Tanúsítvány létrehozása Apache szerverhez

Kérelem létrehozása Apache és Tomcat szerveren, tanúsítvány kérelem beadása, kiadott tanúsítvány telepítése, tanúsítvány megújítása

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

1. Tartalomjegyzék

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 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 egy szerveren, egy IP cím esetén, csak egy 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 és Internet Explorer 7+ esetében érhető el, így hasznossága 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

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 algoritmusa, 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 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, egy 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 címre szóló tanúsítvány csak a www.valami.hu cím eléréséhez jó, a valami.hu cím eléréshez NEM alkalmas;
- általában olyan weboldalhoz javasolt, amely egy címen érhető el.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

- Wildcard tanúsítvány

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

  - a *.valami.hu címre szóló tanúsítvány több aldomain hitelesítésére is alkalmas (például: www.valami.hu, mail.valami.hu, stb.). Mivel a „*” kötelezően helyettesít egy tagot, ezért viszont NEM alkalmas a 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 az 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 és *.valami.hu neveket tartalmazó tanúsítvány lehetővé teszi, hogy oldalunkat elérjük a valami.hu, valamint a www.valami.hu, web.valami.hu, mail.valami.hu címeken;
  - például egy valami.hu, *.valami.hu, valami.eu, *.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 és akarmi.hu neveket tartalmazó tanúsítvány lehetővé teszi, hogy oldalunkat egyaránt elérjük a valami.hu vagy az akarmi.hu néven is;
  - A fenti példák kombinációi alapján több különböző domain név, több TLD (pl.: .hu, .eu) vagy al- és fődomain egyidejű használata esetén javasolt.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 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 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 kiállításhoz fog tudni használni.
3. Miután elindította a parancsot, a tanúsítvány kérelem számára ki kell töltenie néhány adatot.

   Fontos!

   A kitöltésnél ne használjon ékezetes betűket, valamint semmiképp ne töltse 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.

SHA1 algoritmusú UCC igénylés esetén a kérelem beadását követően jelezze felénk, hogy mely kérelem esetén milyen domain neveket szeretne még a tanúsítványban látni. Ezt a domain név megadásával teheti meg emailben.

SHA256 algoritmusú UCC igénylés esetén a SAN mező elemeit a CSR kérelem file-ba tudja belefoglalni.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 Apache megfelelő könyvtárába, a létrejövő kérelmet (.csr) pedig majd a Netlock rendszerbe kell feltöltenie.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 -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

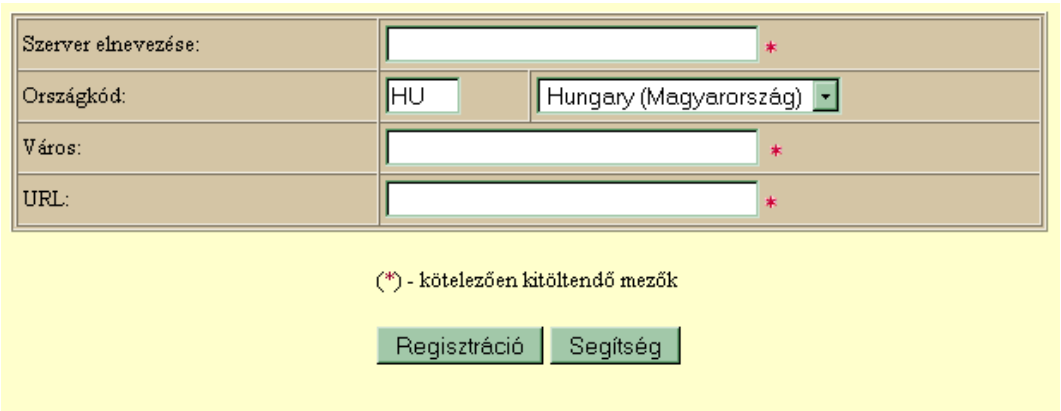
```
C:\>openssl req -newkey rsa:2048 -nodes -keyout domainnev.key -out domainnev.csr

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:\>_
```


NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 oldalra, és kattintson a „Ügyfélmenü – Bejelentkezés Fokozott biztonságú rendszer" menüpontra. Ha még nincs regisztrálva, a függelékben találhatóak alapján regisztráljon.
2. A rendszerbe bejelentkezve válassza az Új szerver regisztrációja gombot. A megjelenő ablakban töltse ki az adatokat az alábbi következő táblázatnak megfelelően.



