NETLOCK
Az Első Hitelesítés-szolgáltató
cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

Tanúsítvány létrehozása Apache szerverhez

Apache szerveren kérelem létrehozása, tanúsítványkérelem beadása, kiadott tanúsítvány telepítése

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

1. Tartalomjegyzék

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

2. Bevezető

Ennek a tájékoztatónak az a célja, hogy az szerveréhez létrehozandó SSL tanúsítvány igénylését minél könnyebben elvégezhesse.

Kérjük olvassa el figyelmesen, és kövesse a leírtakat.

Amennyiben bármilyen kérdése van vagy problémája támad, Ügyfélszolgálatunk az (1) 345-2255-ös telefonszámon, az info@netlock.hu e-mail címen vagy személyesen a 1023 Budapest, Zsigmond tér 10. szám alatt munkanapokon 9 és 17 óra között készséggel áll rendelkezésére.

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

3. Tanúsítvány kérelem létrehozása a szerveren

A kérelem létrehozásának lépései a következők:

1. Csatlakozzon szerveréhez majd adja ki következő parancsot:

   ```
   openssl req -new -keyout domainnev.key -out domainnev.csr
   ```

   Ha jelszóval nem kívánja védeni a kulcsot, akkor a következő parancsot adja ki. (Jól jöhet, automatikusan induló szerverekhez, azonban biztonsági problémát okozhat.)

   ```
   openssl req -new -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 semmiféleképp ne töltse ki az esetleg felajánlott e-mail mezőt, mert 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 törlésre kerül.

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

A tanúsítvány-kérelem kitöltendő mezői:

Common name (CN)	Domain név teljes formájában. (https:// nélkül) (pl. www.akarmi.hu, mail.akarmi.hu) Minden egyes aldomainhez új tanúsítvány szükséges, a wildcard(*-gal kezdődő) tanúsítványok nem támogatottak.
Contry code (C)	Országkód, nagy betűvel Magyarország kódja, vagyis: HU
Locality (L)	Város, a cégkivonat szerinti székhely vagy telephely városa, magánszemély tanúsítványa esetén 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, a 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, nem elfogadható.

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

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

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

3.1. Példa a kulcsgenerálásra és a kérelem létrehozására

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

```
openssl req -new -keyout domainnev.key -out domainnev.csr
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..++++++
.....................++++++
writing new private key to 'domainnev.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
```

Jelszó nélküli teljes kulcsgenerálás

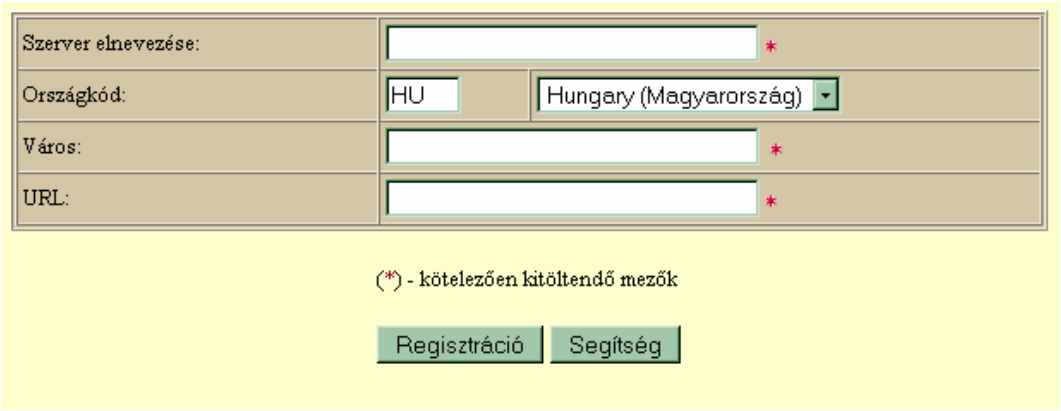
```
>openssl req -new -nodes -keyout domainnev.key -out domainnev.csr
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
....++++++
.....................................................++++++
writing new private key to 'domainnev.key'
-----
You are about to be asked to enter 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]:Test Ceg Rt.
Organizational Unit Name (eg, section) []:.
Common Name (eg, YOUR name) []:www.akarmi.hu
Email Address []:

