

Tanúsítvány létrehozása Courier IMAP SSL szerverhez

Courier IMAP SSL szerveren kérelem létrehozása, tanúsítványkérelem
beadása, kiadott tanúsítvány telepítése, tanúsítvány megújítása

1. Tartalomjegyzék

1.	Tartalomjegyzék.....	2
2.	Bevezető	3
3.	Korlátozások.....	3
4.	Elő követelmények – Openssl telepítése	4
5.	OpenSSL használata Windows alól	4
6.	Előzetes követelmények – néhány döntés, amit meg kell hozni	5
6.1.	A tanúsítványkiadás algoritmusa, a kiadó típusa	5
7.	Az SSL tanúsítvány profilja.....	5
8.	Tanúsítvány kérelem létrehozása a szerveren.....	7
9.	Példa a kulcsgenerálásra és a kérelem létrehozására.....	9
10.	Tanúsítvány kérelem beadása	10
11.	Kiadott tanúsítvány telepítése, konfigurálás	13
12.	SHA-1 kiadók esetén	14
13.	Online SSL kiadó esetén	15
14.	SHA-256 kiadók esetén	16
15.	Függelék A – Regisztráció ügyfélmenübe.....	17
16.	Függelék B – Belépési nyilatkozat készítése	19
17.	Teendők a Belépési nyilatkozattal.....	19
18.	Függelék C – Tanúsítvánnyal kapcsolatos ügyintézés.....	20
19.	Az ügyfélmenü használata.....	20
20.	Bejelentkezés az ügyfélmenübe	20
21.	A tanúsítvány felfüggesztése.....	20
22.	Felfüggesztéssel kapcsolatos fontos információk.....	21
23.	Függelék D – A tanúsítvány megújítása.....	22
24.	Megújított tanúsítványok letöltése	22

2. Bevezető

Ennek a tájékoztatónak az a 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 és 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 a 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. Elő követelmények – Openssl telepítése

Windows esetén:

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>

Linux esetén:

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

5. OpenSSL használata Windows alól

Az Openssl-t Windows esetén parancsról tudja használni. Ennek elérési:

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
```

6. 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.

6.1. 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 vélhetően 2013. 06. 31-ig tart, azután tovább nem használhatók

- **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.

7. Az SSL tanúsítvány profilja

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

- **Szerver tanúsítvány**

Egyszerű, egy domain nevet tartalmazó tanúsítvány, melynek a CN mezőjében a domain név található. Olyan esetekben javasolt, ahol egy 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 eléréshez jó, azonban a valami.hu cím eléréshez NEM alkalmas;
- általában egyszerű weboldalakhoz javasolt, amely egy címen érhető el.

- **Wildcard tanúsítvány**

Olyan tanúsítvány, amely egy domain nevet tartalmaz a bal oldali tag helyén azonban * található.

- a *.valami.hu címre szóló tanúsítvány alkalmas több aldomain hitelesítésére, így a www.valami.hu mellett a mail.valami.hu címre is, azonban a * kötelezően helyettesít egy tagot, így NEM alkalmas a valami.hu cím elérésére;
- a * csak bal oldalon szerepelhet;
- a régebbi telefonok (WM5, WM6, és egyéb régebbi telefonos operációs rendszerek) a Wildcard tanúsítványokat nem támogatják
- általában az UCC tanúsítvány javasolt helyette, mely tartalmazhat wildcard tagokat is;

- **UCC tanúsítvány**

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

- a több domain név lehetővé teszi, hogy domain nevek széles kombinációját használhassuk egy szerveren;
- a 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;
- a 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;
- a valami.hu és akarmi.hu neveket tartalmazó tanúsítvány lehetővé teszi, hogy oldalunkat elérjük a valami.hu vagy az akarmi.hu néven is egyaránt;
- A fentiek kombinációja alapján több különböző domain név, több TLD (pl.: .hu, .eu) vagy al- és fődomain egyaránt történő használata esetén javasolt.

8. 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 -new -keyout domainnev.key -out domainnev.csr
```

Ha **JELSZÓVAL NEM AKARJA** 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 kiállításához 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 töltsse 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.

