgáltatói magánkulcs kompromittálódása;
- a tanúsítvány rosszhiszemű felhasználása;
- a tanúsítványban hibásan rögzített adatok vagy az adatok valótlansága, megváltozása, félrevezetésre alkalmassága;
- amennyiben a tanúsítványra vonatkozó érvényességi információs szolgáltatások fenntartása megszűnik;
- a tanúsítvány műszaki jellemzői a mértékadó szakmai ajánlások alapján az elfogadhatónál nagyobb kockázatot jelentenek bármely félnek (pl. kulcshossz ajánlottnál kisebb mérete);
- bíróság vagy hatóság erre vonatkozó jogerős és végrehajtható határozata;
- a jelen Szabályzat szerinti szolgáltatás megszűnése;
- jogszabály teszi kötelezővé;
- a szolgáltató szabályzatai által meghatározott egyéb körülmény.

A szolgáltató internetes oldalán részletesen tájékoztatja az Ügyfeleket a tanúsítványok visszavonását vagy felfüggesztését maguk után vonó körülmények könnyebb beazonosításáról, ezek bejelentésének valamint a tanúsítványállapot-változás igénylésének módjáról.

4.9.2 Állapotváltozási ügyféligényre jogosultak

A felfüggesztést és visszavonást az alábbi entitások kezdeményezhetik:

Tanúsítvány típusa	**Visszavonást és felfüggesztést igényelheti**
Végfelhasználói személyes authentikációs és titkosító tanúsítvány	Végfelhasználó, Előfizető, Szolgáltató, bíróság vagy más hatóság
Végfelhasználói munkatársi authentikációs és titkosító tanúsítvány	Végfelhasználó, a tanúsítványban Alanyként megjelölt jogi személy/egyéb szervezet képviselője/meghatalmazottja, Előfizető, Szolgáltató, bíróság vagy más hatóság. Amennyiben a Szolgáltató olyan tanúsítvány bocsát ki, mely tanúsítvány képviseleti jogosultságot is igazol, akkor a képviseleti jogosultság megszűnése esetén a képviselt vagy a képviselő személy kérésére jogosult a tanúsítványt visszavonni.
Végfelhasználói szervezeti authentikációs és titkosító tanúsítvány	A tanúsítványban Alanyként megjelölt jogi személy/egyéb szervezet képviselője/meghatalmazottja, Előfizető, Szolgáltató, bíróság vagy más hatóság
Szolgáltatói tanúsítványok	Ügyfél, Szolgáltató, bíróság vagy más hatóság
Tanúsítvány típusa	**Visszavonást igényelheti**
DV SSL tanúsítvány	A tanúsítványban Alanyként megjelölt domain feletti kontrollal rendelkező természetes személy, Előfizető, Szolgáltató, bíróság vagy más hatóság. Kizárólag visszavonás értelmezett.

4.9.3 A visszavonási, felfüggesztési és aktiválási eljárás

4.9.3.1 A visszavonási és a felfüggesztési eljárás

A visszavonási vagy felfüggesztési eljárás a visszavonásra vagy felfüggesztésre vonatkozó Állapotváltoztatási igény Szolgáltatóhoz történő beérkezésével vagy a Szolgáltató döntésével, illetve utasításával kezdődő és a tanúsítvány visszavonásával vagy felfüggesztésével, illetve nem megfelelő igénylés esetén az igénylés visszautasításával záródó folyamat.

DV SSL tanúsítvány esetén a visszavonási eljárás az Ügyfélmenübe történő visszavonás kezdeményezésével és a visszavonással záródó folyamat.

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

Authetnikációs és titkosító tanúsítvány esetén a visszavonási és felfüggesztési igényt az arra jogosultak az alábbi csatornákon keresztül juttathatják el a Szolgáltató részére:

1. visszavonási és felfüggesztési igény benyújtható e-mailben a visszavonas@netlock.hu címre (az igény feldolgozása munkanapokon az alábbiak szerint történik: hétfőn-csütörtök: 8:30 és 16:00 óra, péntek: 8:30-14:00 óra között),
2. visszavonási és felfüggesztési igény benyújtható telefonon az 1.3.2 pontban meghatározott telefonszámon (az igények feldolgozása folyamatosan, 7x24 órában történik),
3. visszavonási és felfüggesztési kérelem kérelmezető ügyfélszolgálati időben személyesen a Szolgáltató székhelyén a Központi Regisztrációs egységnél,
4. felfüggesztési igény benyújtható a szolgáltató internetes oldalán keresztül elérhető ügyfélmenüben is saját felhasználó név és jelszó megadása után (az igény feldolgozása munkanapokon az alábbiak szerint történik: hétfőn-csütörtök: 8:30 és 16:00 óra, péntek: 8:30-14:00 óra között).

DV SSL tanúsítvány esetén a visszavonási igény benyújtható az Ügyfélmenübe bejelentkezve. A Szolgáltató a visszavonás kapcsán nem mérlegel, a visszavonási kérést automatikusan teljesíti.

A visszavonás vagy felfüggesztés vonatkozhat egy végfelhasználói tanúsítványra vagy a szolgáltató valamely köztes hitelesítő egységére.

A visszavonási/felfüggesztési kérelemnek – kivéve az automata rendszer használata esetén - legalább a következő adatokat kell tartalmaznia:

- a tanúsítvány sorszáma vagy egyedi neve,
- a visszavonást/felfüggesztést kérő megnevezése,
- a visszavonást/felfüggesztést kérő elérhetősége,
- a visszavonást/felfüggesztést kérő kapcsolata a tanúsítvány Alanyaként feltüntetett entitással,
- a visszavonás oka (opcionális).

Visszavonás esetén meg kell adni a visszavonás okát. Amennyiben a visszavonást az Ügyfél kéri, és a visszavonás okát nem adja meg, a Szolgáltató úgy tekinti, hogy a visszavonás oka az, hogy a Végfelhasználó a tanúsítványt a továbbiakban nem kívánja használni.

Amennyiben a visszavonást az Ügyfél kéri, okként pedig a kulcskompromittálódás adja meg, a Szolgáltató lehetőséget biztosíthat számára a visszavonási eljárás során, hogy a visszavonandó tanúsítvány helyett Kulcscsere keretében új tanúsítványt igényeljen (lásd 4.7 pont).

A felfüggesztett tanúsítványhoz tartozó magánkulcs használatát a felfüggesztés ideje alatt szüneteltetni kell. A visszavont tanúsítványhoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges.

A tanúsítványok állapotának változásaival kapcsolatban felmerülő tanúsítványelfogadásból származó károkra az alábbi felelősségi szabályok vonatkoznak:

- A visszavonási vagy felfüggesztési igény Szolgáltatóhoz történő megérkezéséig az Ügyfél a felelős az esetleges felmerülő károkért.
- A felfüggesztési vagy visszavonási igény Szolgáltató általi elfogadását követően, a tanúsítvány megváltozott állapotának közzétételéig a Szolgáltató felel az esetleges felmerülő károkért.
- Amennyiben a Szolgáltató már közzétette a tanúsítvány érténytelen (visszavont vagy felfüggesztett állapotát), a Szolgáltató semmilyen felelősséget nem vállal azért, ha bármely Érintett Fél mégis érvényesnek tekinti a tanúsítványt.

A Szolgáltató, amennyiben meggyőződött az Igénylő jogosultságáról valamint az igény szabályosságáról és hitelességéről, a vonatkozó tanúsítvány felfüggesztését/visszavonását a 4.9.1.1 pontban meghatározott időtartam alatt hajtja végre.

4.9.3.2 Az aktiválási eljárás

A felfüggesztett tanúsítvány (újbóli) érvénybe helyezését azon személyek igényelhetik, akik az adott tanúsítvány tekintetében felfüggesztési és visszavonási igénylésre jogosult. Az igénylés a 4.9.3.1 pontban meghatározott módon történhet azzal, hogy az Ügyfélmenüben nem kezdeményezhető a tanúsítvány aktiválása. Amennyiben a felfüggesztés 4.9.12 pont szerinti időtartama alatt a tanúsítvány aktiválására nem kerül sor, a felfüggesztési időtartam leteltével a tanúsítvány automatikusan visszavonásra kerül.

DV SSL tanúsítvány esetén az aktiválási eljárás nem értelmezett.

4.9.4 Az igénylések feldolgozása

A Szolgáltató az állapotváltozási igényeket végrehajtásuk előtt az alábbiak szerint ellenőrzi:

<table>
<tr><th></th><th>E-mail</th><th>Telefon</th><th>Ügyfélmenü</th></tr>
<tr><td>MŰVELET</td><td>Titkosító és authentikációs tanúsítvány esetén: visszavonás, felfüggesztés, aktiválás, DV SSL tanúsítvány esetén visszavonás</td><td>Titkosító és authentikációs tanúsítvány esetén: visszavonás, felfüggesztés, aktiválás, DV SSL tanúsítvány esetén visszavonás</td><td>Titkosító és authentikációs tanúsítvány esetén: felfüggesztés, DV SSL tanúsítvány esetén visszavonás</td></tr>
<tr><td>az igénylő azonosítása (hitelesség)</td><td colspan="2">lásd a 3.4 pontban foglaltakat</td><td rowspan="2">Felhasználó név és jelszó megadása.</td></tr>
<tr><td>az igénylő jogosultsága</td><td colspan="2">lásd a 4.9.2 pontban foglaltakat</td></tr>
<tr><td>az igénylés helyessége</td><td>Az igény egyértelműen tanúsítványállapot-változási igény.</td><td>Az igénylő egyértelműen nyilatkozik tanúsítványállapot-változási igényéről.</td><td>-</td></tr>
<tr><td>a tanúsítvány azonosíthatósága</td><td colspan="2">Amennyiben az Igénylő több tanúsítvány visszavonására is jogosult, a tanúsítvány sorszámának, vagy – amennyiben elkülöníthető és egyértelműen azonosítható – legalább a tanúsítványban lévő 2 (kettő) adat megadása/egyeztetése szükséges.</td><td>-</td></tr>
<tr><td>a művelet végrehajthatósága</td><td colspan="3">1. Visszavonási igény esetén: amennyiben a tanúsítvány nincs még visszavonva.
2. Felfüggesztési igény esetén: amennyiben a tanúsítvány nincs még visszavonva vagy felfüggesztve.
3. Aktiválási igény esetén: a tanúsítvány felfüggesztett állapotban van és a felfüggesztést indukáló körülmények már nem állnak fenn.</td></tr>
<tr><td>művelet időtartama</td><td colspan="3">Lásd a 4.9.5 pontban foglaltakat</td></tr>
</table>

Amennyiben a fenti elvárások nem teljesülnek, akkor az igénylést a Szolgáltató visszautasítja, egyébként – nem automata rendszer használata esetén - további mérlegelés nélkül intézkednie kell a tanúsítvány visszavonása, felfüggesztése vagy aktiválása érdekében. Visszavonási igényt a Szolgáltató ideiglenesen a tanúsítvány felfüggesztésével is kezelheti.

A Szolgáltató minden végrehajtott és visszautasított felfüggesztési, visszavonási és tanúsítványaktiválási igénylésről e-mailben értesíti az Igénylőt és az Előfizetőt.

4.9.5 Állapotváltozási igények feldolgozásának maximális ideje

Az emberi beavatkozást Igénylő visszavonási/felfüggesztési igények feldolgozásának ideje legfeljebb 24 óra. Amennyiben ezen időszak alatt a Szolgáltató önhibáján kívül nem képes a visszavonási, felfüggesztési vagy aktiválási igény jogszerűségéről – a benyújtó személy jogosultságáról -

megbizonyosodni, úgy a továbbiakban – ellenkező tény tudomására jutásáig – a visszavonási/felfüggesztési, illetve aktiválási igényt illetéktelen személytől származónak tekinti, és a visszavonási vagy felfüggesztési, illetve aktiválási folyamatot eredménytelenként lezárja.

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

A Szolgáltató a tanúsítványt mindig a közzétételt követő időre vonja vissza/függeszti fel.

Automata rendszer használata esetén a Szolgáltató a felfüggesztést/visszavonást követően haladéktalanul, de legkésőbb 30 percen belül új visszavonási listát ad ki.

4.9.6 Javasolt eljárás a tanúsítványállapot ellenőrzésére

Az Érintett Felek az egyes tanúsítványok aktuális állapotáról a Szolgáltató internetes oldalán található nyilvános tanúsítványtárban is találhatnak információkat, amennyiben a keresett tanúsítvány Ügyfele hozzájárult a tanúsítvány egyes adatainak nyilvánosságra hozataláról.

A Szolgáltató minden végrehajtott és visszautasított felfüggesztési, visszavonási és tanúsítványaktiválási igénylésről e-mailben értesíti a Végfelhasználót a tanúsítványban rögzített email címen és - amennyiben különbözik a Végfelhasználótól - az Előfizetőt az Ügyfélmenüben rögzített email címen.

Amennyiben a szolgáltatói hitelesítő egység tanúsítványának érvényességi állapota változik, a Szolgáltató az állapotváltozást internetes oldalán közzéteszi. Amennyiben az állapotváltozás oka kulcskompromittálódás, a Szolgáltató minden ésszerű erőfeszítést megtesz annak érdekében, hogy az eseményről közvetlenül értesítse az Érintett Feleket.

4.9.7 A visszavonási lista kibocsátás gyakorisága

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

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

A humán közreműködéssel történő tanúsítvány visszavonása vagy felfüggesztése, illetve aktiválása esetén a tanúsítványállapot-változásnak a Szolgáltató nyilvántartásában való átvezetést követő 1 órán belül a Szolgáltató a kérelem szerint módosított visszavonási állapotot közzéteszi a nyilvános tanúsítványtárban.

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

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

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

4.9.8 A visszavonási lista előállítása és közzététele közötti idő maximális hossza

A Szolgáltató a visszavonási listát (CRL) annak előállítását követően maximum 5 (öt) percen belül közzéteszi.

4.9.9 Online tanúsítványállapot-ellenőrzés rendelkezésre állása

A Szolgáltató online (valós idejű) tanúsítványállapot szolgáltatást (OCSP) nyújt a szolgáltatása keretében kibocsátott authentikációs, illetve titkosító tanúsítványok állapotának ellenőrzéséhez kapcsolódóan az RFC2560 szabvány rendelkezései alapján.

A Szolgáltató az OCSP válaszokat aláírja az alábbi módok valamelyikén:

- az ellenőrizendő tanúsítványt kibocsátó tanúsítványkiadóval, vagy
- az OCSP válaszadó kiadóval, melynek tanúsítványát az a tanúsítványkiadó írta alá, amely az ellenőrizendő tanúsítványt kibocsátotta.

4.9.10 Online tanúsítványállapot ellenőrzésre vonatkozó körülmények

A Szolgáltató támogatja a 'GET' paraméterrel érkező OCSP kéréseket. A Szolgáltató az OCSP-vel szolgáltatott információkat az alábbi időközönként frissíti:

- végfelhasználói tanúsítványokra legalább 4 naponta;
- köztes tanúsítványkiadói tanúsítványokra alapvetően évente;
- köztes tanúsítványkiadói tanúsítvány visszavonása vagy felfüggesztése esetén 24 órán belül.

A Szolgáltató által kibocsátott OCSP válasz csak az adott hitelesítő egység által aláírt, a Szolgáltató Tanúsítványtárában szereplő Tanúsítványokra vonatkozóan tartalmaz "good" állapotinformációt. Egy még ki nem bocsátott tanúsítványra vonatkozó OCSP válasz nem tartalmaz “good” állapotinformációt. Az OCSP kéréseket a Szolgáltató a 6.5 fejezetben foglaltaknak megfelelően ellenőrzi. A 7.1.5 pontban írtaknak nem megfelelő Tanúsítványkiadói tanúsítványra vonatkozó OCSP válasz nem tartalmaz “good” állapotinformációt.

4.9.11 A visszavonási hirdetmények egyéb formái

A visszavonási hirdetmények csak a Szolgáltató tanúsítványtárában és annak biztonsági másolatában, illetve két másik tárban érhetők el. A Szolgáltató saját szolgáltatói tanúsítványának állapotváltozását weboldalán teszi közzé.

4.9.12 A kulcs kompromittálódására vonatkozó speciális követelmények

Magánkulcs kompromittálódása vagy vélelmezett kompromittálódása esetén a visszavonási eljárásban leírt lépések végrehajtandóak (4.9 pont). Kompromittálódott magánkulcs soha többet nem használható, és megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes magánkulcs. Az Ügyfél kötelessége a kompromittálódott magánkulcs által esetlegesen Érintett Felek értesítése, és minden intézkedés megtétele az esetleges károk megelőzése vagy enyhítése érdekében.

4.9.13 A felfüggesztés maximális ideje

Tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 30 naptári napig. A tanúsítvány visszavonásáról, illetve (újbóli) aktiválásáról Szolgáltatónak a lehető leghamarabb intézkednie kell. A felfüggesztett állapot kezdő időpontja a felfüggesztési igény elfogadásától, azaz a 4.9.3.1 pontban foglaltaknak megfelelő igénylés elvégzésétől számítandó. Ha ez idő alatt a visszavonáshoz vezető körülmények gyanúja cáfolatot nem nyer, Szolgáltató a tanúsítványt automatikusan visszavonja.

