

# Tanúsítvány létrehozása Nginx szerverhez

---

Kérelem létrehozása Nginx szerveren, tanúsítvány kérelem beadása,  
kiadott tanúsítvány telepítése, tanúsítvány megújítása

## 1. Tartalomjegyzék

1.	Tartalomjegyzék.....	2
2.	Bevezető .....	4
3.	Korlátozások.....	4
4.	Előzetes követelmények – OpenSSL telepítése.....	5
4.1.	OpenSSL telepítés Linux operációs rendszerre .....	5
4.2.	OpenSSL telepítés Windows operációs rendszerre.....	5
4.2.1.	OpenSSL használata Windows alól .....	5
5.	Előzetes követelmények – néhány döntés, amit meg kell hozni .....	6
5.1.	A tanúsítványkiadás algoritmus, a kiadó típusa.....	6
5.2.	Az SSL tanúsítvány profilja.....	6
6.	Tanúsítvány kérelem létrehozása a szerveren.....	8
6.1.	Példa a kulcsgenerálásra és a kérelem létrehozására.....	10
7.	Tanúsítvány kérelem beadása .....	11
8.	Kiadott tanúsítvány telepítése.....	13
8.1.	Példa a konfigurációs állományra.....	13
9.	OCSP Stapling.....	14
9.1.	Mi az OCSP Stapling?.....	14
9.1.1.	Kapcsolat felépülése OCSP Stapling nélkül .....	14
9.1.2.	Kapcsolat felépülése OCSP Stapling segítségével .....	14
9.2.	Előzetes követelmények 1 – A tűzfalakon szükséges engedélyezés.....	15
9.3.	Előzetes követelmények 2 – A gyökértanúsítványok beszerzése .....	15
9.3.1.	SHA 256 kiadók .....	15
9.3.2.	SHA 1 kiadók.....	15
9.3.3.	Összes kiadó .....	16
9.4.	Az NginX 1.3.7 és későbbi szerver verziók beállítása.....	16
9.	Függelék A – Regisztráció ügyfélmenübe.....	17
10.	Függelék B – Belépési nyilatkozat készítése .....	19
10.1.	Teendők a Belépési nyilatkozattal.....	19
11.	Függelék C – Tanúsítvánnyal kapcsolatos ügyintézés.....	20
11.1.	Az ügyfélmenü használata.....	20
11.2.	Bejelentkezés az ügyfélmenübe .....	20

11.3	A tanúsítvány felfüggesztése.....	21
11.4	Felfüggesztéssel kapcsolatos fontos információk.....	22
12.	Függelék D – A tanúsítvány megújítása.....	23
12. 1	Megújított tanúsítványok letöltése .....	23

## 2. Bevezető

---

E tájékoztató célja, hogy a szerveréhez létrehozandó SSL tanúsítvány igénylését minél könnyebben elvégezhesse.

Kérjük, olvassa el figyelmesen és kövesse a leírtakat.

Amennyiben bármilyen kérdése van vagy problémája támad, Ügyfélszolgálatunk a(z) +36 1 437 6655 telefonszámon, az [info@netlock.hu](mailto:info@netlock.hu) e-mail címen vagy személyesen a 1101 Budapest, Expo tér 5-7. szám alatt hétfőtől - csütörtökig 8:30 és 17 óra között pénteken 8:30 és 14 óra között készséggel áll rendelkezésér

## 3. Korlátozások

---

1. A wildcard (\*) jelet tartalmazó tanúsítványok esetén a szabvány szerint a \* jel egy domain név komponensnek kell, hogy megfeleljen.

Ez példánkon keresztül azt jelenti, hogy a \*.valami.hu tanúsítvány megfelel az alma.valami.hu vagy barack.valami.hu domain névhez, de nem megfelelő a jonatan.alma.valami.hu, illetve a valami.hu domain nevekhez.

Az Internet Explorer ezt a szabványt maradéktalanul betartja.

2. **Https** protokoll korlátozás: a **https** protokoll titkosítatlanul csak az IP címet viszi át, ebből következően 1 szerveren, 1 IP cím esetén, csak 1 tanúsítvány kerülhet elhelyezésre. Több site esetén megoldás lehet az UCC tanúsítvány (többszörös CN/SAN), illetve a wildcard tanúsítvány.
3. Az **SNI** korlátozás: az előző probléma feloldására született az SNI technológia, amely azonban csak Windows Vista, Windows 7 és Internet Explorer 7+ esetében érhető el, így haszna megkérdőjelezhető.

#### 4. Előzetes követelmények – OpenSSL telepítése

Az OpenSSL-lel történő generáláshoz szükség lehet az OpenSSL telepítésére.

##### 4.1. OpenSSL telepítés Linux operációs rendszerre

A gépen, ahol a kérelmet létrehozzák, szükség van az OpenSSL csomag telepítésére. Ezt telepítsük a disztribúciós csomag kezelőjével.

