Szolgáltatási Szabályzat

NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Verzió: 1.3.6.1.4.1.3555.1.2.011015

HIF regisztrációs szám: a nyilvántartásba vétel még nem történt meg

A Szabályzat hatálya: a HIF nyilvántartásba vételének napja, illetve ennek hiányában a nyilvántartásba vétel iránti kérelem beadásának napjától számított 30. nap, amennyiben a HIF a nyilvántartásba vételt nem tagadja meg

1 Felhasználó általános tájékoztatása

A jelen Szolgáltatási Szabályzat a NetLock Kft. (a továbbiakban: Szolgáltató) hitelesítési szolgáltatásának szabályozását tartalmazza.

1.1 A Szolgáltató adatai

- **Név:** NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság
- **Cégjegyzék szám:** 01-09-563961
- **Székhely, telephely:** 1023 Budapest, Zsigmond tér 10.
- **Telefonszám:** (1) 345-2255
- **Telefax szám:** (1) 345-2250
- **Internet cím:** http:// www.netlock.hu
- **Központi e-mail cím:** info@netlock.hu
- **Panaszok bejelentésének helye:** elektronikus levélben a reklamacio@netlock.net címen, írásban a Szolgáltató telephelyére címezve
- **Illetékes fogyasztóvédelmi felügyelőség:** Budapest Főváros Közigazgatási Hivatal Fogyasztóvédelmi Felügyelőség, 1088 Budapest, József krt. 6., Levélcím: 1364. Budapest, Pf. 234., telefon: 4594-918, telefax: 4594-870
- **HIF nyilvántartásba vétel napja:** a nyilvántartásba vétel még nem történt meg
- **Egyéb minősítések:** Ernst and Young AICPA/CICA WebTrust for Certification Authorities audit (2000)

1.2 Szolgáltatási Szabályzat adatai

- **Szolgáltatási Szabályzat verziószám:** 1.3.6.1.4.1.3555.1.3.011015
- **HIF regisztrációs szám**: a nyilvántartásba vétel még nem történt meg
- **Hatályba lépés dátuma:** a HIF nyilvántartásba vételének napja, illetve ennek hiányában a nyilvántartásba vétel iránti kérelem beadásának napjától számított 30. nap, amennyiben a HIF a nyilvántartásba vételt nem tagadja meg
- **Hatályának megszűnése:** visszavonáskor

2 Fogalmak, meghatározások

Aláírás-ellenőrző adat: Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.

Aláírás-létrehozó adat: Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.

Aláírás-létrehozó eszköz: Szoftver vagy hardver, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Aláíró: Az a természetes személy, akihez a hitelesítés szolgáltató által közzétett aláírás-ellenőrző adatok jegyzéke szerint az aláírás-ellenőrző adat kapcsolódik.

Általános Szolgáltatási Feltételek (ÁSZF): A Szolgáltató szolgáltatásainak, tanúsítványainak igénybevételéhez szükséges feltételeket illetve egyéb szerződési feltételeket leíró dokumentum.

Belépési Nyilatkozat: Az ÁSZF elfogadását jelző, aláírt dokumentum.

Biztonságos aláírás-létrehozó eszköz: Az elektronikus aláírás törvény 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.

Biztonsági szintek: (A, B, C) A Szolgáltató által végzett ellenőrzések különböző szintjei.

Elektronikus aláírás: elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.

Ellenőrzési lépések: Az elektronikus aláírás ellenőrzésekor kötelező lépések, melyeket a Szolgáltatási Szabályzat tartalmaz.

Előtanúsítvány: A Szolgáltató által használt kifejezés azon ellenőrzött adathalmazra, mely egy hitelesítés szolgáltató elektronikus aláírásával ellátva tanúsítványt eredményez.

Érintett fél: Az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el.

Felhasználó: Szerződéses partner, aki igénybe veszi a Szolgáltató valamely szolgáltatását.

Fokozott biztonságú elektronikus aláírás: Elektronikus aláírás, amely megfelel a következő követelményeknek:

- alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,
- olyan eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll,
- a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően az iraton, illetve dokumentumon tett - módosítás érzékelhető.

Hitelesítés szolgáltató: Személy (szervezet), amely a hitelesítés szolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványokhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány visszavonási listát.

Kompromittálódás: biztonsági sérülés.

(**Kriptográfiai**) **Kulcs**: Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.

Nyilvános Cégnyilvántartás: Közhitelű adatbázis, mely a bejegyzett és működő cégek különböző adatait tartalmazza. Ilyet üzemeltet például a Cégbíróság is.

Nyilvános (**publikus**) **kulcsú infrastruktúra**: Az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.

Postai adategyeztetés: A Magyar Posta által nyújtott szolgáltatás. Az ügyfelek azonosítása postahivatalokban történik. A közjegyzői azonosításhoz hasonlóan személyes megjelenés szükséges.

