

Tanúsítvány létrehozása Exchange 2007 szerverhez

Exchange 2007 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.	Általános korlátozások, tudnivalók.....	4
5.	A tanúsítvány igénylés előtt előzetesen áttekintendő információk	5
5.1.	Mely szolgáltatásokhoz javasolt belső önaláírt tanúsítvány?.....	5
5.2.	Külső kliensek esetén mely szolgáltatásokhoz javasolt tanúsítványkiadó által kiadott tanúsítvány?	5
5.3.	Külső és belső címről elérhető szerverek névképzési szabályai	5
5.4.	Wildcard tanúsítvány igénylése.....	6
6.	Exchange Management Shell indítása	7
7.	Tanúsítványkérelem létrehozása	7
7.1.	Wildcard tanúsítvány kérelem.....	7
7.2.	NEM wildcard tanúsítvány kérelem	7
8.	Tanúsítvány kérelem beadása	8
9.	Kiadott tanúsítvány telepítése	10
10.	A köztes kiadó tanúsítványának telepítése.....	10
11.	Függelék A – Regisztráció ügyfélmenübe.....	11
12.	Függelék B – Belépési nyilatkozat készítése.....	13
13.	Függelék C – Tanúsítvánnyal kapcsolatos ügyintézés.....	14
13.1.	Az ügyfélmenü használata.....	14
13.2.	Bejelentkezés az ügyfélmenübe	14
13.3.	A tanúsítvány felfüggesztése.....	15
13.3.1.	Felfüggesztéssel kapcsolatos fontos információk.....	16
13.4.	A tanúsítvány megújítása.....	17
13.4.1.	Teendők a Belépési nyilatkozattal.....	18
13.4.2.	Megújított tanúsítványok letöltése	19

13.4.3.	A régi tanúsítvány cseréje az újra	19
14.	Függelék D – Tanúsítványok exportálása és importálása Exchange 2007- ből.....	20
14.1.	Tnúsítvány és kulcsok exportálása Exchange segédeszközök segítségével (PKCS12 (PFX) mentés).....	20
14.2.	PKCS12 (PFX) fájlban található tanúsítvány telepítése Exchange segédeszközök segítségével.....	20
15.	Függelék E – UC tanúsítvány nem adható belső névre.....	21

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 1023 Budapest, Zsigmond tér 10. szám alatt, munkanapokon 9 és 17 óra között készséggel áll rendelkezésére.

3. A dokumentációról

A dokumentáció az Exchange 2007 verzió alapján készült, de a dokumentáció alapján későbbi verziókkal is elvégezhető a tanúsítvány generálás folyamata.

4. Általános korlátozások, tudnivalók

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.
4. UC tanúsítványok: Az Exchange 2007 és Office Communication Server 2007 termékek és későbbi verzióik úgy nevezett UC tanúsítványokat használnak.

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

5. A tanúsítvány igénylés előtt előzetesen áttekintendő információk

Az igénylés előtt pár döntés meghozatala szükséges, a megfelelő igény beadásához.

5.1. Mely szolgáltatásokhoz javasolt belső önaláírt tanúsítvány?

A Microsoft az Exchange működéséből adódóan a következő szolgáltatásokhoz önaláírt tanúsítványt javasol:

- SMTP kapcsolatok Hub Transport szerverek között
- SMTP kapcsolatok Hub Transport szerverek és Edge Transport szerver között
- EdgeSync szinkronizáció Edge Transport szerver és az Active Directory között
- Unified Messaging kommunikáció
- A Client Access szerver, ha csak belső kliensek érik el.

Ezen feltételek esetén nincs szükség tanúsítványkiadótól származó tanúsítvány telepítésére.

5.2. Külső kliensek esetén mely szolgáltatásokhoz javasolt tanúsítványkiadó által kiadott tanúsítvány?

A biztonság az alábbi esetekben követelhet meg tanúsítványkiadó által kiadott tanúsítványt.

- POP3 és IMAP4 kliens hozzáférés az Exchange-hez
- Outlook Web Access
- Outlook Anywhere
- Exchange ActiveSync
- Autodiscover
- Domain Security

Ezen feltételek esetén tanúsítványkiadótól származó tanúsítvány válhat szükségessé.

