NetLock Ügyfél Tájékoztató (ÜT)

1 FELHASZNÁLÓ ÁLTALÁNOS TÁJÉKOZTATÁSA 2
1.1 NYILVÁNOS KULCSÚ TITKOSÍTÁS 2
1.2 A NYILVÁNOS KULCSÚ TITKOSÍTÁS MÜKÖDÉSE 2
1.3 TANÚSÍTVÁNYOKKAL KAPCSOLATOS ALAPOK 2
1.4 PUBLIKUS KULCS INFRASTRUKTÚRA (PKI) A NETLOCKNÁL 4
2 A NETLOCK TANÚSÍTVÁNYOK OSZTÁLYAI ÉS TÍPUSAI 4
2.1 TANÚSÍTVÁNYOK OSZTÁLYAI ÉS TULAJDONSÁGAIK 4
2.2 TANÚSÍTVÁNYTÍPUSOK 5
3 TANÚSÍTVÁNYIGÉNYLÉS MÓDJA 6
3.1 IGÉNYLÖ REGISZTRÁLÁSA 6
3.2 KULCSOK GENERÁLÁSA ÉS VÉDELME 6
4 TANÚSÍTVÁNYKÉRELMEK JÓVÁHAGYÁSA 6
4.1 A TANÚSÍTVÁNYKÉRELMEK JÓVÁHAGYÁSÁNAK KÖVETELMÉNYEI 6
4.2 TESZT TANÚSÍTVÁNY KIADÁSÁRA IRÁNYULÓ KÉRELMEK ELFOGADÁSA 6
4.3 A, B ÉS C OSZTÁLYÚ TANÚSÍTVÁNY KIADÁSÁRA IRÁNYULÓ KÉRELMEK ELFOGADÁSA 6
4.4 TANÚSÍTVÁNYKÉRELMEK ELUTASÍTÁSA 7
5 KIBOCSÁTOTT TANÚSÍTVÁNYOK 7
5.1 A TANÚSÍTVÁNY KIBOCSÁTÁSÁNAK IDÖPONTJA 7
5.2 A TANÚSÍTVÁNY ÉRVÉNYESSÉGE 7
6 TANÚSÍTVÁNYOK ELFOGADÁSA AZ IGÉNYLÖ ÁLTAL 7
6.1 A TANÚSÍTVÁNY ELFOGADÁSÁT JELENTÖ KOMMUNIKÁCIÓS LÉPÉSEK 8
6.2 A TANÚSÍTVÁNYIGÉNYLÖ NYILATKOZATA A TANÚSÍTVÁNY ELFOGADÁSAKOR 8
7 A TANÚSÍTVÁNYOK HASZNÁLATA 8
7.1 DIGITÁLIS ALÁÍRÁS KÉSZÍTÉSE 8
7.2 A DIGITÁLIS ALÁÍRÁSOK ELLENÖRZÉSE 9
7.3 ÉRVÉNYES DIGITÁLIS ALÁÍRÁS KÖVETKEZMÉNYEI 11
7.4 ELJÁRÁS A DIGITÁLIS ALÁÍRÁS ELLENÖRZÉSEKOR FELLÉPÖ HIBÁKNÁL 11
8 TANÚSÍTVÁNYOK VISSZAVONÁSA 11
8.1 OKOK A VISSZAVONÁSRA 11
8.2 KIBOCSÁTÓ HATÓSÁG SAJÁT TANÚSÍTVÁNYÁNAK VISSZAVONÁSA 12
8.3 VISSZAVONÁS HIBÁS KIBOCSÁTÁS ESETÉN 12
8.4 VISSZAVONÁS AZ IGÉNYLÖ KÉRÉSÉRE 12
8.5 A VISSZAVONT TANÚSÍTVÁNYOK LISTÁJA 12
8.6 A FELFÜGGESZTÉS ÉS VISSZAVONÁS KÖVETKEZMÉNYE 12
8.7 A PRIVÁT KULCS VÉDELME VISSZAVONÁS ESETÉN 12
9 TANÚSÍTVÁNY LEJÁRATA 12
9.1 ELÖZETES ÉRTESÍTÉS A TANÚSÍTVÁNY LEJÁRTÁRÓL 12
9.2 TANÚSÍTVÁNY LEJÁRTÁNAK KÖVETKEZMÉNYEI 12
9.3 TANÚSÍTVÁNYOK MEGÚJÍTÁSA 12
10 EGYÉB RENDELKEZÉSEK, INTÉZKEDÉSEK 12
10.1 JOGI SZABÁLYOZÁS 13
10.2 AZ ÜGYFÉL TÁJÉKOZTATÓ MÓDOSÍTÁSAI 13
10.3 SZOLGÁLTATÁSI DÍJAK 13
11 FÜGGELÉK 14
11.1 SZÓJEGYZÉK 14

1 Felhasználó általános tájékoztatása

1.1 Nyilvános kulcsú titkosítás

A nyílt hálózatok (mint például az Internet) felépítéséböl adódóan az üzenetek különbözö szolgáltatók által kontrollált rendszereken haladnak keresztül, így fennáll annak a lehetösége, hogy az üzenetekhez nem csak a címzett férhet hozzá. A biztonság növelésével az a cél, hogy a küldö és a fogadó egyértelmüen azonosítható legyen, az eredeti üzenet ne változhasson meg, illetve mások ne férhessenek az üzenet tartalmához.

Erre a problémára a mai legmodernebb technikai megoldás az aszimmetrikus, más néven a nyilvános kulcsú titkosítási eljárás. Ennek legelterjedtebb változata az RSA nevü eljárás. A nyilvános kulcsú titkosítás elönye, hogy a küldö és fogadó félnek nem kell semmilyen titkos jelszót, kódot, kulcsot cserélnie egymással. Ehelyett minden résztvevö fél rendelkezik egy kulcspárral (egy nyilvános és egy titkos kulccsal), mellyel a biztonságos kommunikáció létrejöhet.

A kulcspár használata biztosítja azt, hogy az elektronikus üzeneteket (elektronikus leveleket, csatolt dokumentumokat, Web oldalakat és szolgáltatásokat, megrendeléseket, pénzügyi utasításokat, számlalekérdezéseket) csak az üzenet címzettje tudja dekódolni. Az eljárás másik fontos tulajdonsága az, hogy az üzenetek feladói pontosan azonosíthatók, az üzenetek nem letagadhatók, bizonyító erövel bírnak. Erre szolgál a *digitális aláírás.*

1.2 A nyilvános kulcsú titkosítás müködése

A kulcspár egyik tagját nyilvános (vagy publikus) kulcsnak, a másikat titkos (vagy privát) kulcsnak hívják. A kulcsok elektronikus formában létezö adatok, s könnyen elöállíthatók ingyenes segédprogramokkal. A nyilvános kulcsok mindenki számára hozzáférhetök az ún. kulcsadatbázisokból, míg a privát kulcsok csak tulajdonosaik által elérhetök.

