Tanúsítvány létrehozása IIS 7.0 szerverhez

Kérelem létrehozása IIS 7.0 szerveren, tanúsítvány kérelem beadása, kiadott tanúsítvány telepítése és megújított tanúsítvány cseréje

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

1. Tartalomjegyzék

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 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 vagy problémája van, Ügyfélszolgálatunk az (40) 22-55-22 telefonszámon, az info@netlock.hu e-mail címen, vagy személyesen a 1101 Budapest, Expo tér 5-7. szám alatt, munkanapokon 9 és 17 óra között készséggel áll rendelkezésére.

3. A dokumentációról

A dokumentáció az IIS 7 verzió alapján készült, de a dokumentáció alapján a tanúsítvány generálás folyamata későbbi verziókkal is elvégezhető.

4. 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) mező, illetve egy 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 haszna megkérdőjelezhető.

5. UCC tanúsítványok

Az Exchange 2007, az Office Communication Server 2007, illetve későbbi verzióik teljeskörű funkcionalitásának kihasználásához UCC profil az optimális választás, melynek generálása eltérő a leírásban szereplőhöz képest. Az eljárásról egy másik útmutatóban olvashat.

Figyelem!

Belső névre UCC tanúsítvány nem adható, mivel támadási felületet jelenthet.

(részleteket lásd: Függelék H)

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

6. IIS szerverhez kapcsolódó hotfix Windows XP és Windows 2003 szervereken

Amennyiben az IIS szerver Windows XP vagy Windows 2003 szerveren fut, szükség lehet az SHA256 hotfix telepítésére.

Ez a hotfix az IIS számára biztosítja az SHA256 támogatást, mert az egyéb SHA256 algoritmust érintő frissítések az operációs rendszer kezelését adják hozzá, nem az IIS szerverét. (Például: Windows XP SP3 telepítése - kliens oldali használat szempontjából - az SHA256 algoritmus használatának alapfeltétele.)

A hotfix és a kapcsolódó tudásbázis anyag a következő címeken érhető el:

http://support.microsoft.com/kb/968730

http://support.microsoft.com/hotfix/KBHotfix.aspx?kbnum=968730&kbln=en-us

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

7. 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.

7.1. A tanúsítvány kiadás 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.

7.2. Az SSL tanúsítvány profilja

A kiadás során használt tanúsítványprofil határozza meg, hogy mire lesz 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 eléréshez jó, a valami.hu cím eléréséhez NEM alkalmas;
- általában olyan weboldalhoz javasolt, amely egy címen érhető el.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 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
- általában az UCC tanúsítvány javasolt helyette, mely tartalmazhat wildcard tagokat is;

- UCC tanúsítvány

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

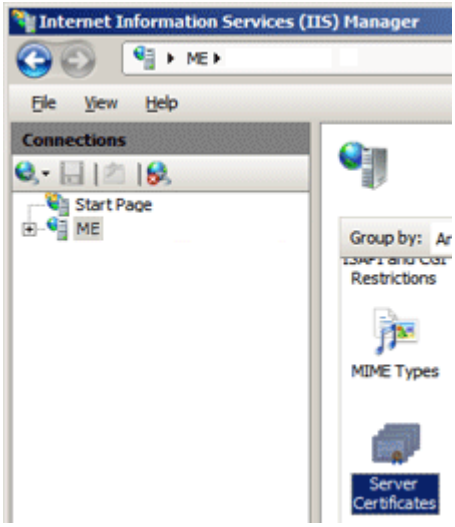
- a több domain név lehetővé teszi, hogy domain nevek széles kombinációját használhassuk egy szerveren;
- például egy valami.hu és *.valami.hu neveket tartalmazó tanúsítvány lehetővé teszi, hogy oldalunkat elérjük a valami.hu, valamint a www.valami.hu, web.valami.hu, mail.valami.hu címeken;
- például 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.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

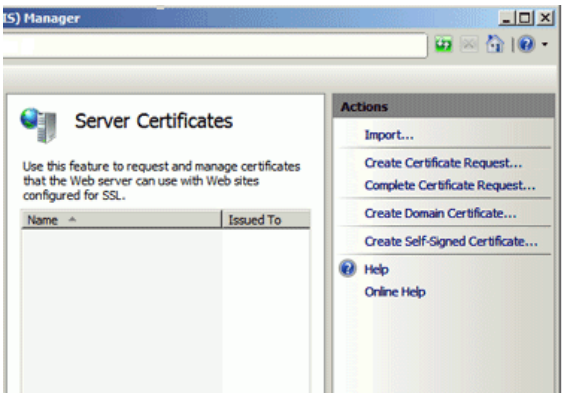
8. Tanúsítvány kérelem létrehozása a szerveren

A kérelem létrehozásának lépései a következők:

1. Indítsa el az IIS konzolját, és válasza ki a website-ot, amihez a tanúsítványt szeretné létrehozni.
   (Vezérlőpult > Felügyeleti eszközök > Internet Information Services Manager)
   (Vezérlőpult > Administrative tools > Internet Information Services Manager)



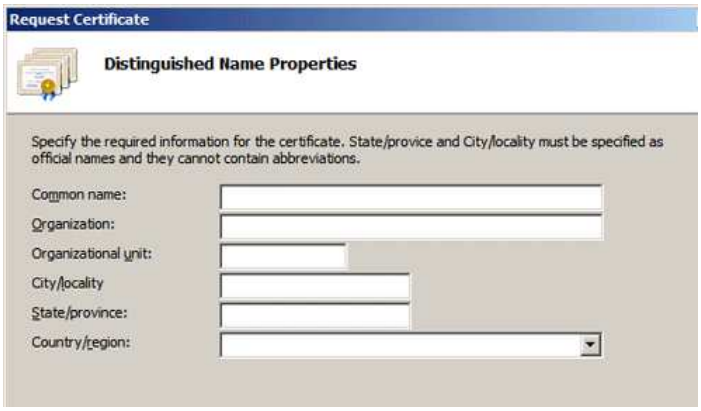
2. Jelölje ki a Kapcsolatok (Connections) oszlopban a website-ot, majd kattintson a Szerver tanúsítványok (Server cetificates) menüpontra.
3. A megjelenő ablakban láthatók a meglévő tanúsítványok, illetve jobb oldalt a választható műveletek. Itt válasszuk ki a Tanúsítvány kérelem készítése (Create Certificate Request…) opciót.



NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

4. A következő ablakban töltse ki az adatlapot:
   - Név (Common Name) - a domain név
   - Szervezet (Organization) - a szervezet cégkivonat szerinti neve, rövid neve
   - Szervezeti egység (Organizational unit) - A szervezetnél található szervezeti egység, opcionális.
   - Város (City/locality) - A szervezet cégkivonat szerinti székhelye
   - Állam/Megye (State/province) - üres
   - Ország / régió (Country/region) - HU (a szervezet bejegyzésének országa)

   A kitöltés után nyomjon Tovább (Next) gombot.



5. A következő ablakban a kriptográfiai szolgáltatót hagyja változatlanul, a bit hosszúságot állítsa legalább 2048-ra (minimum), majd nyomjon a tovább gombra.

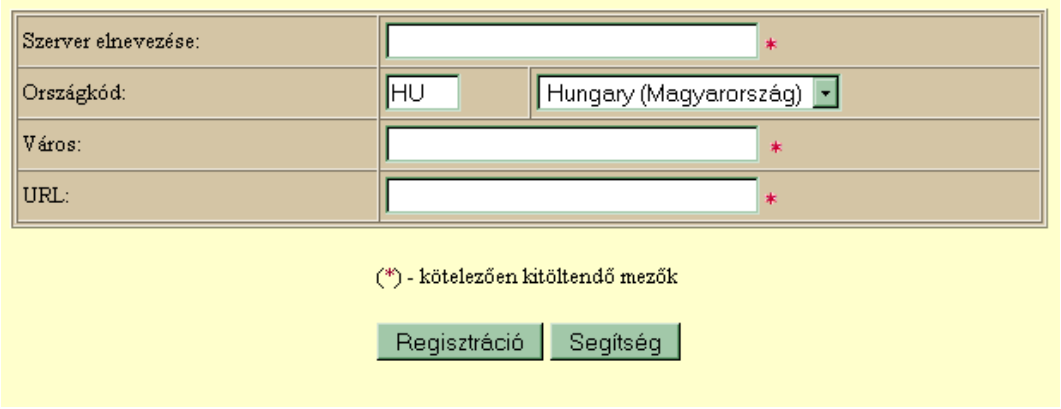
6. A következő ablakban a kérelem fájl tárolásának helyét és nevét kell megadnia. Ezt a fájlt kell majd kitallóznia, amikor feltölti a kérelmet rendszerünkbe. Ezután a Tovább (Next) gomb többszöri megnyomásával, majd a Befejezés (Finish) gomb megnyomásával a kérelem létrejön.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

9. 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 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.

1. 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.
2. 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.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

3. 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. Ezután nyomja meg a Tovább gombot.

4. A következő ablakban válassza ki a használni kívánt tanúsítványkiadót (példánkban „C” osztály) és a felhasználás célját, majd nyomjon a „Kérelem beadása” gombra.

5. 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).

10. Kiadott tanúsítvány telepítése

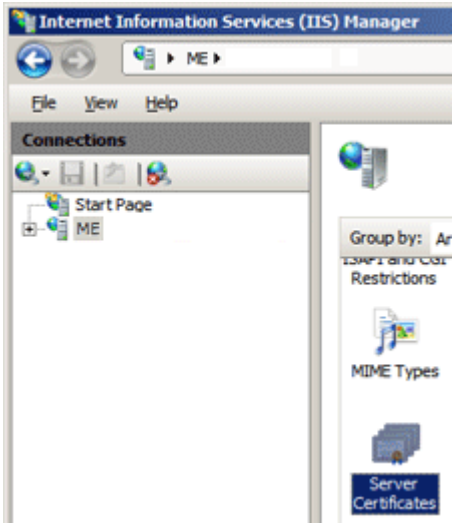
A tanúsítvány kiadása után értesítő levelet kap arról, hogy a tanúsítványa elkészült és letölthető.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

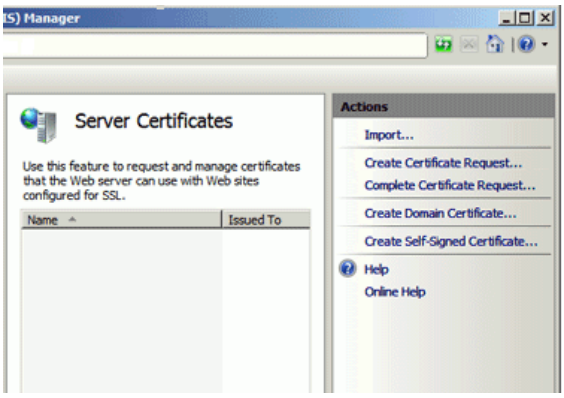
Ezt töltse is le szerverére, és tárolja olyan helyen, ahol könnyen megtalálja.

Ezután telepítheti szerverére, melynek lépései a következők:

1. Indítsa el az IIS konzolját, és válassza ki a website-ot, amihez a tanúsítványt el kezdte létrehozni.
   (Vezérlőpult > Felügyeleti eszközök > Internet Information Services Manager)
   (Vezérlőpult > Administrative tools > Internet Information Services Manager)



2. Jelölje ki a Kapcsolatok (Connections) oszlopban a website-ot, majd kattintson a Szerver tanúsítványok (Server certificates) menüpontra.
3. A megjelenő ablakban láthatók a meglévő tanúsítványok, illetve jobb oldalt a választható műveletek. Itt válasszuk ki a Tanúsítvány kérelem befejezése (Complete Certificate Request…) opciót.



4. Tallózza ki a korábban lementett tanúsítványt, és adjon meg egy Barátságos nevet (Friendly name), ami tetszőleges lehet. Ez a tanúsítvány könnyebb azonosítását szolgálja, nem része az SSL tanúsítványnak (javasolt a domain név megadása).

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

5. Kattintson az Ok gombra.
6. Előfordulhat, hogy bár ezen a szerveren generálta a tanúsítvány kérelmet, de a szerver "Cannot find the certificate request associated with this certificate file. A certificate request must be completed on the computer where it was created." vagy "ASN1 bad tag value met" hibaüzenetet adja.

   Ha ez az a szerver, amelyiken létrehozta a kérelmet, hagyja figyelmen kívül, a hibajelzés általában fals, a Server Certificates listába bekerül a tanúsítvány (F5-tel frissíthető a lista).