5.3. Külső és belső címről elérhető szerverek névképzési szabályai

A vonatkozó biztonsági előírások megkövetelik, hogy a kiadott tanúsítványok csak FQDN neveket tartalmazzanak, azaz ne, lehet benne publikus DNS szerver segítségével nem feloldható név.

Ilyen esetben szükséges az AD struktúra átgondolása, és átnevezése, vagy a belső DNS módosítása, mert a tanúsítvány csak FQDN nevek feltüntetésével adható ki.

(Lásd Függelék E)

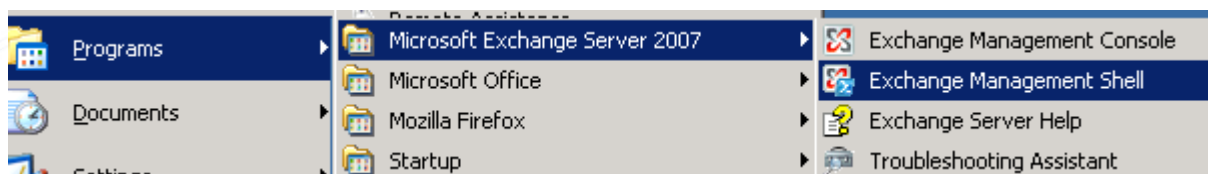
5.4. Wildcard tanúsítvány igénylése

A wildcard tanúsítvány igénylése a névképzést egyszerűbbé teszi, azonban vannak bizonyos korlátozó feltételek:

- A Windows Mobile 5.0 kliensek nem támogatják a wildcard tanúsítványokat.
Ez esetben a SAN mezőbe szükséges a további nevek feltüntetése.
- Az Outlook Anywhere kapcsolódása problémákba ütközik wildcard tanúsítványok esetén.
Ez esetben végre kell hajtani a következő parancsot az Exchange Management Shell-ben:
`Set-OutlookProvider -Identity EXPR -CertPrincipalName msstd:*.akarmi.hu`

6. Exchange Management Shell indítása

Az Exchange Management Shell a Start menüből indítható.



7. Tanúsítványkérelem létrehozása

Annak megfelelően, milyen döntést hoztunk, a következő lépések valamelyikére van szükségünk.

7.1. Wildcard tanúsítvány kérelem

A lefuttatandó parancs a következő:

```
New-ExchangeCertificate -GenerateRequest -Keysize 2048 -SubjectName "C=HU, O=Maci  
Laci Bt, CN=mail.macilaci.hu, L=Budapest" -DomainName *.macilaci.hu  
-Path c:\certificates\wild.req
```

Helyettesítendő:

- mail.macilaci.hu – saját domain névvel
- -Keysize 2048 – ez 1024-es kulcs esetén elhagyható, a 2048 kulcshossz javasolt.
- SubjectName, O=cégnév, L=székhely szerinti város

7.2. NEM wildcard tanúsítvány kérelem

A lefuttatandó parancs a következő:

```
New-ExchangeCertificate -GenerateRequest -Keysize 2048 -SubjectName "C=HU, O=Maci  
Laci Bt, CN=www.macilaci.hu, L=Budapest" -DomainName edge.macilaci.hu,  
activesync.macilaci.hu, akarmi.macilaci.hu -Path c:\certificates\soft.req
```

Helyettesítendő:

- www.macilaci.hu, edge.macilaci.hu, activesync.macilaci.hu, akarmi.macilaci.hu
– saját domain és szolgáltatás nevekkkel
- -Keysize 2048 – ez 1024-es kulcs esetén elhagyható, a 2048 kulcshossz javasolt.
- SubjectName, O=cégnév, L=székhely szerinti város

8. 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 töltsé 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 szervert URL https nélkül, meg kell egyeznie a később tanúsítvány kérelemben lévő URL-lel.

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

9. 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:

Figyelem!

A Certificate Management snap-in-t ne használjuk a telepítésre, mert problémákat fog okozni!

Az Exchange Managment konzolban a következő parancsot kell végrehajtanunk:

```
Import-ExchangeCertificate -Path c:\certificates\macilaci.cer | Enable-ExchangeCertificate -Services SMTP,IIS,POP
```

Helyettesítendő:

- -Services <paraméterek> - amely szolgáltatásokhoz használni kívánjuk, azokat adjuk itt meg.