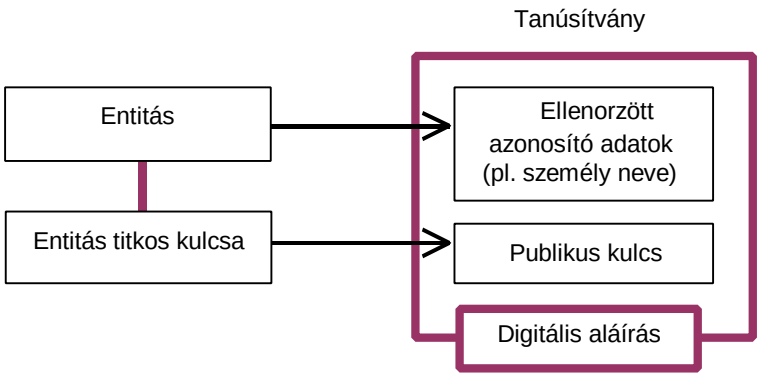
A nyilvános kulcsú titkosítás müködése egy olyan lakat segítségével szemléltethetö, amelynek két kulcslyuka van, egy-egy beleillö kulccsal. Ha a két kulcs közül az egyikkel zárjuk a lakatot, akkor az csak annak párjával nyitható ki, azaz még a bezárást végzö kulccsal sem. Egy üzenet küldésénél a feladó levelét egy ‘ládába’ teszi, a láda lakatját pedig a címzett nyilvános kulcsával bezárja. A bezárt láda - azaz a titkos üzenet - csak a záró kulcs párjával, azaz a címzett titkos kulcsával nyitható. Ezzel a módszerrel egymást nem ismerö személyek között is létrejöhet biztonságos kommunikáció.

A digitális aláírásnál az aláíró az üzenetnek egy speciális matematikai eljárás segítségével elkészített rövidített változatát (digitális lenyomatát) kódolja saját titkos kulcsával. A kódolt lenyomatot nevezzük digitális aláírásnak. Az említett lenyomat egyértelmüen jellemzö az üzenetre, azaz az üzenet legkisebb módosítása a lenyomat teljes megváltozását eredményezi.
A kódolt lenyomat, azaz a digitális aláírás az aláíró nyilvános kulcsával dekódolható. Az így visszakapott lenyomatról pedig eldönthetö, hogy tényleg az aláírt üzenethez tartozik-e, azaz a digitális aláírás érvényes volt-e.

1.3 Tanúsítványokkal kapcsolatos alapok

A nyilvános kulcsú titkosítást használó rendszerek egyik fö eleme az a szolgáltatás, mely a kommunikációs feleket egymásnak ‘bemutatja’, azaz amely segítségével a felek nyilvános kulcsai megszerezhetök. Fontos, hogy garantálják a nyilvántartott felek (személyek, cégek, számítógépek) azonosságát, például közjegyzök közremüködésével.

A hitelesítés szerepe az, hogy tanúsítsa egy felhasználó (személy, szervezet vagy akár egy számítógép) és az általa használt titkos kulcs összetartozását. A felhasználót annak neve, Internet címe vagy más adatai alapján, a titkos kulcsot pedig a hozzá tartozó nyilvános párjával tudjuk egyértelmüen azonosítani (1. Ábra).



1. Ábra: A tanúsítvány szerepe

A tanúsítvány kiadása elött a tanúsítványkiadónak két fontos feladata van:

- az entitás azonosítása
- meg kell győződnie arról, hogy az entitás rendelkezik az általa bemutatott nyilvános kulcs titkos párjával.

```
-----BEGIN CERTIFICATE-----
MIIEdDCCA92gAwIBAgICAQMwDQYJKoZIhvcNAQEEBQAwgcQxCzAJBgNVBAYTAkhV
MRAwDgYDVQQIEwdIdW5nYXJ5MREwDwYDVQQHEwhCdWRhcGVzdDEVMBMGA1UEChMM
TmV0TG9jayBLZnQuMSgwJgYDVQQLEx9OZXRMb2NrIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5MSYwJAYDVQQDEx1OZXRMb2NrIEtvemplZ3l6b2kgS3VsY3NraWFkbzEn
MCUGCSqGSIb3DQEJARYYa296amVneXpvaWNhQG5ldGxvY2submV0MB4XDTk4MDQx
NjAwNDQzMFoXDTk5MDQxNjAwNDQzMFowgY4xCzAJBgNVBAYTAkhVMRAwDgYDVQQI
EwdIdW5nYXJ5MREwDwYDVQQHEwhCdWRhcGVzdDEVMBMGA1UEChMMTmV0TG9jayBL
ZGVudGl0eSBvZiB0aGUgb3duZXIgdW5kZXIgdGhlIHRlcm1zIG9mIE5ldExvY2sg
UHJvZHVjdCBMaWFiaWxpdHkgSW5zdXJhbmNlLiBFemVuIGt1bGNzY3NvbWFnIHR1
bGFqZG9ub3NhbmFrIGtpbGV0ZXQgYSBOZXRMb2NrIEtmdC4gdGVybWVrZmVsZWxv
c3NlZy1iaXp0b3NpdGFzYSBnYXJhbnRhbGphLjAkBgNVHREEHRYbREswMDAwNkIg
PFJvenNhaGVneWkgWnNvbHQ+MBEGCWCGSAGG+EIBAQQEAwIAgDANBgkqhkiG9w0B
AQQFAAOBgQAKbjWEceZg0s/nSXy+ahbwuiTfRqNQSqag2V56QGyxUopvsFv7nfRv
daFvzK8uI6WMtbQpxgfFdapcYXzjwKbQqfeKmctMjF056Fv6JW8D9x+PswGch1as
icKasGY1L5nY77ygZkctWxIALN9AvY1OodAWPzDH1aQGMO2nPE4X7g==
-----END CERTIFICATE-----
```

2. Ábra: Példa egy tanúsítványra

Ezen ellenörzések alapján a kiadó tanúsítványt ad ki, melyet saját digitális aláírásával hitelesít. Az aláírt tanúsítvánnyal a kiadó megerösíti a tanúsítvány tulajdonosát azonosító adatok és a tulajdonos nyilvános kulcsának összetartozását.

A NetLock kibocsátó hatóság digitális aláírása csak olyan tanúsítványokra kerül rá, melyeknél a kibocsátó hatóság – a jelen dokumentumban leírt - azonosítási eljárásokat elvégezte, és meggyözödött a tanúsítvány adatainak helyességéröl.

A kiadott tanúsítványok megfelelnek a CCITT X.509v3 szabványának (
3. Ábra). A tanúsítványok „Alany megnevezése” illetve a „Kibocsátó megnevezése” mezök formátuma megfelel a CCITT X.500 szabványnak.

Alapmezok (Basic Certificate Fields):
- Tanúsítvány verzió (Version)
- Sorszám (Serial number)
- Alany megnevezése (Subject Name)
- Kibocsátó hatóság megnevezése (Issuer Name)
- Érvényesség (Validity)
- Alany publikus kulcsa (Subject Public Key Information)
- Aláírási algoritmus (Signature Algorithm ID)
- Kibocsátó digitális aláírása (Digital Signature)

Szabványos kiegészíto mezok (Standard Extensions):
- Használati kódok (Basic Constraints)
- Kiadási feltételek (Certificate Policies)

Egyéb **kiegészíto mezok (Private Extensions):**
- ...

3. Ábra: A szabványos x509 tanúsítvány mezöi

A NetLock PKI által kiadott tanúsítványok mezöinek pontos leírása illetve további információk a http://www.netlock.net Internet címen találhatók.

1.4 Publikus kulcs infrastruktúra (PKI) a NetLocknál

A NetLock nyilvános kulcs hitelesítö szolgáltatásait PKI hierarchiában végzi, mely hierarchiában jelenleg három vagy több kibocsátó hatóság müködik. A *kibocsátó hatóságok* a különbözö azonosítási funkciók elvégzését kiadhatják ún. *regisztrációs hatóságoknak*.