##### 4.2. OpenSSL telepítés Windows operációs rendszerre

Az OpenSSL Windowson való futtatásához a következő alkalmazások telepítésére lesz szükség:

- OpenSSL win32 disztribúció

<http://www.slproweb.com/products/Win32OpenSSL.html>

- Microsoft Visual C++ 2008 Redistributable Package

<http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en>

##### 4.2.1. OpenSSL használata Windows alól

Az OpenSSL-t Windows esetén parancsról tudja használni. Ennek elérései:

1. A Start menü> Futtatás mezőbe írja be: cmd
2. Ezután a parancsokat a C:\OpenSSL\bin könyvtárban kell kiadni.

A parancssorban a következő parancsokat kell megadni:

C:

```
cd openssl\bin
```

## 5. Előzetes követelmények – néhány döntés, amit meg kell hozni

A tanúsítvány igénylése előtt érdemes pár dolgot megfontolni, és annak alapján választani majd a kérelem feltöltés során.

### 5.1. A tanúsítványkiadás algoritmus, a kiadó típusa

A kiadás során használt hash algoritmus meghatározza, hogy mely kiadóval kerül majd kiadásra a tanúsítvány, illetve hogy milyen kompatibilitási és egyéb problémák fordulhatnak elő.

- SHA1 kiadóktól származó tanúsítvány
  - SHA1 kiadótól származó SHA1 algoritmust tartalmazó tanúsítvány
    - a legtöbb eszköz, szoftver támogatja
    - támogatása az iparági szabványoktól és egyéb külső szabályozásoktól függően hamarosan megszűnik
- SHA-256 kiadók
  - SHA256 kiadótól származó SHA256 algoritmust tartalmazó tanúsítvány
    - a használatához minimum Windows XP SP3 vagy Vista SP1 szükséges
    - hosszú távon használhatók
    - régebbi telefonos operációs rendszereken az ilyen tanúsítványok támogatás és frissítés hiányában nem használhatók.

### 5.2. Az SSL tanúsítvány profilja

A kiadás során használt tanúsítványprofil határozza meg, hogy mire alkalmas a tanúsítvány.

- Szerver tanúsítvány

Egyszerű, 1 domain nevet tartalmazó tanúsítvány, melynek a CN mezőjében a domain név található. Olyan esetekben javasolt, ahol 1 darab domain nevet kell hitelesíteni.

  - csak egy teljes domain név hitelesítésére alkalmas, így a [www.valami.hu](http://www.valami.hu) címre szóló tanúsítvány csak a [www.valami.hu](http://www.valami.hu) cím eléréséhez jó, a [valami.hu](http://valami.hu) cím eléréshez NEM alkalmas;
  - általában olyan egyszerű struktúrájú weboldalhoz javasolt, amely 1 címen érhető el.
  
- Wildcard tanúsítvány

Olyan tanúsítvány, amely 1 domain nevet tartalmaz úgy, hogy a bal oldali tag helyén „\*” szimbólum található.

- a \*.valami.hu címre szóló tanúsítvány több aldomain hitelesítésére is alkalmas (például: [www.valami.hu](http://www.valami.hu), [mail.valami.hu](mailto:mail.valami.hu), stb.). Mivel a „\*” szimbólumnak kötelezően helyettesítenie kell egy tagot, ezért viszont NEM alkalmas a [valami.hu](http://valami.hu) cím elérésére;
- a „\*” szimbólum a domainben csak a bal oldalon szerepelhet;
- a régebbi telefonok (WM5, WM6, és egyéb régebbi telefonos operációs rendszerek) a Wildcard tanúsítványokat nem támogatják
- ehelyett általában UCC tanúsítvány javasolt, mely tartalmazhat wildcard tagokat is;

- UCC tanúsítvány

Olyan tanúsítvány, amely több domain nevet is tartalmazhat, akár wildcard taggal is kombinálva.

- a több domain név lehetővé teszi, hogy domain nevek széles kombinációját használhassuk egy szerveren;
- például egy [valami.hu](http://valami.hu) és [\\*.valami.hu](http://*.valami.hu) neveket tartalmazó tanúsítvány lehetővé teszi, hogy oldalunkat elérjük a [valami.hu](http://valami.hu), valamint a [www.valami.hu](http://www.valami.hu), [web.valami.hu](http://web.valami.hu), [mail.valami.hu](mailto:mail.valami.hu) címeken;
- például egy [valami.hu](http://valami.hu), [\\*.valami.hu](http://*.valami.hu), [valami.eu](http://valami.eu), [\\*.valami.eu](http://*.valami.eu) neveket tartalmazó tanúsítvány lehetővé teszi, hogy oldalunkat elérjük a .hu és .eu tartományon keresztül az előző példának megfelelő variációkban is;
- például egy [valami.hu](http://valami.hu) és [akarmi.hu](http://akarmi.hu) neveket tartalmazó tanúsítvány lehetővé teszi, hogy oldalunkat egyaránt elérjük a [valami.hu](http://valami.hu) vagy az [akarmi.hu](http://akarmi.hu) néven is;
- A fenti példák kombinációján több különböző domain név, több TLD (pl.: .hu, .eu) vagy al- és fődomain egyidejű használata esetén javasolt.