10. A köztes kiadó tanúsítványának telepítése

Amennyiben a tanúsítvány kiadója közbenső (Intermediate) tanúsítványú kiadó, és nem települt automatikusan az Közbenső szintű tanúsítványok közé, akkor szükség lehet a kézi telepítésére.

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 az Exchange szerver újraindítására lehet szüksége.

11. 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"/>	<input type="text" value="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.

12. 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!!!

13. 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.

13.1. 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.

13.2. 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.



The screenshot shows a web browser window with the URL <https://www.netlock.hu/index.cgi?sid=F1Ne264FLna3KouhV68ter=USER/index.ten5lang=HU>. The page features the NetLock logo and navigation links. On the left, there is a sidebar with links for 'Információk', 'Céginformáció', 'Állás', 'Tanúsítványhadás', 'Operatív felület beállítás', 'Dokumentációk', 'Támogatás', and 'Tanúsítványkiadók'. The main content area is divided into four sections: 'Információk', 'Saját adatok', 'Tanúsítványkiadók', and 'Tanúsítványok'. The 'Információk' section provides details about the company and its services. The 'Saját adatok' section allows users to manage their account information. The 'Tanúsítványkiadók' section lists the various types of certificates offered. The 'Tanúsítványok' section displays the user's own certificates and their details.

13.3. A tanúsítvány felfüggesztése

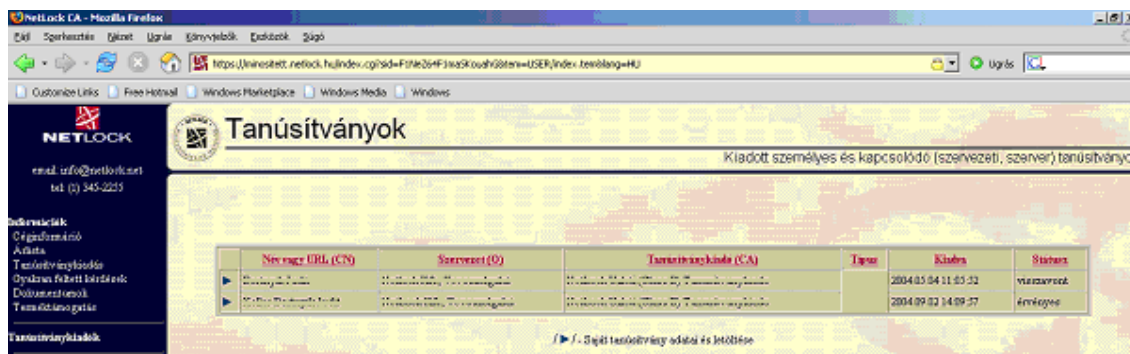
Elektronikus tanúsítványait, akár csak bankkártyáját, gondosan kell kezelnie és őriznie, hiszen a tanúsítványával az Ön nevében végezhetnek elektronikus aláírást, és ez által az Ön nevében tehetnek joghatással bíró nyilatkozatot.

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.

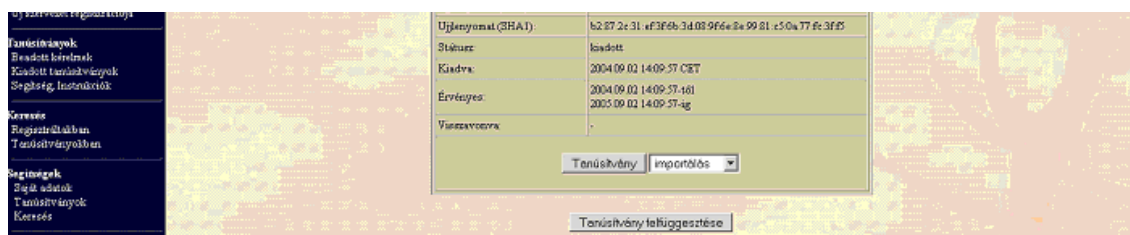
A.) Interneten keresztül a következő módon függesztetheti fel tanúsítványát:

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.