Felfüggesztett tanúsítvánnyal végzett művelet érvénytelennek tekintendő.

4.10 Tanúsítványállapot-szolgáltatások

A Szolgáltató biztosítja a kibocsátott tanúsítványok állapotának (érvényes, felfüggesztett, visszavont) ellenőrzését biztosító szolgáltatásokat.

4.10.1 Működési jellemzők

A tanúsítványállapot-szolgáltatások működése során a Szolgáltató az alábbiakat szerint jár el:

- biztosítja a tanúsítványállapot-információk folyamatos, napi 24 órában, heti 7 napban való online elérhetőségét (a tanúsítvány megfelelő mezőiben megadott URL-eken és a Szolgáltató honlapján);
- PKI alapú aláírással biztosítja a tanúsítványállapot információk sértetlenségét és hitelességét;
- biztosítja, hogy a visszavonási információk legalább a tanúsítvány eredeti érvényességi idejéig szerepeljenek a tanúsítványállapot információk között;
- a tanúsítványállapot ellenőrzésére tanúsítvány visszavonási Lista (CRL) és online tanúsítványállapot ellenőrzés (OCSP) szolgáltatást nyújt;
- gondoskodik arról, hogy CRL és az OCSP szolgáltatások egymással összhangban működjenek és a tanúsítvány állapotának változásáról szóló információk mindkét szolgáltatásban elérhetőek legyenek és megegyezzenek;
- biztosítja, hogy a tanúsítványvisszavonási információk nyilvánosak és nemzetközileg is elérhetőek legyenek;
- biztosítja, hogy a tanúsítványállapot-jelzések között egymástól megkülönböztethető módon megjelenjen a visszavont és felfüggesztett tanúsítványok állapota;
- biztosítja, hogy a felfüggesztett tanúsítványok az aktiválás hatására lekerülnek a tanúsítványvisszavonási (CRL) listából;
- kulcs kompromittálódás miatti tanúsítvány felfüggesztés vagy visszavonás esetén, az állapotváltozás bejegyzése után a Szolgáltató rendkívüli visszavonási listát (CRL) bocsát ki; más okból történő visszavonás vagy felfüggesztés esetén az állapotváltozás legkésőbb a következő tervezett visszavonási listában kerül publikálásra.

4.10.2 Szolgáltatások elérhetősége

A szolgáltatások elérhetősége tekintetében a Szolgáltató az alábbiakat biztosítja:

- a tanúsítványtár, valamint a Szolgáltató által kibocsátott tanúsítványok használatára vonatkozó kikötések és feltételek folyamatos (7x24) elérhetőségét éves szinten legalább 99%-os rendelkezésre állás mellett úgy, ahol az eseti szolgáltatás kiesések maximális időtartama legfeljebb 24 óra;
- visszavonási nyilvántartások és a visszavonás kezelési szolgáltatás éves szinten legalább 99%-os rendelkezésre állását úgy, ahol az eseti szolgáltatás kiesések időtartama legfeljebb 24 óra;
- a tanúsítványokkal kapcsolatos magas prioritású hibabejelentésekre (pl. visszaélésre használnak egy adott tanúsítványt, és ezt az Érintett Fél jelenti be) a folyamatosan (7x24) reagálást és adott esetben a bűnüldöző szervek felé továbbítását és/vagy az érintett tanúsítvány visszavonását;
- a visszavonási nyilvántartások normál terhelés esetén legfeljebb 10 másodperces válaszidejét.

4.10.3 További lehetőségek

A tanúsítványállapot szolgáltatásra vonatkozóan a Szolgáltató további előírást nem alkalmaz.

4.11 Az előfizetés megszűnése

A Szolgáltató által kiadott tanúsítványok érvényességi ideje és az adott tanúsítványszolgáltatás előfizetési ideje összekapcsolódik, vagyis az előfizetési idő megegyezik a tanúsítványban feltüntetett érvényességgel. Mindez nem zárja ki természetesen, hogy a Szolgáltató – kivételesen, egyedileg

meghatározott esetben – a tanúsítványok díjaira vonatkozóan különböző fizetési kedvezményeket határozzon meg (pl. részletfizetés, kedvezmény stb.).

Amennyiben az Előfizető még a tanúsítványban feltüntetett érvényességi idő lejárta előtt kívánja lemondani az előfizetést, úgy a tanúsítvánnyal kapcsolatban a tanúsítvány visszavonására vonatkozó szabályok vonatkoznak (lásd 4.9 pont), míg az előfizetéssel kapcsolatos esetleges visszatérítési igényekkel kapcsolatban a 9.1.5 pont az irányadó. A visszavonással egy időben a Szolgáltatási Szerződés megszűnik.

Ha a tanúsítvány érvényességének lejártát megelőzően az Előfizető a Szolgáltató előírásai szerint (lásd 4.6, **Hiba! A hivatkozási forrás nem található.**, 4.8 pontok) nem újítja meg a tanúsítványt, nem kezdeményezi a kulcscserét vagy a tanúsítvány módosítását, a Szolgáltatási Szerződés automatikusan megszűnik.

4.12 Kulcsletét és kulcshelyreállítás

4.12.1 Kulcsletét és –helyreállítás rendje és szabályai

A magánkulcsok másolatára ugyanolyan szintű biztonsági előírások vonatkoznak, mint az eredeti magánkulcsra. A magánkulcsokról legfeljebb annyi másolatot szabad készíteni, ami elégséges a szolgáltatás fenntartásához.

Végfelhasználói tanúsítványokhoz kapcsolódóan a tanúsítványkibocsátás keretében Szolgáltató kizárólag a titkosító tanúsítványokhoz kapcsolódóan nyújt magánkulcs letéti szolgáltatást.

A Szolgáltató a saját, szolgáltatói magánkulcsait elmentve is tárolja.

4.12.2 Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Szolgáltató nem használ szimmetrikus kulcsokat.

5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

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

DV SSL tanúsítvány kibocsátásához szükséges rendszereit a Szolgáltató egy harmadlagos helyszínen tárolja.

A szolgáltatói rendszerek konfigurációját a Szolgáltató rendszeresen ellenőrzi a biztonsági előírásokat sértő változások kiszűrése érdekében.

A hitelesítő és regisztrációs egységek eszközeit kizárólag az erre felhatalmazott, megfelelően kioktatott és ellenőrzött tudású, szakértelmű kezelőszemélyzet kezeli.

Az egységek adatállományairól biztonsági mentések készülnek (ld. 6.5 alfejezet). A mentéseket a Szolgáltató az 5.5.2 pontban meghatározott ideig megőrzi.

A Szolgáltató a fizikai, eljárásbeli és személyzeti előírásokat rendszeresen elvégzett kockázatelemzéssel vizsgálja. A Szolgáltató az általa használt eszközök (beleértve az információs vagyont is) tekintetében vagyonnyilvántartást vezet, ahol az egyes eszközöket megfelelő kockázati osztályba sorolja.

A Szolgáltató a nem nyilvános Biztonsági Szabályzat tartalmazza az információbiztonsági szabályozással kapcsolatos előírásokat.

A Biztonsági szabályzatot és a vagyonnyilvántartást a Szolgáltató rendszeres időközönként, vagy jelentős változás esetén haladéktalanul felülvizsgálja azok folyamatos alkalmazhatósága, megfelelősége és eredményessége tekintetében.

5.1 Fizikai Óvintézkedések

A fizikai óvintézkedések célja a Szolgáltató bizalmas információira és fizikai körleteire (szerverterem, illetve szerverszoba) irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása. A fizikai hozzáférés tekintetében a Szolgáltató megfelelő jogosultságrendszer alkalmaz az ellenőrzött hozzáférés érdekében és azokat rendszeres időközönként felülvizsgálja.

Az értékek elvesztésének, sérülésének, kompromittálódásának, valamint a működési tevékenység megzavarásának elkerülésére a Szolgáltató a Biztonsági Szabályzatban meghatározott intézkedéseket követi.

A kritikus és érzékeny információt feldolgozó szolgáltatások biztonságos helyszíneken kerülnek megvalósításra a Szolgáltató rendszerében. A biztosított védelem arányban áll a Szolgáltató által végzett kockázatelemzésben megállapított kockázatokkal.

5.1.1 Telephely felépítése

A Szolgáltató telephelyén egy védett számítógép teremben valósítja meg a leginkább veszélyeztetett szolgáltatásokat. A számítógépteremben a fizikai hozzáférés, beléptetés ellenőrzése és felügyelete, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, telekommunikációs hálózat elérhetősége stb. védelmi szempontok egységes érvényesítésére került sor. Illetéktelen személyek a számítógépterembe 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

számítógéptermen belül a szolgáltatói rendszerek egy olyan elkülönült részen kerültek kialakításra, ahova biometrikus azonosítást követően lehet belépni.

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

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

A Szolgáltató Központi Regisztrációs munkatársai a végfelhasználói tanúsítványok kulcsgenerálását (ahol értelmezett), illetve a kulcstároló eszközökkel kapcsolatos előkészítő műveleteket, a tanúsítvány kibocsátását, valamint az állapotváltozás kezelését egy külön erre a célra kialakított, védett szerverszobában valósítják meg. A védett szerverszoba kifejezetten erre a célra készült.

5.1.2 Fizikai hozzáférés

A biztonsági körletek pontos paramétereit, illetve a belépni jogosultak listáját a mindenkori belső operációs dokumentumok tartalmazzák. A biztonsági körletekbe bizalmi munkakört betöltő munkatársakon kívül más személyek csak külön felhatalmazással és kísérettel léphetnek be. A számítógépes termekbe a belépés kártyás azonosítóval történik a belépések fizikai és elektronikus naplózása mellett. A számítógéptermen belül a szolgáltatói rendszerek elkülönült területe biometrikus azonosítást követően közelíthetőek meg. A helyiség kétszerezett (redundáns) klíma-, automata tűzoltó, továbbá illetéktelen behatolást jelző (riasztó) berendezéssel van ellátva. Az eszközök többszörösen túlbiztosított elektromos energiaellátással rendelkeznek. A biztonsági körlet beléptető előhelyiségét, illetve magát a számítógéptermet 24 órás videó kamerás megfigyelő rendszer is védi.

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

A szerverszobába az arra jogosult munkatársak kártyás és biometrikus azonosítást követően léphetnek be; a be-, illetve kilépések folyamatos naplózásra kerülnek. A szerverszoba 24 órás videós kamerás megfigyelő rendszer is védi.

A Szolgáltató kockázatelemzése a kritikus szolgáltatások keretében foglalkozik a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelemmel, a tűzbiztonsági tényezőkkel, a támogató eszközök (különösen áram és klíma) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, valamint a katasztrófa utáni helyreállítással.

A Szolgáltató a szolgáltatói tanúsítványokat a normál operációtól elkülönítetten tárolja, ahhoz kizárólag a bizalmi munkatársak férhetnek hozzá.

5.1.3 Áramellátás, légkondicionálás

A Szolgáltató védett számítógép termének zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében, melynek érdekében a Szolgáltató az alábbi intézkedéseket alkalmazza/alkalmaztatja:

- 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.

A szerverteremben biztosított géptermek épülettől független légkondicionálását. A védett számítógép terme a bejutó levegő tisztaságát megfelelő szűrőrendszerrel biztosítja, gondoskodik a levegőből a különféle szennyeződések kiszűréséről, tovább biztosítja a Szolgáltató munkatársai részére szükséges levegőt. A levegő nedvességtartalma és hőmérséklete folyamatosan ellenőrzött. A légkondicionáló berendezések biztosítják az IT rendszerek megfelelő hűtését. A folyamatos üzemvitelt egy második (tartalék) klímaberendezés is támogatja, mely szükség esetén működésbe lép. A klímaberendezések elhelyezésének módja biztosítja, hogy azok karbantartása ne okozzon zavart a gépterem működésében.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A Szolgáltató szolgáltatási helyszíneit védettek a beázástól és az elárasztódástól. A védett számítógép teremben a biztonságot tovább növeli az álpadló alkalmazása.

5.1.5 Tűzmegelőzés és tűzvédelem

A Szolgáltató szolgáltatási helyszínei a megfelelő tűzvédelmi előírásoknak megfelelően működnek. A szolgáltatási helyszínek az aktuális tűzvédelmi szabályzásoknak megfelelő tűz és füstérzékelőkkel, kézi és automata oltó berendezésekkel rendelkeznek. A kézi oltó berendezések helye és a menekülési útvonal jól látható helyen jelzésre került.

5.1.6 Adathordozók kezelése

Az adathordozók biztonságos tárolására biztonsági körlet, illetve egy bérelt banki széf szolgál. A kritikus adatokról a Szolgáltató több mentési példánnyal rendelkezik. A Szolgáltató folyamatosan gondoskodik és megfelelő intézkedéseket tesz az avulás megakadályozására.

A Szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztől a Biztonsági Szabályzatban előírt módon semmisíti meg, amennyiben azokra már nincs szükség. A selejtezett eszközök tartalmát a Szolgáltató véglegesen törli, vagy az eszközt egyéb módon helyreállíthatatlanul tönkreteszi.

5.1.7 Hulladékelhelyezés

Informatikai eszköz selejtezése esetén a Szolgáltató mindent biztonságosan, olvashatatlanul és helyreállíthatatlanul töröl, illetve, amennyiben ez nem lehetséges, akkor legalább az ilyen elemet hordozó alkatrészt fizikai tönkretétellel megsemmisíti. A fizikailag megsemmisítés kapcsán a Szolgáltató az alábbiak szerint jár el:

- a papíralapú dokumentumok zúzógéppel felaprításra kerülnek,
- a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprításra kerülnek,
- egyéb más mágneses adathordozókat, demagnetizálás után összetörésre kerülnek;
- egyéb más adathordozókat összetörésre kerülnek.

5.1.8 Mentés külső helyszínen

A megőrzendő adatok biztonságos tárolását a Szolgáltató elvégezheti csak írható médiával, távoli helyen tárolt mentéssel, vagy több tárolási helyen történő távoli párhuzamos tárolással.

5.2 Eljárásrendi biztonsági intézkedések

Az eljárásrendi 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.

5.2.1 Bizalmi munkakörök

Bizalmi munkakört kizárólag a Szolgáltatóval munkaviszonyban álló munkatárs tölthet be, a Szolgáltató felső vezetésének formális kinevezését követően.

A Szolgáltató az alábbi bizalmi munkaköröket határozza meg:

Megnevezés	**Rövid leírás**
Biztonsági Tisztviselő	A szolgáltatás biztonságáért általánosan felelős személy
Rendszeradminisztrátor	Az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy
Rendszerüzemeltető	Az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.
Független rendszervizsgáló	A szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy
Informatikai vezető	Szolgáltató informatikai rendszeréért általánosan felelős vezető
Regisztrációs felelős	A végtanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

A Szolgáltató az alábbi tevékenységeket legalább kettő arra kijelölt és közvetlen felhatalmazással rendelkező bizalmi munkatárs együttes fizikai jelenlétével, egy fizikailag védett környezetben, más személyek jelenlétét kizárva végzi:

- köztes kiadó tanúsítványának kibocsátása;
- a szolgáltatói magánkulcsok mentése és visszaállítása;
- a Szolgáltató saját szolgáltatói kulcspárjának generálása

- a szolgáltatói magánkulcsok megsemmisítése.

5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés

A Szolgáltató valamennyi, bizalmi munkakört betöltő munkatársa a zárt körletbe csak a megfelelő azonosítást és hitelesítést követően léphet be, amely a rendszerekhez való hozzáférésnél egyéb, rendszerenként különböző védelemmel egészül ki. Sikeres azonosítás és hitelesítés nélkül a zárt körletbe való bejutás, illetve rendszerhozzáférés nem lehetséges, így egyetlen biztonság szempontjából kritikus tevékenység sem végezhető el.

A bizalmi munkakörhöz tartozó jogosultsági szinteket a Szolgáltató a Jogosultságkezelési Szabályzatában rögzíti.

5.2.4 Egyes szerepkörök összeférhetetlensége

Szolgáltató a rendszereiben olyan biztonsági előírásokat alkalmaz, illetve jogosultsági szinteket határoz meg, amely minimalizálja az azonosítatlan vagy nem szándékolt módosításokat, illetve csökkenti a visszaélési lehetőségeket.

Az összeférhetetlenségre vonatkozó részletszabályokat a Szolgáltató Biztonsági Szabályzata tartalmazza.

5.3 Személyzeti biztonsági intézkedések

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 az alkalmazás során történő ellenőrzését.

A Szolgáltató a Biztonsági Szabályzatának részeként pontosan és részletesen kidolgozott, folyamatosan karbantartott Személyzeti Politikával rendelkezik. A Szolgáltató Személyzeti Politikájában meghatározott ideiglenes és állandó szerepköröket és felelősségeket a megfelelő munkaleírásokban dokumentálja, amelyek tartalmazzák:

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

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

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

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

A Regisztrációs Egység minden bizalmi munkakörére jelölt személynek (emberi megbízhatósága és szakmai alkalmassága ellenőrzése céljából) kezdeti ellenőrzésen (biztonsági alapellenőrzésen) kell keresztülmennie.

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

- a képzettségre vonatkozó adatokat egybevetik a jelölt által benyújtandó bizonyítványokkal, diplomákkal,

- a gyakorlati tapasztalatra vonatkozó állításokat személyes referenciákon keresztül, publikációkra alapozva, illetve egyéb úton igazolják.