A NetLock PKI része a NetLock adatbázis, amelyben a NetLock PKI kibocsátó hatóságai által kiadott tanúsítványok, a visszavont tanúsítványok listái, eljárási rendek, szerzödési feltételek és más dokumentációk találhatók.

2 A NetLock tanúsítványok osztályai és típusai

2.1 Tanúsítványok osztályai és tulajdonságaik

2.1.1 Teszt szintü tanúsítványok

A teszt tanúsítvány a hálózatbiztonsági szolgáltatások tesztelési céljaira kiadott tanúsítvány.

A teszt szinten a kibocsátó hatóság nem végez és nem vesz igénybe entitás-azonosító szolgáltatásokat. A teszt tanúsítvány kiadásának feltétele a beérkezett tanúsítványkérelem és a tanúsítványkiadás folyamán a kommunikációban használt elektronikus levelezési cím. A teszt tanúsítvány csak a fenti elektronikus cím létezését biztosítja a tanúsítványt elfogadók számára, ám a tanúsítvány többi mezöjében található információ nem ellenörzött információnak (NEI) tekintendö.

2.1.2 "C" osztályú tanúsítványok

Az „C" osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát korlátozott, részben emberi beavatkozással történt ellenörzési lépéseken keresztül azonosította a kiadó hatóság. Használata elektronikus levelezéshez, kisebb kockázatú tranzakciókhoz, on-line szolgáltatások igénybevételéhez, szoftver forrásának ellenörzéséhez ajánlott.

A kibocsátó hatóság az "C" osztályú tanúsítvány kiadása elött az ÜT 4.3 pontjában felsorolt ellenörzéseket elvégezte, és ez alapján valószínüsíti az ÜT 4.1 pontjában felsorolt kiadási feltételek meglétét.

2.1.3 "B" osztályú tanúsítványok

A „B” osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát szigorú ellenörzési lépések során azonosította a kiadó hatóság. Használata elektronikus levelezéshez, közepes kockázatú tranzakciókhoz, on-line szolgáltatások igénybevételéhez, szoftver forrásának ellenörzéséhez ajánlott.

A kibocsátó hatóság a “B” osztályú tanúsítvány kiadása elött az ÜT 4.3 pontjában felsorolt ellenörzéseket a töle elvárható legnagyobb gondossággal végezte el, ezáltal meggyözödött az ÜT 4.1 pontjában felsorolt kiadási feltételek meglétéröl.

2.1.4 “A” osztályú tanúsítványok

A „A” osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát szigorú ellenörzési lépések során azonosította a kiadó hatóság. Használata nagy értékü tranzakcióknál, pénzügyi utasítások és információk ellenörzésénél, szerzödéskötéseknél ajánlott.

A kibocsátó hatóság a “A” osztályú tanúsítvány kiadása elött ÜT 4.3 pontjában felsorolt ellenörzéseket közjegyzöi dokumentumokkal és nyilatkozatokkal alátámasztva, a töle elvárható legnagyobb gondossággal végezte el, és meggyözödött az ÜT 4.1 pontjában felsorolt kiadási feltételek meglétéröl.

2.2 Tanúsítványtípusok

A különbözö biztonsági osztályokban (“A”, “B”, “C”) a következö tanúsítványtípusok kiadását végzik a NetLock kibocsátó hatóságai:

2.2.1 Személyes tanúsítvány

Személyes tanúsítványt természetes személy igényelhet a saját nevében.

A tanúsítvány Country és Locality mezöjében az igénylö lakóhelyének országa és városa, az Organization mezöben semmi, a Common Name mezöjében az igénylö neve és (opcionálisan) elektronikus levelezési címe szerepel.

Használati köre hasonló a kézzel készített aláírásához.

2.2.2 Névjegykártya tanúsítvány

Névjegykártya tanúsítványt természetes személy igényelhet egy adott szervezet tagjaként. A szervezet lehet munkahely, egyesület, alapítvány. A tanúsítványban szerepel a személy szervezetben betöltött funkciója is.

A tanúsítvány Country és Locality mezöjében az igénylö lakóhelyének országa és városa, az Organization mezöben szervezetének neve, az Organizational Unit mezöben funkciója, a Common Name mezöjében az igénylö neve és (opcionálisan) elektronikus levelezési címe szerepel.

Használati köre hasonló a névjegykártyáéhoz.

2.2.3 Szervezet tanúsítvány

Ezt a tanúsítvány típust szervezet vagy annak szervezeti egysége igényelheti. A szervezet lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány.

A tanúsítvány Country és Locality mezöjében a szervezet székhelyének országa és városa, az Organization mezöben a szervezet neve, az Organizational Unit mezöben a szervezeti egység neve, a Common Name mezöjében ismételten az Organization és az Organizational Unit értékek, majd (opcionálisan) elektronikus levelezési címe szerepel.

Használati köre hasonló a szervezet pecsétjéhez.

2.2.4 Szerver tanúsítvány

Szerver tanúsítványt Internet címmel (ún. domain névvel) rendelkezö, szervert üzemeltetö természetes személy vagy szervezet igényelhet.

A tanúsítvány Country és Locality mezöjében az üzemeltetö székhelyének vagy lakóhelyének országa és városa, az Organization mezöben az üzemeltetö neve, az Organizational Unit mezöben az üzemeltetö szervezeti egység neve, a Common Name mezöben a szerver internetes elnevezése (ún. host neve) szerepel.

Web szerverekkel való biztonságos kommunikációra használható.

3 Tanúsítványigénylés módja

3.1 Igénylö regisztrálása

A NetLock PKI-ban tanúsítvány hitelesítésének igényével csak regisztrált entitás élhet. A regisztrálható, azaz tanúsítvány igénylésére jogosult entitások jelenleg személyek, szervezetek és WEB szerverek lehetnek.

A regisztráció során az entitások által szolgáltatott adatok önkéntesek, és az entitások írásbeli kérése alapján – tanúsítványaik egyidejü visszavonása mellett – a regisztrációs adatbázisból törlik ezeket.

3.2 Kulcsok generálása és védelme

A NetLock PKI-ban regisztrált entitások saját maguk generálják a tanúsítvány igényléséhez szükséges nyilvános – titkos kulcspárt. A kulcspár generálása történhet saját szoftver segítségével, gyári szoftver termékkel vagy egyéb, biztonságos hardver eszközzel. Az eszközök kiválasztása és használata a tanúsítványigénylö kizárólagos feladata és felelössége.

A nyilvános kulcsú titkosítási eljárás biztonságos használata a késöbbiekben sérülhet, ha a titkos kulcs védelme nem megfelelöen biztosított. A titkos kulcsot legalább jelszóval védve kell tárolni, de ennél biztonságosabb (pl. intelligens kártyás) tárolási mód használata ajánlott. A tárolt tikos kulcs jelszavát olyan módon kell megválasztani, hogy azt a kulcs tulajdonosán kívül más ne ismerje, és találgatással, következtetésekkel ne is ismerhesse meg.