## 6. Tanúsítvány kérelem létrehozása a szerveren

---

A kérelem létrehozásának lépései a következők:

1. Indítson parancssort (Windows), vagy terminál ablakot (Linux), majd adja ki következő parancsot:

```
openssl req -newkey -utf8 rsa:2048 -keyout domainnev.key -out domainnev.csr
```

Ha **NEM AKARJA JELSZÓVAL** védeni a kulcsot, akkor a következő parancsot adja ki: (automatikusan induló szerverekhez jól jöhet, azonban biztonsági problémát okozhat.)

```
openssl req -newkey -utf8 rsa:2048 -nodes -keyout domainnev.key -out domainnev.csr
```

2. Ez a parancs létrehoz két fájlt, az egyik a privát kulcs (.key), a másik a tanúsítvány kérelem (.csr), amit a tanúsítvány kiállításához fog tudni használni.
3. Miután elindította a parancsot, a tanúsítvány kérelem számára ki kell töltenie néhány adatot.

### Fontos!

**A kitöltésnél semmiképp ne töltsse ki az esetleg felajánlott e-mail mezőt, mert az SSL tanúsítványban e-mail cím nem szerepelhet.**

Ha valamit az openssl kitöltve ajánl fel (szögletes zárójel közötti rész), akkor azt Enter gombbal elfogadhatjuk. Pont megadásával a mező alapértelmezett tartalma törlésre kerül.

**UCC kérelem esetén érdemes lehet e-mailen is jelezni a NetLock Kft. felé a kérelemben foglalt további domain neveket, hogy szükség esetén ellenőrizhessük és a tanúsítványba foglalhassuk azokat.**



A tanúsítvány kérelem kitöltendő mezői:

Common name (CN)	A domain név teljes formája (https:// nélkül) Pl.: www.akarmi.hu, mail.akarmi.hu
Country code (C)	Országkód: nagybetűvel Magyarország kódja, vagyis: HU
Locality (L)	Város: a cégkivonat szerinti székhely vagy telephely városa. Magánszemély tanúsítványa esetén a lakcím szerinti város.
State (ST)	Megye: kitöltése opcionális. Javasolt üresen hagyni, azonban ha mégis kitöltjük, ügyeljünk arra, hogy a megyei jogú városok és a fővárosok külön megyének számítanak.
Organization (O)	Szervezet: a cégkivonatban szereplő név, amely lehet rövid név, hosszú név, angol név közül bármelyik. Fontos, hogy az itt megadott név szerepeljen a cégkivonatban.
Organization Unit (OU)	Szervezeti egység: kitöltése opcionális, azonban csak szervezeti egységek nevei szerepelhetnek itt. Ami nem szervezeti egység neve, az nem elfogadható.

Az Email cím ne legyen kitöltve, az extra attribútumok kitöltése pedig felesleges.

A létrejövő fájlok közül a kulcsot (.key) tegye majd az Nginx megfelelő könyvtárába, a létrejövő kérelmet (.csr) pedig majd a Netlock rendszerbe kell feltöltenie.

### 6.1. Példa a kulcsgenerálásra és a kérelem létrehozására

Jelszavas kulcsgenerálás és kérelem létrehozás adatmegadást megelőző lépései  
(kétszer kell megadni a jelszót, amit meg kell jegyeznünk)

```
C:\>openssl req -utf8 -newkey rsa:2048 -keyout domainnev.key -out domainnev.csr
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'domainnev.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Jelszó nélküli teljes kulcsgenerálás