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

Valamennyi bizalmi munkakört betöltő munkatársnak a biztonsági alapellenőrzésen túl időszakos biztonsági ellenőrzéseken is át 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. Bizalmi munkakört csak büntetlen előélettel rendelkező személy tölthet be, amit a felvételi eljárás során 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni.

Az időszakos biztonsági ellenőrzésre évente kerül sor valamennyi bizalmi munkakört betöltő (lásd 5.2.1 pont) munkatárs esetén.

A Központi Regisztrációs Egység területén dolgozó valamennyi munkatárs felvételét követően a 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, jelen Szabályzati szerinti szolgáltatásra vonatkozó egységes biztonságpolitika megismerése, megértése, az ezen alapuló aktuális eljárások és követelmények megismerése és a későbbi helyes alkalmazása érdekében. További részletek a Személyzeti Politikában találhatók.

A Mobil Regisztrációs Egység területén dolgozó valamennyi munkatárs felvételét követően a munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt. A Szolgáltató a Személyzeti Politikában foglaltaknak megfelelő időközönként ezen tudást felülvizsgálja.

A bizalmi munkakört a munkatársak a megfelelő gyakorlati tapasztalat megszerzését követően tölthetnek be.

5.3.2 Ellenőrzési eljárások

A felvételi eljárás során a Szolgáltató a személyek személyazonosságáról fizikai jelenlétük során vagy fényképes személyazonosító okmányaik ellenőrzésével győződik meg. Mindezek mellett a Szolgáltató a felvételi eljárás során figyelembe veszi a korábbi munkahelyekre, releváns végzettséget és szakmai referenciákra vonatkozó információkat is.

A bizalmi munkakör munkatársai az ellenőrzés lefolytatását megelőzően nem kaphatnak hozzáférést a Szolgáltató rendszereihez.

5.3.3 Képzési követelmények

A bizalmi munkakört betöltő munkatársaknak rendelkezniük kell a feladataik ellátásához szükséges tudással. Ennek érdekében a bizalmi munkakört betöltő munkatársaknak kinevezésüket megelőzően tudásuk igazolásáról vizsgát kell tenniük, ameddig sikeres vizsgát nem tesznek, addig nem férhetnek hozzá a szolgáltatói rendszerekhez. A vizsga és a képzés a következők a bizalmi munkakör típusától függően ismeretekre terjed ki:

- PKI alapismeretek;
- hitelesítés és ellenőrzési szabályok és eljárások;
- Biztonsági és adatvédelmi szabályok;
- általános fenyegetések az információhitelesítési eljárásokra (beleértve az adathalász és egyéb social engineering taktikákat);
- a Szolgáltatási Szabályzat és egyéb szabályzatok előírásai;
- egyes tevékenységük jogi következményei;
- Szolgáltató informatikai rendszerének sajátosságai és kezelésének módja.

5.3.4 Továbbképzési gyakoriságok és követelmények

A Szolgáltató továbbképzésre és oktatásra vonatkozó gyakorlatát az éves továbbképzési tervben határozza meg.

Abban az esetben, amikor a jelen Szabályzati szerinti szolgáltatásban jelentős változás következik be, valamennyi munkatárs a szükséges felépítésű és szintű moduláris továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat.

5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

A vonatkozó szabályokat a Szolgáltató Személyzeti Politikája tartalmazza.

5.3.6 Jogosultatlan tevékenységek büntető következményei

A szolgáltató rendszerének nem engedélyezett használatára, illetve a szolgáltatás nyújtása közben elkövetett hibákra, mulasztásokra, károkozásokra vonatkozó szankciókat a Szolgáltató a bizalmi munkakört betöltő személyek munkaszerződésében rendezi.

5.3.7 Szerződéses közreműködőkre vonatkozó követelmények

A Szolgáltató nem munkaviszonyban dolgozó szerződéses közreműködőire ugyanazok a biztonsági szabályok vonatkoznak, mint a munkaviszonyban dolgozókra.

5.3.8 A személyzet számára biztosított dokumentumok

A Szolgáltató folyamatosan biztosítja a szolgáltatásnyújtásban közreműködő személyek részére a szerepkörük ellátásához szükséges aktuális szabályzatokat és dokumentációkat.

5.4 Naplózási eljárások

Szolgáltató hitelesítési rendszere az egyes szabványokban, előírásokban meghatározott követelményeknek megfelelő, széleskörű naplózási tevékenységet folytat a tanúsítványokra vonatkozó műveletek és az ezek során felhasznált adatok megőrzése érdekében. A napló tartalmazza a bejegyzés pontos idejét, a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény típusát, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét, az eseményvégrehajtás sikerességét, illetve sikertelenségét. A Szolgáltató a naplókban feltüntetett időt olyan gyakorisággal szinkronizálja, 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.

5.4.1 A tárolt események típusai

A Szolgáltató által alkalmazott PKI rendszer minden olyan eseményt és hibát regisztrál, amely a rendszer üzemeltetése, visszakereshetősége és adminisztrációja szempontjából kritikus. A naplóállományok automatikusan vagy manuálisan kerülnek rögzítésre. A naplóállományok mellett a Szolgáltató egyes események rögzítésére megfelelő jegyzőkönyvet használ.

A Szolgáltató a Biztonsági Szabályzatban részletezi, hogy az egyes események kapcsán pontosan milyen adatokat/eseményeket rögzít.

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.

5.4.2 A naplófájl feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása napi rendszerességgel megtörténik az arra megfelelő szakértelemmel és jogosultsággal rendelkező rendszerellenőrök által. A kiértékelésre manuálisan és szoftvereszközök segítségével kerül sor. A kiértékelés során az értékelő a vizsgált állományok hitelességét és sértetlenségét is vizsgálja.

A kiértékelés során az értékelő elemzi a rendszerek által generált hibaüzenetet, a forgalmi adatokban bekövetkezett jelentős változásokat, a szokásostól eltérő mintát, valamint a gyanús aktivitásokat. A kiértékelés tényét és eredményét, valamint az esetleges szükséges intézkedéseket az értékelő rögzíteni köteles.

Szolgáltató hálózati védelmi rendszerei automatikus 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.

5.4.3 A naplófájl megőrzési időtartama

A napló állományok keletkezésük helyén tárolódnak, illetve archiválásra kerülnek (ld. 5.5.2 pont), és a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg a velük kapcsolatban felmerült és bejelentett jogvita jogerős lezárásáig megőrződnek. A naplófájlok a rendszerellenőrök számára hozzáférhetőek.

5.4.4 A naplófájl 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 (jellemzően rendszerellenőrök). Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi.

5.4.5 A naplófájl mentési eljárásai

A naplóállományok rendszeresen mentésre kerülnek az 5.1.6 és 5.1.8 pontban meghatározott módon rejtjelezett és aláírt formában. Amennyiben a naplóbejegyzés egy helyen keletkezik, a Szolgáltató 24 (huszonnégy) órán belül gondoskodik a biztonsági másolat létrehozásáról.

5.4.6 A naplózás adatgyűjtési 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.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

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

5.4.8 Sebezhetőség felmérése

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

A Szolgáltató évente kockázatértékelést végez, amely segítségével azonosítja, értékeli és kockázati osztályba sorolja az olyan előrelátható külső és belső fenyegetettségeket amelyek lehetővé tehetik a tanúsítványadatok vagy tanúsítványkezelési folyamatok jogosulatlan elérését, nyilvánosságra hozatalát, megváltoztatását, megsemmisítését vagy más visszaélést. A kockázatelemzés a bekövetkezés esetén a várható kárra is kiterjed. A kockázatelemzés a fentiek mellett tartalmazza a fenyegetettségek elhárítására a Szolgáltató által alkalmazott folyamatok, védelmi intézkedések leírását is.

5.5 Adatok archiválása

A Szolgáltató a jelen Szabályzatban meghatározott szolgáltatásokkal kapcsolatos adatokat az 5.5.2 pontban meghatározott módon és ideig őrzi meg.

5.5.1 Az archiválandó adatok típusai

A Szolgáltató a tanúsítvánnyal kapcsolódó adatokat – beleértve az előállításukkal összefüggőket és egyéb személyes adatokat is – meg kell őriznie. Így tárolásra kerül:

- a Szolgáltatóhoz a tanúsítványigénylés során benyújtott valamennyi elektronikus, illetve papír alapú kérelem (lásd 4.1 pont);
- a kérelmet elfogadó regisztrációs ügyintéző azonosítója;
- a küldő regisztrációs szervezet neve;
- a tanúsítványállapot változási eljárás során közzétett információk (lásd 4.9.3 pont);
- a jelen Szabályzat szerinti naplózott információk (5.4 pont).

5.5.2 Archiválási időtartam

Szolgáltató a tanúsítványokkal kapcsolatos elektronikus információkat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejártától számított tíz évig, illetőleg az elektronikus aláírással, illetve jogvita esetén a jogvita jogerős lezárásáig megőrzi, valamint ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható. E megőrzési kötelezettségnek Szolgáltató minősített elektronikus archiválási szolgáltató igénybevételével is eleget tehet.

5.5.3 Az archívum védelme

Az archívum védelmére az 5.4.4 pontban meghatározott naplófájl védelmére vonatkozó előírások alkalmazandóak.

5.5.4 Az archívum mentési folyamatai

Az archívum mentésére az 5.4.5 pontban meghatározott naplófájl mentésére vonatkozó előírások alkalmazandóak.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

A Szolgáltató az archiválandó adatokat az 5.4.1 pontban meghatározott módon időbélyeggel vagy időadattal látja el.

5.5.6 Az archívum gyűjtési rendszere

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

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül benyújtott kérelem alapján lehet kérni hozzáférést. A hozzáférés az Ügyfélnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.4.1 pont szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és a hozzáférést naplózza.

5.5.8 Egyéb archiválási rendelkezések

Az archívumban esemény típus szerinti keresést lehet végrehajtani. Az archiválásra vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat tartalmazza.

5.6 Kulcscsere

Szolgáltató lecseréli kulcsát, amennyiben saját szolgáltatói tanúsítványa lejár, illetve az általa alkalmazott kulcsok elavulnak. Mindezek mellett a Szolgáltató saját belátása szerint egyéb esetben is dönthet kulcscsere mellett.

A Szolgáltató az új kulccsal kiállított új tanúsítvány esetében annak profilját és adatait az aktuális előírásokhoz és legjobb gyakorlathoz igazítja.

5.7 Katasztrófaelhárítás és helyreállítás

A Szolgáltató a szolgáltatásokat érintő fenyegetettségek azonosítására és a lehetséges kockázatok kezelésére vonatkozóan kockázatkezelési értékelést alkalmaz, illetve a rendkívüli helyeztek kezelésére, a vészhelyzetek minél gyorsabb elhárítása valamint a folyamatos működés biztosítására vonatkozóan Üzletmenetet Folytonossági Tervvel (ÜFT) tervvel rendelkezik.

Amennyiben a biztonság megsértése vagy az adatok sértetlenségének megszűnése vélhetőleg hátrányosan érinti azt a természetes személyt vagy jogi személyt, illetve egyéb szervezetetek, aki/amely a szolgáltatást igénybe vettek, akkor a Szolgáltató ezen személyeket is indokolatlan késedelem nélkül értesíti.

5.7.1 Incidens- és kompromittálódás-kezelési eljárások

Az informatikai rendszerekbe való belépésekre, azok felhasználóira és a szolgáltatásigénylésre vonatkozó rendszertevékenységeket a Szolgáltató folyamatosan ellenőrzi a vonatkozó előírásokban foglaltaknak megfelelően. Az ellenőrzés pontos szempontjait a Biztonsági Szabályzat tartalmazza.

A Szolgáltató által alkalmazott ÜFT tartalmazza a katasztrófa helyreállítási tervet is. Az ÜFT olyan eljárásokat tartalmaz, amelyek leírják a megbízható üzemmenet mielőbbi helyreállításának leggyorsabb módját. A Szolgáltató ellenőrzések végrehajtásával rendszeresen (minimum évente) 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.

5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása

Szolgáltató megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik a hardver- és szoftver meghibásodások valamint az adatsérülések minimalizálása érdekében. A szolgáltatások helyreállíthatóságát Szolgáltató háttérszerződései és saját tartalékeszközei garantálják, amelyek az 5.7.4 pontban vállalt időn belül bármely kieső kritikus eszköz pótlására képesek. Szolgáltató rendszeres mentései (lásd 5.5 pont) és tranzakció naplózása (lásd 5.4 pont) 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 (ÜFT) 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.

A Szolgáltató célja, hogy a hiba elhárítása és a rendszeres integritásának helyreállítása utána a lehető leghamarabb újraindítsa valamennyi szolgáltatását. A szolgáltatás helyreállítása során a tanúsítványállapot információt szolgáltató rendszerelemek elsőbbséget élveznek.

A kritikus rendszerelemek meghibásodására vonatkozó részletes szabályokat az ÜFT tartalmazza.

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

5.7.3.1 Végfelhasználói magánkulcs kompromittálódása

Végfelhasználói magánkulcs kompromittálódására vonatkozóan lásd a 4.9.12 pontban foglaltakat.

5.7.3.2 Szolgáltatói magánkulcs kompromittálódása

A szolgáltatói kulcs kompromittálódására vonatkozó előírásokat és a követendő eljárást az ÜFT tartalmazza. Katasztrófa bekövetkezése esetén a Szolgáltató megteszi a szükséges lépéseket a katasztrófa megismétlődésének elkerülése érdekében.

A szolgáltatói kulcs kompromittálódása esetén a Szolgáltató tájékoztatja Ügyfeleit, szerződéses partnereit és az Érintett Feleket. A tájékoztatás tartalmazza, hogy az érintett szolgáltatói kulccsal kibocsátott tanúsítványok és a visszavonási állapot információ már nem érvényesek. A kompromittálódott magánkulcsot tartalmazó tanúsítványt a Szolgáltató visszavonja.

5.7.3.3 Algoritmus változása

Amennyiben a Szolgáltató által alkalmazott algoritmus vagy ahhoz kapcsolóan valamely paraméter nem felel meg az elvárásoknak a tervezett felhasználási időtartamra (végfelhasználói és szolgáltatói tanúsítvány esetén egyaránt), akkor a Szolgáltató tájékoztatja Ügyfeleit, szerződéses partnereit, az Érintett Feleket, illetve a Szolgáltató megteszi a szükséges lépéseket a tanúsítvány visszavonása érdekében.

5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után

Természeti vagy más katasztrófát követően, illetve a Szolgáltató berendezéseinek meghibásodása esetén Szolgáltató a következő szolgáltatások legfeljebb 24 órán belüli elindítását vállalja:

- visszavonáskezelés-szolgáltatás,
- visszavonási állapot közzététele szolgáltatás.

Minden egyéb szolgáltatás elindítását Szolgáltató 5 munkanapon belül vállalja.

5.8 A tanúsítványkibocsátó vagy regisztrációs egység megszűnése

5.8.1 A szolgáltatási tevékenység megszűnése/megszüntetése

Amennyiben a Szolgáltató tevékenységét tervezetten megszűnteti vagy tartósan szüneteltetni, 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 Alanyként megjelölt személyeket, megjelölve azt a - vele azonos besorolású – szervezetet, amely legkésőbb a tevékenység befejezésekor átveszi a visszavonási állapot közlési nyilvántartásokat, valamint a regisztrációs információ és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket a Szolgáltató számára előírt vagy általa vállalt időtartamra;
- A szolgáltatás megszűnése előtt 30 nappal értesítést tesz közzé Internetes oldalain (ld. 1.1.2 pont), 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, valamennyi regisztrációs szervezetet felhívja a náluk tárolt adatok átadására.
- A regisztrációs információk, és az eseménynapló archívumok megőrzése érdekében, időbélyegzővel ellátott teljes körű mentést hajt végre. A mentés tartalmazza a tanúsítványokkal kapcsolatos korábbi változások adatait, a tanúsítványok helyzetére, esetleges felfüggesztésére, illetve visszavonására vonatkozó adatokat, valamint a tanúsítvány kibocsátásra vonatkozó Szolgáltatói szabályzatokat és az aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását. A mentett adatállományokat a Szolgáltató védi jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását, valamint az adatoknak megőrzési időn belüli, jogosultak számára való hozzáférhetőségét és értelmezhetőségét.
- Saját magánkulcsait megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat visszavonja, és erről honlapján tájékoztatást 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.

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

5.8.2 Regisztrációs pont megszűnése

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

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:

- végfelhasználói tanúsítványokat, CRL és OCSP válaszokat aláíró magánkulcs,
- egyéb tanúsítványokat, CRL és OCSP válaszokat aláíró magánkulcs,
- infrastrukturális és kontrollkulcsok.

Szolgáltatói nyilvános kulcsok:

- a szolgáltatói magánkulcsok nyilvános párjai.

Végfelhasználói magánkulcsok:

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

Végfelhasználói nyilvános kulcsok:

- a végfelhasználói magánkulcsok nyilvános párja.