Regisztrációs egység: Szervezet, amely ellenőrzi a tanúsítvány alanyának személyazonosságát. Egy hitelesítés szolgáltató több ilyen szervezettel is együttműködhet.

Szolgáltatási szabályzat: A hitelesítés szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum.

Tanúsítvány: A hitelesítés szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot az aláíró személyéhez kapcsolja.

Tanúsítványok osztályai: (A, B, C) A tanúsítványok megbízhatósága szerinti megkülönböztetés. A kibocsátást megelőző ellenőrző lépések biztonságosságának jelzése.

Tanúsítvány-típus: Szabályok összessége, amely megmutatja adott tanúsítványok alkalmazhatóságát egy bizonyos közösségre, illetve alkalmazások olyan csoportjára, ahol azonosak a biztonsági követelmények.

Tanúsítvány visszavonási lista: Valamely okból visszavont, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a hitelesítés szolgáltató bocsát ki.

Törvény: 2001. évi XXXV. törvény az elektronikus aláírásról.

3 NetLock Nyilvános Kulcsú Infrastruktúra (PKI)

3.1 A NetLock tanúsítványok osztályai és típusai

A Szolgáltató regisztrációs és hitelesítő funkciót végez, regisztrációs és hitelesítő egységekből áll. A Szolgáltató hitelesítő szolgáltatását PKI hierarchiában végzi, mely hierarchiában négy hitelesítési egység (ún. osztályok) működik.

3.1.1 Tanúsítványok osztályai és tulajdonságaik

3.1.1.1 Teszt osztályú tanúsítványok

A teszt tanúsítvány a hálózatbiztonsági szolgáltatások tesztelési céljaira kiadott tanúsítvány.

A teszt szinten a hitelesítés szolgáltató 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 az érintett felek számára; a tanúsítvány többi mezőjében található információ nem ellenőrzött információnak (NEI) tekintendő.

3.1.1.2 “C” osztályú tanúsítványok

A “C” osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát korlátozott, részben emberi beavatkozással történt ellenőrzési lépéseken keresztül azonosította a hitelesítés szolgáltató. Használata elektronikus levelezéshez, kisebb kockázatú tranzakciókhoz, on-line szolgáltatások igénybevételéhez, szoftver forrásának ellenőrzéséhez ajánlott.

A Szolgáltató a “C” osztályú tanúsítvány kiadása előtt a jelen szabályzat vonatkozó pontjában felsorolt ellenőrzéseket végezte el, és valószínűsítette a jelen szabályzat vonatkozó pontjában felsorolt kiadási feltételek meglétét.

3.1.1.3 “B” osztályú tanúsítványok

A “B” osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát szigorú ellenőrzési lépések során azonosította a hitelesítés szolgáltató. Használata elektronikus levelezéshez, közepes kockázatú tranzakciókhoz, on-line szolgáltatások igénybevételéhez, szoftver forrásának ellenőrzéséhez ajánlott.

A Szolgáltató a “B” osztályú tanúsítvány kiadása előtt a jelen szabályzat vonatkozó pontjában felsorolt ellenőrzéseket a tőle elvárható legnagyobb gondossággal végezte el, ezáltal meggyőződött a jelen szabályzat vonatkozó pontjában felsorolt kiadási feltételek meglétéről.

3.1.1.4 “A” osztályú tanúsítványok

Az “A” osztályú tanúsítvány olyan személyeknek, szervezeteknek vagy szervereknek kiadott tanúsítvány, amely alanyát szigorú ellenőrzési lépések során azonosította a hitelesítés szolgáltató. Használata nagy értékű tranzakcióknál, pénzügyi utasítások és információk ellenőrzésénél, szerződéskötéseknél ajánlott.

A Szolgáltató az “A” osztályú tanúsítvány kiadása előtt a jelen szabályzat vonatkozó pontjában felsorolt ellenőrzéseket közjegyzői dokumentumokkal és nyilatkozatokkal alátámasztva, a tőle elvárható legnagyobb gondossággal végezte el, és meggyőződött a jelen szabályzat vonatkozó pontjában felsorolt kiadási feltételek meglétéről.

3.1.2 Tanúsítványtípusok

Az “A”, “B” és “C” osztályokban a következő tanúsítványtípusok kiadását végzik a Szolgáltató:

3.1.2.1 Személyes aláíró és titkosító tanúsítványok

Személyes tanúsítványokat természetes személy igényelhet a saját nevében.

A tanúsítvány Country és Locality mezőjében az igénylő lakóhelyének országkódja és városa, az Organization és Organization Unit mezőkben semmi, a Common Name mezőjében az igénylő neve és (opcionálisan) elektronikus levelezési címe szerepel. A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

3.1.2.2 Meghatalmazásos aláíró és titkosító tanúsítványok

Meghatalmazásos (névjegykártyás) tanúsítványokat természetes személy igényelhet egy adott szervezet tagjaként. A szervezet - többek között - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány. A tanúsítványban szerepel a személy szervezetben betöltött funkciója is.