Név vagy URL (CN)	Szervezet (O)	Tanúsítványkód (CA)	Típus	Kiadás	Státusz
...	2004.05.04 11:03:52	visszavont
...	2004.09.02 14:09:37	érvényes

3. Ekkor megjelennek a kiválasztott tanúsítvány részletei. Az alul található Tanúsítvány felfüggesztése gombbal kezdeményezheti a tanúsítvány felfüggesztését.



Ujjenymat (SHA1): b2:87:2e:31:ef:3f:eb:3d:03:9f:6e:8a:99:81:e5:0a:77:f6:3f:85

Státusz: visszavont

Kiadás: 2004.09.02 14:09:37 CET

Érvényes: 2004.09.02 14:09:37-161

Visszavonva: 2005.09.02 14:09:37-ág

Tanúsítvány felfüggesztése

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.

13.3.1. 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.

13.4. 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 tanúsítványt ezt követően letölthető az ügyfélmenüből.
7. A kiadott tanúsítványt le kell tölteni a gépére.

13.4.1. 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 (1) 345-2250-es 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 1023 Budapest, Zsigmond tér 10. szám alatt ügyfélfogadási időben: hétfőtől péntekig 9 és 17 óra között. Amennyiben erre nincs lehetősége, közjegyző előtt is aláírhatja azt, majd az eredeti hitelesített példányt kérjük a fenti címre megküldeni.

Fokozott biztonságú „A” osztályú tanúsítvány esetén:

A Belépési nyilatkozatot ebben az esetben közjegyző előtt kell aláírni egy aláírás hitelesítés keretében. A hitelesített példányt eredetiben küldje el a NetLock címére. (1023 Budapest, Zsigmond tér 10.)

Minősített tanúsítvány esetén:

A Belépési nyilatkozatot ebben az esetben közjegyző előtt kell aláírni egy aláírás hitelesítés keretében. A hitelesített példányt eredetiben küldje el a NetLock címére. (1023 Budapest, Zsigmond tér 10.)

13.4.2. 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 D fejezet 14.2 pontja alapján.

13.4.3. A régi tanúsítvány cseréje az újra

Mivel a megújítás során a kulcs változatlan és a tanúsítvány kerül csak cserélésre, ugyanazt a lépést kell végrehajtanunk, mint korábban.

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

Figyelem!

A Certificate Management snap-in-t ne használjuk a telepítésre, mert problémákat fog okozni!

Az Exchange Managment konzolban a következő parancsot kell végrehajtanunk:

```
Import-ExchangeCertificate -Path c:\certificates\macilaci.cer | Enable-ExchangeCertificate -Services SMTP,IIS,POP
```

Helyettesítendő:

- -Services <paraméterek> - amely szolgáltatásokhoz használni kívánjuk, azokat adjuk itt meg.

14. Függelék D – Tanúsítványok exportálása és importálása Exchange 2007-ből

14.1. Tanúsítvány és kulcsok exportálása Exchange segédeszközök segítségével (PKCS12 (PFX) mentés)

Az alábbi parancs segítségével tudjuk telepíteni a PKCS#12 mentésben található tanúsítványunkat:

```
Export-ExchangeCertificate -Thumbprint -BinaryEncoded:$true -Path  
c:\mentett.pfx -Password:(Get-Credential).password
```

Az exportálás során meg kell adnunk a fájl jelszavát.

Értelemszerűen a <c:\mentett.pfx> helyettesítendő az aktuális fájl névvel, azonban a fájl névnek kötelezően .pfx kiterjesztéssel kell rendelkeznie.

14.2. PKCS12 (PFX) fájlban található tanúsítvány telepítése Exchange segédeszközök segítségével

Az alábbi parancs segítségével tudjuk telepíteni a PKCS#12 mentésben található tanúsítványunkat:

```
Import-ExchangeCertificate -Path c:\mentett.pfx -Password:(Get-  
Credential).password
```

Az importálás során felhasználónevet, jelszót kérdez, melynél a felhasználónév érdektelen, de a jelszó a fájl jelszava kell, hogy legyen.

Értelemszerűen a <c:\mentett.pfx> helyettesítendő az aktuális fájl névvel.

15. Függelék E – UC 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.