6.1 Kulcspár generálás és telepítés

6.1.1 Kulcspár előállítása

6.1.1.1 A Szolgáltató által használt algoritmusok

6.1.1.1.1 Lenyomatképző algoritmusok azonosítói

- RIPE-MD160 OID ::= { iso(1) identified-organization(3) TeleTrusT(36) algorithm(3) hashAlgorithm(2) RIDEMD-160 (1) }
- SHA-256 OID ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-256 (1) }
- SHA-384 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-384(2)}
- SHA-512 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-512(3)}

A Szolgáltató figyelemmel kíséri a kriptográfiai algoritmusok alkalmazhatóságára vonatkozó, irányadó nemzetközi dokumentumokat, és az itt meghatározott algoritmusokat az ezen dokumentumokban foglalt irányadó előírások szerint alkalmazza.

6.1.1.1.2 Kriptográfiai algoritmusok azonosítói

- RSA OID ::= { iso(1) member-body (2) USA (840) RSADSI (113549) PKCS (1) PKCS-1 (1) RSA Encryption (1) }
- DSA OID ::= { iso(1) member-body(2) us(840) X9-57 (10040) x9algorithm (4) id-dsa (1) }

A Szolgáltató figyelemmel kíséri a kriptográfiai algoritmusok alkalmazhatóságára vonatkozó, irányadó nemzetközi dokumentumokat, és az itt meghatározott algoritmusokat az ezen dokumentumokban foglalt irányadó előírások szerint alkalmazza.

6.1.1.2 A Szolgáltató által használt kulcstároló eszközök

Kulcstároló eszközök	Hardware és firmware specifikáció	Kulcskezeléshez közvetlenül használt szoftverek specifikációja
Nem Minősített Hitelesítő Egység	• ProtectServer Gold (hardware verzió: B4, firmware verzió:2.07.00, 2.08.00 és 3.00.03 Hardver verziók B2 és B3, förmver verzió 2.08.00; Hardver verzió C / PSG-01-0101, förmver verzió 2.08.00)) • Luna® PCI 3000 V3.0 Hardver verzió: VBD-03-0100, förmver: 4.7.1(3000) • Luna® PCI 7000 V3.0 Hardver verzió: VBD-03-0100, förmver: 4.7.1(7000) • Luna® PCI-e 3000 V3.0 Hardver: VBD-04-0100, förmver: 4.7.1(3000) • Luna® PCI-e 7000 V3.0 Hardver: VBD-04-0100, förmver: 4.7.1(7000) • Luna® PCI-e 3000 SFF V3.0 Hardver: VBD-04-0102, förmver: 4.7.1(3000) • Luna® PCI-e 7000 SFF V3.0 Hardver: VBD-04-0102, förmver: 4.7.1(7000) • Luna® PCI-e kriptográfiai modul Hardver verzió: VBD-05-0100, VBD 05-0101 és VBD-05-0103, förmver verzió: 6.2.1	• ProtectServer Gold (hardver verzió: B4, firmware verzió:2.07.00, 2.08.00 és 3.00.03Hardver verziók B2 és B3, förmver verzió 2.08.00; Hardver verzió C / PSG-01-0101, förmver verzió 2.08.00)) drivere, • Luna kriptogáfiai modulok driverei

Kulcstároló eszközök	Hardware és firmware specifikáció	Kulcskezeléshez közvetlenül használt szoftverek specifikációja
Végfelhasználói eszköz	• IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4, applet IDOneClassIC v1.0 embedded, P5CT072VOP-en, • IDOneClassIC Card (ID-One Cosmo 64 RSA v5.4.1, applet: IDOneCIE v1.01.1 platformok: P5CT072VOP, P5CC072VOP és P5CD072VOP) biztonságos aláírás-létrehozó eszköz • ID-One Cosmo v7.0.1-n kártya IAS ECC 1.0.1 alkalmazással (applet version 1121), NXP P5CC081 V1A (Standard) komponenssel • Gemalto MultiApp ID Citizen 72k intelligens kártya: S3CC91C mikrochip, MultiApp v1.1 Java Card platform és IAS Classic v.3.0 elektronikus aláíró alkalmazás (másnéven: Gemalto TCP IM CC) • SafeNet eToken (Smartcard or USB token), 9.1-es Verzió, Athena IDProtect/OS755 Java Card kártya, Atmel AT90SC25672RCT-USB Microcontrolleren, IDSign applet beágyazással • IAS Classic v3 alkalmazás Java Card platformon P5CC081V1A chippel, MultiApp ID V2.1 nyílt szabvány szerint, szűrővel ellátott MPH117 v2.2 (másnéven: Gemalto ID 340) • ProtectServer Orange (korábbi nevén CSA 8000 Adapter), hardver verzió: G verzió, Cprov förmver verzió: 1.10	• ProtectServer Orange (korábbi nevén CSA 8000 Adapter), hardver verzió: G verzió, Cprov förmver verzió: 1.10 • Oberthur eszközök driverei • Gemalto eszközökhöz driverek • SafeNet eszközök driverei

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

6.1.1.3 Szolgáltatói kulcspár előállítása

A szolgáltatói kulcsok generálása a Szolgáltató fizikailag védett szervertermében két bizalmi munkakört betöltő személy együttes jelenlétében, jegyzőkönyvezetten történik. Azon bizalmi munkakört betöltő személyek listáját, akik jogosultak kulcsgenerálásra, a Szolgáltató Jogosultságkezelési Szabályzata tartalmazza.

A szolgáltatói kulcspárok hossza megfelel a kibocsátáskor hatályos szabványokban előírt hosszúságnak. A kiadói kulcshosszok tekintetében a Szolgáltató minimum RSA 2048 bit hosszúságú kulcspárokat használ.

A Szolgáltatói kulcsok generálására és tárolására a Szolgáltató a jelen Szabályzat **Hiba! A hivatkozási forrás nem található.** pontjában részletezett kriptográfiai hardvermodulokat használja. A Szolgáltató valamennyi szolgáltatói kulcspárát saját maga generálja. A generált magánkulcsok – a mentést (klónozást) leszámítva - teljes életciklusuk alatt a kriptográfiai hardverekben maradnak, megsemmisítéséig azt sehová

nem kell továbbítani. Amennyiben a szolgáltatói kulcspár, bármely okból történő megsemmisítése válik szükségessé, úgy az az eszköz tanúsítványában előírt módon két személyes kontroll mellett történik.

A Szolgáltató kulcsok lejáratát megelőzően a Szolgáltatói az új kiadói kulcsokat úgy generálja és adja ki az új szolgáltatói tanúsítványokat, hogy az átállás az Ügyfél részéről minél zökkenőmentesebben történjen és a tanúsítvány cseréje ne okozzon zavart az Érintett Felek számára.

A Szolgáltatói kulcsok generálására vonatkozó részletszabályokat a Szolgáltató Biztonsági Szabályzata tartalmazza.

6.1.1.4 Végfelhasználói kulcspár Szolgáltató által történő előállítása

A Szolgáltató a végfelhasználói kulcsok generálásra során olyan algoritmusokat használ, amelyek megfelelnek a kibocsátáskor hatályos szabványokban előírt hosszúságnak.

A Szolgáltató visszautasít minden olyan tanúsítványkibocsátásra vonatkozó igénylét, amely nem felel meg hatályos előírásra vonatkozó rendelkezéseknek.

A Szolgáltató a végfelhasználói kulcsok generálását az erre feljogosított munkatársak biztonságos módon, a Szolgáltató védett szerverszobájában végzik. A Szolgáltató és az Ügyfél előzetes megállapodását kivéve a Szolgáltató a végfelhasználói tanúsítványokhoz tartozó magánkulcsok generálását csak abban az esetben végzi, amennyiben a magánkulcs és a hozzá tartozó tanúsítvány tárolása aláírás létrehozó eszközön történik. A Szolgáltató a kulcspárt közvetlenül az aláírás létrehozó eszközben hozza létre, azt semmilyen más módon nem tárolja és menti. Kivételt jelen ez alól a titkosító tanúsítvány, aholis a Szolgáltató az Ügyféllel való előzetes megállapodás alapján eltérhet a titkosító tanúsítványokhoz tartozó kulcspár generálása során a fenti előírásoktól.

6.1.2 Magánkulcs eljuttatása a Végfelhasználóhoz

A végfelhasználók magánkulcsát nem kell továbbítani, ha azt az Ügyfél saját maga állítja elő. Amennyiben a Szolgáltató generálta a végfelhasználói kulcspárt, akkor az eszközt biztonságos módon közvetlenül juttatja el az Átvevőhöz.

6.1.3 Nyilvános kulcs eljuttatás a tanúsítvány kibocsátóhoz

Amennyiben a kulcsgenerálást az Ügyfél végzi, a nyilvános kulcsot a már sikeresen regisztrált Igénylő védett csatornán küldi meg a regisztrációs szervezetnek, amely – miután sikeresen ellenőrizte, hogy az Igénylő által megküldött nyilvános kulcsnak megfelelő magánkulccsal valóban rendelkezik-e az Igénylő – szintén védett csatornán továbbítja a tanúsítványkibocsátó szervezetnek. A tanúsítvány kibocsátást követően a Szolgáltató - az Ügyfél erre vonatkozó kifejezett rendelkezését kivéve – közzéteszi tanúsítványtárában.

Amennyiben a végfelhasználói tanúsítványhoz a kulcspárt a Szolgáltató generálja, úgy nincs szükség a nyilvános kulcs továbbítására.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

A Szolgáltató szolgáltatói tanúsítványai elérhetőek a Szolgáltató honlapján (1.1.2 pont). A honlapon való elérés mellett a Szolgáltató tanúsítványait szabványos módon a tanúsítványban feltüntetett AIA:CAIssuer mezőkön keresztül is elérhetővé teszi.

6.1.5 Kulcsméretek

A Szolgáltató által alkalmazott kulcspárok (szolgáltatói és végfelhasználói tanúsítványok esetén egyaránt) hossza megfelel a kibocsátáskor hatályos szabványokban előírt hosszúságnak. Bővebben lásd a 6.1 pontban foglaltakat.

6.1.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét a Szolgáltató által használt rendszer két szempontból ellenőrzi:

- a paraméterekhez felhasznált véletlenszám-generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),
- a paraméterekre vonatkozó feltételek, összefüggések teljesülésének ellenőrzése.

A véletlenszám-generálás megfelelőségének ellenőrzésének alapja, hogy a rendszerben használt valamennyi kriptográfiai hardver modul képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül.

A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám-generálásukat, melyek hibás teszt esetén leállnak.

6.1.7 A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően

6.1.7.1 A Köztes Hitelesítő Egység kulcsa

A Köztes Hitelesítő egység kulcsa kizárólag a következő célokra használható:

- Végfelhasználói tanúsítványok aláírására
- Alárendelt elektronikus aláírással kapcsolatos szolgáltatások hitelesítésére vonatkozó tanúsítványok aláírására
- Belső szolgáltatói tanúsítványok aláírására (pl. OCSP, CRL)
- Tesztelési célra, amennyiben az éles célra a Köztes Hitelesítő Egység aláírása szükséges

6.1.7.2 A Végfelhasználó tanúsítványok

A Végfelhasználó tanúsítványok az alábbi célokra használható:

- Authentikációs tanúsítvány: véletlen adaton történő hitelesítés végzése azonosítás céljából a tanúsítványhoz tartozó magánkulccsal. A végzett művelet technikailag megegyezik az aláírással, de joghatás nem rendelődik hozzá.
- Titkosító tanúsítvány: adatkódolás, illetve dekódolás
- DV SSL tanúsítvány: kommunikáció titkosítására a kliens és a szerver között

a belefoglalt X509v3 biteknek megfelelően.

DV SSL tanúsítvány esetén a KeyEnciperment, KeyAgreement és KeyExchage bitek, titkosítónál a KeyEnciperment, míg authentikációs tanúsítványnál a DigitalSignature bit kerül beállításra.

6.2 Magánkulcs védelem és kriptográfiai modul előírások

6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások

A szolgáltatói kulcsok létrehozása, mentése, tárolása és megsemmisítése kapcsán a Szolgáltató az alábbiak szerint jár el:

- a kulcsok létrehozása, tárolása, mentése, helyreállítása, megsemmisítése fizikailag biztonságos környezetben, kettős személyi ellenőrzés mellett (két bizalmi munkakört betöltő munkatárs együttes jelenlétében) valósul meg (lásd 6.1.1.1 pont),
- a hitelesítő egységek kulcsai a vonatkozó szabványoknak megfelelően legalább EAL4 tanúsítással rendelkező, az ISO/IEC 15408 vagy ezzel ekvivalens IT biztonsági elvárás szerint, vagy az ISO/IEC 19790 vagy FIP PUB 140-2 level 3 megfelelő hardver kriptográfiai eszközben kerülnek generálásra, tárolásara, illetve felhasználásra (lásd 6.1.1.2 pont),

- 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-, CRL és OCSP aláíró kulcsai különböznek minden más funkcióra szolgáló kulcstól,
- a szolgáltatói kulcsfrissítés out-of-band cserével történik,
- biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a Szolgáltató gondoskodik a kulcs védelméről,
- 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).

6.2.2 Magánkulcs többszereplős (n-ből m) használata

A magánkulcs többszereplős használatára vonatkozó részletszabályokat a Szolgáltató Biztonsági Szabályzata tartalmazza.

6.2.3 Magánkulcs letétbe helyezése

Lásd a 4.12 pontban foglaltakat.

6.2.4 Magánkulcs mentése

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

- a Gyökér Hitelesítő Egység aláíró magánkulcsa,
- a Köztes Hitelesítő Egység aláíró magánkulcsa.

A mentés során a magánkulcsot generáló kriptográfiai hardver modulból – a kriptográfiai hardver modul típusának megfelelően - intelligens kártyákra több darabban, védetten másolódik át a magánkulcs vagy ún. backup HSM modulba kerül.

A magánkulcs mentése és visszaállítása a Szolgáltató védett számítógépes termében, két bizalmi munkakört betöltő munkatárs együttes jelenlétében, jegyzőkönyvezetten történik. 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.

6.2.5 Magánkulcs archiválása

A Szolgáltató sem a szolgáltatói, sem a végfelhasználói magánkulcsokat nem archiválja.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba, vagy onnan történő exportja

Lásd a 6.2.4 pontban foglaltakat.

6.2.7 Magánkulcs tárolása kriptográfiai modulban

Lásd a 6.2.1 pontban foglaltakat.

6.2.8 Magánkulcs aktiválásának módja

A szolgáltatói kulcsok aktiválásának módját a Szolgáltató Biztonsági Szabályzata részletezi.

6.2.9 Magánkulcs deaktiválásának módja

A szolgáltatói kulcsok deaktiválásának módját a Szolgáltató Biztonsági Szabályzata részletezi.

6.2.10 Magánkulcs megsemmisítésének módja

A szolgáltatói kulcsokat a Szolgáltató olyan módon semmisíti meg, hogy az aláíró kulcsok ne legyenek visszanyerhetőek. A megsemmisítése során a Szolgáltató olyan biztonságos törlési folyamatokat alkalmaz, melyek ténylegesen felülírják a kulcsok összes előfordulását az összes olyan tárolóeszközön, melyen a kulcs példányai előfordulhattak.

6.2.11 A kriptográfiai modulok értékelése

Lásd a 6.2.1 pontban foglaltakat.

6.3 A kulcspárkezelés további szempontjai

A Szolgáltató a szolgáltatói aláíró kulcsokat a tanúsítványban feltüntetett módon és érvényességi időtartam alatt használja. A Szolgáltató által használt magánkulcs kompatibilis a 6.1.1 pontban részletezett tanúsítványok aláírására alkalmazott hash és aláíró eljárásokkal és kulcshosszokkal.

A Gyökér Hitelesítő Egység tanúsítványai tanúsítvány attribútuma megfelel az ITU-T X509 szerinti kulcshasználatnak.

6.3.1 Nyilvános kulcs archiválása

A Regisztrációs szervezet minden, a Szolgáltató által előállított tanúsítványt archivál, az alábbi időszakra:

- szolgáltatói tanúsítványok: az érvényesség lejártától számított 10 évig,
- végfelhasználói tanúsítványok: az érvényesség lejártától számított jogszabályban meghatározott ideig (lásd 5.5.2 pont).

Szolgáltatói kulcs használati idejének végén archiválható, hogy esetleg később (nem meghatározott idő múlva) újra használatba vehető legyen.

6.3.2 A tanúsítványok és kulcspárok használatának periódusa

	Típus	**Tanúsítvány élettartam**	**Kulcs élettartam**
1	Végfelhasználói titkosító, authentikációs és DV SSL tanúsítvány	legfeljebb 3 év	A Szolgáltató a kulcs élettartamára vonatkozóan korlátot nem állapít meg, de bármikor előírhatja az új kulcsgenerálás szükségességét
2	Szolgáltatói tanúsítvány	maximum 20 év	A tanúsítvány érvényességi idejével megegyező.
3	CRL és OCSP aláíró magánkulcs	maximum 15 év	A tanúsítvány érvényességi idejével megegyező.

Az érvényességi időtartam a tanúsítványban feltüntetésre kerül. A tanúsítványok érvényességének kezdete a kibocsátás időpontjával egyezik meg.

Valamennyi fenti tanúsítványban szereplő nyilvános kulcs érvényességi ideje annak kriptográfiai biztonságnak megfelelő voltáig tart.