A tanúsítvány Country és Locality mezőjében az igénylő szervezete telephelyének országkódja és városa, az Organization mezőben szervezetének neve, az Organizational Unit mezőben funkciója, a Common Name mezőjében az igénylő neve és (opcionálisan) elektronikus levelezési címe szerepel. A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

3.1.2.3 Szervezet aláíró és titkosító tanúsítványok

Szervezet tanúsítványokat szervezet vagy annak szervezeti egysége igényelhet saját nevében. A szervezet - többek között - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány.

A tanúsítvány Country és Locality mezőjében a szervezet telephelyének országkódja és városa, az Organization mezőben a szervezet neve, az Organizational Unit mezőben a szervezeti egység neve, a Common Name mezőjében ismételten az Organization és az Organizational Unit értékek, majd (opcionálisan) elektronikus levelezési címe szerepel. A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

3.1.2.4 Szerver tanúsítvány

Szerver tanúsítványt Internet címmel (ún. host névvel) rendelkező, szervert üzemeltető természetes személy vagy szervezet igényelhet.

A tanúsítvány Country és Locality mezőjében az üzemeltető székhelyének vagy lakóhelyének országkódja és városa, az Organization mezőben az üzemeltető neve, az Organizational Unit mezőben az üzemeltető szervezeti egység neve, a Common Name mezőben a szerver internetes elnevezése

(ún. host neve) szerepel. A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

3.1.2.5 WAP Gateway tanúsítvány

WAP Gateway tanúsítványt WAP Gateway eszközt üzemeltető természetes személy vagy szervezet igényelhet.

A tanúsítvány Country és Locality mezőjében az üzemeltető székhelyének vagy lakóhelyének országkódja és városa, az Organization mezőben az üzemeltető neve, az Organizational Unit mezőben az üzemeltető szervezeti egység neve, a Common Name mezőben az eszköz internetes elnevezése (ún. host neve) szerepel. A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

3.1.2.6 VPN tanúsítvány

VPN tanúsítványt VPN eszközt üzemeltető természetes személy vagy szervezet igényelhet.

A tanúsítvány a különböző VPN szabványok szerinti adatok szerepelnek, melyek szerint általában a Country és Locality mezőben az üzemeltető székhelyének vagy lakóhelyének országkódja és városa, az Organization mezőben az üzemeltető neve, az Organizational Unit mezőben az üzemeltető szervezeti egység neve, a Common Name mezőben az eszköz internetes elnevezése (ún. host neve) szerepel. A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

3.1.2.7 Láncolt Hitelesítés Szolgáltató tanúsítvány

Egy adott szervezet számára, a szervezet alkalmazottai számára történő tanúsítvány-kibocsátást lehetővé tevő tanúsítvány.

A tanúsítvány Country és Locality mezőjében a szervezet székhelyének országkódja és városa, az Organization mezőben a szervezet neve, az Organizational Unit mezőben az üzemeltető szervezeti egység neve, a Common Name mezőben a szervezeti hitelesítés szolgáltatás neve szerepel. A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

3.2 Tanúsítványigénylés módja

3.2.1 Igénylő regisztrálása

A Szolgáltatónál tanúsítvány hitelesítésének igényével csak regisztrált entitás élhet. A regisztrálható, azaz tanúsítvány igénylésére jogosult entitások jelenleg személyek, szervezetek és WEB szerverek, WAP Gateway-ek és VPN eszközök lehetnek.

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

3.2.2 Kulcsok generálása és védelme

A Szolgáltatónál regisztrált entitások saját maguk generálják a tanúsítvány igényléséhez szükséges nyilvános-magán kulcspárt. A kulcspár generálása történhet saját szoftver segítségével, gyári szoftver termékkel vagy egyéb, biztonságos hardver eszközzel. Az eszközök kiválasztása és használata a tanúsítványigénylő kizárólagos feladata és felelőssége.

A nyilvános kulcsú kódolási eljárás biztonságos használata a későbbiekben sérülhet, ha a magánkulcs védelme nem megfelelően biztosított. A magánkulcsot 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.

3.3 Tanúsítványkérelmek jóváhagyása

3.3.1 A tanúsítványkérelmek jóváhagyásának követelményei

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

- az igénylő benyújtotta kérelmét a tanúsítvány kibocsátónak,
- az entitás (akinek nevében az igénylő eljár) azonos a kérelemben szereplő alannyal,
- az igénylő jogosult a kérelemben szereplő alany nevében kérelmet benyújtani,
- az igénylő birtokában van a kérelemben szereplő nyilvános kulcs titkos párja,
- a kérelemben szereplő adatok ellenőrizhetők és pontosak, kivéve a tájékoztató jellegű adatokat.