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

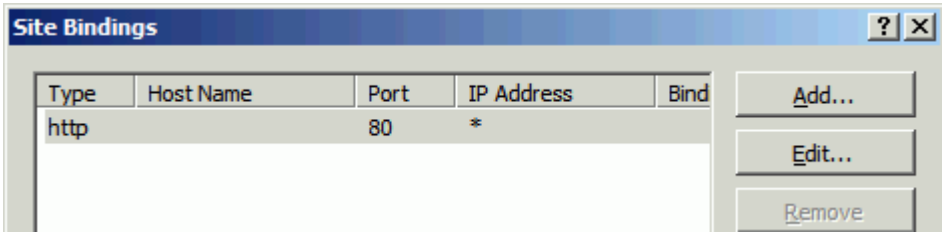
11. A telepített tanúsítvány összerendelése a site-tal

Telepítés után a tanúsítványt és a site-ot össze kell kapcsolnunk (bind).

Ennek lépései a következők:

1. Tallózza ki az IIS Managerben a Website-ot, majd válassza a Kötések (Bindings) opciót.

2. A megjelenő ablakban kattintson a Hozzáadás (Add) gombra.



3. A következő ablakban állítsa be a következő opciókat:
   - Típus (Type) – https
   - IP cím (IP address) – a site IP címe, vagy Minden nem hozzárendelt (All Unassigned)
   - Port – általában 443
   - SSL tanúsítvány (SSL certificate) – a korábban telepített tanúsítvány barátságos neve

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

12. A köztes kiadó tanúsítványának telepítése

SHA256 kiadók és az onlinessl.netlock.hu oldalról igényelt tanúsítvány esetében szükséges beállítani a szerveren a közbenső szintű (Intermediate) tanúsítványkiadót, mert azt a szervernek kell kiszolgálni a vonatkozó TLS szabvány alapján.

Ehhez az alábbi címekről le kell töltenie a következő 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

(Amennyiben úgy egyszerűbb, telepítheti az összeset, ez problémát nem okoz.)

A telepítés lépései:

1. Töltse le a köztes kiadó gyökértanúsítványát a szerverre.
2. Telepítse MMC-vel az „Intermediate Certification Authorities” tárolóba.
   (Ne felejtse el, hogy a Local Computer store -ba kell telepíteni. A függelék bemutatja az MMC használatát.)
3. A telepítés után szükség lehet az IIS újraindítására.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

13. OCSP Stapling

13.1. Mi az OCSP Stapling?

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

13.1.1. 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.

13.1.2. 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 ajánlott az OCSP Stapling beállítása!

13.2. 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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

13.3. 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.

13.3.1. 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

13.3.2. 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

13.3.3. 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

13.4. Az IIS 7 és későbbi szerver verziók beállítása

Figyelem!

Az IIS 7 szervernek a sikeres beállításhoz Windows 2008 vagy későbbi szerveren kell futnia, és alapesetben az OCSP Stapling bekapcsolt állapotú.

Az IIS esetében a következő lépések szükségesek:

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

1. A legfelső szintű tanúsítványok telepítése a szerverre.
2. A köztes kiadó tanúsítványok telepítése a szerverre.

A tanúsítványok telepítésének lépései gyökértanúsítványok esetén

(Arany, SHA1 Közjegyzői, SHA1 Üzleti, SHA1 Expressz esetében):

1. Töltse le a kiadó gyökértanúsítványát a szerverre.
2. Telepítse MMC-vel az „Trusted Root Certification Authorities" tárolóba.
   (Ne felejtse el, hogy a Local Computer store -ba kell telepíteni. A függelék bemutatja az MMC használatát.)
3. A telepítés után szükség lehet az IIS újraindítására.

A tanúsítványok telepítésének lépései köztes (intermediate) tanúsítványkiadók esetén

(SHA256 Közjegyzői, SHA256 Üzleti, SHA256 Expressz, SHA1 OnlineSSL, SHA256 OnlineSSL esetében):

1. Töltse le a köztes kiadó gyökértanúsítványát a szerverre.
2. Telepítse MMC-vel az „Intermediate Certification Authorities" tárolóba.
   (Ne felejtse el, hogy a Local Computer store-ba kell telepíteni. A függelék bemutatja az MMC használatát.)
3. A telepítés után szükség lehet az IIS újraindítására.

14. Függelék A – Regisztráció ügyfélmenübe

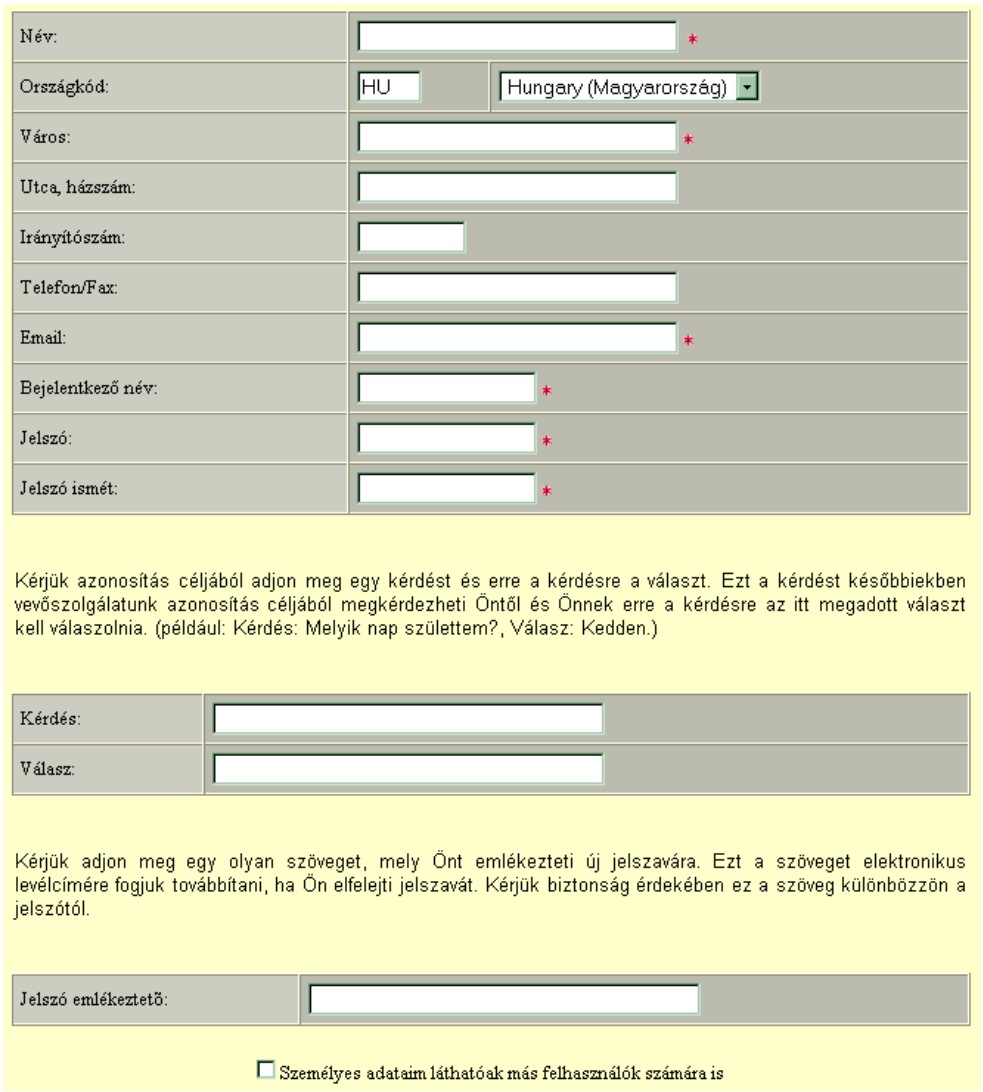
Ahhoz, hogy a felhasználó hozzáférhessen ügyfélmenüjéhez, előzetesen regisztrálnia kell.