```
C:\>openssl req -utf8 -newkey rsa:2048 -nodes -keyout domainnev.key -out domainnev.csr
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'domainnev.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:HU
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:Budapest
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Maci Laci Bt.
Organizational Unit Name (eg, section) []:Kereskedelem
Common Name (eg, YOUR name) []:mezesbodon.hu
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\>
```

## 7. Tanúsítvány kérelem beadása

Az imént létrehozott kérelem beadásának lépései a következők:

1. Ha már volt regisztrálva felhasználóként az oldalunkon, akkor látogasson el a [www.netlock.hu](http://www.netlock.hu) oldalra, és kattintson a „Ügyfélmenü – Bejelentkezés Fokozott biztonságú rendszer” menüpontra. Ha még nincs regisztrálva, akkor a függelékben találhatóak alapján regisztráljon.
2. A rendszerbe bejelentkezve válassza az Új szerver regisztrációja gombot. A megjelenő ablakban töltsé ki az adatokat az alábbi következő táblázatnak megfelelően.

Szerver elnevezése:	<input type="text"/>	*
Országkód:	<input type="text" value="HU"/>	<input type="text" value="Hungary (Magyarország)"/>
Város:	<input type="text"/>	*
URL:	<input type="text"/>	*

(\*) - kötelezően kitöltendő mezők

Szerver elnevezése	Szerver elnevezése: valamilyen beszédes név
Országkód	A személy vagy szervezet igazolt székhelye/lakhelye alapján (cégkivonat, lakcímkártya). Cég számára beszerzendő tanúsítvány esetén a szervezeti adatok, magánszemély által beszerzendő tanúsítvány esetén a személy adatai alapján.
Város	
URL	A szerver URL https nélkül: meg kell egyeznie a későbbi tanúsítvány kérelemben lévő URL-lel.

3. Ezután válassza az Új kérelem beadása menüpontot, majd válassza ki a korábban meghozott döntés alapján, hogy SHA1 vagy SHA256 kiadót szeretne.  
Az SHA1 kiadók alatt, a Webszerver tanúsítványok szekcióban válassza a Webszerver (SSL) menüpontot.  
Az SHA256 kiadók esetén a Szerver tanúsítványok szekcióban válassza a Szerver, Wildcard, UCC opciók valamelyikét.
4. A megfelelő opció kiválasztása után a lap alján válassza ki „PEM formátumú PKCS10 tanúsítvány kérelem feltöltése” opciót, majd nyomja meg a Tanúsítvány kérelem gombot.

5. Az imént regisztrált szerver meg kell jelenjen a kapott találati listában. Azt válassza ki, majd a megjelenő ablak szövegdobozába a vágólapon keresztül másolja be a kérelem generálás során létrejött fájl tartalmát, majd nyomja meg a Tovább gombot.

Kérjük, másolja be a szerveren elkészített tanúsítványkérelmet az lenti üres ablakba!

A kérelem kész:

- a Név (Cím)
- a Város (Lok
- a Megye (St
- kitölteni)
- a Szervezet (
- a Szervezeti
- Regisztráció st
- ne szerepelje:
- fontos, hogy:
- "-----BEGIN C
- "-----END CER

A kérelem elké  
(http://www.ne

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDODCCAQEQAwwXTEQMA4GA1UEAxxMHRdMjY2ZTQ1ELMAkGALUECMAQCCQw
BgNVBAQTCFR1c2p0Y2V7MREwDwYDVQQHEwFkdWRhcgVzdEJMAkGALUECMAQCCQw
G9EVNlUkZ5d0yUjppPKkBC0SSSHH16wQDEKTAENLgqTf6/Gr5JQA5k1qz1P0PW
Q9Z1FVX39wCGwQGTy9qCN3vAR61KAXdPMOCT6AxP7DASV3LSCHL87cWdB18p
SVYX/KChgfrCQsTjUAFxnSamAeAV09cAwEAAACCAZkwgYKkwyBBAGCNW0CAZEM
Fg01LjEuMjYwMC4yMHsGC1sGAQQBglcCAQ4xbTRMA4GA1UdDwEB/wQEAwIE8DBE
BgkqhkiG9w0BCQ8ENZA1MA4GCCGSIb3DQMCAGIAGDA0BgqhkiG9w0DBAICAIAw
BwYFKw4DAgcwCgYIKoZIhvcNAQcwEwDVR0TBAAwCgYIKwYBBQUHAWEwF0GC1sG
AQQBglcCAQ4xge4wgesCAQEwBgBNAGkAYwByAG8AcwBwAGYAdAAgAFIAUwBBACAA
UwEDAG8AYQBAG4AZQBSACAAQwByAHkACAB0AG8AZwByAGEAcAB0AGkAYwAgAF
cgBvAHYAaQBKAGUacgOB1QCtSR8dK5v10wRXJreaBSjJpgw7jnoQI1mvgJv5
7F+H47mzA4bWgNSNorJyuRzmkb4g8FCer7hy1lPyFY1DC1z6ozvzFQR0nEK1S
3ntv28Ver/12weSa05PCRKpKfP3Ku5WjFh4NDyMjcbcdODHAw2jyhmeb4T5j11y
FOAAAAAAAAAAMA0GCsGSIb3DQEBBQUAA4GBA15XKtW+865u5vXEm7bpGQsc
w+h8IK7ba2Dwctd1fHudgJaw5NOUC9Hq9/WdRynEOKLmQbVIK7ZozY41OfsQk/e
Wn52vZBNnN0iu1Cxe72SbuOr0JYx1OmvLu1c1xwVBe4/bkoyV5nmALR/NNvesr3s
Nsyph/e2eLkV1AYN
-----END NEW CERTIFICATE REQUEST-----
    
```

6. A következő ablakban válassza ki a használni kívánt tanúsítványkiadót, és a felhasználás célját, majd nyomjon a „Kérelem beadása” gombra.

Típus:	szerver
Név:	***.***
Országkód:	US
Város:	Budapest
Szervezet:	Tesztceg
Szervezeti egység:	IT
Beadva:	0.00.00
Promóciós kód:	<input type="text"/>
Tanúsítványkiadó:	NetLock Expressz (Class C) Tanúsítványkiadó
Felhasználás:	Általános hitelesítésszolgáltatás

**Kérelem beadása**

7. Az ezután következő lépés a Fizetési feltételek kiválasztása (szükség esetén a sürgösség megjelölése) és a Belépési nyilatkozat létrehozása lesz, majd a szükséges iratokat a tanúsítvány osztályának megfelelő módon el kell juttatni a Netlock Kft. részére (ezekről részletesebben a függelékben olvashat).

## 8. Kiadott tanúsítvány telepítése

---

A tanúsítvány kiadása után értesítő levelet kap arról, hogy a tanúsítványa elkészült és letölthető. Ezt töltsse le, majd másolja fel szerverére, egyesítse a kiadott tanúsítvánnyal, majd konfigurálja be a szervert. (Az egyesítésről a konfigurációnál olvashat.)

SHA256 kiadók és az onlinesl.netlock.hu oldalról igényelt tanúsítvány esetében ezen kívül szükséges letölteni a köztes kiadót, hogy be tudja állítani azt.