3.3.2 Teszt tanúsítvány kiadására irányuló kérelmek elfogadása

Teszt tanúsítványok kiadásához az igénylőnek érvényes elektronikus levelezési címmel kell rendelkeznie. A NetLock Teszt Hitelesítési Egység automatizált lépéseken keresztül végzi a teszt tanúsítvány kiadását. A lépések során a kiadó a megadott elektronikus levelezési címre továbbít utasításokat, és erről a levelezési címről várja a tanúsítvány kiadására vonatkozó kérelem megerősítését.

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

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

A Szolgáltató elfogadja a tanúsítvány kiadására irányuló kérelmet, ha az igényelt tanúsítvány osztályának és típusának megfelelő ellenőrzési lépések végrehajthatók és eredményesen befejeződtek.

Ellenőrzés	C osztály	B osztály	A osztály
Személyek azonosításához	"B" osztályban regisztrált 2 tanú Postacím, telefonszám létezése Személyi igazolvány másolata Adóigazolvány bemutatása Közüzemi számlák másolata	Személyi igazolvány, útlevél bemutatása Postai adategyeztető lap Adóigazolvány bemutatása Közüzemi számlák	Közjegyzői nyilatkozat
Szervezetek azonosításához	Nyilvános cégnyilvántartási adatok Postacím, telefonszám létezése	Cégbíróság, APEH okmányok Kamarai adategyeztető lap	Közjegyzői nyilatkozat
Szerverek azonosításához	Saját domain név	Saját domain név	Saját domain név
Nyilvános kulcs ellenőrzése	Kérelem elektronikus aláírása	Kérelem elektronikus aláírása	Kérelem elektronikus aláírása
Jogosultság ellenőrzéséhez	Igénylő felhatalmazása	Igénylő írásos felhatalmazása	Közjegyzői nyilatkozat
Funkció	Nyilatkozat a funkció ellátásáról	Funkció írásos megerősítése	Közjegyzői nyilatkozat

ellenőrzéséhez

Típusok	C osztály	B osztály	A osztály
Személyes	C oszt. személyazonosítás Nyilvános kulcs	B oszt. személyazonosítás Nyilvános kulcs	Közjegyzői 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	Közjegyzői 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	Közjegyzői 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	Közjegyzői nyilatkozat Nyilvános kulcs

3.3.4 Tanúsítványkérelmek elutasítása

A Szolgáltató elutasítja a tanúsítványkérelmeket, ha a jelen szabályzatban felsorolt feltételek teljesülése nem bizonyítható az igényelt tanúsítvány osztályának és típusának előírt módon.

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

Elutasítás után a kérelmező új kérelemmel fordulhat a Szolgáltatóhoz.

3.4 Kibocsátott tanúsítványok

A Szolgáltató Internet címén elérhető elektronikus adatbázist üzemeltet, amelyben a Szolgáltató által kiadott tanúsítványok, a visszavont tanúsítványok listái, eljárási rendek, szerződési feltételek és más dokumentációk találhatók.

3.4.1 A tanúsítvány kibocsátásának időpontja

A tanúsítvány kibocsátásának időpontja az az időpont, amikor a Szolgáltató az aláírt tanúsítványt elérhetővé teszi Internet címén elérhető adatbázisában.

3.4.2 A tanúsítvány érvényessége

A tanúsítványban szereplő nyilvános kulcs párja csak a tanúsítványban megjelölt időintervallumban használható elektronikus aláírások készítésére. A tanúsítvány érvényességének ellenőrzése a tanúsítványt használó felelőssége.

3.5 Tanúsítványok elfogadása az igénylő által

3.5.1 A tanúsítvány elfogadását jelentő kommunikációs lépések

A Felhasználó elfogadta a kiadott tanúsítványt, ha a következő kommunikációs lépéseket megtette:

3.5.1.1 Teszt és “C” osztályú tanúsítványok esetén

A tanúsítványt elfogadottnak tekintendő, ha a Felhasználó személyes bejelentkező nevével és jelszavával belép a Szolgáltató Interneten elérhető adatbázisába a tanúsítvány letöltése céljából.

3.5.1.2 "B" és "A" osztályú tanúsítványok esetén

A tanúsítvány kiadásának feltétele a Belépési Nyilatkozat aláírása, amely a kiadandó tanúsítvány adatait is tartalmazza, s egyben elfogadó nyilatkozatként is szolgál. A nyilatkozatnak megfelelő tanúsítvány kibocsátásakor automatikusan elfogadottnak tekintendő.