4 Tanúsítványkérelmek jóváhagyása

4.1 A tanúsítványkérelmek jóváhagyásának követelményei

A tanúsítvány kibocsátó csak akkor fogadja el a tanúsítványkérelmet, ha a következö feltételek teljesülnek:

- Az igénylö benyújtotta kérelmét a tanúsítvány kibocsátónak
- Az entitás (akinek nevében az igénylö eljár) azonos a kérelemben szereplö alannyal
- Az igénylö jogosult a kérelemben szereplö alany nevében kérelmet benyújtani
- Az igénylö birtokában van a kérelemben szereplö nyilvános kulcs titkos párja
- A kérelemben szereplö adatok ellenörizhetök és pontosak, kivéve a tájékoztató jellegü adatokat

4.2 Teszt tanúsítvány kiadására irányuló kérelmek elfogadása

Teszt tanúsítványok kiadásához az igénylönek érvényes elektronikus levelezési címmel kell rendelkeznie. A NetLock Tesztkulcs Kiadó teljesen automatizált lépéseken keresztül végzi a teszt tanúsítvány kiadását. A lépések során a kiadó a megadott elektronikus levelezési címre továbbít utasításokat, és erröl a levelezési címröl várja a tanúsítvány kiadására vonatkozó kérelem megerösítését.

A teszt tanúsítvány kiadására irányuló kérelem akkor elfogadott, ha az elektronikus levelezési címmel az elöírt kommunikáció lefolytatható.

4.3 A, B és C osztályú tanúsítvány kiadására irányuló kérelmek elfogadása

A kibocsátó hatóság elfogadja a tanúsítvány kiadására irányuló kérelmet, ha az igényelt tanúsítvány osztályának és típusának megfelelö ellenörzési lépések végrehajthatók és eredményesen befejezödtek.

Ellenörzési lépések	C osztály	B osztály	A osztály
Személyek azonosításához	„B” osztályban regisztrált 2 tanú Postacím, telefonszám létezése Személyi igazolvány másolata Közüzemi számlák másolata	Személyi igazolvány, útlevél bemutatása Postai adategyeztetö lap Adóigazolvány bemutatása Közüzemi számlák	Közjegyzöi nyilatkozat
Szervezetek azonosításához	Nyilvános cégnyilvántartási adatok Postacím, telefonszám létezése	Cégbíróság, APEH okmányok Kamarai adategyeztetö lap	Közjegyzöi nyilatkozat
Szerverek azonosításához	Saját domain név	Saját domain név	Saját domain név
Nyilvános kulcs ellenörzése	Kérelem digitális aláírása	Kérelem digitális aláírása	Kérelem digitális aláírása
Jogosultság ellenörzéséhez	Igénylö felhatalmazása	Igénylö írásos felhatalmazása	Közjegyzöi nyilatkozat
Funkció ellenörzéséhez	Nyilatkozat a funkció ellátásáról	Funkció írásos megerösítése	Közjegyzöi nyilatkozat

Típusok	C osztály	B osztály	A osztály
Személyes	C oszt. személyazonosítás Nyilvános kulcs	B oszt. személyazonosítás Nyilvános kulcs	Közjegyzöi nyilatkozat Nyilvános kulcs
Szervezet	C oszt. személyazonosítás C oszt. jogosultság C oszt. szervezetazonosítás Nyilvános kulcs	B oszt. személyazonosítás B oszt. jogosultság B oszt. szervezetazonosítás Nyilvános kulcs	Közjegyzöi nyilatkozat Nyilvános kulcs
Névjegykártya	C oszt. személyazonosítás C oszt. jogosultság C oszt. szervezetazonosítás C oszt. funkcióazonosítás Nyilvános kulcs	B oszt. személyazonosítás B oszt. jogosultság B oszt. szervezetazonosítás B oszt. funkcióazonosítás Nyilvános kulcs	Közjegyzöi nyilatkozat Nyilvános kulcs
Szerver	C oszt. személyazonosítás C oszt. jogosultság C oszt. szervezetazonosítás C oszt. szerverazonosítás Nyilvános kulcs	B oszt. személyazonosítás B oszt. jogosultság B oszt. szervezetazonosítás B oszt. szerverazonosítás Nyilvános kulcs	Közjegyzöi nyilatkozat Nyilvános kulcs

4.4 Tanúsítványkérelmek elutasítása

A kibocsátó hatóság elutasítja a tanúsítványkérelmeket, ha az ÜT 4.1 pontjában felsorolt feltételek teljesülése nem bizonyítható az igényelt tanúsítvány osztályának és típusának elöírt módon.

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

Elutasítás után a kérelmezö új kérelemmel fordulhat a NetLock PKI kibocsátó hatóságaihoz.

5 Kibocsátott tanúsítványok

A kibocsátó hatóság az Ügyfél Tájékoztatóban illetve a Tanúsítványkezelési Eljárási Rendben leírtak szerint jár el.

5.1 A tanúsítvány kibocsátásának idöpontja

A tanúsítvány kibocsátásának idöpontja az a pillanat, amikor a kibocsátó hatóság az aláírt tanúsítványt elérhetövé teszi Internet honlapján.

5.2 A tanúsítvány érvényessége

A tanúsítványban szereplö nyilvános kulcs titkos párja csak a tanúsítványban megjelölt idöintervallumban használható digitális aláírások készítésére. A tanúsítvány érvényességének ellenörzése a tanúsítványt használó felelössége.

6 Tanúsítványok elfogadása az igénylö által

6.1 A tanúsítvány elfogadását jelentö kommunikációs lépések

Feltételezzük, hogy a felhasználó elfogadta a kiadott tanúsítványt, ha a következö kommunikációs lépéseket megtette:

6.1.1 Teszt és „C" osztályú tanúsítványok esetén

A tanúsítványt elfogadottnak tekintjük, ha a felhasználó személyes bejelentkezö nevével és jelszavával belép a CA megfelelö WEB lapjára a tanúsítvány letöltése céljából.

6.1.2 „B" és „A" osztályú tanúsítványok esetén

A tanúsítvány kiadásának feltétele az ügyfélszerzödés aláírása, amely a kiadandó tanúsítvány adatait is tartalmazza, s egyben elfogadó nyilatkozatként is szolgál. A nyilatkozatnak megfelelö tanúsítványt kibocsátásakor automatikusan elfogadottnak tekintjük.

6.2 A tanúsítványigénylö nyilatkozata a tanúsítvány elfogadásakor

A tanúsítvány elfogadásával együtt a felhasználó kijelenti, hogy:

- Ismeri és elfogadja jelen ÜT-t.
- Minden adat, amit a kibocsátó hatóságnak a tanúsítvány kiadásának céljából átadott, a valóságnak megfelel és azok átadása önkéntes volt.
- A tanúsítványban szereplö minden adat a felhasználó tudomásával és egyetértésével került a tanúsítványba.
- A tanúsítvány érvényességét befolyásoló tényekröl haladéktalanul értesíti a kibocsátó hatóságot.
- Jogosulatlan személy nem férhet hozzá titkos kulcsához.
- Ismeri a digitális aláírás megfelelö használatának módját, tisztában van a digitális aláírás használatának technikai feltételeivel és jogi következményeivel.
- Minden egyes digitális aláírás, amely a tanúsítványban szereplö nyilvános kulcs titkos párjával készült, a felhasználó digitális aláírása.
- Minden aláírás az elfogadott és érvényes (vissza nem vont, nem lejárt) tanúsítvány alapján készült.
- A tanúsítványt kizárólag törvényes célokra, jogszerüen, az ÜT-nek megfelelöen használja.
- Tisztában van azzal, hogy a kulcs védelme és a digitális aláírás készítése kizárólag a felhasználó felelössége, s ezzel kapcsolatban a kibocsátó hatóságot semmiféle felelösség nem terheli.
- A felhasználó végfelhasználó, azaz nem kibocsátó hatóság, és nem fogja a tanúsítványban megadott nyilvános kulcs titkos párját újabb tanúsítványok vagy bármely más formátumú tanúsított nyilvános kulcs, visszavonási lista kiadására használni; hacsak erröl külön írásbeli szerzödésben a kibocsátó hatósággal meg nem egyezett.
- Felhatalmazza a kibocsátó hatóságot a tanúsítvány nyilvánosságra hozatalával, és saját vagy más nyilvános tanúsítványgyüjtö helyeken történö elhelyezésével.