Ehhez az alábbi címekről le kell töltenie a kiadói tanúsítványok egyikét:

Közjegyzői	(SHA256)	<a href="http://www.netlock.hu/index.cgi?ca=caca">www.netlock.hu/index.cgi?ca=caca</a>
Üzleti	(SHA256)	<a href="http://www.netlock.hu/index.cgi?ca=cbca">www.netlock.hu/index.cgi?ca=cbca</a>
Expressz	(SHA256)	<a href="http://www.netlock.hu/index.cgi?ca=ccca">www.netlock.hu/index.cgi?ca=ccca</a>
OnlineSSL	(SHA256)	<a href="http://www.netlock.hu/index.cgi?ca=olsslgca">www.netlock.hu/index.cgi?ca=olsslgca</a>

### 8.1. Példa a konfigurációs állományra

---

A következő példa egy konfigurációs állomány, mely egy SSL kapcsolattal működő szerver konfigurálását mutatja be:

```
server {
    listen          443 ssl;
    server_name     www.vargaviktor.hu;
    ssl_certificate  www.vargaviktor.hu.chained.crt;
    ssl_certificate_key www.vargaviktor.hu.key;
    ssl_protocols   SSLv3 TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers     RC4:HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers on;
}
```

A fentiekben az SSL\_CIPHERS és SSL\_PREFER\_SERVER\_CIPHERS opcióktól eltérhet a konfigurációban, ez a BEAST támadás elkerülése végett lett a konfigurációban így beállítva.

Az SSL\_CERTIFICATE\_KEY opcióban a tanúsítvány kulcsát tartalmazó fájlt kell megadni, a kulcs BASE64 PEM formátumú kell legyen.

Az SSL\_CERTIFICATE opcióban a tanúsítványt és láncát kell megadnunk. A tanúsítványok BASE64 formában egymás után kell szerepeljenek a fájlban, először a szerver tanúsítványa (ami kiadásra került) és utána a köztes kiadó, amit az előző fejezet alapján töltött le.

## 9. OCSP Stapling

---

### 9.1. Mi az OCSP Stapling?

---

Az OCSP Stapling előnye a Stapling nélküli és a Stapling használatával történő működés bemutatásának különbségein keresztül érzékelhető.

#### 9.1.1. Kapcsolat felépülése OCSP Stapling nélkül

---

A visszavonás ellenőrzés OCSP segítségével hagyományos esetben a következőképpen történik:

1. A kliens böngészője felveszi a kapcsolatot a webszerverrel.
2. A kliens böngészője a megkapott tanúsítványt lekérdezi a tanúsítványkiadó szerverétől, OCSP vagy CRL esetében.
3. Létrejön a kapcsolat.

Mint látható, minden kliens maga kommunikál a tanúsítványkiadóval, ami magas terhelés esetén a felhasználó számára hosszú válaszidőket eredményezhet a kliens oldalon.

#### 9.1.2. Kapcsolat felépülése OCSP Stapling segítségével

---

Az OCSP Stapling kihasználja azt, hogy a kapcsolat kiépülésekor a már kiépített kapcsolaton keresztül akár a visszavonási információk lekérését is el lehet küldeni a kliens számára.

A visszavonás ellenőrzés OCSP segítségével - hagyományos esetben - a következőképpen történik:

Előkészítő lépés: a webszerver időnként letölti a tanúsítványához tartozó OCSP válaszokat, majd meghatározott időnként frissíti azt.

1. A kliens böngészője felveszi a kapcsolatot a webszerverrel
2. A webszerver elküldi az OCSP választ a kliens részére
3. Létrejön a kapcsolat.

Mint látható, a szerver gyakorlatilag „előre betárazza” az OCSP a választ, így a kapcsolat kiépülésének sebessége nem függ külső szervertől, ezért az OCSP Stapling beállítása különösen ajánlott!

## 9.2. Előzetes követelmények 1 – A tűzfalakon szükséges engedélyezés

Ahhoz, hogy az OCSP Stapling használható legyen, a szervezet tűzfalain a szerver számára engedélyezni kell a következő címek elérését.

<http://www.netlock.hu>

<http://ocsp1.netlock.hu>

<http://ocsp2.netlock.hu>

<http://ocsp3.netlock.hu>

Javasolt a fenti esetek DNS alapú beállítása, mert a szolgáltatások felhőbe költözése esetén az IP címek változhatnak.

## 9.3. Előzetes követelmények 2 – A gyökértanúsítványok beszerzése

Ahhoz, hogy az OCSP Stapling működjön, egyes szervereken szükséges a gyökértanúsítványok és köztes tanúsítványok szerver számára elfogadható módon történő telepítése.

A tanúsítványok kiadója alapján szükséges a következők tanúsítványok letöltése. Mivel egyes böngészők ezt automatikusan megnyitják, a tanúsítvány letöltéséhez célszerű Internet Explorer-t használni.

Az egyes kiadók elérése a következő alfejezetben olvasható.

### 9.3.1. SHA 256 kiadók

Az SHA256 algoritmusú kiadók a következő URL-eken érhetőek el.