6.4 Aktiváló adat

Végfelhasználói tanúsítványok esetén az aktiváló adatokkal kapcsolatos előírások kizárólag abban az esetben értelmezhetőek, ha a kulcspárt a Szolgáltató állítja elő kriptográfiai hardvereszközre (Ügyféleszköz).

A szolgáltató tanúsítványok esetén a kulcspár helyreállítására és telepítésére a 6.2 pont rendelkezései tartalmaznak előírásokat.

6.4.1 Aktiváló adat generálás és telepítés

A Szolgáltató az Ügyféleszközhöz tartozó aktiváló adatokat (PIN kód) biztonságos módon, az eszközöktől elkülönítetten állítja elő. A PIN kód beállítása az Ügyféleszköz tanúsítója által előírt módon történik.

A Szolgáltató az aktiváló adatot lezárt borítékban juttatja el Végfelhasználóhoz. Az aktiváló adat megadását és cseréjét követően van lehetősége Végfelhasználónak Tanúsítványa aktiválására (lásd 4.9.3.2 pont, amennyiben azt Szolgáltató felfüggesztett állapotban feltöltötte Ügyféleszközre) vagy Ügyféleszközre történő feltöltésére (lásd 4.3 pont, amennyiben Szolgáltató csak a magánkulcs generálását végezte el Ügyféleszközre, a tanúsítványt pedig Ügyfélmenüből teszi elérhetővé).

6.4.2 Aktiváló adat védelme

A Szolgáltató az Ügyféleszközhöz tartozó aktiváló adatokat (PIN kód) csak abból a célból rögzíti, hogy azt a szolgáltatást igénybe vevő személy számára – másolat megőrzése nélkül – átadhassa.

6.4.3 Egyéb aktiváló adattal kapcsolatos előírások

A Végfelhasználónak gondoskodnia kell arról, hogy a részére átadott kriptográfiai eszközök aktiválása és deaktiválása biztonságos módon történjen.

6.5 Informatikai biztonsági előírások

A Szolgáltató rendszereit csak az arra jogosult személyek érhetik el. A Szolgáltató a belső zónák határait tűzfalakkal védi és megteszi a szükséges intézkedéseket arra vonatkozóan, hogy az érzékeny adatok az adathordozók újrafelhasználása során ne legyenek feltárhatóak.

A Szolgáltató által alkalmazott Jogosultságkezelési szabályzat biztosítja, hogy a tanúsítványtárhoz az adatok hozzáadása, illetve a tanúsítványállapot változásával kapcsolatos intézkedéseket (felfüggesztés, visszavonás, aktiválás) csak az arra jogosultak számára legyen elérhető.

A végfelhasználó tanúsítványhoz tartozó kulcspár generálására, valamint a tanúsítvány kibocsátására a Szolgáltató védett szerverszobájában kerül sor (5.1.1. pont). A Szolgáltató a jogosulatlan hozzáférések kiszűrésére monitorozó és riasztó eszközöket alkalmaz.

6.5.1 Speciális informatikai biztonsági műszaki követelmények

A Szolgáltató a Biztonsági Szabályzatában részletezett módon multifaktorális azonosítást követel meg minden tanúsítványkiadásra jogosult felhasználó esetében.

6.5.2 Informatikai biztonság értékelése

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

6.6 Életciklusra vonatkozó biztonsági előírások

6.6.1 Rendszerfejlesztési óvintézkedések

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

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

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

6.6.2 Biztonságkezelési előírások

A Szolgáltató olyan megbízható rendszereket és termékeket használ, amelyek védettek a módosítás ellen és biztosítják az ellátott műveletek műszaki biztonságát és megbízhatóságát. A Szolgáltató különös figyelmet fordít a biztonságra a beszerzések során is: a kulcsfontosságú rendszereinek szállítói a Beszerzési Szabályzat szabályai szerint értékelt beszállítók, illetőleg a beszerzett eszközök értékelt eszközök. Kiválasztásuk gondos mérlegelés alapján történt, a beruházás megtörténte után a kapcsolat hosszabb távú. Az eszközök gyártói számos referenciával és megbízható háttérrel rendelkező szervezetek. Ezen szabályok biztosítják, hogy Szolgáltató eszközeihez szükség esetén megkapja a szükséges támogatást, illetve meghibásodás esetén a szállítóval szembeni jótállási, szavatossági igények érvényesíthetők legyenek. A felhasznált, beépített eszközök nagyrészt a kereskedelmi forgalomban könnyen beszerezhetők, így azok pótlása számos forrásból, viszonylag gyorsan megoldható.

A Szolgáltató védi az informatikai rendszereit és információit a vírusoktól, a rosszindulatú és nem engedélyezett szoftverektől. A Szolgáltató olyan eljárásokat alkalmaz, amely biztosítja, hogy a biztonsági javítások ésszerű időn (6 hónapon) belül alkalmazásra kerüljenek. A Szolgáltató nem alkalmazza a biztonsági javításokat abban az esetben, ha azok további biztonsági réseket tartalmaznak, illetve ha azok instabilitást okoznak.

6.6.3 Az életciklusra vonatkozó biztonsági előírások

A Szolgáltató folyamatosan monitorozza a kapacitáskihasználtságot és előrejelzéseket készít annak érdekében, hogy elegendő tárhely és feldolgozási kapacitás álljon rendelkezésre a jövőben is.

6.7 Hálózati biztonság

A Szolgáltató szolgáltatása során használt rendszereit különböző ún. biztonsági zónákba sorolja. A biztonsági zónákba sorolást követően a Szolgáltató gondoskodik arról, hogy az egyes zónák között a kommunikáció biztonságos módon történjen. A Szolgáltató a szolgáltatásnyújtás során minden olyan kapcsolatot, portot tilt vagy eltávolít, amelyek nem kapcsolódnak a szolgáltatásnyújtáshoz. A biztonsági zónákhoz való hozzáférést a Jogosultkezelési Szabályzat tartalmazza.

A Szolgáltató a szolgáltatói rendszerek számára külön hálózatot alakított ki. A produktív rendszerek elkülönülnek a fejlesztési, tesz és egyéb felhasználású rendszerektől. A Szolgáltató hálózati kapcsolatát redundáns módon alakította ki azokban az esetekben, aholis a szolgáltatáshoz nagy rendelkezésre állású külső elérés szükséges.

A biztonság folyamatos fenntartása érdekében a Szolgáltató rendszeresen (negyedévenkénti vagy szignifikáns hálózati változás esetén mihamarabbi) sebezhetőségi ellenőrzést végez.

A Szolgáltató a sebezhetőségi ellenőrzések mellett éves periódusban, vagy szignifikáns infrastrukturális változás esetén mihamarabb betörési ellenőrzést is végez.

7 Tanúsítvány, CRL és OCSP profilok

A szolgáltató a tanúsítványok tartalmát és funkcióját elsősorban tanúsítvány profilokon keresztül szabályozza. A tanúsítvány Alanya, Alanyai meghatározzák a bele foglalandó alany adatokat, míg a felhasználás célja az X509 kiterjesztéseken keresztül meghatározza a tanúsítvány felhasználhatóságát.

7.1 Tanúsítványprofil

A Szolgáltató az alábbi tanúsítványprofilokat alkalmazza:

1. **<u>A végfelhasználó tanúsítványban az alábbi kiadásra vonatkozó adatok találhatóak meg.</u>**

Név	Tartalom	Megjegyzés
Verzió (Version)	3 (0x2)	
Sorszám (Serial Number)	sorszám	24 bit entrópiát tartalmazó sorszám
Kiadói aláírás algoritmusa (SignatureAlgorithm)	sha256withRSA	
Kiadó (Issuer)	A tanúsítványt kiadó CA adatai, a CA tanúsítványban található adatokkal egyezően	
Érvényesség (Validity)	A tanúsítvány érvényességének kezdete és vége	
A tanúsítvány aláírása	A tanúsítványt kiadó CA kulcsával végzett aláírás eredménye	

2. A Személyes végfelhasználói tanúsítványok adattartalma, nevek értelmezése (authentikációs, titkosító)

Mezőnév	Definíció
Subject mezők	
commonName (CN) Kötelező	A természetes személynek – amennyiben értelmezett, közhiteles adatbázis szerinti - az azonosításra szolgáló igazolvány szerinti teljes neve.
surname (SN) Kötelező	A commonName mezőben szereplő név vezetéknév része, a névfelbontási javaslat szerint.
givenName (G) Kötelező	A commonName mezőben szereplő név keresztnév része, a névfelbontási javaslat szerint.
emailAddress (E) Opcionális/Kötelező	Személy saját email címe (opcionális).
serialNumber (CNSN) (1.) Kötelező	OID alapú permanentID (szolgáltató egyedi szervezetazonosítója+entitás azonosítója).
serialNumber (2.) Opcionális	Egyedi személyazonosító az ügyfél, vagy ügyfelek egy csoportja által kért tartalommal.
countryName (C) Kötelező	Személy lakóhelyének országa, ISO 3166-1 szerinti kétbetűs országkód.
localityName (L) Opcionális	Személy lakhelyének helységneve.
Subject Alternative Name mezők	
email Opcionális	Személy saját email címe. Megegyezik az E mezővel.
othername Kötelező	OID alapú szolgáltatóazonosító

Megkötések:

A mezőkből csak egy szerepelhet, kivéve a serialNumber mezőt.

Nem szereplő mezők:

title, pseudonym, organizationName, organizationalUnitName, organizationIdentifier.

A tanúsítványba foglalt adattartalom értelmezése:

A magánszemély alany teljes neve található a CN mezőben, a vezetékneve az SN mezőben, kereszt neve a G mezőben. A személy email címe az emailAddress és a SubjectAlternativeName/email mezőben is egyaránt megtalálható.

A szolgáltatónál a személyhez rendelt első serialNumber a felhasználóhoz rendelt egyedi szám.

A C és L a magánszemély lakcím adatai alapján kitöltött országkódot és várost tartalmazza.

3. Munkatársi végfelhasználói tanúsítványok adattartalma, nevek értelmezése (authetnikációs, titkosító)

Mező neve	Definíció
Subject mezők	
commonName (CN) Kötelező	A természetes személynek – amennyiben értelmezett, közhiteles adatbázis szerinti - az azonosításra szolgáló igazolvány szerinti teljes neve..
surname (SN) Kötelező	A commonName mezőben szereplő név vezetéknév része, a névfelbontási javaslat szerint.
givenName (G) Kötelező	A commonName mezőben szereplő név keresztnév része, a névfelbontási javaslat szerint.
serialNumber (1.) (CNSN) Kötelező	OID alapú permanentID (szolgáltató egyedi szervezetazonosítója+személy azonosítója).
serialNumber (2.) Opcionális	Egyedi személyazonosító az ügyfél, vagy ügyfelek egy csoportja által kért tartalommal és formátumban (lásd: kitöltési szabályok).
emailAddress (E) Opcionális/Kötelező	A természetes személy saját email címe (Opcionális).
organizationName (O) Kötelező	A szervezet hiteles cégkivonatában (más típusú szervezet esetén ennek megfelelő okiratában) szereplő neve vagy rövid neve.
organizationalUnitName (OU) Opcionális	Az organizationName mező által azonosított szervezeten belüli szervezeti egység neve. Csak igazoltan létező szervezeti egység nevét tartalmazhatja. Ennek hiányában a mező nem szerepel a tanúsítványban.
organizationIdentifier Kötelező	A szervezet nyilvántartott azonosítója (lásd: kitöltési szabályok).
title (T) Opcionális	A tanúsítványalany szervezetben viselt szerepe, munkaköre. Minden esetben csak igazolt adat kerülhet ebbe a mezőbe. Egyes titulusok csak kitüntetett esetekben adhatók ki: pl. „ügyvéd”: csak ügyvédi tanúsítványra jogosultaknál. „önálló cégjegyzésre jogosult” vagy „együttes cégjegyzésre jogosult”: cégjegyző tanúsítványok jelzésére.
countryName (C) Kötelező	Szervezet hivatalos székhelyének országa, ISO 3166-1 szerinti kétbetűs országkód.
localityName (L) Kötelező	Szervezet hivatalos székhelyének helységneve.

Subject Alternative Name mezők	
email Opcionális/Kötelező	Személy saját email címe (opcionális). Megegyezik az E mezővel.
othername Kötelező	OID alapú szolgáltatóazonosító
dirname Opcionális	Speciális esetekben az Alany neve a CommonName-ben szereplőtől eltérő írásmóddal.

Megkötések:
A mezőkből csak egy szerepelhet, kivéve a serialNumber mezőt.

Nem szereplő mezők:
Pseudonym

A tanúsítványba foglalt adattartalom értelmezése:
A magán személy alany teljes neve található a CN mezőben, a vezetékneve az SN mezőben, keresztneve a G mezőben.
A személy email címe az emailAddress és a SubjectAlternativeName/email mezőben is egyaránt megtalálható.
A szolgáltatónál a személyhez rendelt első serialNumber a felhasználóhoz rendelt egyedi szám.
A személy a tanúsítványban található O nevű szervezethez tartozik (azon belül, ha megjelölt, az OU szervezeti egységhez), és a szervezet egyedi azonosítója található meg az organizationIdentifier mezőben. (A mező kitöltésére a vonatkozó ajánlások szerint történik.)
A C és L a szervezet székhelyének vagy telephelyének ellenőrizhető adatok alapján kitöltött országkódot és várost tartalmazza.

4. Az ügyvédi tanúsítvány – a munkatársi tanúsítványok egy speciális esete.

Mezőnév	Definíció
Subject mezők	
commonName (CN) Kötelező	Az ügyvéd (tanúsítványalany) közhiteles adatbázis szerinti teljes személyneve.
surname (SN) Kötelező	A commonName mezőben szereplő név vezetéknév része, a névfelbontási javaslat szerint.
givenName (G) Kötelező	A commonName mezőben szereplő név keresztnév része, a névfelbontási javaslat szerint.
serialNumber (1.) (CNSN) Kötelező	OID alapú permanentID (szolgáltató egyedi szervezetazonosítója+személy azonosítója).
serialNumber (2.) Kötelező	A kamarák által nyilvántartott ún. Kamarai Azonosító Szám (KASZ) az alábbi formátumban: kasz:36XXXXXX
title (T) Kötelező	A tanúsítány alanyának hivatása, jelen esetben: „ügyvéd”.
emailAddress (E) Kötelező	A természetes személy saját email címe.
organizationName (O) Kötelező	Az ügyvédi iroda vagy egyéni ügyvéd kamara által bejegyzett neve (egyéni ügyvéd esetén az “egyéni ügyvéd” megnevezéssel).
organizationalUnitName (OU) Opcionális	Az ügyvédi irodán belüli szervezeti egység neve. Csak igazoltan létező egységet tartalmazhat. Ennek hiányában a mező nem szerepel a tanúsítványban.
countryName (C) Kötelező	Az ügyvédi iroda vagy egyéni ügyvéd kamara által bejegyzett címe szerinti ország, ISO 3166-1 szerinti kétbetűs országkód.
localityName (L) Kötelező	Ügyvédi iroda / egyéni ügyvéd bejegyzett címének helységneve.
Subject Alternative Name mezők	
email Kötelező	Személy saját email címe. Megegyezik az E mezővel.
othername Kötelező	OID alapú szolgáltatóazonosító
dirname Kötelező	Ügyvéd ügyvédi neve, az igényléskor az igénylő ügyvéd által kért módon.

Megkötések:
A mezőkből csak egy szerepelhet, kivéve a serialNumber mezőt, abból több.
A serialNumber mezőkből az első a permanens azonosítót a második az ügyvéd KASZ számát tartalmazza, ez utóbbit egyeztetett formában. (“kasz:<azonosító>)

Nem szereplő mezők:
Pseudonym, organizationIdentifier

A tanúsítványba foglalt adattartalom értelmezése:
A magán személy alany teljes neve található a CN mezőben, a vezetékneve az SN mezőben, keresztneve a G mezőben. A személy foglalkozása az „ügyvéd”, mely a T mezőben találhat.
A személy email címe az emailAddress és ez a SubjectAlternativeName/email mezőben is egyaránt megtalálható.
A szolgáltatónál a személyhez rendelt serialNumber a felhasználóhoz rendelt egyedi szám.
A személy a tanúsítványban található O nevű szervezethez tartozik (azon belül, ha megjelölt, az OU szervezeti egységhez).
A C és L a szervezet székhely vagy egyéni ügyvéd esetén lakóhely ellenőrizhető adatai alapján kitöltött országkódot és várost tartalmazza.

5. DV SSL tanúsítványok adattartalma,

A DV SSL tanúsítvány olyan tanúsítvány, ahol csak a domain név feletti kontroll kerül ellenőrzésre.

Mezőnév	Definíció
Subject mezők	
commonName (CN) Opcionális	Ha a mező jelen van, akkor egy domain nevet tartalmazhat a SAN/dNSName-ben szereplők közül. Csak létező és az igénylő által használt domain név tüntethető fel. A DV SSL tanúsítvány nem lehet álneves, illetve nem tartalmazhat wildcard/UCC karaktert.
Subject Alternative Name mezők	
DNSname Kötelező	A tanúsítvány által hitelesített weboldalak domain neve. Nem tartalmazhat wildcard/UCC tagot.