7 A tanúsítványok használata

A tanúsítványok digitális aláírások és ezzel üzenetek integritásának ellenörzésére használandók. A digitális aláírás ellenörzésével gyözödünk meg arról, hogy (i) a digitális aláírás a tanúsítványban szereplö nyilvános kulcs titkos párjával készült, és (ii) az aláírt üzenet nem változott meg a digitális aláírás elkészülte óta.

Amennyiben a nyilvános kulcsú titkosítást használó felek az ÜT szerint járnak el a digitális aláírások használatakor, akkor a digitálisan aláírt dokumentummal kapcsolatos jogos érdekeiket bíróság elött érvényesíthetik.

7.1 Digitális aláírás készítése

Azért a folyamatért, amelynek végén a digitálisan aláírt dokumentum megszületik, elsösorban az aláíró a felelös. Ö birtokolja a titkos kulcsot, ö az, akinek ismernie kell az aláírandó üzenet tartalmát, ö dönt az aláírási szándékról és általában ö az, aki az aláírást elvégzö technikai eszközt üzemelteti.

A digitális aláírást készítö felhasználó tanúsítványának igénylésével automatikusan elfogadja a NetLock Általános Szolgáltatási Feltételeit (ÁSZF), mely szerint digitális aláírást az itt leírt eljárás szerint kell készítenie. Amennyiben az aláíró nem körültekintöen jár el a leírt lépések során, úgy az ebböl származó kárért elsösorban ö a felelös. A követendö lépések a következök:

7.1.1 Titkos kulcs megörzése

A digitális aláírás csak akkor biztonságos, ha a titkos kulcs az elöfizetön kívül soha, senki más számára nem hozzáférhetö. A kulcsot jelszóval kódoltan vagy hardver védelemmel kell ellátni. A kulcsot idegen gépre átvinni védelem nélkül nem szabad. A kulcs elvesztéséböl, véletlen vagy szándékos nyilvánosságra hozatalából eredö károkért az elöfizetö felelös. A kulcs kompromittálódását az elöírt módon (ÜT 8. pont) a kibocsátó hatóságnál be kell jelenteni. A szabályosan bejelentett letiltási kérelem után az ÜT-ben meghatározott visszavonási ideig még az elöfizetöt terheli az összes felelösség.

7.1.2 Aláírandó dokumentum tartalmának ellenörzése

Míg hagyományos aláírásnál általában könnyen, addig számítógépes környezetben nem mindig egyszerüen tisztázható az aláírónak az aláírt dokumentumra vonatkozó aláírási szándéka.

Az egyszerübben, észrevétlenebbül készíthetö digitális aláírás alkalmazásának kockázata csökkentendö azzal, ha az elöfizetö csak a számára biztonságosnak tartott számítógépes környezetben, ismert és elfogadott digitális aláíró eszközöket használ. Ezen eszközök akkor alkalmasak feladatuk ellátására, ha az aláírás elött biztonságosan megállapítható, hogy pontosan milyen üzenetre fog rákerülni a digitális aláírás.

Az aláírt dokumentum tartalmával kapcsolatos felelösségek elsösorban az aláírót terhelik. Amennyiben azonban nyilvánvalóan tévesen aláírt dokumentumról van szó, amit az elfogadó felismerhet, akkor az elfogadót is felelösség terheli (ÜT 7.2 pontja).

7.1.3 Digitális aláírás végrehajtása

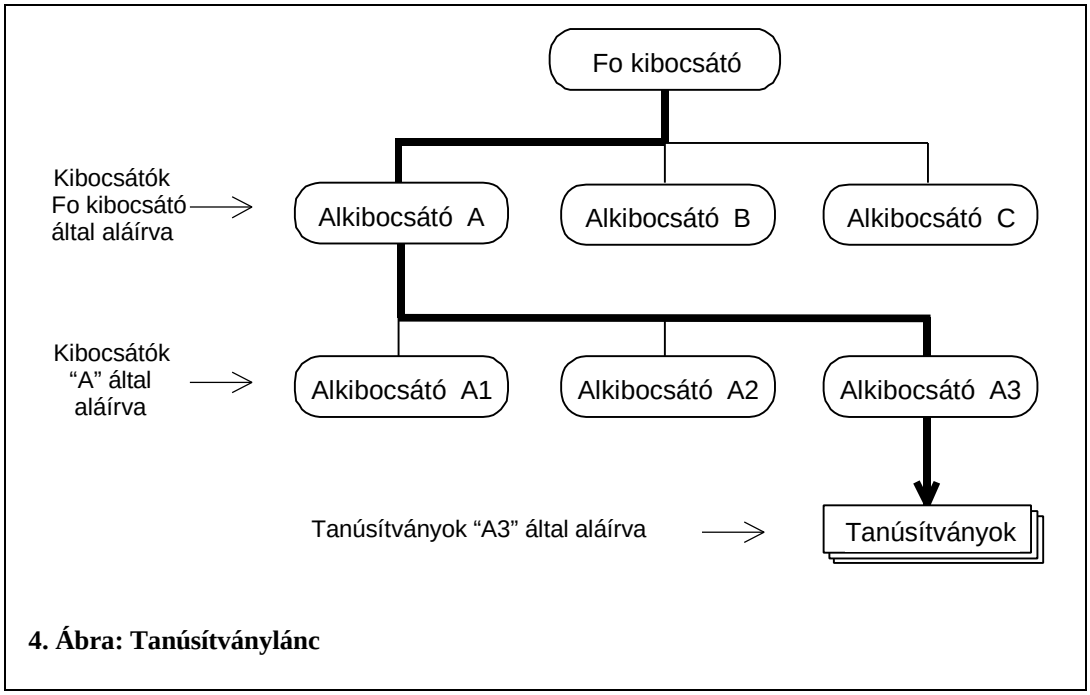
Az aláírási folyamat során felmerülhetnek technikai hibák (pl. az aláíró szoftver hibás aláírást készít vagy megváltoztatja a dokumentum tartalmát aláírás elött). A digitális aláírás létrehozásakor csak olyan digitális aláíró eszközt szabad használni, amelyben az aláíró megbízik. Az aláíró döntési körébe tartozik a megfelelö aláíró berendezés kiválasztása és használata, ezért az aláírás hibátlan végrehajtásáért elsösorban ö a felelös.

7.2 A digitális aláírások ellenörzése

A digitális aláírás elfogadója csak akkor számíthat az elektronikus dokumentum jogi hatására és az azon alapuló elönyökre, ha a digitális aláírások elfogadásakor az ÜT-ben leírt módon jár el. Ezen lépésekröl a digitális aláírás készítöjének tájékoztatnia kell az elfogadót, de legalább utalást kell tennie a leírt követendö lépésekre. A digitális aláírás ellenörzésének a következö lépésekböl kell állnia:

7.2.1 Tanúsítványláncok kialakítása és a megfelelö kiválasztása

A digitális aláírás ellenörzéséhez a felhasználandó tanúsítványokat hitelesítéseik alapján láncba kell rendezni. Meg kell gyözödni arról, hogy a tanúsítványláncok közül a legmegfelelöbbet választjuk ki a digitális aláírás ellenörzéséhez. Elképzelhetö ugyanis, hogy egy tanúsítvány ellenörzésénél több tanúsítványláncot is találunk, amin keresztül egy elfogadható root tanúsítványhoz jutunk. Ilyenkor célszerü azt a láncot választani, amely a legmagasabb megbízhatósági szintü kibocsátó hatóság tanúsítványánál ér véget (4. Ábra).