#### **Legfelső szintű kiadó:**

Arany (SHA256) [www.netlock.hu/index.cgi?ca=gold](http://www.netlock.hu/index.cgi?ca=gold)

#### **Köztes szintű kiadó:**

Közjegyzői (SHA256) [www.netlock.hu/index.cgi?ca=caca](http://www.netlock.hu/index.cgi?ca=caca)

Üzleti (SHA256) [www.netlock.hu/index.cgi?ca=cbca](http://www.netlock.hu/index.cgi?ca=cbca)

Expressz (SHA256) [www.netlock.hu/index.cgi?ca=cca](http://www.netlock.hu/index.cgi?ca=cca)

OnlineSSL (SHA256) [www.netlock.hu/index.cgi?ca=olsslga](http://www.netlock.hu/index.cgi?ca=olsslga)

### 9.3.2. SHA 1 kiadók

Az SHA1 algoritmusú kiadók a következő URL-eken érhetőek el.

#### **Legfelső szintű kiadók:**

Közjegyzői (SHA1) <https://www.netlock.hu/index.cgi?ca=kozjegyzoi>

### 9.3.3. Összes kiadó

Természetesen használható egy előre összeállított csomag is erre a célra, amely a következő címen érhető el (javasolt a `netlock_osszes_ssl_kiado.pem` fájl használata a csomagból):  
[http://www.netlock.hu/docs/letoltes/ssl\\_kiadok\\_csomag.zip](http://www.netlock.hu/docs/letoltes/ssl_kiadok_csomag.zip)

### 9.4. Az NginX 1.3.7 és későbbi szerver verziók beállítása

Az Nginx 1.3.7 vagy későbbi verziójú webservert esetén a konfigurációs állományban a következőket kell megadni az OCSP Stapling bekapcsolásához:

```
## OCSP Stapling
resolver 127.0.0.1;
ssl_stapling on;
ssl_stapling_verify on;
ssl_trusted_certificate <file>;
```

- A Resolver értéke a DNS szerver értéke legyen, nem a példában szereplő 127.0.0.1, azaz localhost. Ha a gép tud DNS nevet feloldani, akkor megfelelő lehet a fenti példa is.
- Az SSL Stapling működéséhez és az ellenőrzéshez szükséges, hogy a szerverre a gyökér és köztes tanúsítványok telepítve legyenek.
- Az `ssl_trusted_certificate` esetén a fájl neve arra a fájlra kell, hogy mutasson, amely a gyökér- és köztes tanúsítványokat tartalmazza.

A tanúsítványok sorrendje: köztes kiadó, gyökérkiadó.



## 9. Függelék A – Regisztráció ügyfélmenübe

Ahhoz, hogy a felhasználó hozzáférhessen ügyfélmenüjéhez, előzetesen regisztrálnia kell.

A felhasználó regisztrációjának lépései a következők

1. Látogasson el a [www.netlock.hu](http://www.netlock.hu) oldalra, és ott válassza a „Fokozott biztonságú tanúsítvány igénylése” menüpontot, majd a megjelenő oldalon válassza a Regisztráció menüpontot.
2. A megjelenő adatlapon töltsse ki személyes adatait az igazolványainak (személyi igazolvány, lakcímkártya) megfelelő adatokkal (ahol ez értelmezhető).

Név:	<input type="text"/>	*
Országkód:	<input type="text" value="HU"/>	<input type="text" value="Hungary (Magyarország)"/>
Város:	<input type="text"/>	*
Utca, házszám:	<input type="text"/>	
Irányítószám:	<input type="text"/>	
Telefon/Fax:	<input type="text"/>	
Email:	<input type="text"/>	*
Bejelentkező név:	<input type="text"/>	*
Jelszó:	<input type="text"/>	*
Jelszó ismét:	<input type="text"/>	*

Kérjük azonosítás céljából adjon meg egy kérdést és erre a kérdésre a választ. Ezt a kérdést későbbiekben vevőszolgálatunk azonosítás céljából megkérdezheti Öntől és Önnek erre a kérdésre az itt megadott választ kell válaszolnia. (például: Kérdés: Melyik nap születtem?, Válasz: Kedden.)

Kérdés:	<input type="text"/>
Válasz:	<input type="text"/>

Kérjük adjon meg egy olyan szöveget, mely Önt emlékezteti új jelszavára. Ezt a szöveget elektronikus levélcímre fogjuk továbbítani, ha Ön elfelejti jelszavát. Kérjük biztonság érdekében ez a szöveg különbözzön a jelszótól.

Jelszó emlékeztető:	<input type="text"/>
---------------------	----------------------

Személyes adataim láthatóak más felhasználók számára is

A kitöltendő adatok a következők:

Név	Az érvényes személyes adatok az igazolványok alapján.
Országkód	
Város	
Utca, házsám	
Irányítószám	
Telefon/Fax	Telefonszám, ahol elérhető
Email	Email cím, ahol elérhető. Javasolt a majdan tanúsítványba kerülő mail címet megadnia.
Bejelentkező név	Választott bejelentkező név
Jelszó	Választott jelszó
Jelszó ismét	Választott jelszó még egyszer
Kérdés	Telefonos azonosítás során a Netlock által feltett kérdés, amire csak a felhasználó tudja a választ
Válasz	Válasz a fenti kérdésre
Jelszó emlékeztető	Olyan emlékeztető szöveg, melyet kérésre az automata rendszer elküld, így az elfelejtett jelszó esetleg beugorhat.
Személyes adataim láthatóak más felhasználók számára is	Ha megjelöli, a többi regisztrált láthatja személyes adatait.