Megkötések:

Nem szereplő mezők:
title, pseudonym, givenName, surname, serialNumber, organizationName, organizationalUnitName, organizationIdentifier, countryName, localityName

A tanúsítványba foglalt adattartalom értelmezése:
A tanúsítvány SSL célra került igénylésre.
A SubjectAlternativeName/DNSName mezőben találhatóak a hitelesíteni kívánt domain nevek, ezek közül egy a CN mezőben is megtalálható, ha az kitöltésre került.
A hitelesített domain nevek nem tartalmazhatnak wildcard/UCC tagot.

6. Teszt tanúsítvány

A Szolgáltató titkosító és authetnikációs tanúsítvány típus és osztály esetén jogosult teszt tanúsítvány kibocsátására a tanúsítvány osztályban foglalt előírások megtartásával. Teszt tanúsítvány esetén a Szolgáltató minden esetben egyértelműen jelzi (minimálisan a CN mezőben feltüntetve), hogy az adott tanúsítvány csak és kizárólag tesztelési célra használható.

DV SSL tanúsítvány esetén a tesz tanúsítvány nem értelmezett.

Teszt tanúsítványt igényelhet Szolgáltató munkavállalója a Szolgáltató belső ellenőrének jóváhagyását követően, illetve igényelhet az Ügyfél.

7. Végfelhasználói közös tanúsítvány kiterjesztések

Minden végfelhasználói tanúsítvány tartalmazza a következő tanúsítvány mezőket:

Kiterjesztés	Kritikusság (igen/nem)	Tartalom	Megjegyzés
basicConstraints	igen	CA:FALSE	-
subjectKeyIdentifier	nem	Alany saját kulcsazonosítója	-
authorityKeyIdentifier	nem	A tanúsítvány kiadó CA kulcsazonosítója	-
crlDistributionPoints	nem	A CRL elérhetősége	Három URL http protokollon
authorityInfoAccess:CAIssuers	nem	A kiadói tanúsítvány elérhetősége	Három URL http protokollon
authorityInfoAccess:OCSP	nem	Az OCSP elérhetősége	Három URL http protokollon

8. Végfelhasználói kulcshasználat kiterjesztések

Az egyes felhasználási célok és alanyok eltérő kiterjesztéseket jelenthetnek a tanúsítvány X509 v3 mezői között is.

	Kritikus (igen/nem)	Titkosító	Authentikációs	DV SSL
Keyusage	Igen	KeyEncipherment	digitalSignature	keyAgreement, KeyEncipherment, KeyExchange
extendedKeyUsage	Nem	Nem tartalmazza.	clientAuth	serverAuth

9. CertifcatePolicies azonosító

A Szolgáltató, ahol lehet kizárólag szabványos azonosítót használ, amely mellé opcionálisan szolgáltatói azonosítót is rendelhet.

Felhasználási cél / Profil	Authentikációs	Titkosító	SSL
Személyes tanúsítvány	LCP [22.], NCP [23.], NCP +[24.]	LCP [22.]	-
Munkatársi tanúsítvány	LCP [22.], NCP [23.], NCP +[24.]	LCP [22.]	-

Felhasználási cél / Profil	Authentikációs	Titkosító	SSL
Ügyvédi tanúsítvány	LCP [22.], NCP [23.], NCP +[24.]	LCP [22.]	
DV SSL tanúsítvány	-	-	DVCP

10. QcType és SemanticIdentifier

Fokozott tanúsítvány kiadás esetén a tanúsítvány típusa és birtokosa jelezhető a QcStatements/QcType mezővel, értékként a következőket vehetik fel:

- Id-etsi-qct-web – DV SSL tanúsítvány esetén (röviden: web)
- titkosító és authentikációs tanúsítvány nem tartalma ilyet

A tanúsítványba továbbá foglalható továbbá a QcStatements/SemanticIdentifier, opcionális jelleggel, jelentése:

- id-etsi-qcs-semanticsId-Natural
  ha a tanúsítványban található személy azonosítója a szabványos formák egyikének felel meg (röviden:natural)
- id-etsi-qcs-SemanticsId-Legal
  ha a tanúsítványban található szervezety azonosítója a szabványos formák egyikének felel meg (röviden:legal)
- Titkosító, authentikációs tanúsítvány nem tartalmaz ilyet.

Az alábbi táblázat tartalmazza a Qctype tartalmát egyes típusok esetén, illetve azt, hogy az opcionális semanticIdentifier, beállítása esetén mely típusban milyen értéket kell felvegyen. A táblázat üres értéke azt jelzi, hogy ott nem beállítható.

A titkosító, illetve authentikációs tanúsítvány nem tartalmazza egyiket sem.

11. Egyéb certificate policyvel kapcsolatos kérdések

A Szolgáltató nem használ „policy constrainst” kiterjesztést. A Szolgáltató nem használ kritikus certificatePolicies kiterjesztést.

A szolgáltató a policyqialfierek közül csak az „explicitText” mezőt használja, melynek tartalma ember által olvasható formában a tanúsítványra érvényes policy rövid szöveges leírása, megjelölése vagy kiegészítése korlátozó információkkal.

12. Igényelhető alany és kiterjesztés kombinációk

A táblázat meghatározza, hogy az adott profilú tanúsítvány milyen felhasználásra vehető igénybe. (A profil meghatározza a Subject adatok tartalmát, míg a felhasználás a tanúsítvány X509v3 Extension mezőinek tartalmába szól bele.)

Felhasználási cél / Profil	Authentikációs	Titkosító	SSL
Személyes tanúsítvány	x	x	-
Munkatársi tanúsítvány	x	x	-

Felhasználási cél Profil	Authentikációs	Titkosító	SSL
Ügyvédi tanúsítvány	x	x	-
DV SSL tanúsítvány	-	-	x

13. Szolgáltatói Főtanúsítvány profilja

Mező neve	Tartalom	Kritikus (critical)?
basicConstraints	CA:TRUE	Igen
Certificate Serial Number	nem szekvenciális minimum 20 bit entrópiával	Nem
keyusage	keyCertSing, cRLSign	Igen
private and public key	lásd minimum algoritmusok táblázat	Nem
Validity	tanúsítványban szereplő notbefore-notafter érték	Nem
Subject Key identifier	subject kulcs hash	Nem
subject:commonName (CN)	tanúsítvány kiadó neve	Nem
subject:countryName (C)	HU	Nem
subject:localityName (L)	Budapest	Nem
subject:organizationalUnitName	Tanúsítványkiadók (Certification Services)	Nem
subject:organizationName (O)	NetLock Kft.	Nem
Signature	Kiadó aláírása SHA256 algoritmussal	Nem

Megkötések:

Nem szereplő mezők:

certificatePolicy, extendedKeyusage

14. Szolgáltatói Köztes kiadói tanúsítvány

Mező neve	Tartalom	Kritikus (critical)?
AIA:Ca issuers	A tanúsítványt kiadó CA tanúsítványának elérhetősége http URL-en	Nem
AIA:OCSP	A tanúsítványt kiadó CA OCSP szolgáltatásának elérhetősége http URL-en	Nem
basicConstraints	CA:TRUE	Igen
CDP	A tanúsítványt kiadó CA CRL szolgáltatásának elérhetősége http URL-en	Nem
Certificate Serial Number	Nem szekvenciális sorozatszám legalább 20 bit entrópiával	Nem
keyusage	keyCertSing, cRLSign	Igen
private and public key	lásd minimum algoritmusok táblázat	Nem
Validity	tanúsítványban szereplő notbefore-notafter érték	Nem
Subject Key identifier	Köztes kiadó kulcs hash	Nem
Authority Key dentifier	Legfelsőbb kiadó kiadói kulcs hashe	Nem
subject:commonName (CN)	tanúsítvány kiadó neve	Nem
subject:countryName (C)	HU	Nem
subject:localityName (L)	Budapest	Nem
subject:organizationName (O)	NetLock Kft angol vagy magyar elnevezéser	Nem
Signature	Kiadó aláírása SHA256 algoritmussal	Nem

Megkötések:

Nem szereplő mezők:

certificatePolicy, extendedKeyusage

7.1.1 Verzió szám(ok)

A Szolgáltató az X.509v3 specifikáció szerint bocsátja ki a tanúsítványokat.

7.1.2 Tanúsítvány kiterjesztések

A Szolgáltató az X.509v3 specifikáció szerinti tanúsítványkiterjesztéseket használja úgy, hogy a kritikus mezőket jelzi.

7.1.3 Az algoritmus objektum azonosítója

A Szolgáltató a tanúsítványban jelzi azt az algoritmust és paramétereit, amellyel a tanúsítvány hitelesítésre került.

7.1.4 Névformák

Az Alany névformái tekintetében a 3.1 pont rendelkezései az irányadóak.

A tanúsítvány "Issuer" mezőjében szereplő érték megegyezik a kibocsátó Tanúsítványának "Subject" mezőjében szereplő értékkel.

7.1.5 Névhasználati megkötések

A Szolgáltató az alkalmazott névhasználati megkötéseket a "nameConstraints" mezőben tünteti fel.

7.1.6 Hitelesítési Rend azonosítója

A Szolgáltató a Hitelesítési Rend alapján kibocsátott tanúsítványokba jelzi a Hitelesítési Rend OID azonosítóját.

7.1.7 A szabályzati korlátozás kiterjesztés használata

A Szolgáltató nem alkalmaz erre vonatkozóan külön előírásokat.

7.1.8 S Szabályzatminősítő szintaxis és szemantika

A Szolgáltató a Hitelesítési rend (Certificate Policy) kiterjesztés Szabályzatminősítő (Policy Qualifier) mezejében rövid információt helyezhet el a Tanúsítvány felhasználhatóságával kapcsolatban. A mezőnek tartalmazza a Szolgáltatási szabályzat on-line elérhetőségét is (URL).

7.1.9 A kritikus Hitelesítési Rend kiterjesztés feldolgozása

A Szolgáltató nem alkalmaz külön megkötéseket.

7.2 Tanúsítványvisszavonási profil

7.2.1 Verziószám(ok)

A szolgáltat x509 szabványnak és az RFC5280 szabványnak megfelelő és az visszavonási listákat bocsát ki, a szabályzatban meghatározott sűrűséggel és tartalommal.

7.2.2 Tanúsítvány visszavonási lista kiterjesztések

A CRL tartalmában nincs kritikus jelzéssel ellátott mező. A Szolgáltató a visszavonási listákat egyesével növekvő sorozatszámmal látja el.

7.2.2.1 A tanúsítvány visszavonási (CRL) lista profilja

Mező	Tartalom
Version	V2
Issuer	A CRL-t kiadó tanúsítványkiadó Issuer adata
Last update	Utolsó kibocsátás dátuma
Next update	Következő kibocsátás dátuma
Signature	Kibocsátó elektronikus aláírása
CRL entry	Az érvénytelenített tanúsítvány sorozatszáma, érvénytelenítés dátuma, időpontja, oka RFC 5280-nak megfelelő formában.
CRL entry extension	

7.2.2.2 A CRL-t aláíró tanúsítvány profilja

Mező neve	Tartalom	Kritikus (critical)?
basicConstraints	CA:TRUE	Igen
Certificate Serial Number	nem szekvenciális minimum 20 bit entrópiával	Nem
keyusage	CRLSign	Igen
private and public key	lásd minimum algoritmusok táblázat	Nem
Validity	tanúsítványban szereplő notbefore-notafter érték	Nem
Subject Key identifier	subject kulcs hash	Nem
subject:commonName (CN)	Hozzárendelt kiadóra utaló név	Nem
subject:countryName (C)	HU	Nem
subject:localityName (L)	Budapest	Nem
subject:organizationalUnitName	Tanúsítványkiadók (Certification Services)	Nem
subject:organizationName (O)	NetLock Kft.	Nem

Megkötések:

Nem szereplő mezők:
certificatePolicy, extendedKeyusage

7.3 Online tanúsítvány-állapot szolgáltatás (OCSP) profil

7.3.1 Verziószám(ok)

Az OCSP szolgáltatás során a Szolgáltató az RFC 6960 szabvány V1 verziója alapján létrehozott tanúsítványállapot kérdéseket és válaszokat támogatja.

7.3.2 OCSP kiterjesztések

Az OCSP válaszadó tanúsítvány tartalmazza a NoCheck kiterjesztést, így az OCSP válaszadók ügyfél általi ellenőrzése nem szükséges.

7.3.2.1 OCSP válaszadó tanúsítvány profilja

Mező neve	**Tartalom**	**Kritikus (critical)?**
basicConstraints	CA:FALSE	Igen
Certificate Serial Number	nem szekvenciális minimum 20 bit entrópiával	Nem
extendedKeyusage	OCSPSigning	Nem
keyusage	digital signature	Igen
private and public key	lásd minimum algoritmusok táblázat	Nem
Validity	tanúsítványban szereplő notbefore-notafter érték	Nem
Subject Key identifier	subject kulcs hash	Nem
Authority Key dentifier	kiadói kulcs hashe	Nem
OCSPNocheck	üres tartalom	Nem

Megkötések:

Nem szereplő mezők: certificatePolicy

8 A megfelelőség vizsgálata

A Szolgáltató – összhangban az Európai Uniós és hazai szabályozással, valamint a Hitelesítési Rendben meghatározott követelményekkel – az alábbi szabványok szerint végzi szolgáltatási tevékenységét.

Szabvány azonosító	Angol rövid elnevezés
ETSI EN 319 401 [16.]	General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1 [17.]	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
ETSI EN 319 412-1 [18.]	Certificate Profiles; Part 1: Overview and common data structures
ETSI EN 319 412-2 [19.]	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI EN 319 412-3 [20.]	Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
ETSI EN 319 412-4 [21.]	Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations

A Szolgáltató megfelelőségi vizsgálatokat és ellenőrzéseket végez, illetve végeztet annak érdekében, hogy a Szolgáltatásaival kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljenek a vonatkozó szakmai követelményeknek.

8.1 Az ellenőrzések körülményei és gyakorisága

A Szolgáltató évente külső megfelelőségi vizsgálatot hajtat végre. Amennyiben a Szolgáltató Kihelyezett Regisztrációs Egységet működtet, úgy annak a folyamatait évente ellenőrzi.

Az ellenőrzések eredményei, valamint az azok alkalmával készült dokumentumok bizalmas jellegűek, hozzáférést csak a megfelelő jogosultsággal rendelkező személyek kapnak.

A Szolgáltató a külső auditon túl saját belső ellenőrzéseket (évente egyszer) is végez, amely segítségével rendszeresen vizsgálja a korábbi auditoknak való megfelelőséget és eltérés esetén megteszi a szükséges lépéseket.

A Szolgáltató a jelen Szabályzat 1.1.2 pontjában részletezett ISO 9001, valamint ISO 27001 szabványmegfelelőségét külső auditor/értékelő szervezet értékeli és vizsgálja felül folyamatosan, legalább évente egy alkalommal.

8.2 Az értékelő és szükséges képesítése

A Szolgáltató megfelelőségi vizsgálatai lehetnek külső vagy belső ellenőrzések, illetve auditok. A Szolgáltató olyan eljárást alkalmaz, mely során biztosítja, hogy a belső ellenőrzéseket végző szervezetek, személyek függetlenek legyenek a Szolgáltató szolgáltatásokért felelős szervezeti egységétől.

A belső ellenőrzéseket csak megfelelő jogi és szakmai ismeretek birtokában lévő, olyan tapasztalt szakemberek végezhetik, akik rendelkeznek felsőfokú képesítéssel és legalább 5 éves szakmai gyakorlattal szabályozás, informatikai rendszeraudit vagy a jelen Szabályzat szerinti szolgáltatás területén.

A külső auditok/értékelések során a Szolgáltató olyan természetes vagy jogi személlyel, vagy természetes személyek csoportjával működik együtt, akik/amelyek

- képesek a jelen fejezetben megadott szabványokra vonatkozó audit elvégzésére;
- megfelelnek a 8.3 pontban foglalt követelménynek;

- megfelelő jártassággal bírnak a PKI, az IT illetve IT biztonsági megoldások, technológiák és auditok terén, valamint Kihelyezett Regisztrációs Egységnél végzett audit során annak funkcióival kapcsolatban;
- ETSI szabványok alapján végzett auditok/értékelések esetén rendelkezik vagy rendelkeznek az auditáláshoz szükséges akkreditációval
- WebTrust audit végzése esetén rendelkezik vagy rendelkeznek WebTrust audit elvégzéséhez szükséges engedéllyel;
- tevékenységét vagy tevékenységüket jogszabályok vagy szakmai etikai kódex szabályozza;
- rendelkezik az értékelő tevékenység végzéséből eredő mulasztások, hibák esetére szóló, legalább egymillió USD fedezetű biztosítással.

8.3 Az auditor és az auditált entitás kapcsolata

A külső auditokat végző értékelők függetlenek az alábbiak tekintetében:

- a vizsgált szolgáltató tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban a Szolgáltatóval;
- díjazása nem függ az audit során végzett tevékenységének végkimenetelétől.

A Szolgáltató jogosult a belső auditokat a rendszerellenőri szerepkörrel felruházott bizalmi munkatársai segítségével is elvégezni.

8.4 Az értékelés/audit által lefedett területek

Az auditok/értékelések során az alábbi területek kerülnek ellenőrzésre:

- műszaki szabványoknak való megfelelés;
- Hitelesítési rend(ek)nek és Szolgáltatási szabályzat(ok)nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a fizikai biztonság megfelelősége ;
- a személyi állomány megfelelősége;
- az IT biztonság megfelelősége;
- az adatvédelmi szabályok betartása.

8.5 A hiányosságok kezelése

A külső és belső értékelések eredményét a Szolgáltató egy értékelésjelentésben foglalja össze, amely jelentés kitér a vizsgálat területére. A dokumentum tartalmazza az ellenőrzés során felhasznált bizonyítékokat és megállapításait. A jelentés tartalmazza továbbá az ellenőrzés során feltárt hiányosságokat, eltéréseket és a kijavításukra kitűzött határidőket. A feltárt hiányosságok súlyosságuknak megfelelően az alábbi kategóriába tartoznak:

- “Enyhe” eltérés, mely kapcsán a helyesbítő intézkedéseket igazoló dokumentumokat a következő értékelés alkalmával kell bemutatni.
- “Súlyos” eltérés, mely kapcsán a megvalósított helyesbítő intézkedést igazoló dokumentum benyújtása kötelező.

A Szolgáltató köteles a független auditor által felvett eltérésekre írásában válaszolni, kijavításukra tett intézkedéséről a következő értékelés alkalmával beszámolni.

8.6 Az eredmények közzététele

A Szolgáltató nem hozza nyilvánosságra az ellenőrzésről, értékelésekről készült részletes vizsgálati jelentést, ugyanakkor az értékelési időszakot követő 3 (három) hónapon belül nyilvánosságra hozza a jelentést.

9 Egyéb üzleti és jogi tudnivalók

Előfizető köteles a tanúsítványkibocsátási szolgáltatások és az ezek mellett vagy igénylésük során igénybevett egyéb szolgáltatások (pl. opcionális szolgáltatások) ellenértékét, illetve egyéb a Szolgáltató által megállapított díjakat (pl. adminisztrációs díj) előre, a Szolgáltató weboldalán (1.1.2) közzétett mindenkori árlista és szolgáltatáscsomag ajánlatok szerint az ÁSZF-ben [8.] foglalt módon megfizetni.

A szolgáltatások ellenértékének kiegyenlítésére vonatkozó szabályoktól a Szolgáltató egyedi esetekben, saját döntése, illetve az Előfizetővel való külön megállapodás alapján jogosult eltérni.

9.1 Díjak

A Szolgáltató a weboldalán közzétett árlistában és ajánlatokban különösen, de nem kizárólagosan az alábbi, jelen Szabályzat szerinti szolgáltatások és kapcsolódó opcionális szolgáltatások díjait határozza meg.

Szolgáltatások:

- Tanúsítványkibocsátási szolgáltatás;
- Tanúsítványkibocsátás megismétlése szolgáltatás;
- Tanúsítványmegújítási szolgáltatás;
- Tanúsítványmódosítási szolgáltatás.

Opcionális szolgáltatások:

- Mobil regisztrációs szolgáltatás;
- Ügyféleszköz átadása kézbesítési megbízott által;
- Elektronikus cégkivonat lekérése;
- Blokkolt ügyféleszköz feloldása;
- Ügyféleszköz cseréje;
- Egyedi adminisztrációs díj.

Az egyes opcionális szolgáltatások pontos leírását és feltételeit a Szolgáltató a weboldalán teszi közzé. Az opcionális szolgáltatások nyújtását Szolgáltató felfüggesztheti.

A Szolgáltató a fentiek mellett egyéb opcionális szolgáltatásokról és díjakról (pl. elektronikus cégkivonat lekérdezése, blokkolt PIN feloldása, fizetési információk) a honlapján tesz közzé tájékoztatást.

A szolgáltatások igénylésével kapcsoltban az azzal együtt nyújtott opcionális szolgáltatások díjait az adott szolgáltatás díjával együtt kell Előfizetőnek megfizetni.

A szolgáltatásokat a Szolgáltató szolgáltatáscsomagok keretében is értékesítheti, ebben az esetben a szolgáltatás díját a szolgáltatáscsomag díja tartalmazza. Ennek feltételeit és a Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF [8.] tartalmazza.

A Szolgáltató a tanúsítványtár használatáért (lásd 9.1.2 pont), illetve a tanúsítványállapot szolgáltatásokért (CRL, OCSP) alapesetben díjat nem számít fel.

9.1.1 A tanúsítványkiadás és -megújítás díjai

A tanúsítványkiadás és -megújítás díja az alábbiakat tartalmazza:

- igénylés feldolgozása;
- tanúsítvány kibocsátása;
- tanúsítvány közzététele;
- tanúsítvány tárolása.

A Szolgáltató az Előfizetővel való előzetes egyeztetés alapján a nyilvános árlistában feltüntetett díjaktól eltérhet. A Szolgáltató az egyes szolgáltatások tekintetében részletfizetést engedhet. Az egy évnél hosszabb érvényességi idővel kiadott tanúsítványok esetén a kibocsátás díját a Szolgáltató egyenlő mértékű éves előfizetési díjként határozhatja meg. Amennyiben a Szolgáltató a weboldalán közzétett

árlistában nem tüntet fel külön tanúsítványmegújítási díjat, akkor a Tanúsítványkibocsátási díjat alkalmazza megújítás esetén is.

9.1.2 Tanúsítvány hozzáférési díjak

A tanúsítványtár online igénybevételéért a Szolgáltató nem számít fel díjat, amennyiben az igénybevétel a Szolgáltató erre a célra fenntartott, a weboldalán elérhető lekérdezőfelületen kerül sor, és a tanúsítványok lekérdezése egyesével, az egyes tanúsítványok megtekintéséhez szükséges adatok manuális megadásával történik.

A tanúsítványtár egyéb módon történő igénybevételét (pl. tömeges automatikus lekérdezést) a Szolgáltató kizárólag külön megállapodás vagy szerződés alapján, a megállapodás vagy szerződés szerinti szolgáltatási díj ellenében biztosítja.

9.1.3 A tanúsítványállapot-változtatási és tanúsítványállapot-szolgáltatás díjai

A tanúsítványállapot-változtatási és tanúsítványállapot-szolgáltatás jelen Szolgáltatási szabályzatban leírt módon való igénybevételéért (lásd 4.9 pont) a Szolgáltató nem számít fel díjat.

A tanúsítványállapot-szolgáltatás egyéb módon történő igénybevételét (pl. gyakori és tömeges OCSP lekérdezést) a Szolgáltató kizárólag külön megállapodás vagy szerződés alapján, a megállapodás vagy szerződés szerinti szolgáltatási díj ellenében biztosítja.

9.1.4 Egyéb szolgáltatások díjai

A Szolgáltató jelen szabályzatban nem rendezett szolgáltatásokért is számíthat fel díjat, amennyiben azokat az ÁSZF-nek [8.] megfelelően közzéteszi weboldalán, vagy Előfizetővel ilyen szolgáltatás nyújtására előzetesen megállapodott.

9.1.5 Visszatérítési politika

Indokolt esetben a Szolgáltató a szolgáltatások és az ezekhez kapcsolódó, opcionális szolgáltatások díjait egyedi elbírálás alapján, és - amennyiben értelmezett - arányosan téríti vissza Előfizetőnek az ÁSZF [8.] vonatkozó előírásai szerint.

9.1.5.1Általános szabályok

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 egy összegben történik. Részletfizetés esetén a Szolgáltató – az adott csomaghoz (pl. ügyvédi csomag) kapcsolódóan, amennyiben értelmezett – a honlapján tesz közzé részletes tájékoztatást. Részletfizetés esetén – amennyiben értelmezett – a hűségidő lejártát követően jogosult az Ügyfél visszatérítésre oly módon, hogy a Szolgáltató a felmondással érintett hónapra vonatkozó előfizetési díj időarányos részét téríti vissza.

A díj visszatérítési igényét az Előfizetőnek a tanúsítvány kibocsátását vagy megújítását követő 30 naptári napon belül a Központi Regisztrációs Szervezetnél kérvényben kell beadnia a Szolgáltató részére. A kérvény pozitív elbírálása esetén (mely során a Szolgáltató ellenőrzi és megvizsgálja az igénylés jogosságát) a Szolgáltató a tanúsítványt visszavonja és amennyiben értelmezett, a visszajáró összeget az Alany/Igénylő számára a kérelemben megjelölt bankszámlaszámra 20 naptári napon belül visszautalja. Szolgáltató a visszatérítési igényt legkésőbb a beérkezésétől számított 30 naptári napon belül bírálja el.

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

9.1.5.2A tanúsítvány elfogadását megelőzően

A Tanúsítvány 4.4 pont szerinti elfogadását megelőzően a Szolgáltató a tanúsítvány díját kizárólag az alábbi esetekben téríti meg:

- a Tanúsítvány adattartama bizonyítottan a Szolgáltató mulasztása miatt hibás és ezt Előfizető vagy Igénylő még azelőtt jelezte a Szolgáltatónak, hogy a Tanúsítvány elfogadottnak tekinthetővé vált;
- a Tanúsítványban szereplő nyilvános kulcshoz tartozó magánkulcs bizonyítottan a Szolgáltató hibájából sérült, elveszett vagy az aktuális biztonsági elvárásoknak nem felel meg;
- a Szolgáltató más bizonyított szerződés- vagy kötelezettségszegése esetén.

A Szolgáltató az Előfizetővel való megállapodás esetén a tanúsítvány díjának visszatérítése helyett eljárhat úgy is, hogy megfelelő adattartalommal egy új tanúsítványt bocsát ki.

9.1.5.3A tanúsítvány elfogadását követően

A tanúsítvány 4.4 pont szerinti elfogadását követően a Szolgáltató kizárólag a magánkulcs elvesztése esetén és kizárólag a tanúsítvány kibocsátását követő 30 naptári napon belül, egyetlen alkalommal nyújt visszatérítést Tanúsítványkibocsátás megismétlése szolgáltatás keretében az alábbiak szerint.

- Magánszemély Előfizető esetén a Szolgáltató térítésmentesen kiad egy az előzővel teljesen megegyező adattartamú (kivéve: nyilvános kulcs és tanúsítványsorszám) tanúsítványt új kulcspárral.
- Amennyiben Előfizető jogi személy/egyéb szervezet (vagyis abban az esetben, ha a Tanúsítvány Alany adataiban szervezeti adatok is szerepelnek), a Szolgáltató az eredeti díj 50 százalékáért kiad egy az előzővel teljesen megegyező adattartamú (kivéve: nyilvános kulcs és tanúsítványsorszám) tanúsítványt új kulcspárral.

A Tanúsítványkibocsátás megismétlés szolgáltatás igénybevételéhez Igénylőnek Ügyfélmenüben új Tanúsítványigénylést kell kezdeményeznie. A szolgáltatás jelen feltételekkel kulcsvesztés miatt újra kiadott tanúsítvány kulcsának ismételt elvesztése esetén már nem vehető igénybe.

Amennyiben Igénylő vagy Előfizető a magánkulcs elvesztését 30 naptári napon túl jelzi Szolgáltatónak, a Tanúsítványkiadás megismétlése érdekében Előfizetőnek a Tanúsítványkiadás aktuális árlista vagy ajánlat szerinti teljes díját kell megfizetnie, Igénylő általi új tanúsítványigénylés elküldését követően.

Tanúsítvánnyal kapcsolatos kifogást, panaszt illetve a magánkulcs elvesztését az Ügyfél a Szolgáltató Ügyfélszolgálata felé jelezheti a weboldalon közzétett elérhetőségeken.

9.2 Pénzügyi felelősség

Ügyféllel és/vagy Előfizetővel szemben Szolgáltató a Polgári törvénykönyvben [4.] meghatározott szerződésszegésért való felelősség szabályai szerint felelős a Tanúsítvánnyal okozott kárért, ha jogszabályokban foglalt kötelezettségeit megszegte.

A Szolgáltató biztosítási szerződése alapján a Szolgáltató felelősségvállalási értéke káreseményenként minimum 3.000.000 (hárommillió) Ft. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

9.2.1 Biztosítási fedezet

A Szolgáltató biztosítója azon bizonyított károkért, amelyek a Szolgáltató felelősségi körében annak saját hibájából vagy mulasztásából keletkeztek, kártérítést fizet a fenti, káreseményenkénti felső határral (9.2 pont).

9.2.2 Egyéb eszközök

Nincsenek további eszközök.

9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák

Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személynek okozott kárért a Polgári Törvénykönyv [4.] általános szabályai szerint felel.

9.3 Bizalmas üzleti információk kezelése

A Szolgáltató a birtokába jutott bizalmas adatokat a hatályos jogszabályi rendelkezésekre figyelemmel és az 5. fejezet előírásainak megfelelően tárolja és kezeli.

9.3.1 A bizalmas információk köre

A Szolgáltató bizalmas információnak tekint minden, az egyes Ügyfelekre vonatkozó adatot a 9.3.2 pontban foglaltak kivételével.

9.3.2 A bizalmas információk körén kívül eső adatok

A Szolgáltató az alábbi adatokat nem tekinti bizalmas információnak:

- a tanúsítványállapot-szolgáltatások biztosításához publikálni szükséges tanúsítványadatokat;
- a tanúsítványba kerülő összes adat, mely a Szolgáltató nyilvános tanúsítványtárában publikálásra kerül, megtekinthető és letölthető, kivéve, ha Ügyfél kifejezetten külön máshogy rendelkezik, illetve DV SSL tanúsítvány esetén, ahol a Szolgáltató nyilvános tanúsítványtárat nem üzemeltet;
- egyéb személyes jellegüktől megfosztott adatokat úgy, hogy azok semmiképpen nem köthetők az információ birtokosához vagy ahhoz, akire vonatkozóan az információból következtetés vonható le.

A bizalmasnak nem tekintett adatokat a Szolgáltató nyilvánosságra hozhatja, megoszthatja partnereivel, illetve nyilvánosságra kerülésükért nem tartozik felelősséggel.

9.3.3 A bizalmas információk védelme

A Szolgáltató a törvényi előírásokon és jelen Szolgáltatási szabályzat követelményein túlmenően saját belső szabályozási rendszerében is rögzített módon mindent megtesz az ügyfelek adatainak biztonságos kezelése érdekében. Biztonságos fizikai tárolással, illetve logikai védelmi rendszerrel biztosítja az adatok biztonságát, lehetővé téve az adatvesztés, adatsérülés, az adatok helytelen vagy illetéktelen használatának elkerülését.

Azon adatokat, melyekhez a Szolgáltató elektronikus formában jutott hozzá, elektronikus formában, amelyekhez pedig papír alapon, azokat papír alapon és/vagy elektronikus formában őrzi meg és kezeli a fentieknek megfelelően.

A Szolgáltató a birtokába jutott bizalmas adatokhoz csak azon 5.2.1 pont szerinti bizalmi munkatársai számára ad hozzáférést, akiknek munkájuk elvégzéséhez ez elengedhetetlen (pl. Regisztrációs felelős).

A Szolgáltató az alábbi esetekben fedheti fel a bizalmas adatokat:

- Bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből külön törvényben meghatározott feltételek teljesülése esetén a nyomozó hatóság és/vagy a nemzetbiztonsági szolgálatok részére való átadás során. Az adatátadás tényét a Szolgáltató rögzíti, az adatátadásról a Szolgáltató a jogszabály értelmében Ügyfelet nem tájékoztathatja.
- Információszolgáltatás polgári vagy büntető peres eljárás keretében.
- A szolgáltatás megszűnése esetén a megszüntetendő szolgáltatással kapcsolatos az adatok átadása az átvevő szolgáltató részére.

9.4 Személyes adatok kezelése

A Szolgáltató az Ügyfelek személyes adatait a 9.3 pont szerinti bizalmas adatnak tekinti.

9.4.1 Adatkezelési szabályok

A Szolgáltató az Ügyfelek személyes adatait

- jelen Szabályzat,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [6.],
- az Európai Parlament és a Tanács személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve [7.], és
- a Szolgáltató www.netlock.hu weboldalon közzétett Adatkezelési Szabályzat

rendelkezéseit betartva kezeli.

A Szolgáltató adatvédelmi elveiről a weboldalán közzétett Tájékozató a személyes adatok bizalmas kezelésének alapelveiről című dokumentum útján is tájékoztatja részletesen az Ügyfeleket.

Szolgáltatót a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) nyilvántartásába vette, mint adatkezelőt.

9.4.2 Személyes adatok

A Szolgáltató minden olyan birtokába kerülő adatot személyes adatnak tekint,

- mely alapján természetes személy beazonosítható - különös tekintettel a természetes személy nevére vagy hatóság által nyilvántartott azonosítójára -, vagy
- ami természetes személlyel kapcsolatba hozható, vagy
- melyből a természetes személyre vonatkozó következtetés levonható.

A Szolgáltató nem tekinti bizalmas adatnak a 9.3.2 pont szerinti adatok közé tartozó személyes adatokat.

A Szolgáltató csak az adott szolgáltatás nyújtásához szükséges személyes adatokat kéri el az Ügyfelektől. Ez nem zárja ki, hogy a Szolgáltató a szolgáltatásnyújtáshoz kapcsolódóan olyan adatokat is elkérjen, amely birtokában a Szolgáltató hatékonyabban végezheti tevékenységét. Ezen adatok megadása nem kötelező.