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.

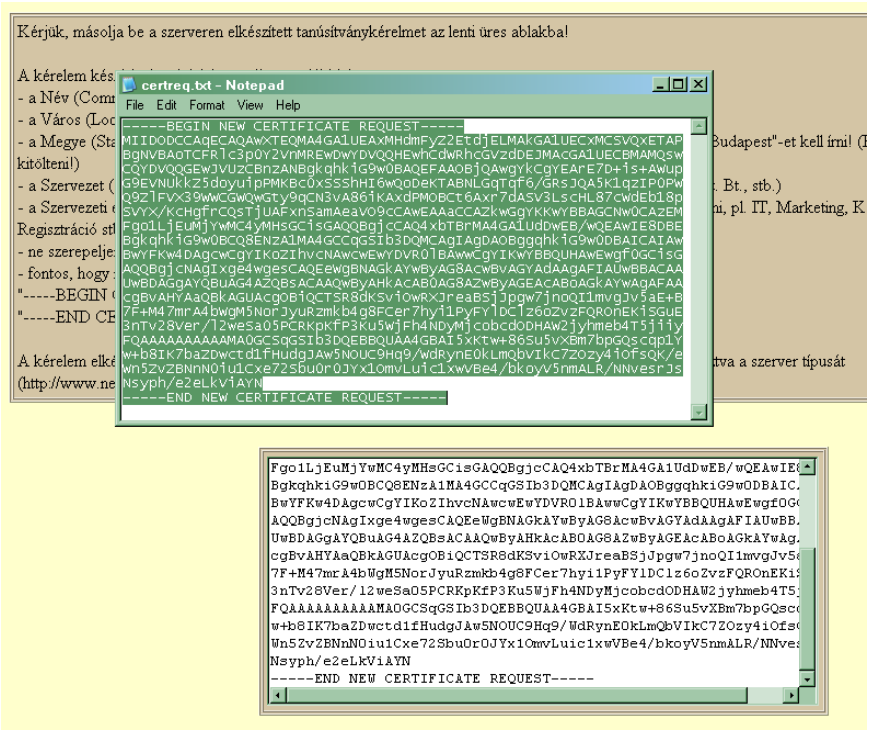
3. Ezután válassza az Új kérelem beadása menüpontot, majd válassza ki a korábban meghozott döntés alapján, hogy SHA1 vagy SHA256 kiadót szeretne.

   Az SHA1 kiadók alatt, a Webszerver tanúsítványok szekcióban válassza a Web szerver (SSL) menüpontot.

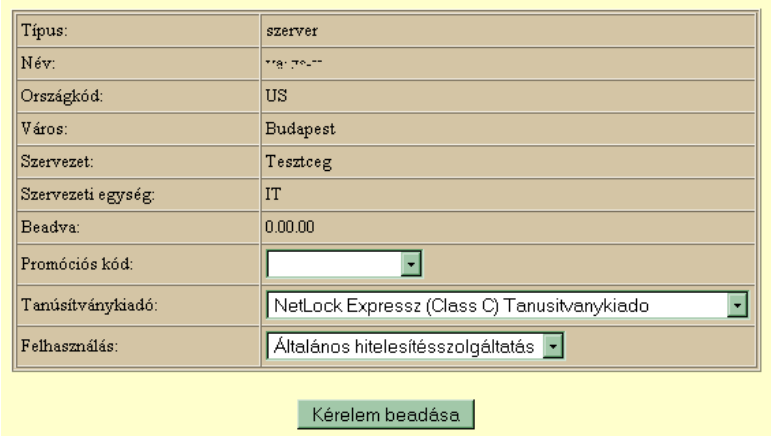
   Az SHA256 kiadók esetén a Szerver tanúsítványok szekcióban válassza a Szerver, Wildcard, UCC opciók valamelyikét.
4. A megfelelő opció kiválasztása után a lap alján válassza ki „PEM formátumú PKCS10 tanúsítvány kérelem feltöltése" opciót, majd nyomja meg a Tanúsítvány kérelem gombot.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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.



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



7. Az ezután következő lépés a Fizetési feltételek kiválasztása (szükség esetén a sürgősség 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).

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

8. Kiadott tanúsítvány telepítése

A tanúsítvány kiadása után értesítő levelet kap arról, hogy a tanúsítványa elkészült és letölthető. Ezt töltse le, majd másolja fel szerverére, az Apache megfelelő könyvtárába, majd konfigurálja be a szervert.