A tanúsítvány-kérelem kitöltendő mezői:

Common name (CN)	Domain név teljes formájában. (https:// nélkül) (pl. www.akarmi.hu, mail.akarmi.hu)
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 majd az Courier megfelelő könyvtárába, a létrejövő kérelmet (.csr) kell majd a Netlock rendszerbe feltöltenie.

9. 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 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

```
>openssl req -new -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]: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 []:

>
```

10. 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 töltsé ki az adatokat a következő táblázatnak megfelelően.

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

(*) - kötelezően kitöltendő mezők

1. Szerver elnevezése	2. Szerver elnevezése, valamilyen beszédes név
3. Országkód	4. 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.
5. Város	
6. URL	7. A szerver URL https nélkül, meg kell egyeznie a később tanúsítvány kérelemben lévő URL-lel.

3. Itt döntést kell hoznia, hogy SHA1 vagy SHA256 algoritmussal készüljön a tanúsítványa. SHA1 esetén a korábban használt paraméterek nem változnak, ugyanakkor az SHA1 algoritmusú tanúsítványok 2013 folyamán visszavonásra kerülhetnek. Erre vonatkozó döntést a kapcsolódó szabványokért felelős szervek hoznak, az ő döntésük a Hitelesítés szolgáltatók számára az irányadók.

4. SHA256 algoritmus esetén a szerverre le kell telepíteni a köztes kiadókat (részletesen később), illetve a felhasználói oldalnak a legfrissebb operációs rendszerrel kell rendelkeznie. A biztonságosabb kódolás miatt ezt a módozatot javasoljuk.

5. Ezután válassza az Új kérelem beadása > SHA1 vagy SHA256 > Szerver tanúsítványok menüpontot > majd a megfelelő opciót, a lap alján válassza ki a „PEM formátumú PKCS10 tanúsítvány kérelem feltöltése” opciót, majd nyomja meg a Tanúsítványkérelem gombot.

Szerver tanúsítványok

<input type="radio"/> Szerver (SHA256)	<input type="radio"/> Wildcard (SHA256)
<input checked="" type="radio"/> UCC (SHA256)	<input type="radio"/> Egyedi (SHA256)

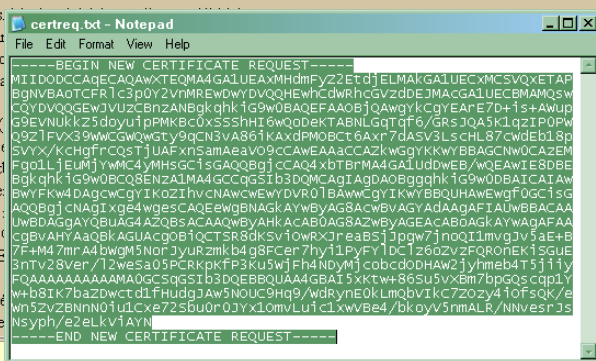
6. Az imént regisztrált szerver meg kell jelenjen a kapott találati listában, azt válassza ki, majd a megjelenő ablak szövegdobozába a vágólapon keresztül másolja be a kérelem generálás során létrejött fájl tartalmát, majd nyomja meg a Tovább gombot.

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

A kérelem készítése során meg kell adni a következő információkat:

- a Név (Cím)
- a Város (Lokalizáció)
- a Megye (Statisztikai terület)
- a Szervezet (Név)
- a Szervezeti cím
- ne szerepeljen a címben a cég neve
- fontos, hogy a cím megadása során ne használjon speciális karaktereket (pl. IT, Marketing, Kft.)

A kérelem elkészítése során a rendszer generál egy fájl tartalmát, amelyet a következő URL-en lehet letölteni: <http://www.netlock.hu>



```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDODCCAQECAQAwXTEQM4GA1UEAxBHJmYXZlZjE1MAkGA1UECmVxMjE1
BgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAGIAGDA0BgkqhkiG9w0D
BATICAwBwYFKw4DAgcwCgYIKoZIhvcNAQcwEwYDVR01BAwwCgYIKwYBBQ
HAWEwgF0GC1SGAQOBjcnAgI1xge4wgesCAQEEwgnBNAgkAYwByAG8AcwBy
AGYAdAAgAFIAUwBBAAUwBDAGAYQBuaG4AZQBSACAAQwByAHKAcAB0AG8
AZwByAGEAcABoAGkAYwAgcgBvAHYAaQBkAGUAcgOB1QCTSR8dKSv1OwR
KJreaBSjJpgw7jnoQIImvgJv567F+H47mrA4bWgM5NorJyuRzmkb4g8FCer7hy
i1PyFY1DC1z6ozvzFQR0nEK1S3ntv28Ver/12weSa05PCRkPKfP3Ru5WjFh4NDyMj
cobcdODHAW2jyhmeb4T5FQAAAAAAMAAOAGCSqGSIb3DQEBAQA4GBAI5xKt
w+86Su5vXEm7bpQScw+bs8IK7baZdwctd1fHudgJAw5NOUC9Hq9/wdRyn
EOKLmQbVikC7ZozY4iOfsQK/eWn5ZvZBNNOiulCxe72Sbu0r0JYx1Om
vLuic1xwVBe4/bkoyv5nmALR/NNvesr3NsypH/e2eLkv1AYN
-----END NEW CERTIFICATE REQUEST-----
                    
```

7. 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

8. 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 juttatni a NetLock Kft. részére. (ezekről részletesebben a függelékben olvashat.)

11. Kiadott tanúsítvány telepítése, konfigurálás

A következő példa konfigurációs állományok SSL kapcsolattal működő szerver konfigurálását mutatja be:

Az alábbi konfigurációs állományt használva a benne hivatkozott fájlokat kell a használathoz megfelelő tartalommal feltöltenünk.

Az alábbi opciókat kell beállítani (vastag betűs) az

```
/etc/courier-imap/pop3d-ssl
```

```
/etc/courier-imap/imapd-ssl
```

fájlokban.

```
SSLPORT=993
SSLADDRESS=0
SSLPIDFILE=/var/run/courier/imapd-ssl.pid
IMAPDSSLSTART=YES
IMAPDSTARTTLS=YES
IMAP_TLS_REQUIRED=0
COURIERTLS=/usr/bin/couriertls
TLS_PROTOCOL=SSL3
TLS_STARTTLS_PROTOCOL=TLS1
TLS_CERTFILE=/etc/courier/ssl.pem
TLS_TRUSTCERTS=/etc/courier/chain.pem
TLS_VERIFYPEER=NONE
```

Ezt követően a szolgáltatás újraindítása szükséges:

```
service courier-imap restart
```


12. SHA-1 kiadók esetén

SHA-1 kiadók esetében az állományoknak a láncon felfelé haladva kell tartalmazniuk a tanúsítványt.

Azaz a következőképpen:

A sorrend a chainben:

1. az SSL tanúsítványt kiadó Root tanúsítványa:

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

A sorrend szerver tanúsítványban:

1. a szerver tanúsítványához tartozó kulcs
2. a szerver SSL tanúsítványa
3. az SSL tanúsítványt kiadó láncc root:

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

Ez konkrétan:

ssl.pem

```
-----BEGIN RSA PRIVATE KEY-----  
<mail.testsrv.hu privat kulcsa>  
-----END RSA PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
<mail.testsrv.hu tanusitvanya>  
-----END CERTIFICATE-----
```

chain.pem

```
-----BEGIN CERTIFICATE-----  
<NetLock Kozjegyzoi Tanusitvanykiado tanusitvanya>  
-----END CERTIFICATE-----
```

13. Online SSL kiadó esetén

Az OnlineSSL kiadó esetében az állományoknak a láncon felfelé haladva kell tartalmazniuk a tanúsítványt.

Azaz a következőképpen:

A sorrend a chainben:

1. OnlineSSL CA <https://www.netlock.hu/index.cgi?ca=olsslga>
2. Gold root CA <https://www.netlock.hu/index.cgi?ca=gold>

A sorrend szerver tanúsítványban:

1. a szerver tanúsítványhoz tartozó kulcs
2. a szerver SSL tanúsítványa
3. OnlineSSL CA <https://www.netlock.hu/index.cgi?ca=olsslga>
4. Gold root CA <https://www.netlock.hu/index.cgi?ca=gold>

Ez konkrétan:

ssl.pem

```
-----BEGIN RSA PRIVATE KEY-----  
<mail.testsrv.hu privat kulcsa>  
-----END RSA PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
<mail.testsrv.hu tanusitvanya>  
-----END CERTIFICATE-----
```

chain.pem

```
-----BEGIN CERTIFICATE-----  
<Netlock Online SSL CA tanusitvanya>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<NetLock Gold CA tanusitvanya>  
-----END CERTIFICATE-----
```

14. SHA-256 kiadók esetén

SHA-256 kiadók esetében az állományoknak a láncon felfelé haladva kell tartalmazniuk a tanúsítványt.

Azaz a következőképpen:

A sorrend a chainben:

1. a köztes tanúsítványkiadó tanúsítványa:

NetLock Közjegyzői (Class A): <https://www.netlock.hu/index.cgi?ca=caca>

NetLock Üzleti (Class B): <https://www.netlock.hu/index.cgi?ca=cbca>

NetLock Expressz (Class C): <https://www.netlock.hu/index.cgi?ca=ccca>

2. a főtanúsítvány:

NetLock Arany (Class Gold): <https://www.netlock.hu/index.cgi?ca=gold>

A sorrend szerver tanúsítványban:

1. a szerver tanúsítványához tartozó kulcs

2. a szerver SSL tanúsítványa

3. a köztes tanúsítványkiadó tanúsítványa:

NetLock Közjegyzői (Class A): <https://www.netlock.hu/index.cgi?ca=caca>

NetLock Üzleti (Class B): <https://www.netlock.hu/index.cgi?ca=cbca>

NetLock Expressz (Class C): <https://www.netlock.hu/index.cgi?ca=ccca>

2. a főtanúsítvány:

NetLock Arany (Class Gold): <https://www.netlock.hu/index.cgi?ca=gold>

15. 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 töltsé ki személyes adatait az igazolványainak (személyi igazolvány, lakcímkártya) megfelelő adatokkal. (Ahol ez értelmezhető természetesen)

Név:	<input type="text"/>
Országkód:	<input type="text" value="HU"/> Hungary (Magyarország) <input type="button" value="-"/>
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 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.

16. 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, 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!!!

17. 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.

Expressz tanúsítványkiadók esetén (SHA1 C, SHA 256 CL, SHA256 CNAC) esetén:

Küldje el aláírva a NetLock Kft.-hez faxon az +36 1 700 2828-as számra, illetve e-mailen szkennelve a kerelmek@netlock.hu címre.

Üzleti tanúsítványkiadók esetén (SHA1 B, SHA 256 BL, SHA256 BNAC) esetén:

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. Ezen osztály esetében választható a mobil regisztrációs szolgáltatás is, melynek díjszabásáról az alábbi oldalon tájékozódhat: Ennek a szolgáltatásnak felára van, amelynek mértékéről az alábbi oldalon tájékozódhat: <http://www.netlock.hu/html/ar.html#opt>

A osztály tanúsítványkiadók esetén (SHA1 A, SHA 256 AL, SHA256 ANAC) 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 tanúsítványkiadók esetén (SHA1 QA, SHA 256 Q) esetén:

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. Ezen osztály esetében választható a mobil regisztrációs szolgáltatás is, melynek díjszabásáról az alábbi oldalon tájékozódhat: Ennek a szolgáltatásnak felára van, amelynek mértékéről az alábbi oldalon tájékozódhat: <http://www.netlock.hu/html/ar.html#opt>

18. 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.

19. Az ügyfélmenü használata

Tanúsítványkérelmeinek 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.

20. Bejelentkezés az ügyfélmenübe

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

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) Bejelentkezés a fokozott biztonságú rendszerbe linkre.

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



21. A tanúsítvány felfüggesztése

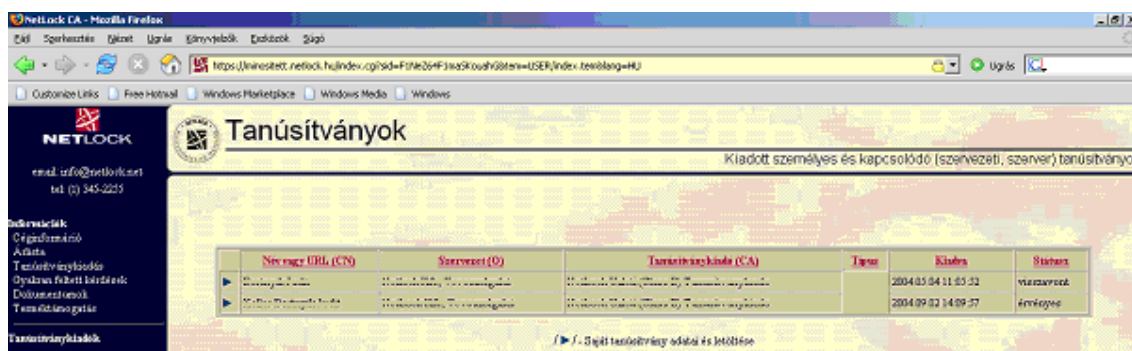
Elektronikus tanúsítványait, akár csak bankkártyáját, gondosan kell kezelnie és őriznie, hiszen a tanúsítványával az Ön nevében végezhetnek elektronikus aláírást, és ez által az Ön nevében tehetnek joghatással bíró nyilatkozatot.

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

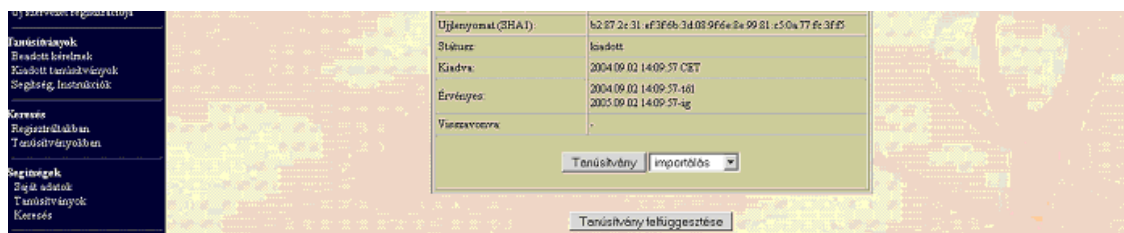
Ha nem tud minden kétséget kizáróan meggyőződni arról, hogy időközben a magánkulcsot nem használta illetéktelen személy, intézkedjen a tanúsítvány végleges visszavonásáról. A felfüggesztési, visszavonási lépéseket a NetLock Kft. Szolgáltatási Szabályzatában szereplő módon (Internetes ügyfélmenün keresztül,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

A.) Interneten keresztül a következő módon függesztetheti fel tanúsítványát:

1. Jelenkezzen 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.

22. Felfüggesztéssel kapcsolatos fontos információk

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

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

23. 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 ügyfél menüjébe
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.

24. 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 szerver szolgáltatás újraindítására.