4. Ábra: Tanúsítványlánc

7.2.2 Az üzenet aláírási idöpontjának ellenörzése

A digitális aláírás ellenörzéséhez meg kell állapítani az üzenet aláírásának idöpontját. Csak az a digitális aláírás érvényes, amely a hozzá tartozó tanúsítvány érvényességi ideje alatt készült (ld. ÜT 6.2 pontja). Ugyanezzel az ellenörzéssel kerülhetö el az üzenet-visszajátszásból eredö támadás is. A legjobb módszer egy megbízható harmadik fél által kiadott idöpecsét alkalmazása, melynek érvényességét a digitális aláíráséhoz hasonlóan ellenörizni kell. Kevésbé megbízható, de elfogadható az üzenetben szereplö dátum is. A fentiek mindegyikét nélkülözö üzenet elfogadása nagyobb kockázattal jár, még ha a körülményekböl a keletkezés idöpontja meg is állapítható.

7.2.3 A tanúsítványlánc tagjainak ellenörzése a NetLock PKI adatbázisának alapján

Az elfogadó személynek meg kell gyözödnie arról, hogy a láncban szereplö tanúsítványok mindegyike érvényes volt az aláírás idöpontjában, azaz a bennük jelölt érvényességi idöintervallumban történt az aláírás, és nem szerepelnek valamely visszavonási listán. A láncban szereplö egyes tanúsítványok ellenörzéséhez célszerü a megfelelö kibocsátó hatóság visszavonási listáját használni.

7.2.4 Az aláíró kulcs használatára vonatkozó korlátozások ellenörzése

A kibocsátó hatóság korlátozhatja az általa kiadott tanúsítványhoz tartozó titkos kulcs felhasználási körét. Az ilyen korlátozásokról, vagyis arról, hogy mely esetekben nem tekinthetö a kiadott tanúsítvány megbízhatónak, a tanúsítványban találhatunk információkat. A digitális aláírást ellenörzö személynek meg kell gyözödnie arról, hogy a tanúsítványláncolatban nincsen egyetlen olyan tanúsítvány sem, amely - az adott esetben - korlátozná a végfelhasználó digitális aláírását.

7.2.5 A digitálisan aláírt adatok pontos kiválasztása az üzenetböl

A digitális aláírás technikai ellenörzéséhez pontosan kell tudni, mi az az üzenet, adat, amit aláírtak.

7.2.6 Az aláíró feltételezett vagy jelzett szándéka szerinti értelmezés meghatározása

Csak olyan elektronikus dokumentumtól várható jogi hatás, amelyen szereplö digitális aláírás elfogadásakor jóhiszemüen járt el az elfogadó.

Amennyiben a körülmények további ellenörzési lépéseket tesznek szükségessé, az elfogadó a töle elvárható legnagyobb gondossággal köteles ezeket végrehajtani. A digitális aláírás elfogadója a körülmények mérlegelésekor – többek között - köteles figyelembe venni a tanúsítvány osztályát is.

7.2.7 Az aláírási jogosultság ellenörzése

Elképzelhetö, hogy az aláírt dokumentumon szereplö digitális aláírás minden technikai követelménynek megfelel: az üzenethez tartozik, érvényes, a hitelesítö tanúsítványlánc hibátlan, de az aláíró személynek nem volt joga, felhatalmazása az adott dokumentumot aláírni. Ugyanez a helyzet lehetséges a hagyományos aláírásnál is: az aláírás nem hamis, de az aláírónak nem volt joga az aláíráshoz. Az aláírási jogosultság ellenörzése az aláírást elfogadó feladata.

7.2.8 A digitális aláírás és az aláírt üzenet összetartozásának ellenörzése

A tanúsítványban szereplö nyilvános kulcs és egy, az elfogadó által megbízhatónak tartott technikai eszköz (hardver, szoftver) segítségével végre kell hajtani azon matematikai müveleteket, melyek során kiderül, hogy az aláírt üzenetrész és digitális aláírása összetartoznak-e.

7.3 Érvényes digitális aláírás következményei

Az elektronikusan aláírt dokumentumok jogi hatással bírhatnak. Ez a jogi hatás a felek – az aláíró, az elfogadó és a kibocsátó hatóság – nyilatkozatain és szerzödésein alapul, melyeket a felek a következö módon fogadnak el:

(i) A kibocsátó hatóság részéröl az Általános Szolgáltatási Feltételek és Ügyfél Tájékoztató nyilvánosságra hozatalával.
(ii) Az aláíró az ügyfélszerzödés aláírásával, a tanúsítványkérelem benyújtásával ill. a tanúsítvány elfogadásával.
(iii) Az elfogadó fél részéröl pedig az aláírt dokumentum ÜT 7.2 pontja szerinti elfogadásával.

Amennyiben a felek az ÜT szerint járnak el a digitális aláírások használatakor, akkor a digitálisan aláírt dokumentummal kapcsolatos jogos érdekeiket bíróság elött érvényesíthetik.

7.4 Eljárás a digitális aláírás ellenörzésekor fellépö hibáknál

Nem érvényes digitális aláírás esetén, vagy ha az ellenörzés nem az ÜT pontjainak megfelelöen történt, akkor az aláírás nem tekinthetö valódinak, és az elfogadásból eredö minden kár és kockázat az elfogadót terheli.

8 Tanúsítványok visszavonása

8.1 Okok a visszavonásra

A tanúsítványok visszavonásra kerülnek, ha kétely merül fel az ÜT 4.1 pontjában felsorolt feltételek teljesülésével kapcsolatban és a kétely alapja bizonyítható. A tanúsítványok visszavonásra kerülnek akkor is, ha a kiadott tanúsítvány alanya kérelmezi tanúsítványának visszavonását. Visszavonási ok többek között a tanúsítványhoz tartozó titkos kulcs biztonságának sérülése; a regisztráló hatóság megtévesztése a tanúsítvány kiadását érintö kérdésekben vagy a tanúsítás alanyának visszavonási kérelme.

A visszavonási kérelmet a regisztráló hatósághoz kell eljuttatni, mely a visszavonási jogosultság és az indokok ellenörzése után visszavonja a tanúsítványt.

A regisztráló hatóság legjobb belátása szerint jogosult a visszavonási kérelmet benyújtó személyazonosságát, jogosultságát és a visszavonás indokát vizsgálni. Általános irányelv, hogy a visszavonandó tanúsítvány biztonsági szintjének megfelelö ellenörzés történjék meg.

8.2 Kibocsátó hatóság saját tanúsítványának visszavonása

Szélsöséges esetben elöfordulhat, hogy magának a kibocsátó hatóságnak a tanúsítványát kell visszavonni. Ez esetben a kibocsátó hatóság tanúsítványa érvényét veszti, azonban ez nem befolyásolja automatikusan a kibocsátó hatóság által a visszavonást megelözöen kiadott tanúsítványok érvényességét.