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

>
```

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

4. Tanúsítvány kérelem beadása

Az imént létrehozott kérelem beadásának lépései a következők:

1. Ha már volt regisztrálva felhasználóként 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. Bejelentkezve a rendszerbe válassza az Új szerver regisztrációja gombot. A megjelenő ablakban töltse ki az adatokat a 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 szervezeti adatok, magánszemély által beszerzendő esetén a személy adatai alapján.
Város	
URL	A szerver URL https nélkül, meg kell egyeznie a később tanúsítvány kérelemben lévő URL-lel.

3. Ezután válassz az Új kérelem beadása > Szerver tanúsítványok > Web szerver (SSL) > menüpontot, a lap alján válasza ki „PEM formátumú PKCS10 tanúsítvány kérelem feltöltése" opciót, majd nyomja meg a Tanúsítványkérelem gombot.

4. 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.

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

6. Az ezután következő lépés a Fizetési feltételek kiválasztása (szükség esetén a sürgősség megjelölése) és a Belépési nyilatkozat létrehozása lesz, majd a szükséges iratokat a tanúsítványosztálynak megfelelő módon el kell jutatni a Netlock Kft. részére. (ezekről részletesebben a függelékben olvashat.)

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

7. 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.

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

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

```
# Az SSL kikapocslása 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

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

#klienstől elfogadott kódolások
#(itt minden, kivéve NULL, ennél kevesebb javasolt)
#Ban = tiltva
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 (SSLisable kikapcsolja a site-ra)

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

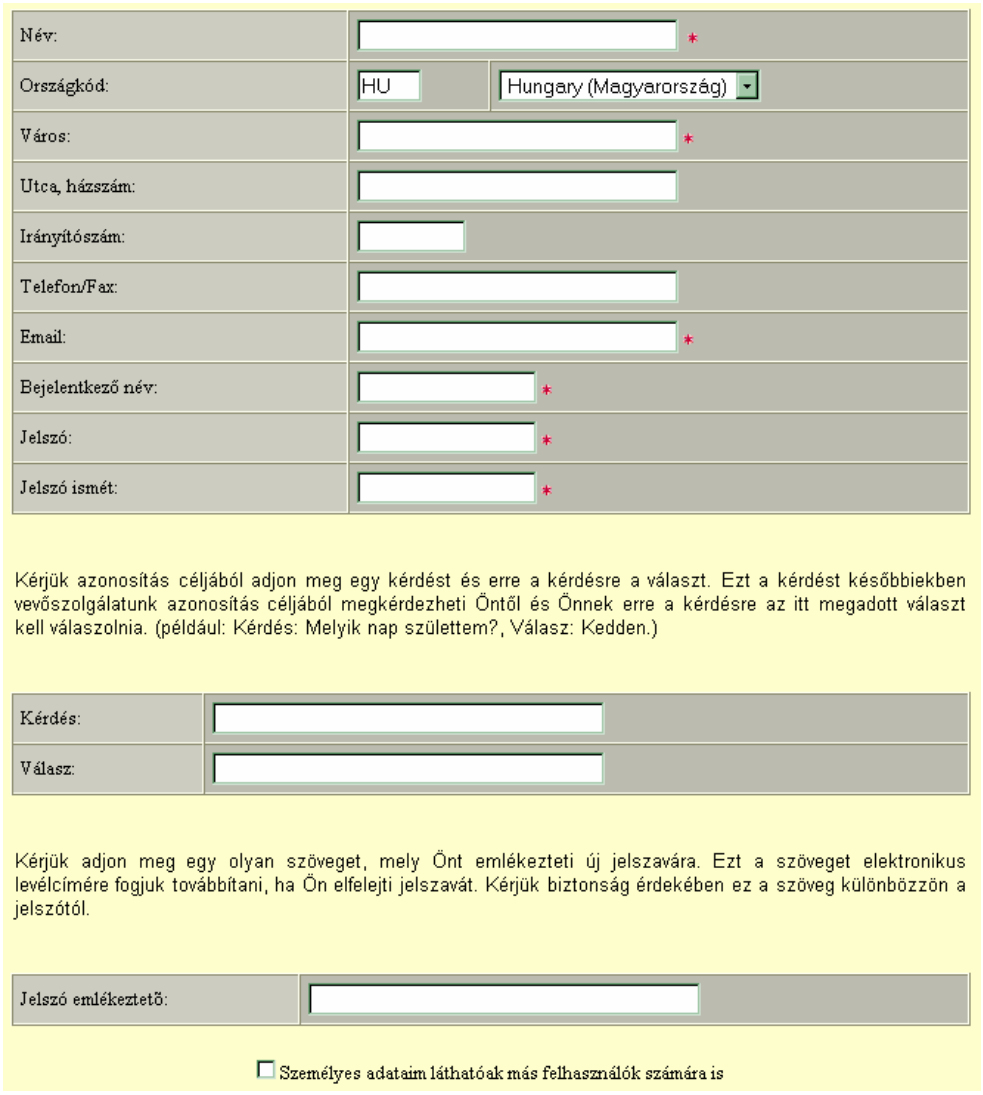
cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

8. 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 természetsen)



cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

A kitöltendő adatok a következők:

Név	Az érvényes személyes adatok 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.

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

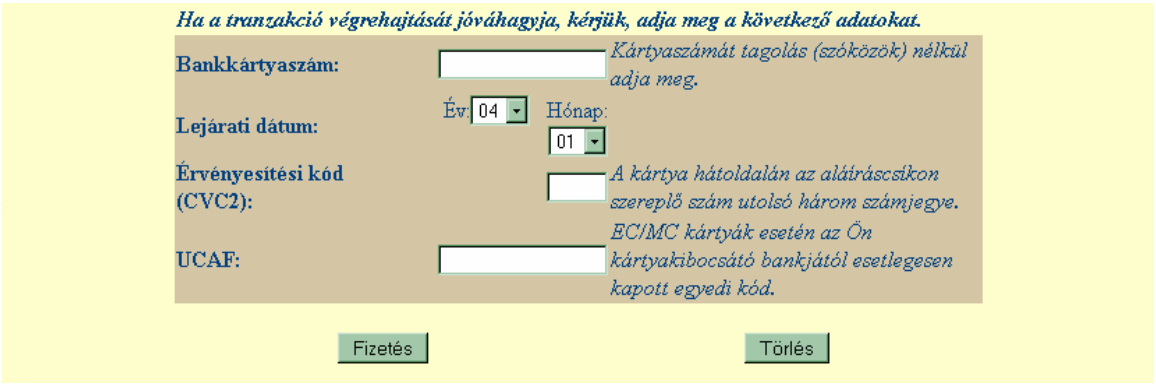
5. Függelék B – Fizetési ügyintézés

A menüpontot beállítva kiválaszthatja fizetési módját (Átutalás/Bankkártya) illetve jelezheti igényét sürgősségi, tehát a többi nem sürgősségi tanúsítványt megelőző kibocsátásra is.

Az opciókat kiválasztva a „Fizetési mód kiválasztása!" gombot megnyomva a fizetési módnak megfelelő lépés következik.

Bankkártyás fizetés esetén meg kell adnia a számlázáshoz a postázási címet, majd az „On-line bankkártyás fizetés!" gombra kattintva, majd a következő oldalt kapja.

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu



Ezen az oldalon keresztül kártyája megterhelésre kerül a jelzett összeggel, a számlát utólag, postán kapja meg.

Átutalásos fizetést választva meg kell adnia a számla postázási címét, illetve az eltér a számlán szerepeltetni kívánt címtől akkor azt is. A számla postázásra kerül, melyet majd át kell utalnia.

Amennyiben az átutaló intézmény neve az átutalásban nem szerepel (pl. iskola esetén a fenntartó önkormányzat fizet) kérjük e-mailben jelezze a kerelmek@netlock.hu email címre, hogy az összeg kipontozása minél hamarabb megtörténhessen.

A fizetési .opciók beállítása után a műveletet átutalásos fizetés esetén folytathatjuk a Belépési nyilatkozat létrehozásával. (Lásd **Error! Reference source not found.**)

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

6. Függelék C – 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, melyet 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!!!