SHA256 kiadók és az onlinessl.netlock.hu oldalról igényelt tanúsítvány esetében ezen kívül szükséges beállítani az SSLCertificateChainFile opciót is.

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

Közjegyzői	(SHA256)	www.netlock.hu/index.cgi?ca=caca
Üzleti	(SHA256)	www.netlock.hu/index.cgi?ca=cbca
Expressz	(SHA256)	www.netlock.hu/index.cgi?ca=ccca
OnlineSSL	(SHA256)	www.netlock.hu/index.cgi?ca=olsslgca

8.1. Példa a konfigurációs állományra

A következő példa konfigurációs állomány SSL és nem SSL kapcsolattal működő szerver konfigurálását mutatja be:

```
# Az SSL kikapcsolása általánosan
SSLDisable

# Kapcsolat fogadása 80 (http) és 443 (https) portokon
Listen 80
Listen 443

# alapértelmezett konfiguráció
SSLLogFile /utvonal/SSL_log
SSLCertificateFile /utvonal/tanusitvany.pem
SSLCertificateKeyFile /utvonal/kulcs.pem

#A CACHAIN file megadasa akkor szukseges, ha a kiadott tanusitvany koztes
#kiadotol szarmazik
#SSLCertificateChainFile /utvonal/onlinesslCA.pem
#SSLCertificateChainFile /utvonal/cbca.cer
#SSLCertificateChainFile /utvonal/ccca.cer

#kliens ellenőrzés opciók
#nincs tanúsítványos kliens ellenőrzés opció,
#tanusítványlánc ellenőrzése 10 szintig
#(értelemszerűen ha kikapcsolva, akkor nincs
SSLVerifyClient 0
SSLVerifyDepth 10
```


NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

```
#klienstől elfogadott kódolások
#(itt minden, kivéve NULL, ennél kevesebb javasolt)
#Ban = tiltva
#FIGYELEM!!! EZ EGY MINTA SZAKASZ, A SAJAT SZERVER BEALLITAS MEGTARTASA
#A KODOLASOK ESETEBEN JAVASOLT LEHET!!!
SSLRequiredCiphers NULL-MD5:RC4-MD5:EXP-RC4-MD5:RC2-CBC-MD5:IDEA-CBC-
MD5:DES-CBC-MD5:DES-CBC-SHA:DES-CBC3-MD5:DES-CBC3-SHA:DES-CFB-M1
SSLRequireCipher NULL-MD5 RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 IDEA-CBC-MD5 DES-
CBC-MD5 DES-CBC-SHA DES-CBC3-MD5 DES-CBC3-SHA DES-CFB-M1
SSLBanCipher NULL

#logolás helye
SSLLogFile utvonal/ssl_log

#most jön az SSL védett szerver

<VirtualHost www.akarmi.hu:443>
SSLEnable
DocumentRoot /utvonal/
ScriptAlias /cgi-bin/ /utvonal/
TransferLog utvonal/fajl
ErrorLog utvonal/fajl
</VirtualHost>

# itt következik a nem SSL védett site (SSLDisable kikapcsolja a site-ra)

<VirtualHost www.akarmi.hu:80>
SSLDisable
DocumentRoot /utvonal/
ScriptAlias /cgi-bin/ /utvonal/
ErrorLog utvonal/fajl
TransferLog utvonal/fajl
</VirtualHost>
```


NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.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 érhetők el.

Legfelső szintű kiadó:

Arany	(SHA256)	www.netlock.hu/index.cgi?ca=gold

Köztes szintű kiadó:

Közjegyzői	(SHA256)	www.netlock.hu/index.cgi?ca=caca
Üzleti	(SHA256)	www.netlock.hu/index.cgi?ca=cbca
Expressz	(SHA256)	www.netlock.hu/index.cgi?ca=ccca
OnlineSSL	(SHA256)	www.netlock.hu/index.cgi?ca=olsslgca

9.3.2. SHA 1 kiadók

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

Legfelső szintű kiadók:

Közjegyzői	(SHA1)	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 az netlock_osszes_ssl_kiado.pem fájl használata a csomagból): http://www.netlock.hu/docs/letoltes/ssl_kiadok_csomag.zip

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

9.4. Az Apache 2.3 és későbbi szerver verziók beállítása

Az Apache 2.3 vagy későbbi verziójú webszerver esetén az Apache konfigurációs állományban a következőket kell megadni az OCSP Stapling bekapcsolásához:

1. A Szerveren ellenőrizzük, hogy az OpenSSL legalább 0.9.8h verziója legyen megtalálható, ha ez nem így van, akkor frissítsük azt. Az ellenőrzés elvégezhető a következő paranccsal.