3.5.2 A tanúsítványigénylő nyilatkozata a tanúsítvány elfogadásakor

A tanúsítvány elfogadásával együtt a Felhasználó kijelenti, hogy:

- ismeri, érti és elfogadja jelen és kapcsolódó szabályzatokat,
- minden adat, amit a Szolgáltatónak a tanúsítvány kiadásának céljából átadott, a valóságnak megfelel és azok átadása önkéntes volt,
- a tanúsítványban szereplő minden adat a Felhasználó tudomásával és egyetértésével került a tanúsítványba,
- a tanúsítvány érvényességét befolyásoló tényekről haladéktalanul értesíti a Szolgáltatót,
- jogosulatlan személy nem férhet hozzá magánkulcsához,
- ismeri az elektronikus aláírás megfelelő használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,
- minden egyes elektronikus aláírást, amely a tanúsítványban szereplő nyilvános kulcs párjával készült, a Felhasználó saját elektronikus aláírásának ismeri el,
- tudomással bír arról, hogy az elektronikus aláírással ellátott elektronikus iratok az írásbafoglalás jogszabályi követelményének megfelelnek,
- minden aláírás az elfogadott és érvényes (vissza nem vont, nem lejárt) tanúsítvány alapján készült,
- a tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályoknak és törvényi előírásoknak megfelelően használja,
- tisztában van azzal, hogy a kulcs védelme és az elektronikus aláírás készítése kizárólag a Felhasználó felelőssége, s ezzel kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
- a Felhasználó végfelhasználó, azaz nem hitelesítés szolgáltató, és nem fogja a tanúsítványban megadott nyilvános kulcs párját újabb tanúsítványok vagy bármely más formátumú tanúsított nyilvános kulcs, visszavonási lista kiadására használni; hacsak erről külön írásbeli szerződésben a Szolgáltatóval meg nem egyezett,
- felhatalmazza a Szolgáltatót a tanúsítvány nyilvánosságra hozatalával, és saját vagy más nyilvános tanúsítványgyűjtő helyeken történő elhelyezésével.

3.6 A tanúsítványok használata

Az aláíró tanúsítványok elektronikus aláírások és ezzel üzenetek integritásának ellenőrzésére, a titkosító tanúsítványok üzenetek titkosítására használandók. Az elektronikus aláírás ellenőrzésével lehet meggyőződni arról, hogy (i) az elektronikus aláírás a tanúsítványban szereplő nyilvános kulcs titkos párjával készült, és (ii) az aláírt üzenet nem változott meg az elektronikus aláírás elkészülte óta.

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

3.6.1 Elektronikus aláírás készítése

Azért a folyamatért, amelynek végén az elektronikusan aláírt dokumentum megszületik, elsősorban az aláíró a felelős. Ő birtokolja a magánkulcsot, ő az, akinek ismernie kell az aláírandó üzenet tartalmát, ő dönt az aláírási szándékról és általában ő az, aki az aláírást elvégző technikai eszközt üzemelteti.

Az elektronikus aláírást készítő Felhasználó tanúsítványának igénylésével automatikusan elfogadja a Szolgáltató Általános Szolgáltatási Feltételeit (ÁSZF), mely szerint elektronikus aláírást az itt leírt eljárás szerint kell készítenie. Amennyiben az aláíró nem körültekintően jár el a leírt lépések során, úgy az ebből származó kárért elsősorban ő a felelős. A követendő lépések a következők:

3.6.1.1 Magánkulcs megőrzése

Az elektronikus aláírás csak akkor biztonságos, ha a magánkulcs az előfizetőn kívül soha, senki más számára nem hozzáférhető. A kulcsot jelszóval kódoltan vagy hardver védelemmel kell ellátni. A kulcsot idegen gépre átvinni védelem nélkül nem szabad. A kulcs elvesztéséből, véletlen vagy szándékos nyilvánosságra hozatalából eredő károkért az előfizető felelős. A kulcs kompromittálódását az előírt módon a Szolgáltatónál be kell jelenteni. A szabályosan bejelentett letiltási kérelem után a jelen szabályzatban meghatározott visszavonási ideig még az előfizetőt terheli az összes felelősség.

3.6.1.2 Aláírandó dokumentum tartalmának ellenőrzése

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

Az egyszerűbben, észrevétlenebbül készíthető elektronikus aláírás alkalmazásának kockázata csökkentendő azzal, ha az előfizető csak a számára biztonságosnak tartott számítógépes környezetben, ismert és elfogadott elektronikus aláíró eszközöket használ. Ezen eszközök akkor alkalmasak feladatuk ellátására, ha az aláírás előtt biztonságosan megállapítható, hogy pontosan milyen üzenetre fog rákerülni a elektronikus aláírás.

Az aláírt dokumentum tartalmával kapcsolatos felelősségek elsősorban az aláírót terhelik. Amennyiben azonban nyilvánvalóan tévesen aláírt dokumentumról van szó, amit az érintett fél felismerhet, akkor az érintett felet is felelősség terheli.