Ezután a „Regisztráció” gombot megnyomva a regisztráció megtörténik.

## 10. Függelék B – Belépési nyilatkozat készítése

A menüpont segítségével a kérelemhez legenerálható a belépési nyilatkozat.

A megjelenő mezőket a vonatkozó iratok alapján ki kell tölteni, majd a „Belépési nyilatkozatának elkészítése” gombra nyomni, ami legenerálja azt. Ezt már csak kinyomtatnia, aláírnia és a Netlock részére megfelelő módon elküldenie kell.

Az adatokat mindig újra be kell itt gépelni, még ha korábban meg is adta, mert a rendszer személyiségvédelmi okokból ezeket nem tárolja!

### 10.1 Teendők a Belépési nyilatkozattal

A Belépési nyilatkozatnak kiemelt szerepe van az igénylés vagy megújítás során, mivel elengedhetetlen dokumentum a tanúsítvány tulajdonosának azonosításához! A kinyomtatott Belépési nyilatkozatot a tanúsítvány osztályának megfelelően a következőképpen kell kezelni.

#### **Fokozott biztonságú „C” osztályú tanúsítvány esetén:**

Küldje el aláírva a NetLock Kft.-hez faxon az +36 1 700 2828-as számra vagy e-mailben szkennelve a [kerelmek@netlock.hu](mailto:kerelmek@netlock.hu) címre.

#### **Fokozott biztonságú „B” osztályú tanúsítvány esetén:**

A tanúsítvány tulajdonosa személyesen írja alá a NetLock regisztrációs munkatársa előtt a 1101 Budapest, Expo tér 5-7. szám alatt, ügyfélfogadási időben: hétfőtől péntekig 9 és 17 óra között. Amennyiben erre nincs lehetősége, közjegyző előtt is aláírhatja azt, majd az eredeti hitelesített példányt kérjük a fenti címre megküldeni.

#### **Fokozott biztonságú „A” osztályú tanúsítvány esetén:**

A Belépési nyilatkozatot ebben az esetben közjegyző előtt kell aláírni egy aláírás hitelesítés keretében. A hitelesített példányt eredetiben küldje el a NetLock címére (1101 Budapest, Expo tér 5-7.).

## 11. Függelék C – Tanúsítvánnyal kapcsolatos ügyintézés

### Figyelem!

Az ebben a fejezetben leírtakra csak akkor van szüksége, ha tanúsítványát megújítja, vagy valamilyen okból a felfüggesztése, visszavonása mellett dönt.

#### 11.1 Az ügyfélmenü használata

Tanúsítvány kérelmeinek létrehozása és beadása során ügyfélmenü jött létre az Ön számára a NetLock Kft. honlapján. Itt tekintheti meg a saját és mások tanúsítványait, innen intézheti a tanúsítványokkal kapcsolatos ügyeit.

#### 11.2 Bejelentkezés az ügyfélmenübe

Az ügyfélmenübe bejelentkezni a [www.netlock.hu](http://www.netlock.hu) oldalon lehet.

A bejelentkező név és jelszó megadása után kattintson

**Minősített tanúsítvány** esetén (QA osztály) a „Bejelentkezés a minősített rendszerbe” linkre.

**Fokozott tanúsítvány** esetén (A, B, és C osztály) a „Bejelentkezés a fokozott biztonságú rendszerbe” linkre.

A bejelentkező név és jelszó megadása után az alábbi képernyő jelenik meg. A bal oldalon és középen is megtalálható menüpontok közül választhat.



### 11.3 A tanúsítvány felfüggesztése

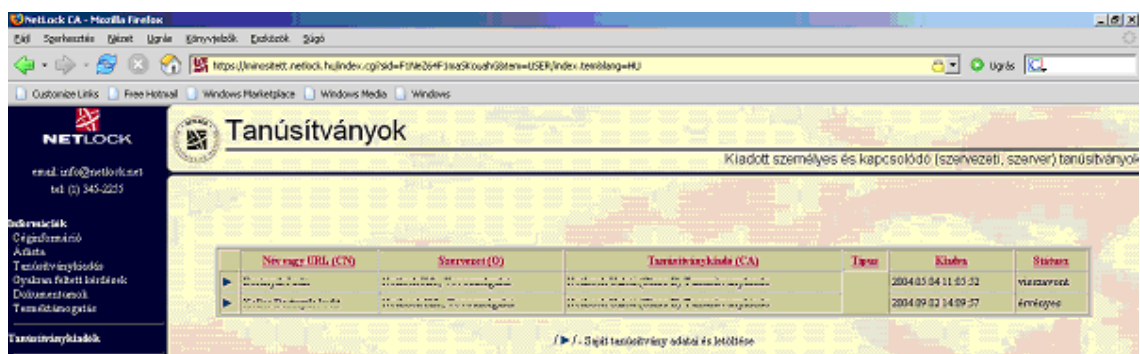
Elektronikus tanúsítványait - akár csak bankkártyáját - gondosan kell kezelnie és őriznie, hiszen a tanúsítványával az Ön nevében végezhetnek elektronikus aláírást és ez által az Ön nevében tehetnek joghatással bíró nyilatkozatot.