   ```
   openssl –version
   ```

2. A szerver modul betöltő részéhez (általában a httpd.conf fájlban található ez a szakasz) adjuk hozzá a következő szakaszt:

   ```
   LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
   ```

   Ez a beállítás betölti a megfelelő modult. Ellenőrizzük és szükség esetén telepítsük, ha nem található szerverünkön ez a modul.

3. A szerver SSL részt beállító szakaszához adjuk hozzá a következő bejegyzéseket:

   ```
   #stapling bekapcsolása, cache es cache timeout beallitasa
   SSLUseStapling On
   SSLStaplingCache shmcb:/path/to/datafile[(512000)]
   SSLStaplingStandardCacheTimeout 3600
   SSLStaplingResponseMaxAge 3600
   #a valaszado lekeres timeout beallitasa
   SSLStaplingResponderTimeout 30
   #hibas ocsp eseten a valasz timeoutja
   SSLStaplingErrorCacheTimeout 600
   #ha a szerver nem tud staplingolni, trylater-t küld a kliensnek
   SSLStaplingReturnResponderErrors on
   SSLStaplingFakeTryLater on
   ```

   A „/path/to/datafile” értéket helyettesítsük be. Javasolt lehet a következő:

   ```
   /var/cache/mod_shmcb/stapcache
   ```

   Az útvonal és a fájl legyen létrehozva, jogosultsága legyen a webszerver jogosultságával egyező.

   A fentiek megadása és az Apache szerver újraindítása után az OCSP Stapling -nak működnie kell.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

10. Apache Tomcat beállítása

Amennyiben a tanúsítványa PFX állományban (PKCS #12) található, akkor azt a Tomcat szerver közvetlenül is tudja használni.

A konnektor beállításaihoz a következő három sor hozzáfűzése szükséges:

```
keystoreType= "PKCS12 "
keystoreFile= "/utvonal/akarmi.pfx "
keystorePass= "akarmijelszo"/
```