3.6.1.3 Elektronikus aláírás végrehajtása

Az aláírási folyamat során felmerülhetnek technikai hibák (pl. az aláíró szoftver hibás aláírást készít vagy megváltoztatja a dokumentum tartalmát aláírás előtt). Az elektronikus aláírás létrehozásakor csak olyan elektronikus aláíró eszközt szabad használni, amelyben az aláíró megbízik. Az aláíró döntési körébe tartozik a megfelelő aláíró berendezés kiválasztása és használata, ezért az aláírás hibátlan végrehajtásáért ő a felelős.

3.6.2 Az elektronikus aláírások ellenőrzése

Az elektronikus aláírás elfogadója csak akkor számíthat az elektronikus dokumentum jogi hatására és az azon alapuló előnyökre, ha az elektronikus aláírások elfogadásakor a jelen és kapcsolódó szabályzatokban és törvényi előírásokban leírt módon jár el. Ezen lépésekről az elektronikus aláírás készítőjének tájékoztatnia kell az érintett felet, de legalább utalást kell tennie a leírt követendő lépésekre. Az elektronikus aláírás ellenőrzésének a következő lépésekből kell állnia:

3.6.2.1 Tanúsítványláncok kialakítása és a megfelelő kiválasztása

Az elektronikus aláírás ellenőrzéséhez a felhasználandó tanúsítványokat hitelesítéseik alapján láncba kell rendezni. Meg kell győződni arról, hogy a tanúsítványláncok közül a legmegfelelőbbet választjuk ki az elektronikus aláírás ellenőrzéséhez. Ha egy tanúsítvány ellenőrzésénél több tanúsítványláncot is található, amin keresztül egy elfogadható gyökér tanúsítványhoz lehet jutni, úgy ilyenkor azt a láncot kell választani, amely a legmagasabb megbízhatósági szintű hitelesítés szolgáltató tanúsítványánál ér véget.

3.6.2.2 Az üzenet aláírási időpontjának ellenőrzése

Az elektronikus aláírás ellenőrzéséhez meg kell állapítani az üzenet aláírásának időpontját. Csak az az elektronikus aláírás érvényes, amely a hozzá tartozó tanúsítvány érvényességi ideje alatt készült. Az időpont meghatározása az érintett fél felelőssége, legjobb módszer egy megbízható harmadik fél által kiadott időpecsét alkalmazása, melynek érvényességét az elektronikus aláíráséhoz hasonlóan ellenőrizni kell.

3.6.2.3 A tanúsítványlánc tagjainak ellenőrzése a Szolgáltató adatbázisának alapján

Az érintett félnek meg kell győződnie arról, hogy a láncban szereplő tanúsítványok mindegyike érvényes volt az aláírás időpontjában, azaz a bennük jelölt érvényességi időintervallumban történt az aláírás, és nem szerepelnek valamely visszavonási listán. A láncban szereplő egyes tanúsítványok ellenőrzéséhez célszerű a megfelelő hitelesítés szolgáltató visszavonási listáját használni.

3.6.2.4 Az aláíró kulcs használatára vonatkozó korlátozások ellenőrzése

A hitelesítés szolgáltató korlátozhatja az általa kiadott tanúsítványhoz tartozó magánkulcs felhasználási körét. Az ilyen korlátozásokról, vagyis arról, hogy mely esetekben nem tekinthető a kiadott tanúsítvány megbízhatónak, a tanúsítványban találhatunk információkat. Az elektronikus aláírást ellenőrző személynek meg kell győződnie arról, hogy a tanúsítványláncolatban nincsen egyetlen olyan tanúsítvány sem, amely - az adott esetben - korlátozná a végfelhasználó elektronikus aláírását.

3.6.2.5 Az elektronikusan aláírt adatok pontos kiválasztása az üzenetből

Az elektronikus aláírás technikai ellenőrzéséhez pontosan kell tudni, mi az az üzenet, adat, amit aláírtak.

3.6.2.6 Az aláíró feltételezett vagy jelzett szándéka szerinti értelmezés meghatározása

Csak olyan elektronikus dokumentumtól várható jogi hatás, amelyen szereplő elektronikus aláírás elfogadásakor jóhiszeműen járt el az érintett fél.

Amennyiben a körülmények további ellenőrzési lépéseket tesznek szükségessé, az érintett fél a tőle elvárható legnagyobb gondossággal köteles ezeket végrehajtani. Az elektronikus aláírás elfogadója a körülmények mérlegelésekor – többek között - köteles figyelembe venni a tanúsítvány osztályát is.

3.6.2.7 Az aláírási jogosultság ellenőrzése

Elképzelhető, hogy az aláírt dokumentumon szereplő elektronikus aláírás minden technikai követelménynek megfelel: az üzenethez tartozik, érvényes, a hitelesítő 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 ellenőrzése az aláírást elfogadó feladata.