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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

2. A megjelenő adatlapon töltse ki személyes adatait az igazolványainak (személyi igazolvány, lakcímkártya) megfelelő adatokkal (ahol ez értelmezhető).



A kitöltendő adatok a következők:

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

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

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.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

15. 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!

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

16. 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.

16.1. 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.

16.2. Bejelentkezés az ügyfélmenübe

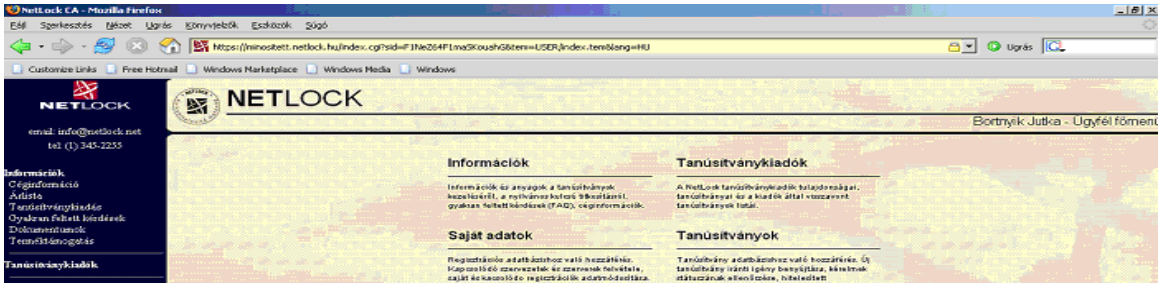
Az ügyfélmenübe bejelentkezni a www.netlock.hu oldalon tud.

A bejelentkező név és jelszó megadása után kattintson

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

Minősített tanúsítvány esetén (QA osztály) a „Bejelentkezés a minősített 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.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

16.3. A tanúsítvány felfüggesztése

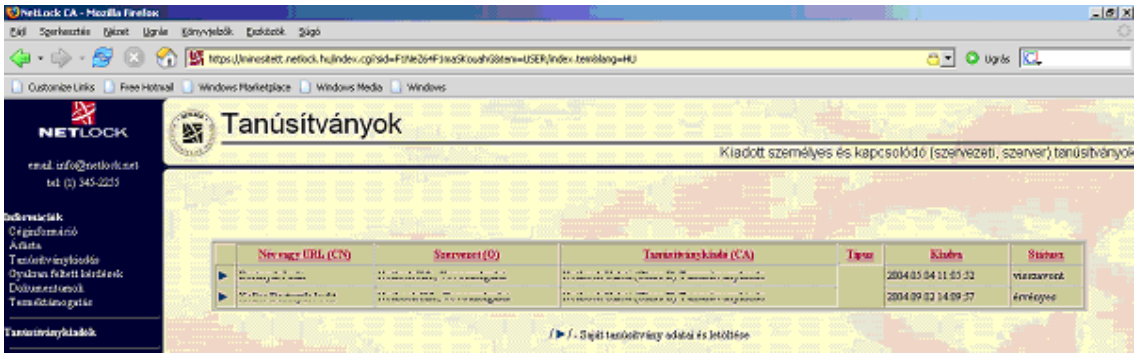
Elektronikus tanúsítványait - akárcsak bankkártyáját - gondosan kell kezelnie és őriznie, hiszen a tanúsítványával az Ön nevében végezhetnek elektronikus aláírást, és ez által az Ön nevében tehetnek joghatással bíró nyilatkozatot.

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 függesztetheti 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.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

16.3.1. 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 többet használni már nem lehet.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

16.4. 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 ügyfél menüjébe.
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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

16.4.1. 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.

Expressz tanúsítványkiadók esetén („C" osztály):

Küldje el aláírva, e-mailen szkennelve a kerelmek@netlock.hu címre vagy a NetLock Kft -hez faxon az (1) 700-1101-es számra

Üzleti tanúsítványkiadók esetén („B" osztály):

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, mely feláras. A díjszabásáról az alábbi oldalon tájékozódhat: http://www.netlock.hu/html/ar.html#opt

Közjegyzői tanúsítványkiadók esetén („A" osztály):

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.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

16.4.2. Megújított tanúsítványok letöltése

Amennyiben tanúsítványait megújította, és a tanúsítvány kiadásra került, az új tanúsítványok cserélendők az operációs rendszerben (szerveren).

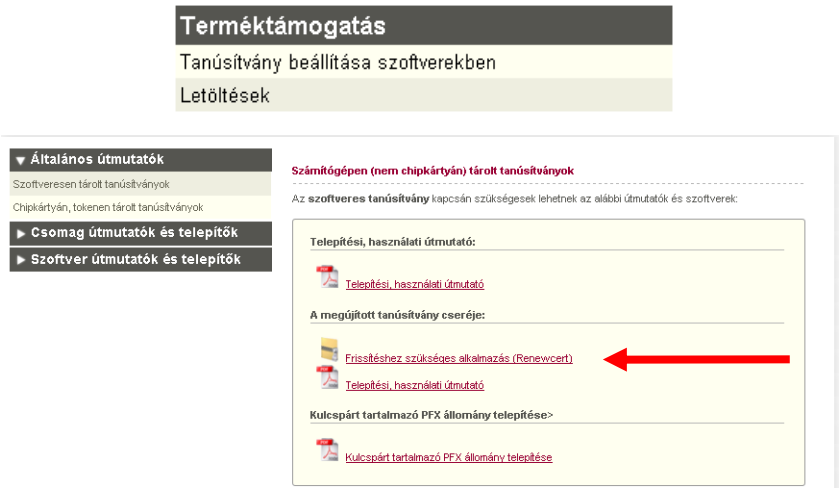
A megújított tanúsítvány kiadásáról e-mail értesítést fog kapni.