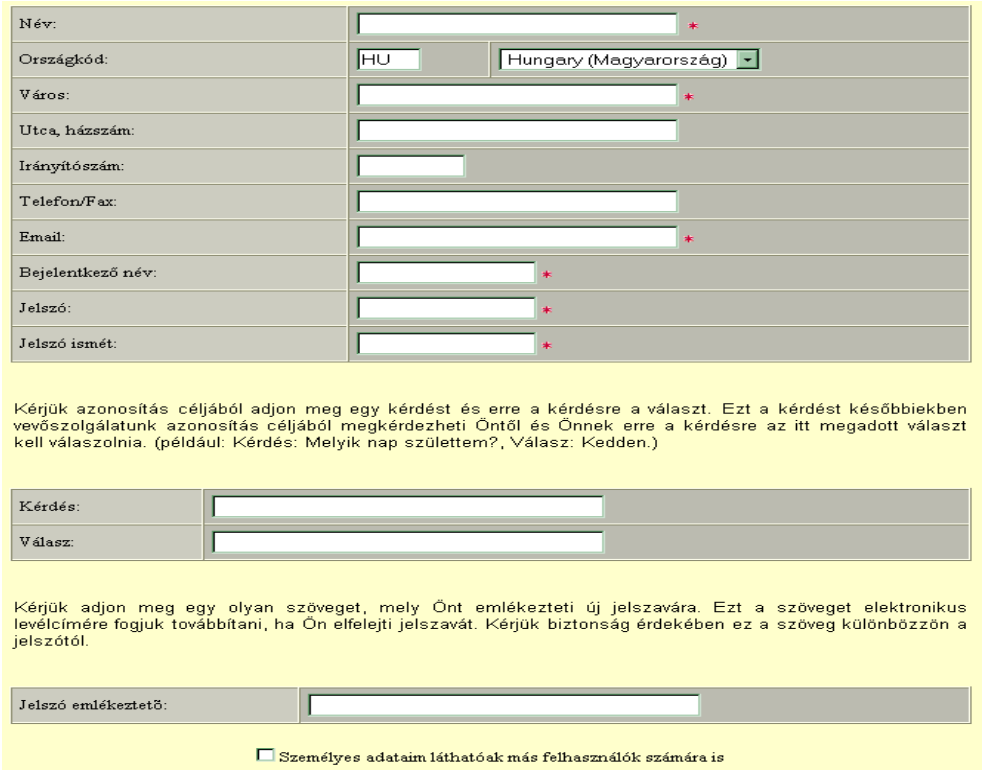

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 oldalra, és ott válassza a „Fokozott biztonságú tanúsítvány igénylése" menüpontot, majd a megjelenő oldalon válassza a Regisztráció menüpontot.
2. A megjelenő adatlapon töltse ki személyes adatait az igazolványainak (személyi igazolvány, lakcímkártya) megfelelő adatokkal (ahol ez értelmezhető).



NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

A kitöltendő adatok a következők:

Név	Az érvényes személyes adatok az igazolványok alapján.
Országkód	
Város	
Utca, házszám	
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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 a 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 (1) 700 1101-es számra vagy e-mailben szkennelve a 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.).

Minősített 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.).

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 saját maga és mások tanúsítványait, innen intézheti a tanúsítványokkal kapcsolatos ügyeit.

11.2 Bejelentkezés az ügyfélmenübe

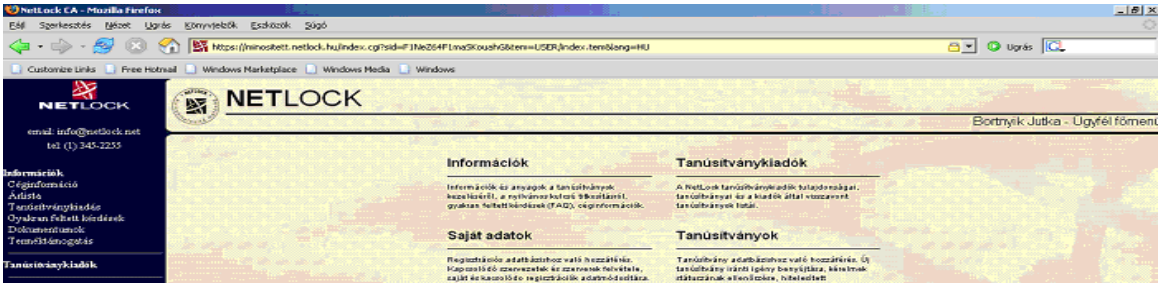
Az ügyfélmenübe bejelentkezni a www.netlock.hu oldalon lehet.

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.



NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

11.3 A tanúsítvány felfüggesztése

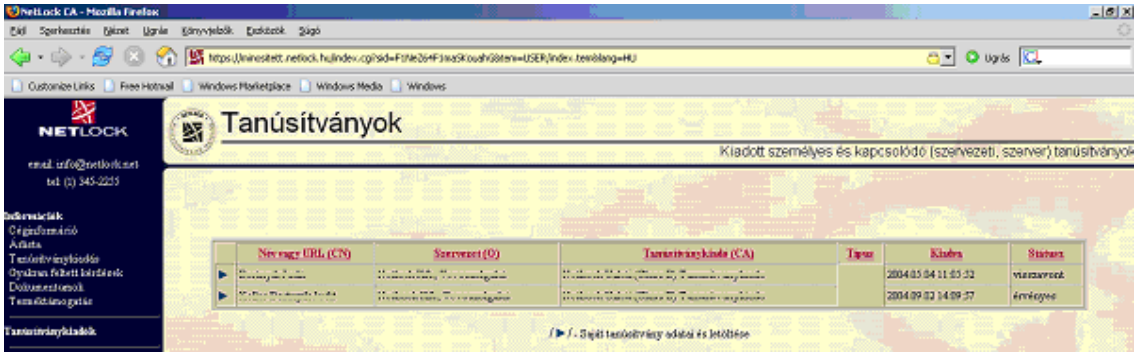
Elektronikus tanúsítványait - akárcsak bankkártyáját - gondosan kell kezelnie és őriznie, hiszen a tanúsítványával az Ön nevében végezhetnek elektronikus aláírást és ez által az Ön nevében tehetnek joghatással bíró nyilatkozatot.

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 e-mail címen jelezhet.

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

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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 lejáró 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 lejáró, 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 tanúsítvány 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 tanúsítványok cserélendők 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 lehet a webszerver újraindítására.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu