

Tanúsítvány létrehozása IIS 5.0+ szerverhez

IIS 5.0 szerveren kérelem létrehozása, tanúsítványkérelem beadása,
kiadott tanúsítvány telepítése és megújított tanúsítvány cseréje

1. Tartalomjegyzék

1.	Tartalomjegyzék.....	2
2.	Bevezető	4
3.	A dokumentációról	4
4.	Korlátozások.....	4
5.	UCC tanúsítványok.....	5
6.	IIS szerverhez kapcsolódó hotfix Windows XP és Windows 2003 szervereken.....	5
7.	Előzetes követelmények – néhány döntés, amit meg kell hozni	6
7.1.	A tanúsítványkiadás algoritmusa, a kiadó típusa	6
7.2.	Az SSL tanúsítvány profilja.....	6
8.	Teendő, ha ez egy jelenleg is működő szerver	8
8.1.	Az új site létrehozásának lépései	8
8.2.	Az új site kezelése a tanúsítvány kiadását követően	9
9.	Tanúsítvány kérelem létrehozása a szerveren.....	10
10.	Tanúsítvány kérelem beadása	15
7.	Kiadott tanúsítvány telepítése.....	16
8.	A köztes kiadó tanúsítványának telepítése.....	18
7.	Függelék A – Regisztráció ügyfélmenübe.....	19
11.	Függelék B – Belépési nyilatkozat készítése	21
12.	Függelék C – Tanúsítvánnyal kapcsolatos ügyintézés.....	22
12.1.	Az ügyfélmenü használata.....	22
12.2.	Bejelentkezés az ügyfélmenübe	22
12.3.	A tanúsítvány felfüggesztése	23
12.3.1.	Felfüggesztéssel kapcsolatos fontos információk.....	23
12.4.	A tanúsítvány megújítása.....	25
12.4.1.	Teendők a Belépési nyilatkozattal	26
12.4.2.	Megújított tanúsítványok letöltése	27
12.4.2.1.	A régi tanúsítvány cseréje az újra	27
12.4.2.2.	Tanúsítvány lecserélése szerveren.....	28

13.	Függelék D – Biztonsági másolat készítése tanúsítványairól és kulcsairól MMC segítségével	30
14.	Függelék E – PKCS12 (PFX) fájlban található tanúsítvány telepítése Windows tanúsítványtárba MMC segítségével.....	32
15.	Függelék F – Tanúsítvány kezeléséhez MMC konzol létrehozása, mentése	33
16.	Függelék G – Tanúsítvány helyreállítása IIS szerveren	35
16.1.	Az IIS tanúsítványkezelése.....	35
16.1.1.	A lépések:.....	35
17.	Függelék H – UCC tanúsítvány nem adható belső névre	38

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 (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 5 verzió alapján készült, de a dokumentáció alapján későbbi verziókkal is elvégezhető a tanúsítvány generálás folyamata.

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 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 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 hasznossága megkérdőjelezhető.

5. UCC tanúsítványok

Az Exchange 2007 és Office Communication Server 2007 termékek és későbbi verzióik UCC profilt igényelnek, melyek generálása eltérő a leírásban szereplőhöz képest. Az eljárásról egy másik útmutatóban olvashat.

Figyelem!

Korlátozás: belső névre UC tanúsítvány nem adható, mivel támadási felületet biztosít (részleteket lásd Függelék H)

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 az SHA256 algoritmus használatának alapfeltétele kliens oldali használat szempontjából.)

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&kbld=en-us>

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 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.

7.2. 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. Teendő, ha ez egy jelenleg is működő szerver

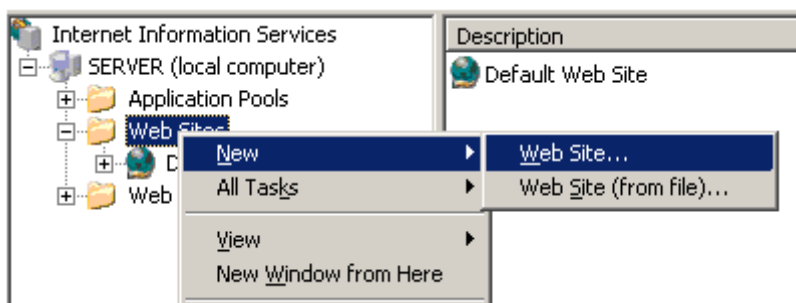
Figyelem!

Amennyiben a szerveren, amihez tanúsítványt igényel, már van működő SSL szerver és hozzá való tanúsítvány (legyen az akármilyen), amelyet a kiadás időtartama alatt is üzemeltetni kívánnak (tehát a kérelem beadása után visszakapcsolnának oda), abban az esetben a tanúsítvány igényét kezdje egy új site létrehozásával, majd annál hajtsa végre az alább következő lépéseket.

8.1. Az új site létrehozásának lépései

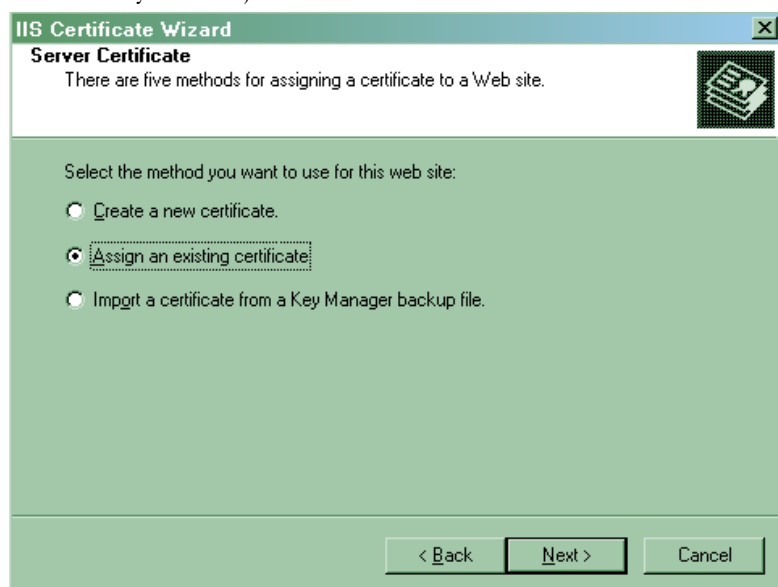
Kattintunk a WEB Sites fülön jobb egér gombbal, és válasszuk a new > new website (új > Új website) lehetőséget.

Ezek után ki kell tölteni az adatokat, majd létrejön az új site.



8.2. Az új site kezelése a tanúsítvány kiadását követően

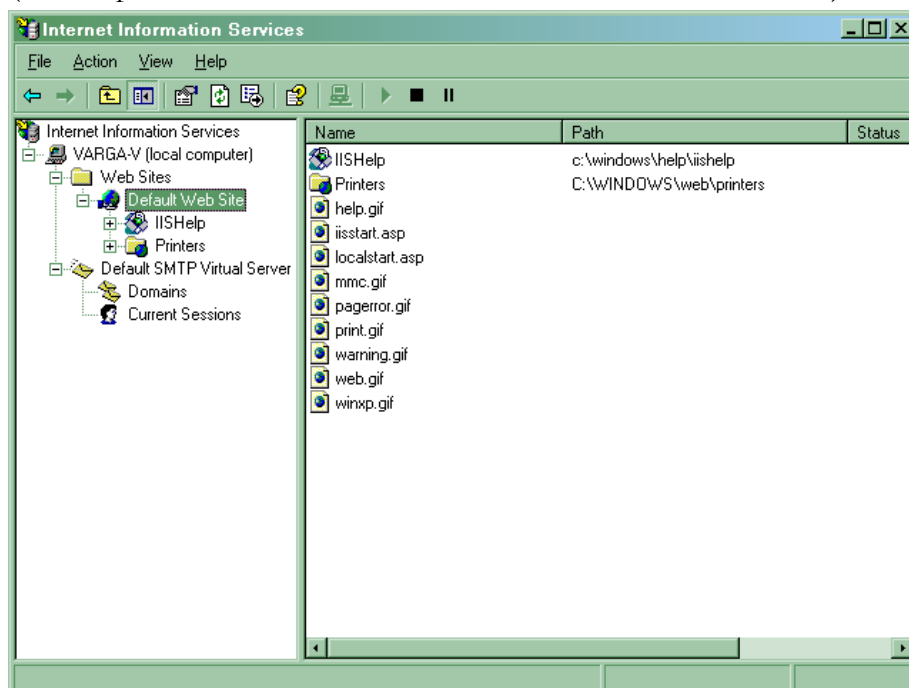
A tanúsítványt kiadása után a töltsse fel azt a szerverre az igényléshez létrehozott site alá, majd az éles site-nál a Directory > Server Certificate > Assign an existing certificate opciójával a tanúsítványt rendelje hozzá az éles site-hoz.



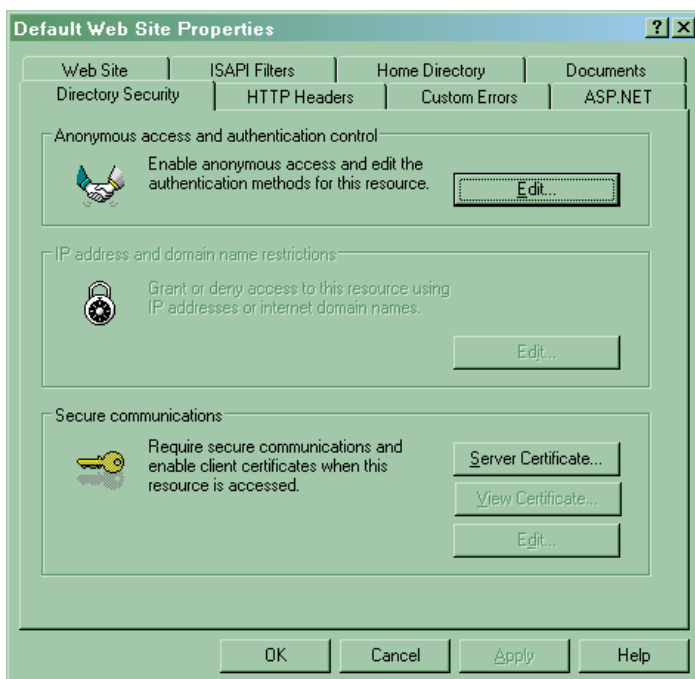
9. Tanúsítvány kérelem létrehozása a szerveren

A kérelem létrehozásának lépései a következők:

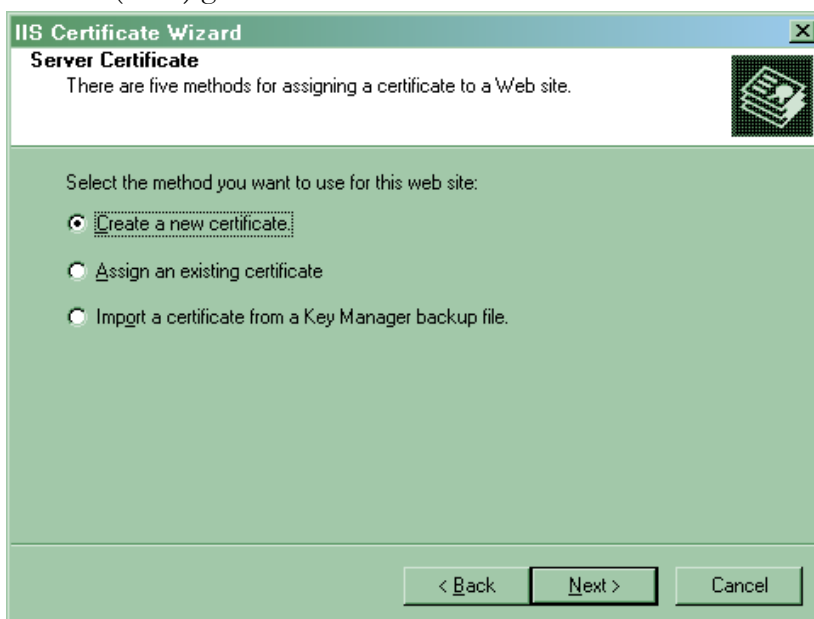
1. Indítsa el az IIS konzolját, és válasza ki a website-ot, amihez a tanúsítványt szeretné létrehozni. (Vezérlőpult > Felügyeleti eszközök > Internet information Server)
(Vezérlőpult > Administrative tools > Internet information Server)



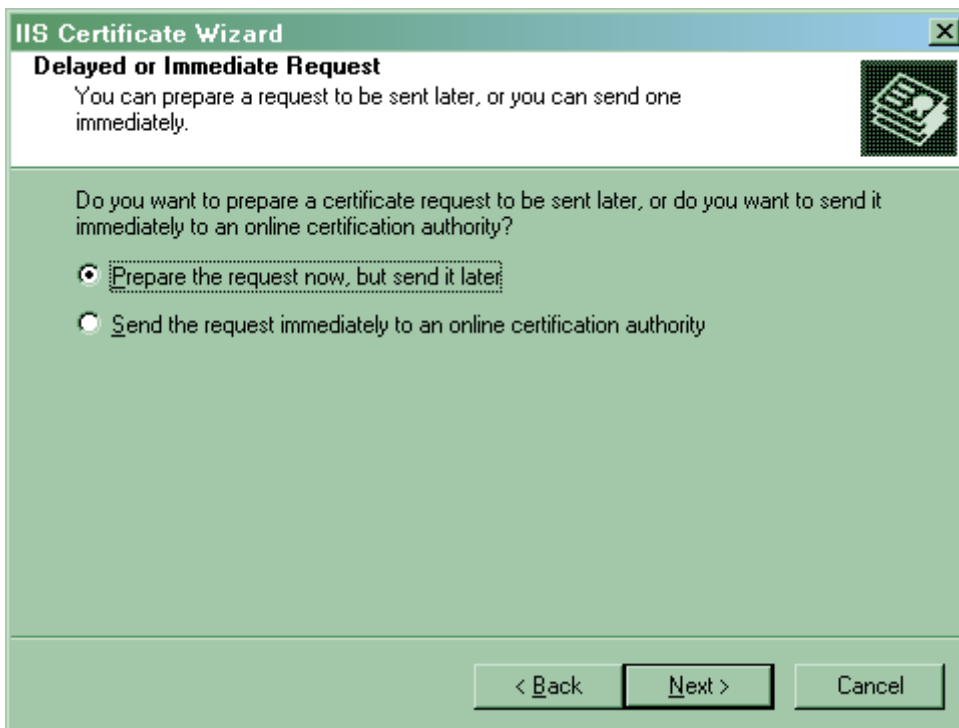
2. Jelölje ki a website-ot, kattintson rajta jobb gombbal, majd válassza ki a Properties (Tulajdonságok) opciót.
3. A Directory fülön kattintson a Server Certificate gombra, és a varázsló elindul.



4. Válassza a Create a New Certificate opciót (Új tanúsítvány készítése), majd nyomjon Tovább (Next) gombot.



5. A következő ablakban válasszuk a kérelem létrehozása most, küldése később opciót.
(Prepare the request...)



IIS Certificate Wizard

Delayed or Immediate Request

You can prepare a request to be sent later, or you can send one immediately.

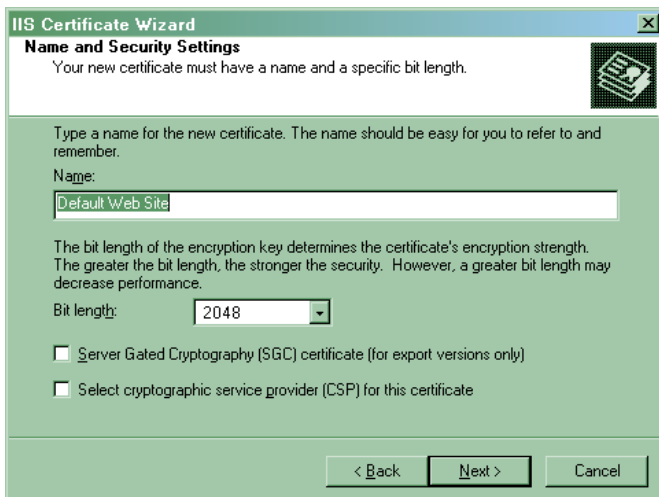
Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

☒ Prepare the request now, but send it later

☐ Send the request immediately to an online certification authority

< Back Next > Cancel

6. A következő ablakban a kulchossz legyen minimum 2048 bites, a többi opció alapértelmezésen hagyható, majd nyomjon Tovább (Next) gombot.



IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name:

Default Web Site

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length: 2048

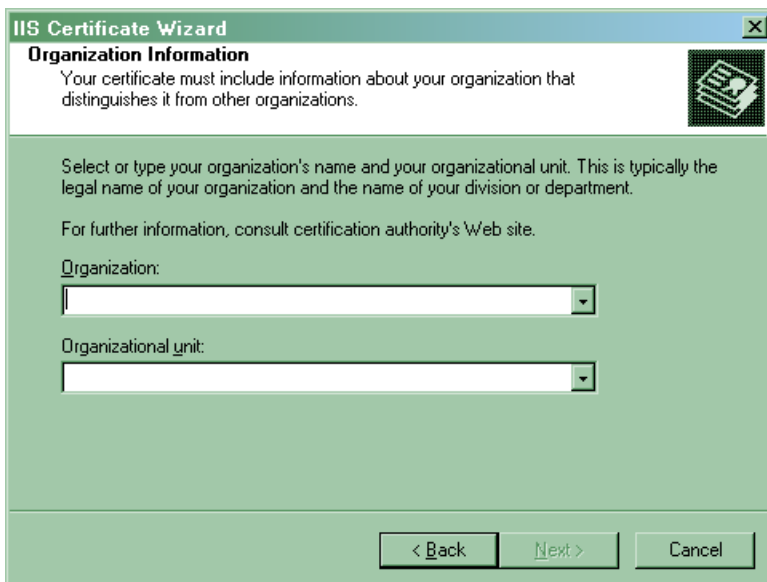
☐ Server Gated Cryptography (SGC) certificate (for export versions only)

☐ Select cryptographic service provider (CSP) for this certificate

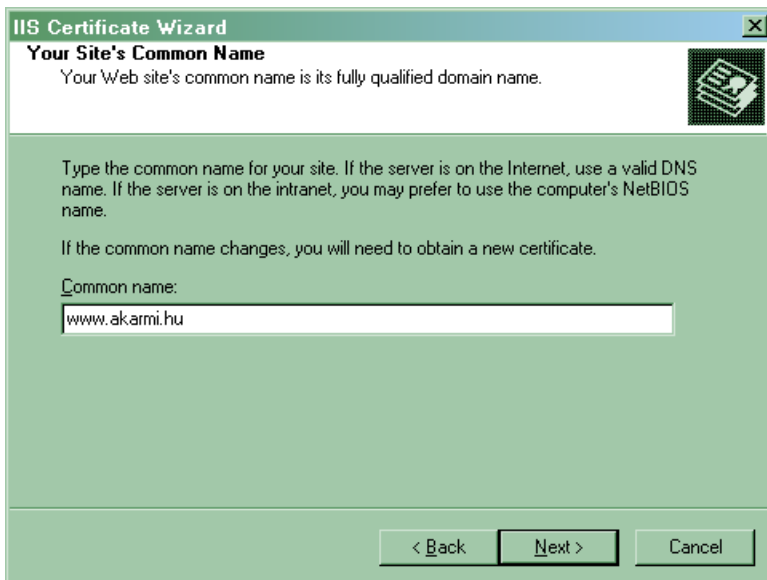
< Back Next > Cancel

7. A következő ablakban töltsé ki a szervezet nevét és a szervezeti egységet.

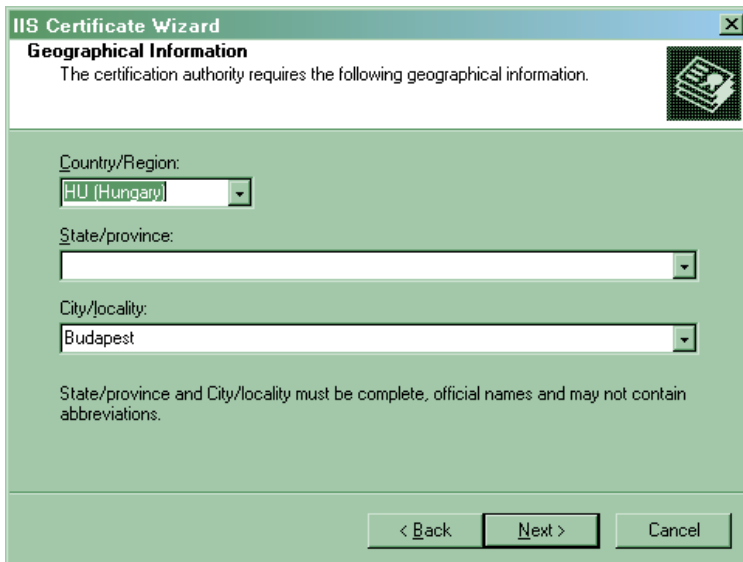
A szervezet nevének cégkivonatban megtalálható hosszú vagy rövid névvel kell egyeznie, (a szervezeti egységként megadható a szervezetnél található egység.), majd nyomjon Tovább (Next) gombot.



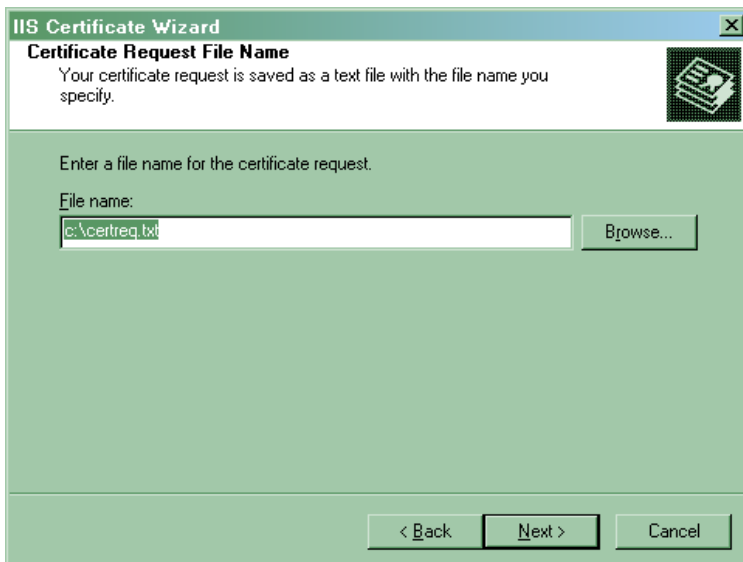
8. A következő ablakban adja meg a szerver URL címét. (https:// nélkül), majd nyomjon Tovább (Next) gombot.



9. A következő ablakban töltsé ki az Országkód (Country/Region) (HU), és a Város (City/Locality) mezőt. A mezőket a cégkivonat alapján kell kitölteni. (A State/province mezőbe megye írható, opcionális nem szükséges kitölteni.) Ezután nyomjon Tovább (Next) gombot.



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



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 szervert regisztrációja gombot. A megjelenő ablakban töltsen ki az adatokat a következő táblázatnak megfelelően.

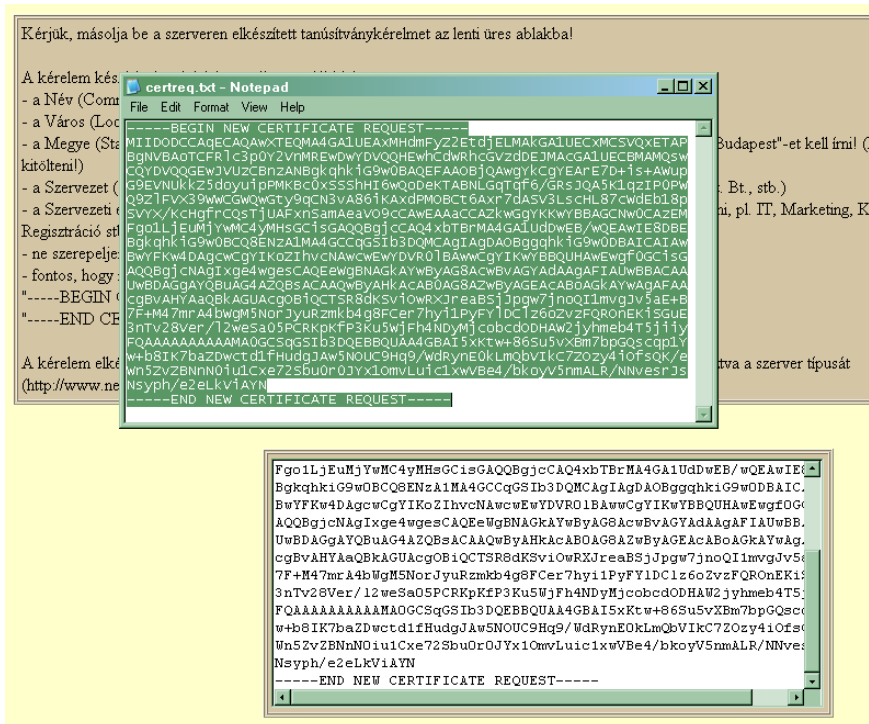
Szerver elnevezése:	<input type="text"/>	*
Országkód:	<input type="text" value="HU"/>	<input type="text" value="Hungary (Magyarország)"/>
Város:	<input type="text"/>	*
URL:	<input type="text"/>	*

(*) - kötelezően kitöltendő mezők

Szerver elnevezése	Szerver elnevezése, valamilyen beszédes név
Országkód	A személy vagy szervezet igazolt székhelye/lakhelye alapján (cégkivonat, lakcímkártya) Cég számára beszerzendő tanúsítvány esetén 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.

- 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.



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

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

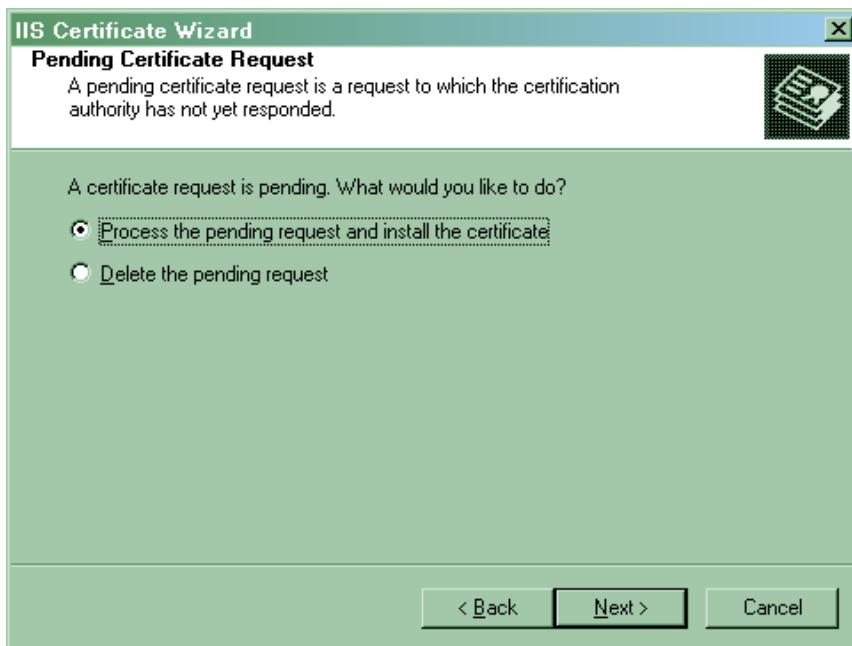
Kérelem beadása

- 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.)

7. Kiadott tanúsítvány telepítése

A tanúsítvány kiadása után értesítő levelet kap arról, hogy a tanúsítványa elkészült, és letölthető. Ezt utána telepítheti szerverére, melynek lépései a következők:

1. Navigáljon el a már ismert Server Certificate menüpontra, majd megjelenő ablakban a folyamatban lévő tanúsítványkérelem folytatása opciót válassza. (Process the pending...)



2. Ezután tallózza ki a lementett állományt, majd nyomjon a Tovább (Next) gombra.
3. Az összes további teendő a Tovább (Next) és Befejezés (Finish) gomb megnyomása.

Ezzel az SSL tanúsítvány telepítésre került.

8. 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 le kell töltenie a következő kiadói tanúsítványok egyikét az alábbi címekről:

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 az úgy egyszerűbb, telepítheti az összeset, problémát nem okoz egy felesleges tanúsítvány.)

A telepítés lépései:

4. Töltse le a köztes kiadó gyökértanúsítványát a szerverre.
5. 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.)
6. A telepítés után az IIS újraindítására lehet szüksége.

7. 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 tölts 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) ▾	
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 levélcímére 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, 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.

11. 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!!!

12. 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.

12.1. 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.

12.2. 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) 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 baloldalon és középen is megtalálható menüpontok közül választhat.



12.3. A tanúsítvány felfüggesztése

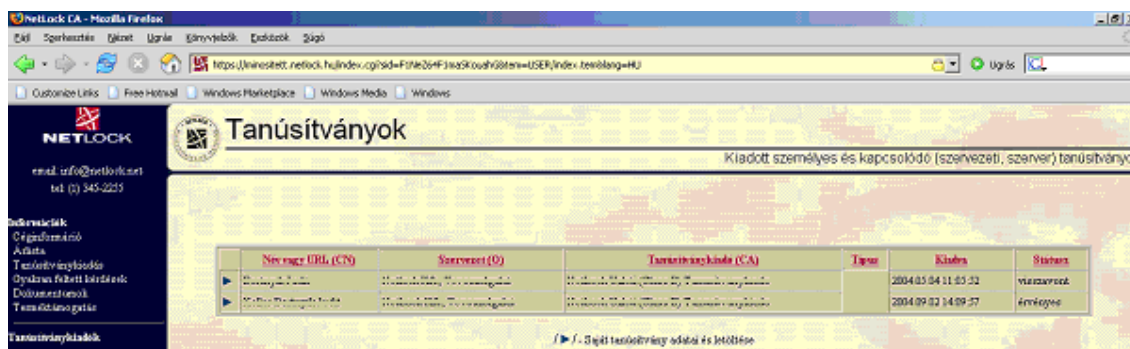
Elektronikus tanúsítványait, akár csak bankkártyáját, gondosan kell kezelnie és őriznie, hiszen a tanúsítványával az Ön nevében végezhetnek elektronikus aláírást, és ez által az Ön nevében tehetnek joghatással bíró nyilatkozatot.

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

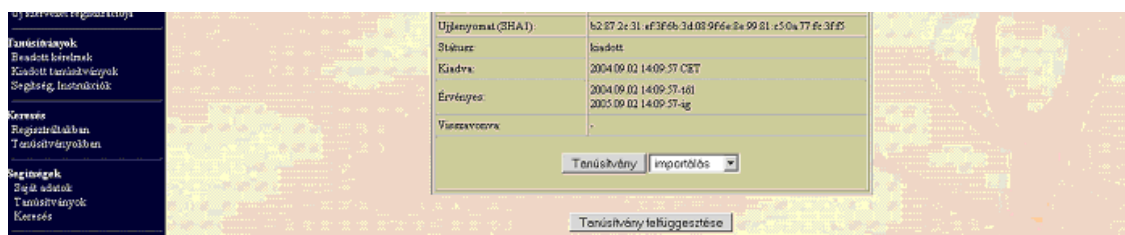
Ha nem tud minden kétséget kizáróan meggyőződni arról, hogy időközben a magánkulcsot nem használta illetéktelen személy, intézkedjen a tanúsítvány végleges visszavonásáról. A felfüggesztési, visszavonási lépéseket a NetLock Kft. Szolgáltatási Szabályzatában szereplő módon (Internetes ügyfélmenün keresztül,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

A.) Interneten keresztül a következő módon 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.

12.3.1. 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.

12.4. 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.

12.4.1. 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 +36 1 700-2828-as számra, illetve e-mailen szkennelve a kerelmek@netlock.hu címre.

Fokozott biztonságú „B” osztályú tanúsítvány 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.

Fokozott biztonságú „A” osztályú tanúsítvány esetén:

A Belépési nyilatkozatott 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 nyilatkozatott 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.)

12.4.2. Megújított tanúsítványok letöltése

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

A megújított tanúsítvány kiadásáról e-mail értesítést fog kapni.

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

12.4.2.1. A régi tanúsítvány cseréje az újra

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

1. Látogasson el a www.netlock.hu oldalra
2. A Terméktámogatás/Letöltések menüpont alól töltsse le a Renewcert programot

Terméktámogatás

Tanúsítvány beállítása szoftverekben

Letöltések

Szoftver útmutatók és telepítők

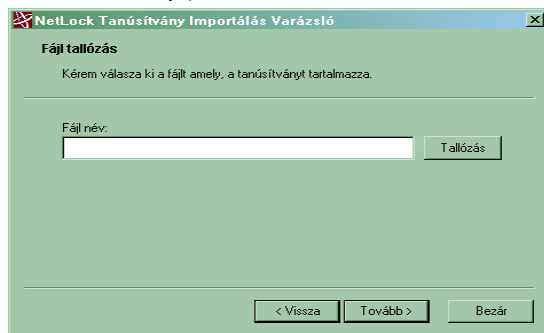
[MOKKA hitelesítő szoftver](#)

[PDFSigno PDF hitelesítő szoftver](#)

[Renewcert](#)

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

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



6. Kattintson a Tovább gombra, és az új tanúsítvány a régi kulcsok felett lecserélésre kerül.
7. A Befejezés gomb segítségével zárja be a Renewcert alkalmazást.

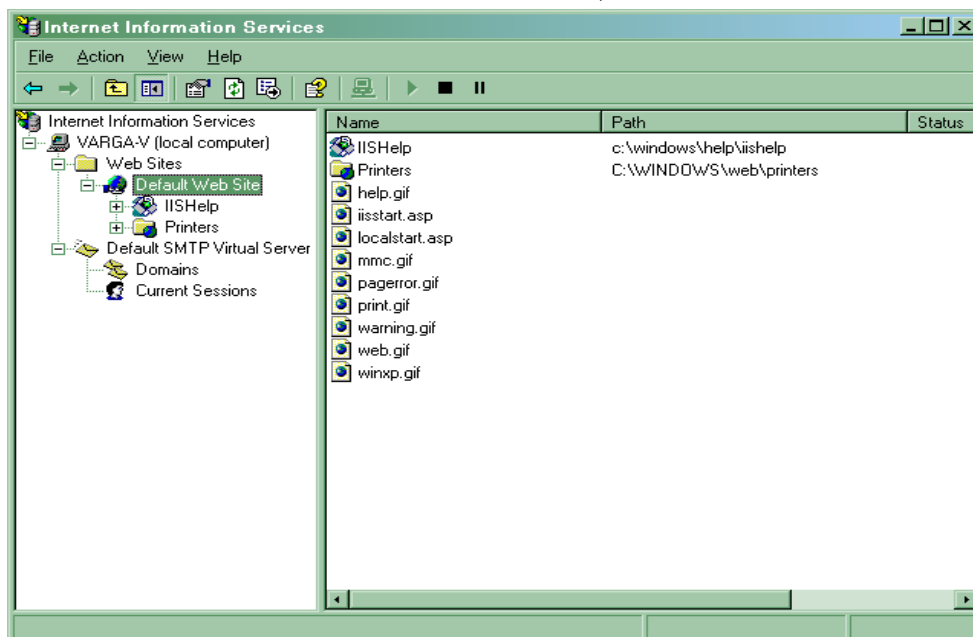
8. Ez után mindenféleképpen javasolt lementeni a már megújított tanúsítványt a kulcsaival együtt. (lásd.: Függelék D - Biztonsági másolat készítése tanúsítványairól és kulcsairól MMC segítségével)

12.4.2.2. Tanúsítvány lecserélése szerveren

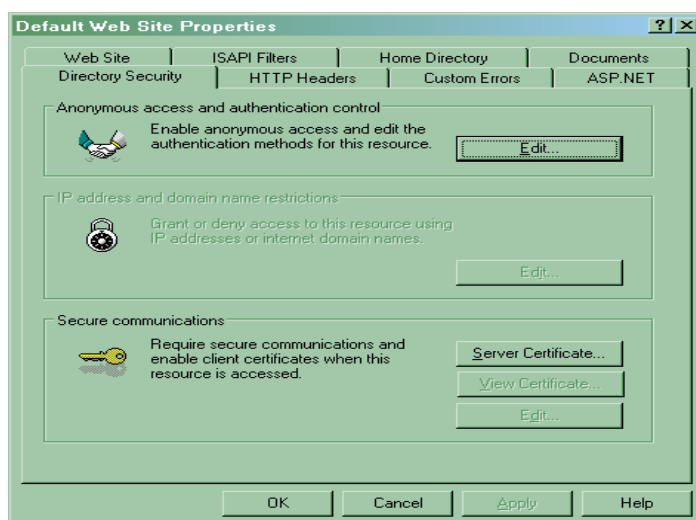
A tanúsítvány korábbiakban mutatott cseréje után, az IIS megfelelő site-ja esetén a site-hoz tartozó tanúsítványt újra ki kell választania.

A kiválasztás lépései:

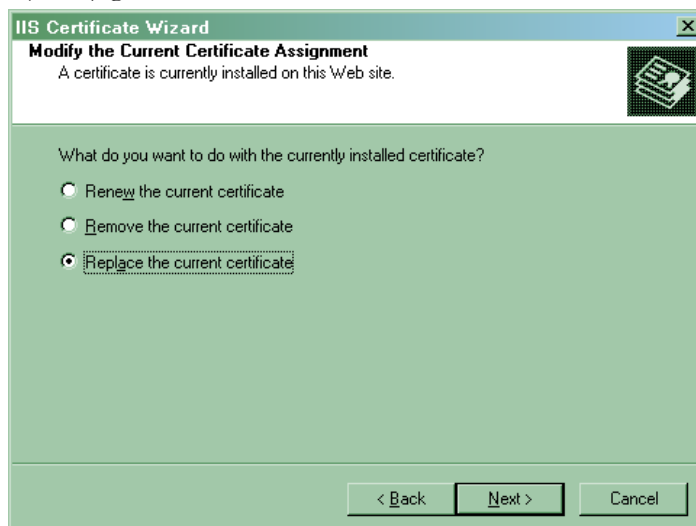
1. Indítsa el az IIS konzolját, és válasza ki a website-ot, amihez a tanúsítványt szeretné beállítani. (Vezérlőpult > Felügyeleti eszközök > Internet information Server) (Vezérlőpult > Administrative tools > Internet information Server)



2. Jelölje ki a website-ot, kattintson rajta jobb gombbal, majd válassza ki a Properties (Tulajdonságok) opciót.
3. A Directory fülön kattintson a Server Certificate gombra, és a varázsló elindul.



4. Válassza a Replace the current certificate opciót (Tanúsítvány cseréje), majd nyomjon Tovább (Next) gombot.



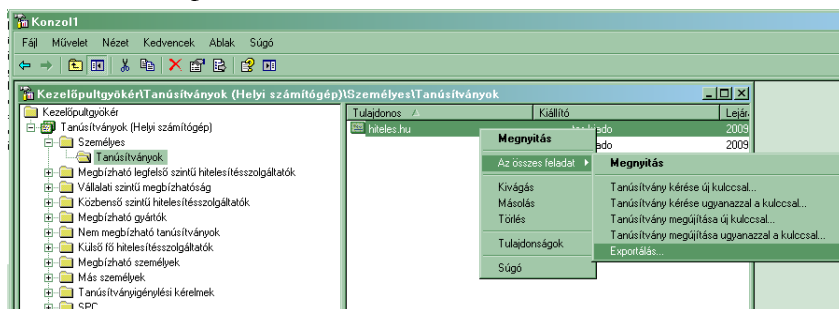
5. A megjelenő ablakban válassza ki a tanúsítványt, majd Next (Tovább) és Finish (Befejezés) gombokkal navigáljon el a varázsló végére.

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

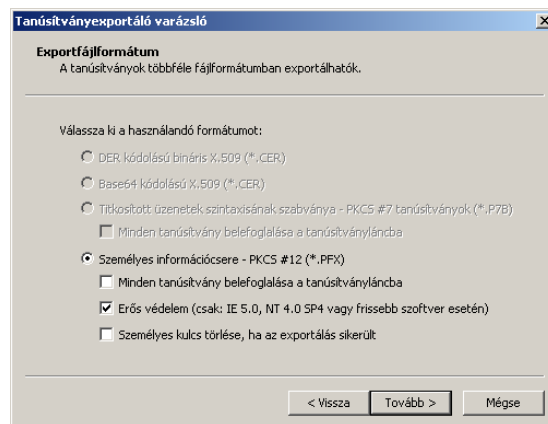
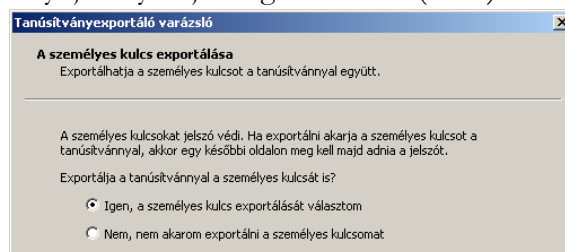
Ha tanúsítványa fokozott biztonságú és NEM kriptográfiai eszközön kapta meg, akkor érdemes a tanúsítványáról PKCS#12 (*.pfx) állományban biztonsági másolatot készíteni, hiszen a számítógép sérülése, illetve újraterelítése után csak ebből tudja a tanúsítványt visszaállítani.

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 szeretne a fájlnak adni. Ezt jegyezze meg jól, mert ennek ismeretében tudja telepíteni másik gépen tanúsítványát.
7. A következő ablakban kiválaszthatjuk a fájlnevet, és a helyet, ahol a fájl létre szeretnénk hozni.
8. Miután ezt beállította, már csak a Tovább (Next) és végül a Befejezés (Finish) gombot kell megnyomni, valamint a megnyitott ablakokat OK gombbal bezárni.



A tanúsítvány exportálása ezzel megtörtént.

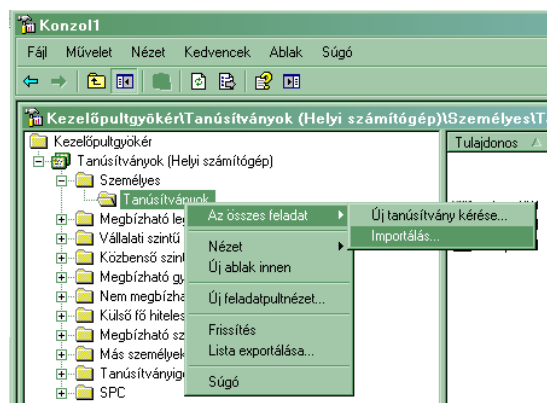
Ezt az állományt érdemes biztonságos helyen elzárni valamilyen adathordozón.

14. 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 tanúsítványtárba 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, majd az Importálás menü választásával tudja kezdeményezni a tanúsítvány feltöltését.
3. A következő ablakban ki tudja tallózni a PFX file-t.



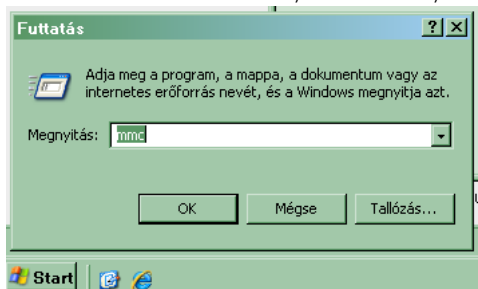
4. Az üdvözlő képernyőn nyomja meg a Tovább (Next) gombot.
5. A második képernyőn az importálandó fájl nevét látja. Itt nincs semmi teendő, lépjen tovább a Tovább (Next) gomb segítségével.
6. A következő képernyőn adja meg a PKCS#12 fájlhoz tartozó jelszót. Itt állíthatja be a tanúsítvány erős védelmét 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.



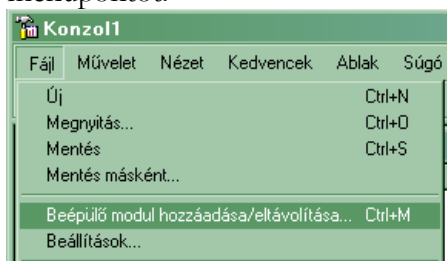
A tanúsítvány telepítése ezzel megtörtént.

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

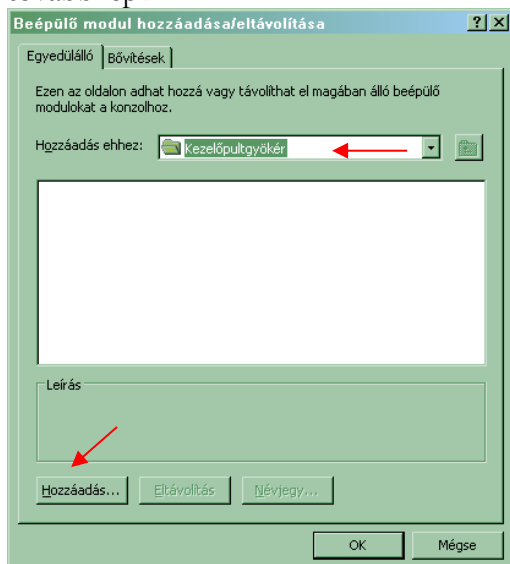
1. Indítsa el a Start menü / Futtatás ./ MMC parancsot.



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



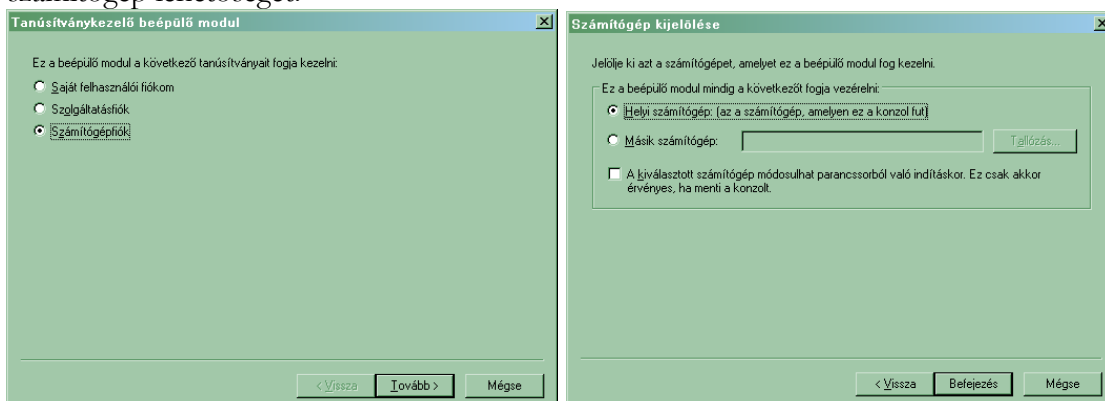
3. A következő ablakban a Kezelőpultgyökér-hez a Hozzáad... gomb megnyomásával kell tovább lépni.



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



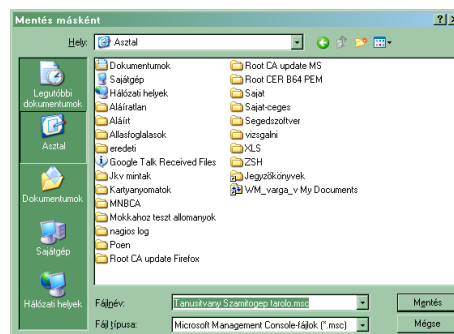
5. Ezután a megjelenő ablakban a Számítógépfiók lehetőséget kell választani, majd a Helyi számítógép lehetőséget.



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 újra indíthatja a konzolt



16. Függelék G – Tanúsítvány helyreállítása IIS szerveren

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

16.1. Az IIS tanúsítványkezelése

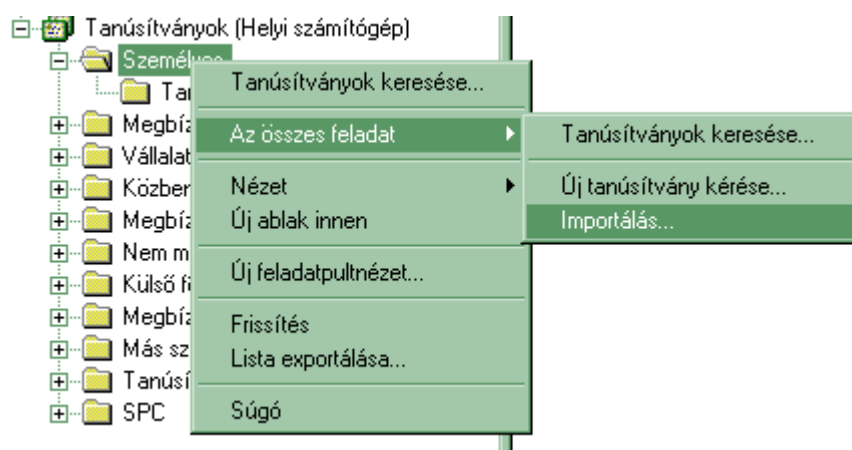
Abban az esetben, ha az Ön IIS szerverén fut egy website, és új kérelmet generál, az aktuális site működése felfüggesztődik.

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

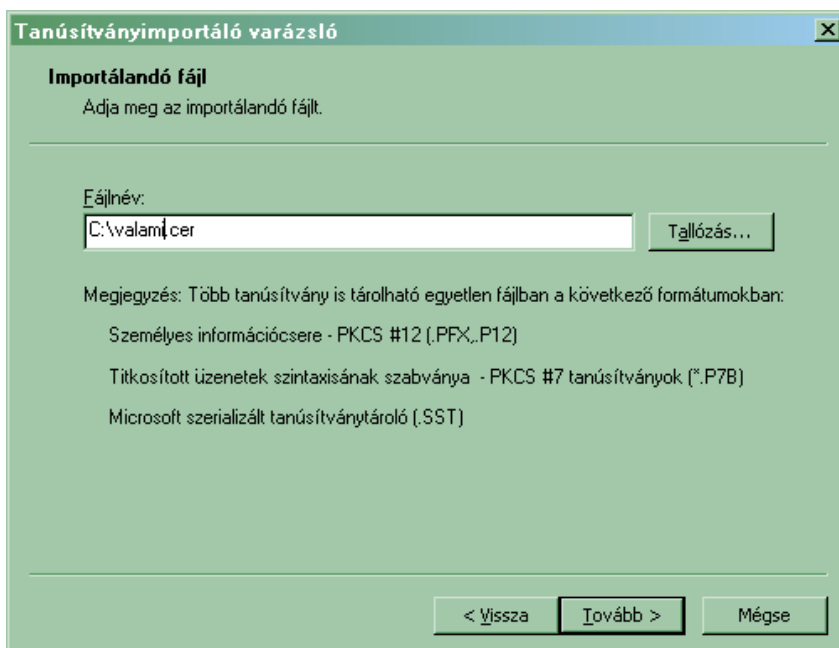
Ennek megkerülésére lehetőség van a generálásokról szóló útmutató intelmeit követve (6. fejezet), azonban ha bekövetkezett a baj, a következő lépések alapján helyre tudja állítani az új tanúsítványhoz tartozó kulcsokat.

16.1.1. A lépések:

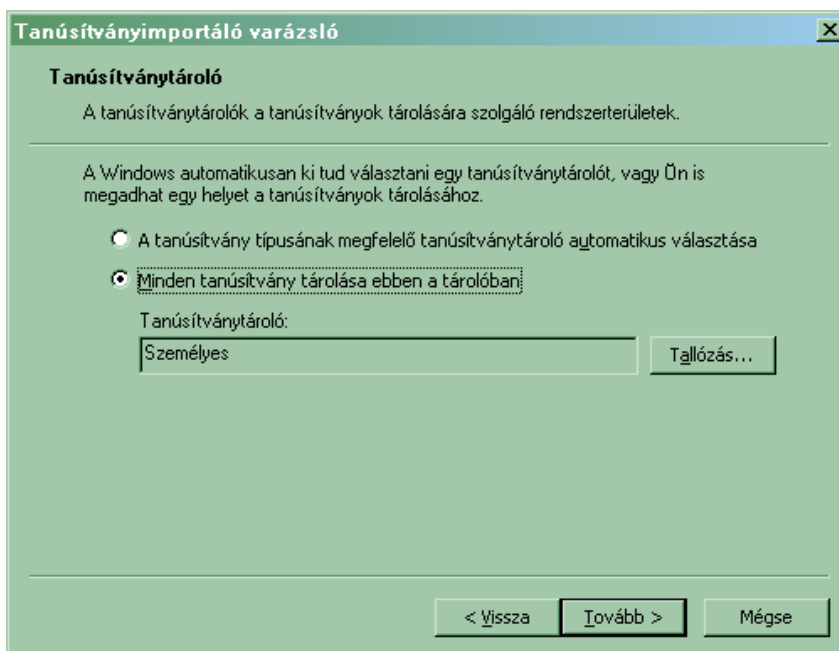
1. Indítson MMC-t és menjen a Tanúsítvány beépülő modul Local Computer tárolójába.
(Az MMC beállítását az F függelékben tekintheti meg.)
2. Az itt található Személyes mappán (Personal) válassza Az összes feladat (All tasks) majd Import menüpontokat.



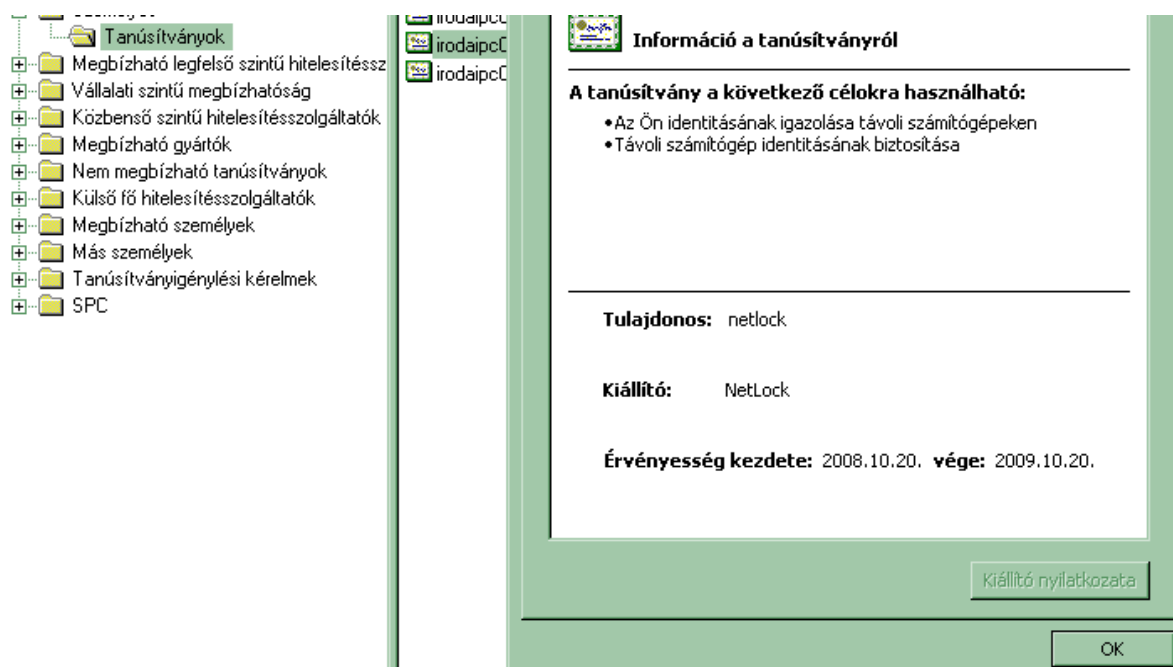
3. Az importálás során tallózza ki a kapott tanúsítványt, majd nyomjon Tovább (Next) gombra.



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 válasza 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.



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 kiválasztása a tanúsítványnak a website beállításai között lehetségessé válik.

17. Függelék H – UCC tanúsítvány nem adható belső névre

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

Az ilyen tanúsítványok MITM 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, megismeri belőle a belső nevet.
3. A támadó a hitelesítés szolgáltató felé bead egy saját domain névre egy hitelesítési kérést, 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 saját domain nevére.
5. A támadó a hálózatba belső oldalra bejutva, a saját tanúsítványát a szervere hitelesítésére használja, és a forgalmat eltéríti, tanúsítványa belső nevek miatt hitelesnek látszik.

Amennyiben a cél másik szervezet:

A megkapott tanúsítvány más szervezetenél, amennyiben van egyező név felhasználható MITM támadás kivitelezésére.

A fentiek miatt biztonsági okokból nem javasolt egy hálózatban belülről és kívülről is elérhető szerver kétféle néven történő elérhetővé tétele, és biztonsági okok miatt ilyen tanúsítvány, amely a két nevet tartalmazza nem adható.

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