A kiadott tanúsítvány telepítésének feltétele, hogy a régi tanúsítvány a kulcsaival együtt megtalálható legyen a szerver tanúsítványtárában . Amennyiben nincs ott, telepítse a Függelék E fejezet alapján.

16.4.2.1. A régi tanúsítvány cseréje az újra

Ahhoz, hogy a régi tanúsítványt lecserélje az újra, szükséges lesz egy program letöltése a NetLock honlapjáról.

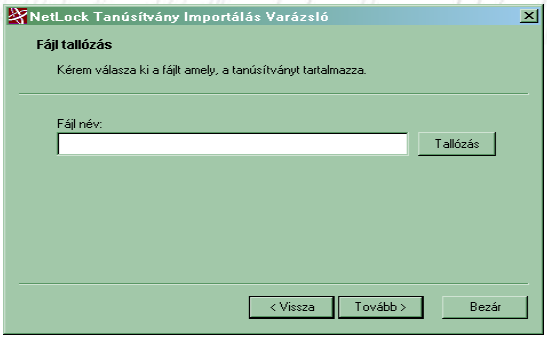
1. Indítson webböngészőt és látogasson el vele a www.netlock.hu oldalra.
2. A Terméktámogatás/Letöltések/Szoftveresen tárolt tanúsítványok menüpont alól töltse le a Renewcert programot



3. Lépjen be az Ügyfélmenüjébe, ahonnan mentse le a kiadott új tanúsítványt (CER állomány).
4. Indítsa el a Renewcert programot.
5. Az üdvözlőképernyőn kattintson a Tovább gombra.

   A megjelenő ablakban Tallózza ki a korábban a gépre letöltött új tanúsítványt (CER állomány)

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu



6. Kattintson a Tovább gombra és így az új tanúsítvány a régi kulcsok felett lecserélésre kerül.
7. A Befejezés gomb segítségével zárja be a Renewcert alkalmazást.
8. Ezután mindenképpen javasolt lementeni a már megújított tanúsítványt a kulcsaival együtt (lásd.: Függelék D - Biztonsági másolat készítése tanúsítványairól és kulcsairól MMC segítségével).

16.4.2.2. Tanúsítvány lecserélése szerveren

A tanúsítvány korábbiakban mutatott cseréje után, az IIS megfelelő site-ja esetén a site-hoz tartozó tanúsítványt újra ki kell választania.

Ennek lépései megegyeznek „A telepített tanúsítvány összerendelése a site-tal” fejezet alatt leírtakkal.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

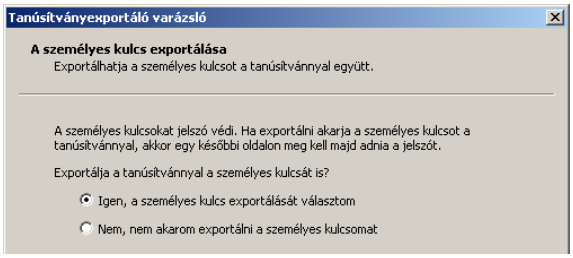
17. Függelék D – Biztonsági másolat készítése tanúsítványairól és kulcsairól MMC segítségével

Ha tanúsítványa fokozott biztonságú és NEM kriptográfiai eszközön kapta meg, akkor érdemes a tanúsítványáról PKCS#12 (*.pfx) állományban biztonsági másolatot készíteni, hiszen a számítógép sérülése, illetve újratelepítése után csak ebből tudja a tanúsítványt visszaállítani.

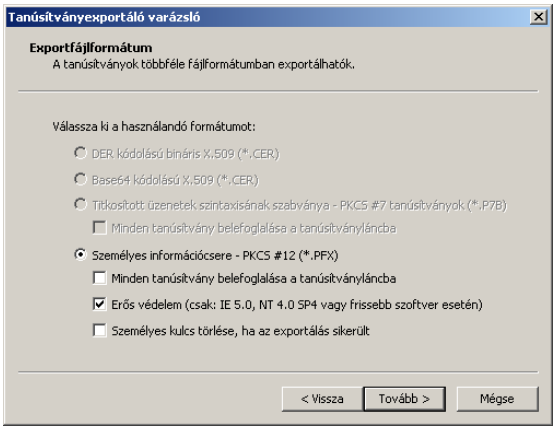
Megújítás esetén ezzel az eljárással tud az új tanúsítványról és régi kulcsairól PFX file-t készíteni.

1. A kulcs és tanúsítvány exportálásához indítsa el az MMC konzolt.
2. A Tanúsítványok -> Személyes tanúsítványok -> tanúsítvány (példánkban hiteles.hu), melyre jobb egér gombbal kattintva „Az összes feladat" választása és az „Exportálás" kijelölése után lehet elindítani az exportálást.

3. A megjelenő tanúsítvány exportáló varázsló üdvözlő képernyőjén nyomja meg a Tovább (Next) gombot.



4. A következő ablakban válassza a privát kulcs exportálását is (Yes, export the private...), majd kattintson a Tovább (Next) gombra.
5. A következő ablakban a második rádiógombhoz tartozó szekció érhető csak el. Itt állítson be Erős titkosítást (Enable strong protection). Ha szüksége van arra, hogy a tanúsítvánnyal együtt a hozzá tartozó gyökértanúsítványt is exportálja, akkor jelölje ki a Minden tanúsítvány exportálása opciót (Include all certificates...) is. Ha a privát kulcsot törölni akarja az exportálás után erről a gépről, akkor jelölje be a privát kulcs törlése (Delete the Private...) opciót is.



6. A következő ablakban adja meg kétszer azt a jelszót, amelyet a fájlnak szeretne adni. Ezt jegyezze meg jól, mert ennek ismeretében tudja telepíteni egy másik gépen a tanúsítványát.
7. A következő ablakban kiválaszthatjuk a fájlnevet és a helyet, ahol a fájlt létre szeretnénk hozni.
8. Miután ezt beállította, már csak a Tovább (Next) és végül a Befejezés (Finish) gombot kell megnyomnia, valamint a megnyitott ablakokat OK gombbal bezárnia.

   A tanúsítvány exportálása ezzel megtörtént.

   Ezt az állományt érdemes biztonságos helyen (valamilyen adathordozón) elzárni.

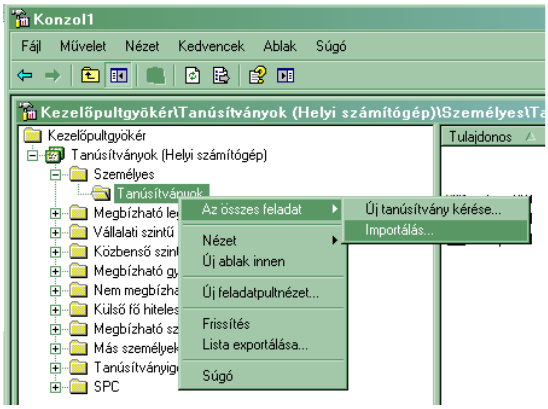
NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

18. Függelék E – PKCS12 (PFX) fájlban található tanúsítvány telepítése Windows tanúsítványtárba MMC segítségével

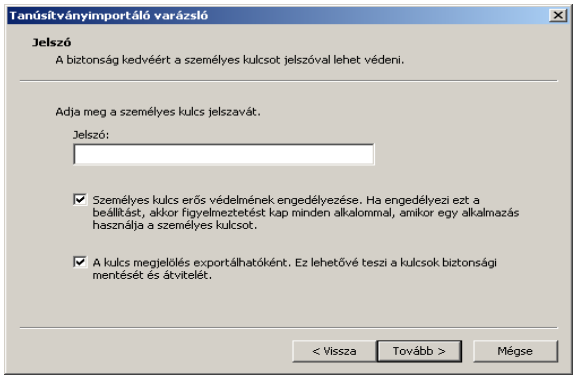
A tanúsítványairól és kulcsairól készült PKCS#12 (.pfx) formátumú mentett állomány segítségével tudja tanúsítványát mentésből telepíteni.

A szerver tanúsítványtárába a tanúsítvány és kulcs importálásának folyamata a következő:

1. Indítsa el az MMC konzolt, amely a Tanúsítványokat helyi számítógépen kezeli (létrehozást lásd.: Függelék F)
2. A Személyes tanúsítványok menüpontra jobb egérrel kattintva „Az összes feladat" (All tasks), majd az „Importálás" (Import) menü választásával tudja kezdeményezni a tanúsítvány feltöltését.
3. A következő ablakban ki tudja tallózni a PFX file-t.



4. Az üdvözlő képernyőn nyomja meg a Tovább (Next) gombot.
5. A második képernyőn az importálandó fájl nevét látja. Itt nincs semmi teendő, lépjen tovább a Tovább (Next) gomb segítségével.



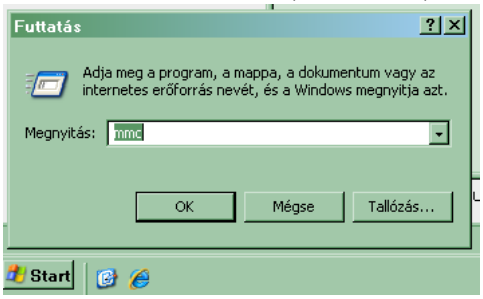
6. A következő képernyőn adja meg a PKCS#12 fájlhoz tartozó jelszót. Itt állíthatja be a tanúsítvány erős védelmét és későbbi exportálhatóságát. Javasoljuk mindkét opciót kipipálni és ezután a Tovább (Next) gombot megnyomni.
7. A következő képernyő megkérdezi, hogy automatikus vagy kézzel történő elhelyezést kíván a megfelelő tanúsítványtárolóban. Itt válassza az Automatikus kiválasztást (Automatically...), majd kattintson a Tovább (Next) gombra.
8. Az utolsó képernyőn kattintson a Befejezés (Finish) gombra.

A tanúsítvány telepítése ezzel megtörtént.

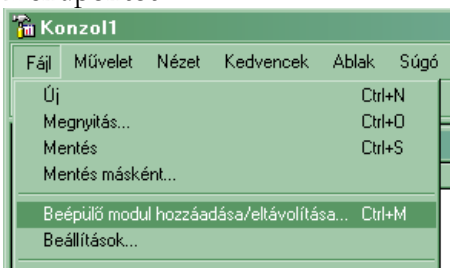
NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

19. Függelék F – Tanúsítvány kezeléséhez MMC konzol létrehozása, mentése

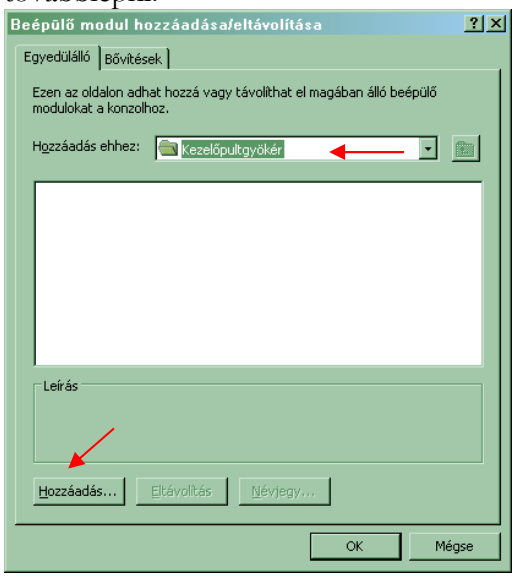
1. Indítsa el a Start menü / Futtatás / MMC parancsot.