8.3 Visszavonás hibás kibocsátás esetén

A kibocsátó hatóság visszavonja azokat a tanúsítványokat, melyekröl kiderül, hogy nem az aktuális TER-ben leírt eljárási rend alapján adták ki öket. A kibocsátó hatóság felfüggesztheti a tanúsítvány érvényességét arra az idötartamra, mely alatt a kérdéses tanúsítvány kibocsátásának körülményeit vizsgálja.

8.4 Visszavonás az igénylö kérésére

A kibocsátó hatóság visszavonja azon tanúsítványokat, melyek visszavonását a tanúsítvány alanya vagy annak nevében jogosultan eljáró kéri. A regisztráló hatóság nem vizsgálja a visszavonás indokát, amennyiben a tanúsítvány visszavonását a fentiek valamelyike kéri.

8.5 A visszavont tanúsítványok listája

A visszavont tanúsítványok azonosítói a *visszavont tanúsítványok listájára* kerülnek. A listát a kiadó rendszeresen frissíti, a legújabb változata NetLock PKI adatbázisából letölthetö. A lista a visszavont tanúsítványok *tárgy* és *sorszám* mezöit illetve a visszavonás okának kódját tartalmazza, mindezt a tanúsítványt kiadó és visszavonó kibocsátó hatóság digitális aláírása hitelesíti.

A kibocsátó hatóság - a megfelelö díjazás mellett - biztonságos kommunikációs csatornán keresztül nyújthat információt egyedi tanúsítványok érvényességével kapcsolatban.

8.6 A felfüggesztés és visszavonás következménye

A tanúsítvány érvényessége szünetel a felfüggesztés idötartama alatt, illetve a visszavonás pillanatától végérvényesen megszünik. A kibocsátó hatóság tanúsítványának visszavonásakor a hatóság tanúsítvány aláírási joga is megszünik, de ez nem érinti automatikusan a visszavonás elött kibocsátott tanúsítványok érvényességét.

8.7 A privát kulcs védelme visszavonás esetén

A titkos kulcs védelméröl a felhasználó a tanúsítvány visszavonása után is köteles gondoskodni. A felhasználónak joga van a visszavont tanúsítványhoz tartozó titkos kulcs megsemmisítésére.

9 Tanúsítvány lejárata

9.1 Elözetes értesítés a tanúsítvány lejártáról

A lejáró tanúsítványokról annak alanya illetve a nevében eljárni jogosult részére 30 nappal a lejárat elött, elektronikus formában értesítést küld a regisztráló hatóság.

9.2 Tanúsítvány lejártának következményei

A lejárt tanúsítvány érvénytelen. A lejárattal nem vesznek el azon kötelezettségek, melyek a tanúsítvány kérelmével, kibocsátásával, elfogadásával és használatával kapcsolatosak.

9.3 Tanúsítványok megújítása

Lejárt tanúsítvány alanya számára a tanúsítvány megújítása kérhetö. A kérelemhez csak a megváltozott adatokat kell csatolni, az igényelt tanúsítvány típusának és osztályának megfelelö módon. Ezek alapján a Kibocsátó vagy új tanúsítványt állít ki az alany új kulcspárjához, vagy a régi tanúsítványt meghosszabbítja.[1]

10 Egyéb rendelkezések, intézkedések

[1] A *meghosszabbítást* egyelore nem támogatjuk.

10.1 Jogi szabályozás

Magyarországon egyelöre nincs elfogadott törvény, amely az elektronikus iratok jogi hatását szabályozná. Egy törvénytervezet elökészítése folyamatban van, s a NetLock Hálózatbiztonsági és Informatikai Szolgáltató Kft. részt vesz ebben. A NetLock PKI eljárási rendjei és szerzödései a várható törvényi rendelkezésekkel összhangban van.

10.2 Az Ügyfél Tájékoztató módosításai

A mindenkor érvényes ÜT megtalálható a NetLock Internet honlapján (http://www.netlock.net). A NetLock Kft. jogosult az ÜT egyoldalú módosítására. A NetLock Kft. minden töle elvárhatót megtesz azért, hogy az ÜT módosításáról megfelelö tájékoztatást adjon.

10.3 Szolgáltatási díjak

A mindenkor érvényes szolgáltatási díjak megtalálhatók a NetLock Internet honlapján (http://www.netlock.net).

11 Függelék

11.1 Szójegyzék

Fogalom	**Magyarázat**
Adatbázis	Összefüggö információk sorozata, melyeket számítógépes információs rendszer hoz létre, tárol és használ.
Aláírás	Eljárás, mellyel dokumentumok készítöi azonosítják magukat és hitelesítik a dokumentum tartalmát. Az aláíráskor és elfogadáskor követendö eljárásnak az Elfogadó által is ismertnek kell lennie. (ld. még: Digitális Aláírás)
Aláírási szándék	Az aláíró – egy adott dokumentum hitelesítésére vonatkozó - határozott szándéka.
Általános Szolgáltatási Feltételek	A NetLock PKI szolgáltatásainak, tanúsítványainak igénybevételéhez szükséges feltételeket illetve egyéb szerzödési feltételeket leíró dokumentum.
ÁSZF	ld. Általános Szolgáltatási Feltételek
Aszimmetrikus	Nem szimmetrikus. Jelen környezetben egy kódolási eljárás tulajdonsága, melyben a kódoláshoz és a dekódoláshoz két különbözö, de összetartozó kulcsot használnak.
Biztonsági szintek (A, B, C)	A NetLock PKI által végzett ellenörzések különbözö szintjei.
Digitális aláírás	Az elektronikus környezetben használandó aláírási eljárás. Mind az aláírót, mind az aláírt adatot egyértelmüen azonosító, egyedi jelsorozat.
Digitális aláírások ellenörzése	Az aláírt adat és a digitális aláírás összetartozását ellenörzö eljárás. Érvényes digitális aláírás esetén kijelenthetö, hogy az aláírt adatot az ellenörzéshez használt tanúsítvány tulajdonosa írta alá, s az aláírt adat az aláírás óta nem változott meg, sértetlen.
Domain név	ld. Internet cím
Elektronikus üzenet	Elektronikusan (pl. elektronikus levélben) továbbított adat.
Elfogadási Nyilatkozat	Az ÁSZF elfogadását jelzö, aláírt dokumentum.
Elfogadható root tanúsítvány	A tanúsítványlánc végsö eleme, mely saját maga által hitelesített, s melyben a digitális aláírást ellenörzö megbízik.
Ellenörzési lépések	A digitális aláírás ellenörzésekor kötelezö lépések, melyeket az Ügyfél Tájékoztató tartalmaz.
Elöfizetö	Szerzödéses partner, aki igénybe veszi a NetLock PKI valamely szolgáltatását.
Elötanúsítvány	A NetLock PKI által használt kifejezés azon ellenörzött adathalmazra, mely egy Kibocsátó Hatóság digitális aláírásával ellátva tanúsítványt eredményez.
Hitelesítö hatóság	A Kibocsátó Hatóság és Regisztrációs Hatóságok funkcióit egyesítö szolgáltató.
Idöpecsét	Elektronikus dokumentumokon a készítés idöpontjának meghatározására alkalmas adat.
Intelligens kártya	Hitelkártya formájú és méretü számítógép. Fö alkalmazási területei a távközlés (telefonkártya), személyi azonosítás (digitális személyi igazolvány) és a hálózatbiztonság (digitális aláíró kártya).
Internet	Nyílt hálózat, amelyhez számítógéppel csatlakozhatunk. A hálózaton üzeneteket küldhetök és adatbázisok érhetök el.
Internet cím	Az Internethez csatlakoztatott számítógépek eléréséhez használt név. A WWW szolgáltatásoknál ez általában www.cégnév.hu
Internet honlap	Egy cég vagy szervezet WEB lapjai közül a bemutatkozó elsö oldal.
Jelölt érvényességi idöintervallum	A tanúsítványban megjelölt idöintervallum, mely alatt a tanúsítványhoz tartozó titkos kulcs aláírásra használható.
Kiadási feltételek	Feltételek, amelyek teljesülésekor a NetLock PKI tanúsítványt adhat ki.
Kibocsátó hatóság	Szervezet, mely elötanúsítványok digitális aláírásával, a kész tanúsítványok és visszavonási listák terjesztésével foglalkozik.
Kompromittálódás	A biztonság sérülése. Titkos kulcs esetén pl. lehet jelszó nyilvánosságra kerülése.
Közjegyzök	Dokumentumok és események hitelesítésével foglalkozó, kamarába tömörült személyek.

Közjegyzői dokumentumok és nyilatkozatok	Közjegyzök aláírásával hitelesített, eredeti dokumentumok.
Kulcsadatbázis	Adatbázis, melyben a kibocsátó hatóságok által kiadott tanúsítványok elérhetök és letölthetök.
Kulcspár	Összetartozó nyilvános és titkos kulcs.
Aláíró eszköz	Olyan technikai eszköz (pl. számítógépes program), mely segítségével az aláírás készítéséhez szükséges lépések biztonsággal és ellenörizhetöen elvégezhetök.
NEI	Nem Ellenörzött Információ
Nem Ellenörzött Információk	Tájékoztató jellegü információk, melyek valódiságát a kibocsátó hatóság nem ellenörzi.
NetLock	A NetLock PKI létrehozójának és üzemeltetöjének neve.
NetLock adatbázis	Adatbázis, melyben a NetLock PKI müködése során keletkezö dokumentumokat, tanúsítványokat kezelik.
Nyílt hálózat	Hálózat, melyben a felhasználók által küldött üzenetek általuk nem kontrollált csomópontokon keresztül is haladnak (pl. Internet).
Nyilvános Cégnyilvántartás	Közhitelü adatbázis, mely a bejegyzett és müködö cégek különbözö adatait tartalmazza. Ilyet üzemeltet például a Cégbíróság is.
Nyilvános kulcs	A kulcspár azon tagja, amelyet a küldendö üzenet titkosítására illetve a kapott üzenet digitális aláírásának ellenörzésére használunk.
Nyilvános kulcsú titkosítás	Kódolási eljárás, mely olyan partnerek közti kommunikáció esetén is gyakorlati titkosságot nyújt, akik az üzenetküldést megelözöen soha nem találkoztak. Lényege az, hogy külön kulcsot használ a titkosításra (nyilvános kulcs) és külön kulcsot az üzenetek dekódolására (titkos kulcs).
PKI	Ld. Publikus Kulcs Infrastruktúra
Postai adategyeztetés	A Magyar Posta által nyújtott szolgáltatás. Az ügyfelek azonosítása postahivatalokban történik. A közjegyzöi azonosításhoz hasonlóan személyes megjelenés szükséges.
Privát kulcs	Ld. Titkos Kulcs
Publikus Kulcs Infrastruktúra	Nyilvános kulcsú kódolást lehetövé tevö rendszer. Elemei a kibocsátó hatóságok, a tanúsítványok, visszavonási listák, eljárásai rendek és szolgáltatási feltételek.
Publikus Kulcs	ld. Nyilvános Kulcs
Regisztrációs adatbázis	Adatbázis, melyben a PKI ügyfelek adatai találhatók. A tanúsítványkérelmek és tanúsítványok mindig egy, a regisztrációs adatbázisban szereplö felhasználóhoz kapcsolódnak.
Regisztrációs hatóság	Szervezet, amely az elötanúsítványt állítja elö. Elöírt lépésekkel ellenörzi a tanúsítvány alanyának kilétét és titkos kulcsával való összetartozását. Egy kibocsátó hatóság több regisztrációs hatósággal müködhet együtt.
Regisztrált	Felhasználó, akinek adatai a regisztrációs adatbázisban szerepelnek.
RSA	Az RSA az egyik legelterjedtebb, rendkívül biztonságos nyilvános kulcsos titkosító algoritmus, melyet Ron Rivest, Adi Shamir és Len Adelman professzorok fejlesztettek ki.
Szolgáltatási díj	A felhasználók által igénybevett, NetLock PKI szolgáltatások ellenértéke.
Szoftver	Számítógépen futó program.
Tanúsítvány	A kibocsátó hatóság által digitálisan aláírt elektronikus dokumentum, mely megbonthatatlanul tartalmazza a tanúsítvány tulajdonosának azonosítására szolgáló adatokat (pl. neve) és a tulajdonos nyilvános kulcsát. A digitális aláírások ellenörzésekor használjuk öket.
Tanúsítvány alanya	Az a felhasználó, akinek adatai és nyilvános kulcsa a tanúsítványban szerepelnek.
Tanúsítvány elfogadása	A kibocsátott tanúsítvány adatainak ellenörzése után a felhasználó kijelentése arról, hogy az a saját adatait tartalmazza.
Tanúsítványigénylés	Eljárás, mely során a felhasználó tanúsítvány kibocsátását kéri egy kibocsátó hatóságtól.
Tanúsítványkezelési Eljárási Rend	A regisztráló és kibocsátó hatóságok lépéseit és eljárásait leíró dokumentum. A kibocsátó ezen dokumentumban elöírt eljárásokat végzi pl. a tanúsítványok kiadásakor, visszavonásakor.
Tanúsítványlánc	A digitális aláírás ellenörzésekor használt tanúsítványok, melyek aláíróik alapján láncba szervezhetök.

Tanúsítványok osztálya (A, B, C)	A tanúsítványok megbízhatósága szerinti megkülönböztetés. A kibocsátást megelözö ellenörzö lépések biztonságosságának jelzése.
Titkos kulcs	A kulcspár azon kulcsa, amelyet a küldendö üzenet digitális aláírásának készítésére használunk. Fontos, hogy ehhez a kulcshoz csak tulajdonosa férjen hozzá.
Ügyfélszerzödés	A NetLock PKI szolgáltatásainak igénybevételéröl szóló szerzödés. Formailag az ÁSZF elfogadásával jön létre.
Ügyfél Tájékoztató	A tanúsítványok, digitális aláírások használatát leíró dokumentum. A NetLock PKI felhasználóinak az Ügyfél Tájékoztatót ismerniük kell ahhoz, hogy biztonságosan alkalmazzák a nyilvános kulcsú titkosítást.
ÜT	Ld. Ügyfél Tájékoztató
Üzenetek integritása	Üzenetek sértetlensége, változatlansága.
Üzenet-visszajátszás	A kommunikáció biztonsága elleni aktív támadás, mely során egy, már egyszer elküldött üzenetet a támadó újra eljuttat a régi címzetthez (pl. a támadó lopott jelszóval próbál szolgáltatást igénybe venni).
Visszavont tanúsítványok listája	Valamilyen okból visszavont, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista. A tanúsítványokat kiadó kibocsátó hatóság digitális aláírása hitelesíti.
X.500 szabvány	Felhasználói adatok pontos leírását szabályozó nemzetközi szabvány.
X.509v3 szabvány	A tanúsítványok formai és tartalmi követelményeit szabályozó nemzetközi szabvány. A NetLock PKI a szabványnak megfelelö tanúsítványokat használ.