Ha úgy gondolja, hogy a tanúsítványához illetéktelenek hozzáférhettek, a tanúsítványt fel kell függesztetnie.

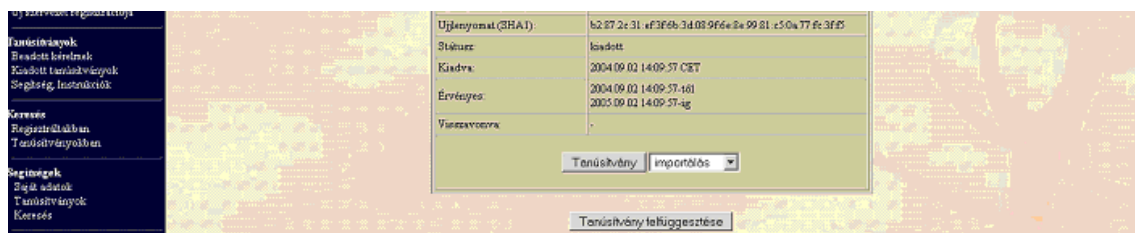
Ha nem tud minden kétséget kizáróan meggyőződni arról, hogy időközben a magánkulcsot nem használta illetéktelen személy, intézkedjen a tanúsítvány végleges visszavonásáról. A felfüggesztési, visszavonási lépéseket a NetLock Kft. Szolgáltatási Szabályzatában szereplő módon (Internetes ügyfélmenün keresztül, e-mailben, telefonon) teheti meg.

#### A.) Interneten keresztül a következő módon függesztheti fel tanúsítványát:

1. Jelentkezzen be az ügyfélmenüjébe és válassza ki a bal oldali menüsorban a **Kiadott tanúsítványok** menüpontot.
2. A megjelenő ablakban láthatja a tanúsítványai adatait. Kattintson a megfelelő tanúsítvány előtti háromszögre.



3. Ekkor megjelennek a kiválasztott tanúsítvány részletei. Az alul található Tanúsítvány felfüggesztése gombbal kezdeményezheti a tanúsítvány felfüggesztését.



B.) E-mail-ben munkaidőben (9:00–17:00) az [info@netlock.hu](mailto:info@netlock.hu) e-mail címen jelezhet.

C.) Telefonon 0 – 24 órában a (40) 22-55-22 telefonszámon jelezhet.

#### 11.4 Felfüggesztéssel kapcsolatos fontos információk

A felfüggesztett tanúsítvány legkésőbb 6 órán belül jelenik meg a tanúsítvány-visszavonási listán, és a felfüggesztés ténye ekkor válik közismertté az Interneten.

**Ha tanúsítványát felfüggesztette és 5 naptári napon keresztül nem történik semmilyen intézkedés, akkor a tanúsítvány véglegesen visszavonásra kerül és azt többet használni már nem lehet.**

## 12. Függelék D – A tanúsítvány megújítása

Az Ön által használt tanúsítvány lejártáról e-mail értesítést küldünk a tanúsítványban megadott e-mail címére a következő megjelöléssel: „Értesítés lejártó tanúsítványról”.

Tanúsítványa csak egy alkalommal újítható meg. Amennyiben ez már egyszer megtörtént, új tanúsítvány igényt kell benyújtania.

Megújítás esetén kérjük, kövesse az alábbi lépéseket:

1. Jelentkezzen be ügyfélmenüjébe
2. A kiadott tanúsítványok közül válassza ki a rövidesen lejártó, de **még érvényes** tanúsítványát. Kattintson a sor elején található háromszögre. Ekkor a megjelenő ablakban láthatja a tanúsítványának adatait.
3. Kattintson a lap alján található Tanúsítvány megújítása gombra.
4. Ezt követően meg kell adni a fizetési módot, majd el kell készíteni a Belépési nyilatkozatot, melyet a tanúsítvány típusa szerint kell benyújtania a meghosszabbításhoz.
5. A dokumentáció beérkezését követően kezdjük meg a megújítási kérelem feldolgozását!
6. A tanúsítvány kiadását követően a tanúsítványban megadott e-mail címre értesítést küldünk. A tanúsítványt ezt követően letölthető az ügyfélmenüből.
7. A kiadott tanúsítványt le kell tölteni a gépére.

### 12.1 Megújított tanúsítványok letöltése

Amennyiben tanúsítványait megújította, és a tanúsítvány kiadásra került, az új tanúsítványokat cserélni kell a szerveren.

A megújított tanúsítvány kiadásáról e-mail értesítést fog kapni.

A kiadott tanúsítványt a gépre fel kell másolni és az ott megtalálható tanúsítvány állományt egyszerűen le kell cserélni. Szükség esetén a korábbi tanúsítvány esetében végzett előkészítő műveletet (lánc összemásolása a tanúsítvánnyal) is el kell végezni.

Szükség lehet a webszerver újraindítására.