3.6.2.8 Az elektronikus aláírás és az aláírt üzenet összetartozásának ellenőrzése

A tanúsítványban szereplő nyilvános kulcs és egy, az érintett fél által megbízhatónak tartott technikai eszköz (hardver, szoftver) segítségével végre kell hajtani azon matematikai műveleteket, melyek során kiderül, hogy az aláírt üzenetrész és elektronikus aláírása összetartoznak-e.

3.6.3 Érvényes elektronikus aláírás következményei

Az elektronikusan aláírt dokumentumok jogi hatással bírhatnak. Ez a jogi hatás a felek – az aláíró, az érintett fél és a hitelesítés szolgáltató – nyilatkozatain és szerződésein alapul, melyeket a felek a következő módon fogadnak el:

I. a hitelesítés szolgáltató részéről az Általános Szolgáltatási Feltételek és Szolgáltatási Szabályzat nyilvánosságra hozatalával,
II. az aláíró a Belépési Nyilatkozat aláírásával, a tanúsítványkérelem benyújtásával ill. a tanúsítvány elfogadásával,
III. az érintett fél részéről pedig az aláírt dokumentum elfogadásával.

Amennyiben a felek a jelen és kapcsolódó szabályzatok, törvényi rendelkezések szerint járnak el az elektronikus aláírások használatakor, akkor az elektronikusan aláírt dokumentummal kapcsolatos jogos érdekeiket bíróság előtt érvényesíthetik.

3.6.4 Eljárás az elektronikus aláírás ellenőrzésekor fellépő hibáknál

Nem érvényes elektronikus aláírás esetén, vagy ha az ellenőrzés nem a szabályzatok pontjainak megfelelően történt, az aláírás nem tekinthető valódinak, és az elfogadásból eredő minden kár és kockázat az érintett felet terheli.

3.7 Tanúsítványok visszavonása

3.7.1 Okok a visszavonásra

A tanúsítványok visszavonásra kerülnek, ha kétely merül fel a szabályzatokban felsorolt feltételek teljesülésével kapcsolatban és a kétely alapja bizonyítható. Visszavonási ok többek között:

- a tanúsítványhoz tartozó magánkulcs biztonságának sérülése;
- hibás vagy megváltozott adatokat tartalmazó tanúsítvány,
- a tanúsítvány alanyának visszavonási kérelme.

A visszavonási kérelmet a regisztrációs egységhez kell eljuttatni, mely a visszavonási jogosultság és az indokok ellenőrzése után visszavonja a tanúsítványt.

A regisztrációs egység legjobb belátása szerint jogosult a visszavonási kérelmet benyújtó személyazonosságát, jogosultságát és a visszavonás indokát vizsgálni. Általános irányelv, hogy a visszavonandó tanúsítvány biztonsági szintjének megfelelő ellenőrzés történjék meg.

3.7.2 Szolgáltató saját tanúsítványának visszavonása

Szélsőséges esetben előfordulhat, hogy magának a Szolgáltatónak a tanúsítványát kell visszavonni. Ez esetben a Szolgáltató tanúsítványa érvényét veszti, azonban ez nem befolyásolja automatikusan a Szolgáltató által a visszavonást megelőzően kiadott tanúsítványok érvényességét.

3.7.3 Visszavonás hibás kibocsátás esetén

A Szolgáltató visszavonja azokat a tanúsítványokat, melyekről kiderül, hogy nem az aktuális szabályzatokban, dokumentumokban leírt eljárási rend alapján vagy egyéb módon hibásan adták ki őket. A Szolgáltató felfüggesztheti a tanúsítvány érvényességét arra az időtartamra, mely alatt a kérdéses tanúsítvány kibocsátásának körülményeit vizsgálja.

3.7.4 Visszavonás az igénylő kérésére

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

3.7.5 A visszavont tanúsítványok listája

A visszavont tanúsítványok azonosítói a *visszavont tanúsítványok listájára* kerülnek. A listát a Szolgáltató rendszeresen frissíti, a legújabb változata Szolgáltató adatbázisából letölthető. A lista a visszavont tanúsítványok *tárgy* és *sorszám* mezőit illetve a visszavonás okának kódját tartalmazza, mindezt a tanúsítványt kiadó és visszavonó hitelesítő egység elektronikus aláírása hitelesíti.

A Szolgáltató - a megfelelő díjazás mellett - biztonságos kommunikációs csatornán keresztül nyújthat információt egyedi tanúsítványok érvényességével kapcsolatban.

3.7.6 A felfüggesztés és visszavonás következménye

A tanúsítvány érvényessége szünetel a felfüggesztés időtartama alatt, illetve a visszavonás pillanatától végérvényesen megszűnik. A Szolgáltató tanúsítványának visszavonásakor a Szolgáltató tanúsítvány aláírási joga is megszűnik, de ez nem érinti automatikusan a visszavonás előtt kibocsátott tanúsítványok érvényességét.

3.7.7 A magánkulcs védelme visszavonás esetén

A magánkulcs védelméről a Felhasználó a tanúsítvány visszavonása után is köteles gondoskodni. A Felhasználónak joga van a visszavont tanúsítványhoz tartozó magánkulcs megsemmisítésére.

3.8 Tanúsítvány lejárata

3.8.1 Előzetes értesítés a tanúsítvány lejártáról

A lejáró tanúsítványokról annak alanya illetve a nevében eljárni jogosult részére 30 nappal a lejárat előtt, elektronikus formában értesítést küld a regisztrációs egység.

3.8.2 Tanúsítvány lejártának következményei

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

3.8.3 Tanúsítványok megújítása

Lejárt tanúsítvány alanya számára a tanúsítvány megújítása kérhető. A kérelemhez csak a megváltozott adatokat kell csatolni, az igényelt tanúsítvány típusának és osztályának megfelelő módon. Az új kérelemhez tartozó Belépési nyilatkozat aláírása után a Szolgáltató új tanúsítványt állít ki az alany új kulcs-párjához.

4 A szolgáltatás díjai

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató Internet honlapján közzéteszi.

5 Felelősségvállalás feltételei, módja, mértéke

Felek felelőssége az Általános Szolgáltatási Feltételekben rögzítettek.

6 Egyéb rendelkezések, intézkedések

6.1 Alkalmazott kriptográfiai algoritmusok

- Szolgáltató jelenleg az RSA (x500 oid: 1.2.840.113549.1.1.1) kriptográfiai algoritmust támogatja.
- Szolgáltató jelenleg az MD5 (x500 oid: 1.2.840.113549.2.5) és az SHA-1 (x500 oid: 1.3.14.3.2.26) lenyomatképző algoritmusokat támogatja.

6.2 Alkalmazott aláíró eszközök

- A osztályban NCA (NetLock Kft. által fejlesztett termék) off-line aláíró eszköz működik,
- B, C és Teszt osztályban CSA (az Eracom Technologies terméke) on-line aláíró eszköz működik.

6.3 Rendelkezésre állás

- A kibocsátott tanúsítványokat és a visszavonási információt tartalmazó tanúsítvány adatbázis rendelkezésre állási mutatója:
  - Munkanapokon 9-17 óráig terjedő időszakokra: 99.5%
  - Ezen kívüli időszakokra: 99.5%
- Szolgáltató a web oldalak esetében nem garantál rendelkezésre állási mutatókat.

6.4 Szabályzatok

Szolgáltató a jelen szabályzatot, általános szolgáltatási feltételeket valamint a tanúsítványok használatára vonatkozó általános tájékoztatóját Internet címén, letölthető módon közzéteszi.

6.4.1 Adatkezelési szabályok

Szolgáltató a regisztráció során kitöltött regisztrációs adatlap adatait elektronikus formában, a jelen szabályzatban meghatározott azonosítási eljárások végrehajtása során fénymásolat formájában birtokába jutott adatokat papír alapon tárolja.

Szolgáltató a birtokába jutott adatokat a személyes adatok kezeléséről szóló törvényi rendelkezésekre figyelemmel kezeli.

Szolgáltató a birtokába került személyes adatokat az adott adat rögzítéséhez kapcsolódó tanúsítvány lejártát, illetve a tanúsítvánnyal összefüggésbe hozható jogi eljárás lezárását követő 5 évig (2001. évi XXXV. Törvény 9.§ 7. bekezdés) őrzi meg.

Szolgáltató a birtokában lévő személyes adatokat harmadik félnek, kizárólag a 2001. évi XXXV. Törvény 11.§ 2., 3. és 4. bekezdésében foglalt esetekben és formában, illetve a Felhasználó kérésre adja át.

6.4.2 Jogi szabályozás

A Szolgáltató a 2001. évi XXXV. elektronikus aláírásról szóló törvény rendelkezéseinek megfelelő tevékenységet folytat.

6.4.3 A szabályzatok módosításai

A mindenkor érvényes Szolgáltatási Szabályzat, valamint az ÁSZF megtalálható a Szolgáltató Internet címén (www.netlock.hu) címen.

Szolgáltató jogosult a felsorolt szabályzatok törvényi előírásokra is figyelemmel történő egyoldalú módosítására. Szolgáltató a módosításokról, azok hatályba lépését megelőző 30 nappal a Hírközlési Főfelügyeletet tájékoztatja, a hatályos szabályzatok változtatásokkal egységes szerkezetbe foglalt verzióját 14 nappal a hatálybalépés előtt közzéteszi.