9.4.3 Személyes adatnak nem minősülő információk

A személyes adatnak nem minősülő információk esetében a 9.3.2 pont rendelkezései alkalmazandók.

9.4.4 Személyes adatok védelme

A személyes adatok védelme esetében a 9.3.3 pont rendelkezései alkalmazandók. A Szolgáltató védi továbbá az adatokat a jogosulatlan hozzáférés és megváltoztatás ellen, az adatvesztés, károsodás és a nem engedélyezett feldolgozás ellen. Az adatok védelmére és megőrzésére az 5.5 pontban foglalt rendelkezések az irányadók.

9.4.5 Személyes adatok felhasználása

A tanúsítványok kibocsátásával kapcsolatos és a tanúsítványban nem szereplő személyes adatokat a Szolgáltató biztonságosan tárolja és védi, és csak és kizárólag az információs önrendelkezésre vonatkozó törvényben [6.] foglaltak szerint használja fel.

9.4.6 Adatkezelés

A Szolgáltató a birtokába jutott személyes adatokat a hatályos jogszabályi rendelkezésekre figyelemmel és az 5 fejezet előírásainak megfelelően tárolja és kezeli és azokat csak a 9.3.3 pontban felsorolt, jogszabályok által meghatározott esetekben adhatja ki a jogszabályok szerinti harmadik félnek

9.4.7 Egyéb adatvédelmi követelmények

Nincsenek egyéb adatvédelmi követelmények.

9.5 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.

A Szolgáltató által ügyfelei részére kibocsátott magán- és nyilvános kulcs tulajdonosa az Előfizető, teljes jogú felhasználója pedig a Végfelhasználó. A Szolgáltató által ügyfelei részére kibocsátott tanúsítvány tulajdonosa a Szolgáltató, teljes jogú felhasználója pedig a Végfelhasználó.

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat a benne szereplő nyilvános kulccsal és egyéb adatokkal együtt közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.

A Szolgáltató tulajdonát képezi a tanúsítványvisszavonási állapotinformáció, amit nyilvánosságra hozhat. A Szolgáltató által az Ügyfelek részére kibocsátott egyedi azonosító (OID) a szolgáltató tulajdonát képezi.

A Szolgáltató működése során ügyel arra, hogy harmadik személyek szellemi tulajdonjogait ne sértse.

9.6 Felelősség és garanciák

A Szolgáltató felelős:

- szabályzatai keretei között végzett szolgáltatói tevékenységekért;
- A Szolgáltató Regisztrációs és Tanúsítványkibocsátó egységének működéséért akkor is, ha egyes funkciókat Szolgáltatói Partnerek végeznek.

9.6.1 A tanúsítványkibocsátó egység felelőssége

A Tanúsítványkibocsátó egység munkatársai felelősek az alábbi tevékenységek végzéséért:

- szabványos X509 tanúsítvány kibocsátása, megújítása, felfüggesztése, aktiválása, visszavonása a Regisztrációs Egység erre vonatkozó kérelme esetén;
- tanúsítvány felfüggesztésének vagy visszavonásának publikálása CRL-en;
- saját tanúsítványának nyilvánosságra hozatala;
- saját magánkulcsának teljes körű védelme, a kulcs dedikált kriptográfiai hardver modulban történő tárolásával;
- a hitelesítő kulcspár kompromittálódásának feltételezése, a kulcspár sérülése, megsemmisülése esetén a PKI közösség tagjainak (lásd 1.3 pont) késedelem nélküli értesítése elektronikusan (pl. elektronikus levélben, weboldalon közzététellel stb.), illetve erre vonatkozó előírás esetén out-of-band módon, továbbá a Szabályzat Elfogadó Egység bármely tagjának írásban vagy személyesen történő megkeresésével;
- úgy működni, hogy semmilyen módon ne sértsék a szolgáltatás biztonságát;
- tevékenységüket saját maguk ellátni.

9.6.2 A regisztrációs egység felelőssége

A Regisztrációs egység munkatársai felelősek az alábbi tevékenységek végzéséért:

- úgy működni, hogy semmilyen módon ne sértsék a szolgáltatás biztonságát;
- tevékenységüket saját maguk ellátni;
- az Igénylő tanúsítványra vonatkozó kérelmeinek (kibocsátás, megújítás, felfüggesztés, visszavonás) kezelése;
- az ügyféladatok összegyűjtése és a 3. fejezet szerinti ellenőrzése, majd döntés meghozatala azok valódiságára vonatkozóan;
- a nem nyilvános ügyféladatok megfelelő szintű védelme;

- Ügyfelek és Érintett felek értesítése a tanúsítvány kibocsátásáról és a tanúsítvánnyal végezhető műveletekről;
- a tanúsítvány elérhetővé tétele Ügyfél számára.

9.6.3 Ügyfelek felelőssége és kötelezettségei

Az Igénylő felelősséggel tartozik:

- a Szolgáltató részére megadott adatok valódiságáért, pontosságáért és érvényességéért;
- kibocsátása után a tanúsítványban szereplő adatok ellenőrzéséért, eltérés észlelése esetén pedig a Szolgáltató értesítéséért az eltérésről;
- az adataiban bekövetkezett változások haladéktalan bejelentéséért;
- a szolgáltatás igénybevétele előtt a jelen Hitelesítési Rend és a vonatkozó Szolgáltatási szabályzat tartalmának megismeréséért;
- a Szolgáltató által kért, a szolgáltatás igénybevételéhez szükséges adatok hiánytalan megadásáért, valamint a valóságnak megfelelő adatok szolgáltatásáért;
- a tanúsítvány kiadásához szükséges adatok ellenőrzésében köteles együttműködni a Szolgáltatóval, valamint mindent megtenni azért, hogy az ellenőrzés a lehető leghamarabb befejeződhessen.

A Végfelhasználó felelősséggel tartozik:

- Ügyféleszközének, kulcsának és tanúsítványának a szabályzatoknak megfelelő felhasználásáért; kulcsának és aktivizáló kódjának biztonságos kezeléséért;
- az Ügyféleszköz biztonságos kezeléséért;
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért a tanúsítványhoz vagy alkalmazásához köthető vitás ügyekben;
- amennyiben az Végfelhasználó kulcsa, Ügyféleszköze vagy az eszköz aktiválásához szükséges titkos adatok illetéktelen kezekbe kerültek vagy megsemmisültek, Végfelhasználó ezt köteles haladéktalanul jelezni a Szolgáltatónak, kezdeményeznie kell a tanúsítvány(ok) felfüggesztését vagy visszavonását és meg kell szüntetnie a tanúsítvány használatát;
- a szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a tanúsítványban hivatkozott OID azonosítójú szabályzatokban foglaltaknak megfelelő használatáért.

Az Előfizetőre vonatkozó kötelezettségek:

- a szolgáltatás igénybevétele előtt meg kell ismernie a Hitelesítési Rend és a jelen Szabályzat tartalmát;
- a Szolgáltató által kért, a szolgáltatás igénybevételéhez szükséges adatokat köteles hiánytalanul megadni, valamint a valóságnak megfelelő adatokat szolgáltatni;
- amennyiben tudomására jut, hogy az általa megadott, a szolgáltatás igénybevételéhez szükséges adat - különösen valamely tanúsítványban is megjelenő adat - megváltozott, haladéktalanul köteles erről írásban értesíteni a Szolgáltatót, köteles kérni a tanúsítvány felfüggesztését vagy visszavonását, továbbá köteles megszüntetni a tanúsítvány használatát;
- a szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a tanúsítványban hivatkozott OID azonosítójú szabályzatokban, a hivatkozott dokumentumokban foglaltaknak megfelelően használhatja;
- köteles biztosítani, hogy a szolgáltatás igénybevételéhez szükséges adatokhoz és eszközökhöz illetéktelen személyek ne férhessenek hozzá;
- a Szolgáltatót haladéktalanul írásban kell értesítenie, amennyiben valamely, a szolgáltatással kapcsolatos elektronikus aláírással, illetve tanúsítvánnyal kapcsolatban jogvita indul;
- a tanúsítvány kiadásához szükséges adatok ellenőrzésében köteles együttműködni a Szolgáltatóval, valamint mindent megtenni azért, hogy az ellenőrzés a lehető leghamarabb befejeződhessen;

- felelősséggel tartozik a Végfelhasználói kötelezettségek betartásáért, olyan mértékben, mennyiben azokra hatással van;
- díjfizetési kötelezettségének eleget tenni.

9.6.4 Más érintett felek felelőssége

Az Érintett Feleknek a Szolgáltató által garantált biztonsági szint megtartásához szükséges körültekintő eljárás érdekében javasolt:

- a Szolgáltató Hitelesítési Rendjében és jelen Szabályzatban megfogalmazott követelmények, előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a tanúsítvány visszavonási állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján;
- a tanúsítvány felhasználására vonatkozó valamennyi korlátozás figyelembe vétele.

Az Érintett Felek saját belátásuk és/vagy szabályzataik alapján jogosultak dönteni az egyes tanúsítványok elfogadásáról, illetve azok felhasználási módjáról.

9.6.5 Egyéb résztvevők felelőssége

Amennyiben a szervezet képviselője nem személyesen jár le a tanúsítvány igénylése során, akkor a szervezet képviselője felelősséggel tartozik az általa kiállított igazolásokért, különös tekintettel az Igénylő részére adott meghatalmazásra és annak tartalmára.

9.7 Szavatosság kizárása

A jelen Szabályzatban meghatározott szolgáltatásokkal kapcsolatban, a Szolgáltatóval szemben támasztott jótállási, szavatossági vagy kártérítési igényeket Szolgáltató visszautasítja, amennyiben annak alapját képező eset Ügyfél mulasztására, kötelezettségeinek és felelősségeinek be nem tartására vagy egy külső, előre nem látható eseményre/eseményekre vezethető vissza.

9.8 Felelősség korlátozása

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy Ügyfél vagy az Érintett Felek a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályoknak, illetve szolgáltatói szabályzatoknak megfelelően jártak el, vagy nem tanúsították az 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.

A felelősség tekintetében lásd még a 9.2 pontban foglaltakat.

9.9 Kártérítés, kártalanítás

A kártérítési és kártalanítási eljárásokra vonatkozó leírásokat Szolgáltató az ÁSZF-ben [8.] szabályozza.

A jótállási, szavatossági vagy kártérítési, kártalanítási igényekkel kapcsolatban lásd még a 9.7, 9.8 pontban foglaltakat.

9.10 Hatály

A Szabályzat tárgyi hatálya a jelen Szolgáltatási szabályzat 1.1 pontja szerinti szolgáltatások nyújtását és igénybevételét foglalja magában.

A Szabályzat személyi hatálya közvetlenül a Szolgáltató bizalmi munkatársaira és az Ügyfelekre, közvetetten pedig minden Érintett félre terjed ki.

9.10.1 Érvényesség

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

Az adott verzió hatályba lépésének napja a Szolgáltatási Szabályzat fedlapján kerül meghatározásra.

9.10.2 Megszűnés

A Szabályzat időbeli hatálya a szolgáltatási tevékenység beszüntetéséig, illetve egy újabb szabályzat verzió hatályba lépéséig tart.

9.10.3 A megszűnés következményei

A Szabályzat visszavonása esetén a Szolgáltató weboldalán teszi közzé a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket. A Szolgáltató vállalja, hogy a Szolgáltatási Szabályzat visszavonása esetén is érvényben maradnak a mindenkor hatályos vonatkozó jogszabályokban meghatározott bizalmas adatok védelmére vonatkozó előírások.

9.11 Egyedi értesítések és a résztvevők közti kommunikáció

A Szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát, telefonos ügyfélszolgálatot működtet a 1.1.2 pontban megadott elérhetőségekkel.

Ügyfélszolgálat a végfelhasználói tanúsítványokkal kapcsolatos ügyintézések és eljárások során elsősorban közvetlenül az Ügyfélnek küldött e-mailek útján kommunikál Ügyféllel.

9.12 Módosítások

A Szolgáltató a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén megváltoztathatja Szolgáltatási Szabályzatát.

9.12.1 A módosítási eljárás

Szolgáltató szabályzatainak karbantartását Szolgáltató Szabályzat Elfogadó Egysége végzi.

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 Szabályzat Hitelesítési Rendjében meghatározott követelményeknek való megfelelőségét és a formai megfelelést a RFC 3647 szabványnak.

A Szolgáltató jóváhagyás előtt megvizsgálja a Szabályzatot a Szabályzat megfelelőség szempontjából, hogy a Szabályzat tartalmilag és formailag megfelel-e a Hitelesítési Rendeknek. A Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik.

9.12.2 Az értesítések módja és határideje

A Szabályzat módosításáról Szolgáltató Ügyfeleket és Érintett Feleket a hatálybalépés előtt lehetőség szerint 30 nappal tájékoztatja az új szabályzat tervezetének weboldalon való közzétételével. Különösen indokolt esetben a Szolgáltató ezen időtartamról eltérhet.

9.12.3 A dokumentumazonosító változása

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 és/vagy a műszaki szabványkörnyezet változása esetén kerül sor. Szolgáltató a működése során szerzett gyakorlati tapasztalatok alapján folyamatosan felülvizsgálja Szolgáltatási szabályzatát.

9.13 Vitás kérdések rendezése

A Szolgáltató (beleértve a regisztrációs egységeket is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az info@netlock.hu e-mail címen, illetve telefonon vagy személyesen a Szolgáltató ügyfélszolgálati irodájában fogad.

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

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

9.13.1 Panaszok kezelésének eljárása

A panaszokat a Szolgáltató levélben, e-mailben az info@netlock.hu címen, telefonon és személyesen fogadja (ld. 1.1.2 pont).

A telefonon érkezett panaszról a Szolgáltató külön jegyzőkönyvet vesz fel, és a kivizsgálás eredményéről – a Felek eltérő megállapodását kivéve – e-mailben tájékoztatja a panasz benyújtóját. A panasz kivizsgálásának véghatárideje a bejelentéstől számított 30 naptári nap, amennyiben a panasz jellege miatt a kivizsgálás ettől hosszabb időt vesz igénybe, erről a Szolgáltató külön tájékoztatja a Felet.

E-mailben és postai úton érkezett panasz kivizsgálására a telefonon érkezett panasz kivizsgálására vonatkozó szabályok az irányadóak azzal, hogy külön jegyzőkönyv ebben az esetben kerül felvételre.

A Szolgáltató a panaszt kivizsgálását követően – amennyiben értelmezett - 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.

9.14 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar és Európai Uniós jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők.

9.15 A hatályos jogszabályoknak való megfelelés

A Szolgáltató tevékenységét az alábbi jogszabályi követelményeknek, szabványoknak és egyéb szabályzatoknak megfelelően végzi:

[1.] **Nytv.:**1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról

[2.] **Szmtv.:** 2007. évi I. törvény a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról

[3.] **Harmtv:** 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról

[4.] **Ptk.:** 2013. évi V. törvény a Polgári Törvénykönyvről

[5.] 45/2014 (II. 26.) Kormányrendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól

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

[7.] az Európai Parlament és a Tanács személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve, és

[8.] Általános Szerződési Feltételek (ÁSZF) – NETLOCK Kft., mindenkor hatályos változata

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

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

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

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

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

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

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

[16.] ETSI EN 319 401 General Policy Requirements for Trust Service Providers

[17.] ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements

[18.] ETSI EN 319 412-1 Certificate Profiles; Part 1: Overview and common data structures

[19.] ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[20.] ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[21.] ETSI EN 319 412-4 Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations

[22.] LCP: Lightweight Certificate Policy, Könnyített Hitelesítési Rend, OID: 0.4.0.2042.1.3

[23.] NCP: Normalized Certificate Policy, Normalizált Hitelesítési Rend, OID: 0.4.0.2042.1.1

[24.] NCP+: Extended Normalized Certificate Policy, Kiterjesztett (Ügyféleszköz használatát megkövetelő) Hitelesítési Rend, OID: 0.4.2042.1.2

[25.] DVCP: Domain Validation Certificate Policy Domain ellenőrzött SSL tanúsítványokra vonatkozó Hitelesítési Rend, OID: 0.4.0.2042.1.6

9.16 Vegyes rendelkezések

1.1.1 Teljességi záradék

Teljességi záradékot a Szolgáltató nem köt ki.

9.16.1 Átruházás

Jelen Szabályzat alapján nyújtott szolgáltatásokba bevont Szolgáltatói partnerek csak a Szolgáltató előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és/vagy ruházhatják át kötelezettségeiket harmadik félnek.

9.16.2 Részleges érvénytelenség

Jelen Szabályzat egyes rendelkezéseinek bármilyen okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.3 Igényérvényesítés

A Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben a Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben, vagy a Szolgáltatási szabályzat más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.4 Vis maior

A Szolgáltató nem felelős a Szabályzatban megfogalmazott követelmények hibás vagy késedelmes teljesítéséért, ha a hiba vagy késedelem oka a Szolgáltató ellenőrzési körén kívül eső, előre nem látható körülmény volt.

9.17 Egyéb rendelkezések

9.17.1 Illetékes fogyasztóvédelmi felügyelőség

Budapest Főváros Kormányhivatal, Fogyasztóvédelmi Felügyelőség, elérhetőségei:

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