2. A megjelenő konzolon a File menüből válassza a Beépülő modul hozzáadása/eltávolítása menüpontot.

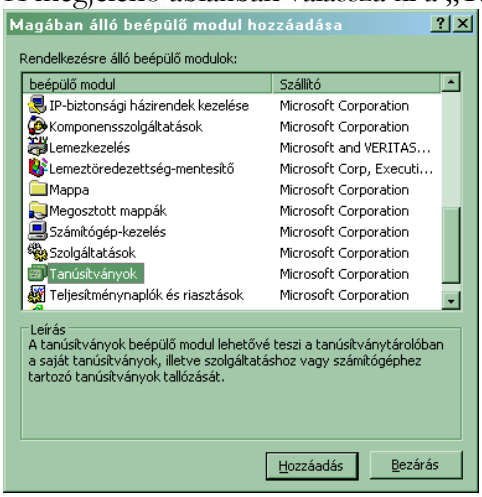


3. A következő ablakban a Kezelőpultgyökér -hez a Hozzáad… gomb megnyomásával kell továbblépni.

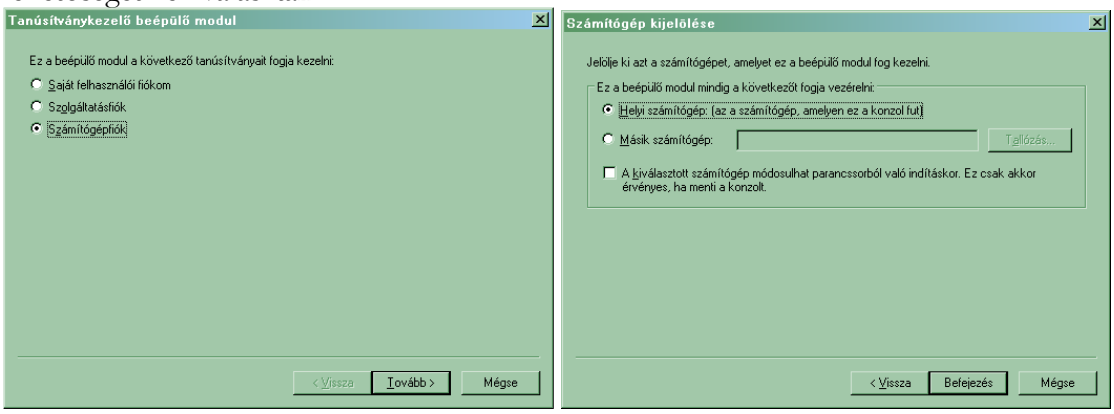


NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

4. A megjelenő ablakban válassza ki a „Tanúsítványok” lehetőséget.



5. A megjelenő ablakban ezután a Számítógépfiók lehetőséget,majd a Helyi számítógép lehetőséget kell választani.

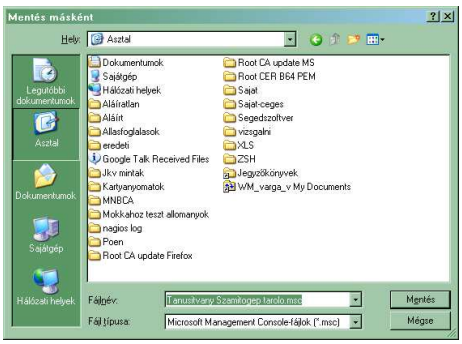


6. Ezt követően kattintson a Befejezés (Finish) gombra az ablak bezárásához.

Mentse el a létrejött panelt alábbi lépések szerint.

1. Válassza a File / Mentés másként, majd adja meg a helyet, ahova menteni kívánja a konzolt.

2. Ezt követően az új ikonnal bármikor újraindíthatjuk a konzolt



NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

20. Függelék G – Tanúsítvány helyreállítása IIS szerveren

Amennyiben egy tanúsítvány üzemelése mellett igényelt tanúsítvány, és az üzemelő site visszakapcsolásával a kérelemhez tartozó kulcs eltűnt, az alábbi eljárással tudja visszaállítani az elveszett kulcsokat.

20.1. Az IIS tanúsítványkezelése

Abban az esetben, ha az Ön IIS szerverén fut egy website, és új kérelmet generál, az aktuális site működése felfüggesztődik.

Amennyiben az aktuális site-ot visszaállította, az IIS a kulcsot „eltünteti”.

Ennek megkerülésére lehetőség van a generálásokról szóló útmutató leírásait követve (6. fejezet), azonban ha bekövetkezett a baj, a következő lépések alapján helyre tudja állítani az új tanúsítványhoz tartozó kulcsokat.

20.1.1. A lépések:

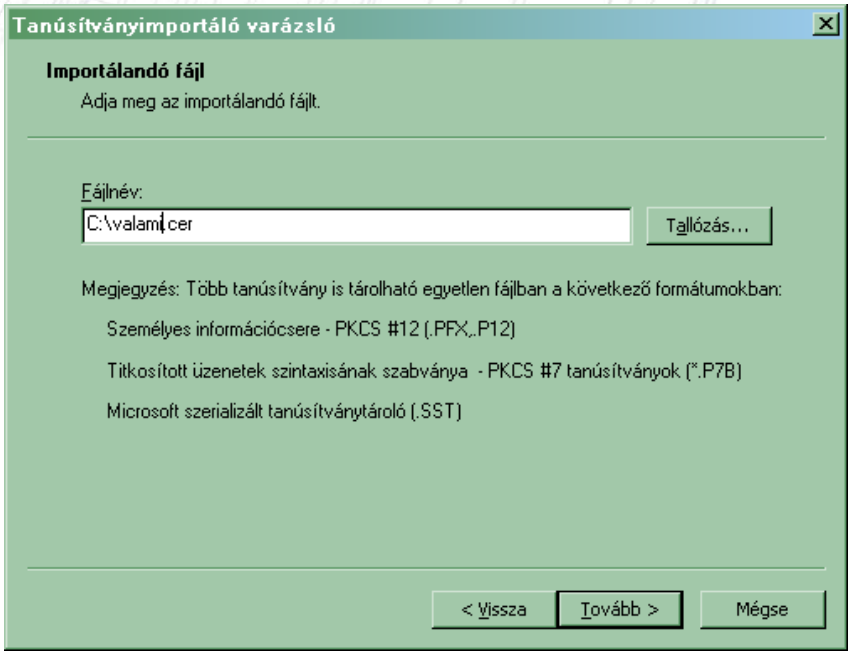
1. Indítson MMC-t és menjen a Tanúsítvány beépülő modul Local Computer tárolójába.

   (Az MMC beállítását az F függelékben tekintheti meg.)

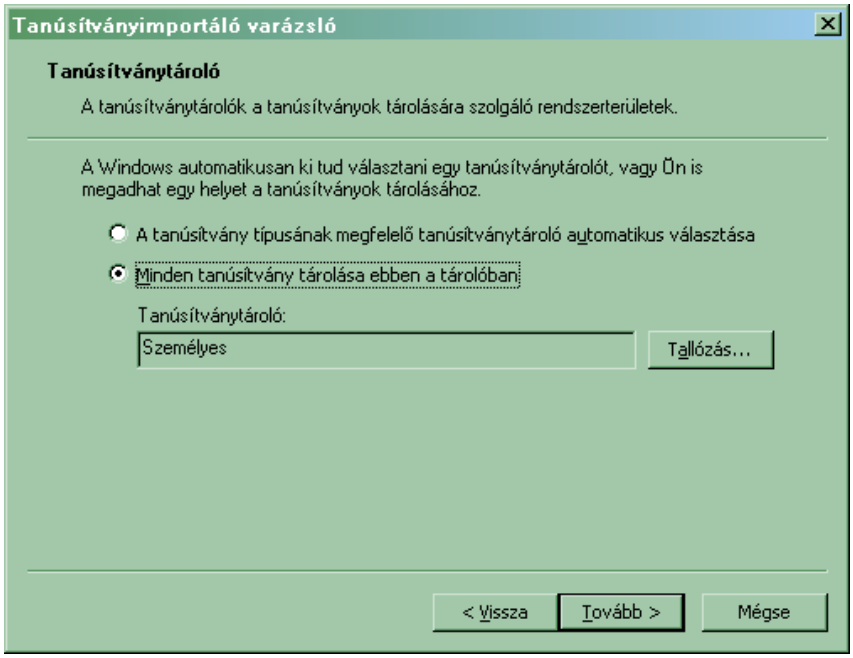
2. Az itt található Személyes mappán (Personal) válassza Az összes feladat (All tasks) majd Import menüpontokat.

3. Az importálás során tallózza ki a kapott tanúsítványt, majd nyomjon Tovább (Next) gombra.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

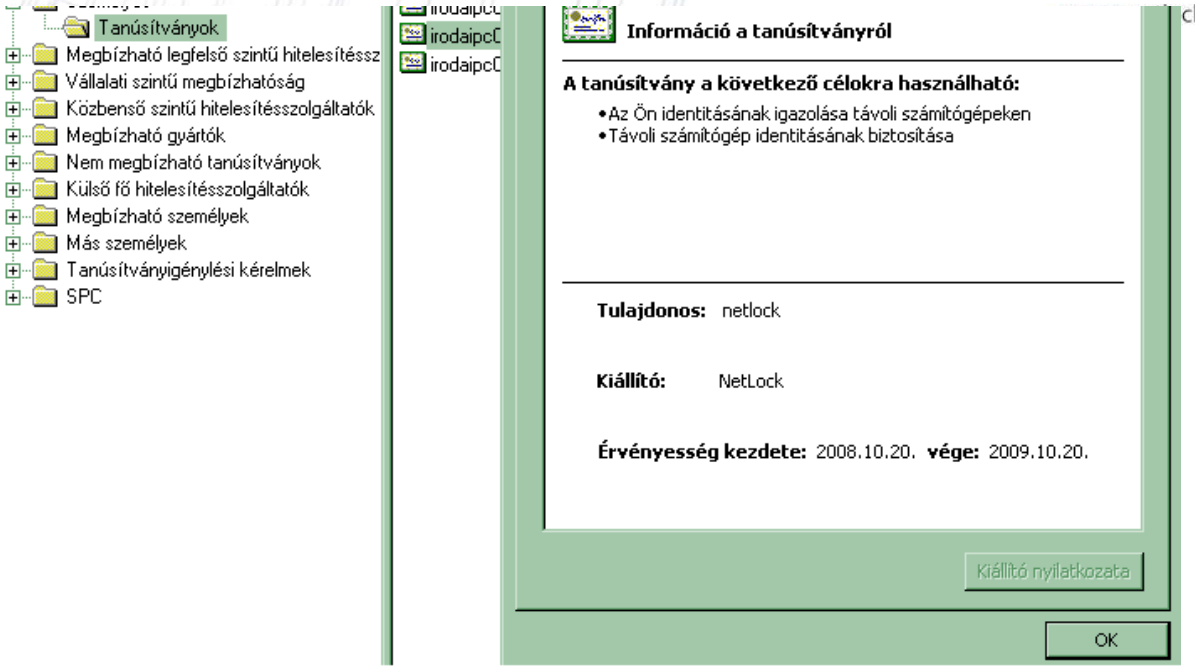


4. A tároló választása során a kézi kiválasztás (Minden tanúsítvány tárolása…) és a Személyes (Personal) tároló legyen kiválasztva. Szükség esetén ezt tallózza be (Browse).



5. Ezek után válassza az alapértelmezett opciókat, amíg a tanúsítvány nem települ.
6. A tanúsítvány bekerül a tárolóba, azonban duplán kattintva rajta nem jelzi az adatlap, hogy van hozzá privát kulcs.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu



7. A tanúsítvány ablakban váltsunk át a Részletek fülre, keressük meg a sorozatszámot, majd célszerűen másoljuk vágólapra.
8. Indítsunk parancssort és adjuk meg a következő parancsot:

   certutil -repairstore my "<sorozatszám>"
9. A parancs megadása után a kulcs javítása megtörténik. A tanúsítvány adatlapját kitallózva már látszódnia kell a hozzá tartozó privát kulcsnak, illetve a website beállításai között lehetségessé válik a tanúsítvány kiválasztása.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

21. Függelék H – UCC tanúsítvány nem adható belső névre

A belső, nem FQDN névre szóló név elhelyezése a tanúsítványban biztonsági okok miatt nem engedélyezett.

Az ilyen tanúsítványok MITM (Man-in-the-middle) támadásokat tesznek lehetővé saját és más hálózatokban is, mert a tanúsítványban tárolt több név közül bármelyik egyezősége esetén a hitelesség elfogadottnak tekinthető.

Egy ilyen támadás a következőképpen kivitelezhető:

Amennyiben a cél az Önök elleni támadás:

1. A hitelesítés szolgáltató kiad egy FQDN-t és nem FQDN-t is tartalmazó tanúsítványt.
2. A támadó fél a külső tanúsítványt megismerve, az abban található adatok alapján tanúsítványt igényel, melyből megismeri a belső nevet.
3. A támadó a hitelesítés szolgáltató felé bead egy hitelesítési kérést egy saját domain névre, melyben egy nem FQDN-re szóló név is megtalálható. Ez a belső név megegyezik a korábban kiadott tanúsítványban található belső névvel.
4. A kiadó a támadó tanúsítványát kiadja, a belső nevet nem vizsgálva, hiszen a támadó jogosult a saját domain nevére.
5. A támadó a hálózatba, belső oldalra bejutva a saját tanúsítványát a szervere hitelesítésére használja, a forgalmat eltéríti, miközben tanúsítványa belső nevek miatt hitelesnek látszik.

Amennyiben a cél másik szervezet:

A megkapott tanúsítvány más szervezetnél - amennyiben van egyező név - felhasználható MITM támadás kivitelezésére.

A fentiek miatt - biztonsági okokból - nem javasolt egy hálózatban, hogy egy belülről és kívülről is elérhető szerver kétféle néven is elérhető legyen. Biztonsági okból nem adható olyan tanúsítvány, amely a két nevet tartalmazza.

A belső neves elérés megtartása esetén érdemes a belső névhez hozzárendelni egy A rekordot a belső DNS kiszolgálóban, mely a külső névre mutat, vagy az AD tartomány átnevezése lehet még megoldás.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu