Tanúsítvány létrehozása Exchange 2007 szerverhez

Exchange 2007 szerveren kérelem létrehozása, tanúsítvány kérelem beadása, kiadott tanúsítvány telepítése és megújított tanúsítvány cseréje

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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/UCC tanúsítvány igénylése 6
6. Előzetes követelmények – néhány döntés, amit meg kell hozni 7
6.1. A tanúsítványkiadás algoritmusa, a kiadó típusa 7
6.2. Az SSL tanúsítvány profilja 7
7. Exchange Management Shell indítása 9
8. Tanúsítvány kérelem létrehozása 9
8.1. UCC / Wildcard tanúsítvány kérelem 9
8.2. Hagyományos (nem UCC/Wildcard) tanúsítvány kérelem 9
9. Tanúsítvány kérelem beadása 10
10. Kiadott tanúsítvány telepítése 11
11. A köztes kiadó tanúsítványának telepítése 12
12. Függelék A – Regisztráció ügyfélmenübe 13
13. Függelék B – Belépési nyilatkozat készítése 15
14. Függelék C – Tanúsítvánnyal kapcsolatos ügyintézés 16
14.1. Az ügyfélmenü használata 16
14.2. Bejelentkezés az ügyfélmenübe 16
14.3. A tanúsítvány felfüggesztése 17
14.3.1. Felfüggesztéssel kapcsolatos fontos információk 17
14.4. A tanúsítvány megújítása 18
14.4.1. Teendők a Belépési nyilatkozattal 19
14.4.2. Megújított tanúsítványok letöltése 20

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

14.4.3. A régi tanúsítvány cseréje újra 20
15. Függelék D – Tanúsítványok exportálása és importálása Exchange 2007-ből 21
15.1. Tanúsítvány és kulcsok exportálása Exchange segédeszközök segítségével (PKCS12 (PFX) mentés) 21
15.1.1. A tanúsítvány Thumbprint-jének kiderítése az exporthoz 21
15.2. PKCS12 (PFX) fájlban található tanúsítvány telepítése Exchange segédeszközök segítségével 22
16. Függelék E – UCC tanúsítvány nem adható belső névre 23
17. Függelék F – Regisztrált domain név használata a belső domain név helyett Exchange 2007 és Exchange 2010 szerveren 23
17.1. Az Exchange szerver átirányítása a külső név használatához 24
18. Kulcs helyreállítása 25

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

2. Bevezető

E tájékoztató célja, hogy a szerveréhez szükséges SSL tanúsítvány igénylését minél könnyebben elvégezhesse.

Kérjük, olvassa el figyelmesen, és kövesse a leírtakat.

Amennyiben bármilyen kérdése van vagy problémája támad, Ügyfélszolgálatunk a(z) +36 1 437 6655 telefonszámon, az info@netlock.hu e-mail címen vagy személyesen a 1101 Budapest, Expo tér 5-7. szám alatt hétfőtől - csütörtökig 8:30 és 17 óra között pénteken 8:30 és 14 óra között készséggel áll rendelkezésér

3. A dokumentációról

A dokumentáció az Exchange 2007 verzió alapján készült, de ez 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, 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 a wildcard tanúsítvány.

3. Az **SNI** korlátozás: az előző probléma feloldására született az SNI technológia, amely azonban csak Windows Vista és Internet Explorer 7 esetében érhető el, így haszna megkérdőjelezhető.

4. UCC tanúsítványok: az Exchange 2007 és Office Communication Server 2007 termékek és későbbi verzióik úgynevezett UCC tanúsítványokat használnak.

   Korlátozás: belső, nem FQDN névre szóló domain elhelyezése a tanúsítványban biztonsági okok miatt nem engedélyezett (lásd Függelék – E)

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

5. A tanúsítvány igénylés előtt előzetesen áttekintendő információk

A tanúsítvány igénylése előtt érdemes pár dolgot megfontolni, és annak alapján választani majd a kérelem feltöltés során.

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 megfelelő biztonság érdekében az alábbi esetekben lehet fontos egy tanúsítványkiadó által kiadott tanúsítvány.

- 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 nem 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)

Ugyanakkor, ha már belső neves struktúrát alakított ki szerverén, úgy van mód, hogy azt is megfelelően beállítsa (Lásd Függelék F).

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

5.4. Wildcard/UCC tanúsítvány igénylése

Az Exchange 2007, az Office Communication Server 2007, illetve későbbi verzióik teljeskörű funkcionalitásának kihasználásához UCC profil az optimális választás.

Figyelem!
Belső névre UCC tanúsítvány nem adható, mert támadási felületet biztosít (részleteket lásd.: Függelék H).

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
  ```


NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

6. Előzetes követelmények – néhány döntés, amit meg kell hozni

A tanúsítvány igénylése előtt érdemes pár dolgot megfontolni, és annak alapján választani majd a kérelem feltöltése során.

6.1. A tanúsítványkiadás algoritmusa, a kiadó típusa

A kiadás során használt hash algoritmus határozza meg, hogy mely kiadóval kerül majd kiadásra a tanúsítvány, illetve hogy milyen kompatibilitási és egyéb problémák fordulhatnak vele 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.

6.2. Az SSL tanúsítvány profilja

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

- Szerver tanúsítvány

Egyszerű, 1 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, azonban a valami.hu cím eléréshez NEM alkalmas;
  - általában olyan egyszerű struktúrájú weboldalhoz javasolt, amely 1 címen érhető el.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 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 „*” szimbólum található.

  - a *.valami.hu címre szóló tanúsítvány több aldomain hitelesítésére is alkalmas (például: www.valami.hu, mail.valami.hu, stb.) Mivel azonban a „*” szimbólumnak kötelezően helyettesítenie kell egy tagot, ezért 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
  - ehelyett általában UCC tanúsítvány javasolt, mely tartalmazhat wildcard tagokat is;

- UCC tanúsítvány

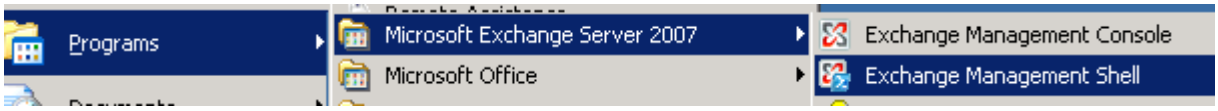
Olyan tanúsítvány, amely több domain nevet is tartalmazhat, akár wildcard taggal is kombinálva.

  - 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, stb. 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. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

7. Exchange Management Shell indítása

Az Exchange Management Shell a Start menüből indítható.



8. Tanúsítvány kérelem létrehozása

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

8.1. UCC / 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 -PrivateKeyExportable $true
```

Helyettesítendő:

- mail.macilaci.hu – saját domain névvel
- -Keysize 2048 –a 2048 kulcshossz a minimum
- SubjectName, O=cégnév, L=székhely szerinti város
- A –PrivateKeyExportable $true opció csak akkor adandó meg, ha később ki szeretné exportálni a kulcsokat.

8.2. Hagyományos (nem UCC/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 -
PrivateKeyExportable $true
```

Helyettesítendő:

- www.macilaci.hu, edge.macilaci.hu, activesync.macilaci.hu, akarmi.macilaci.hu

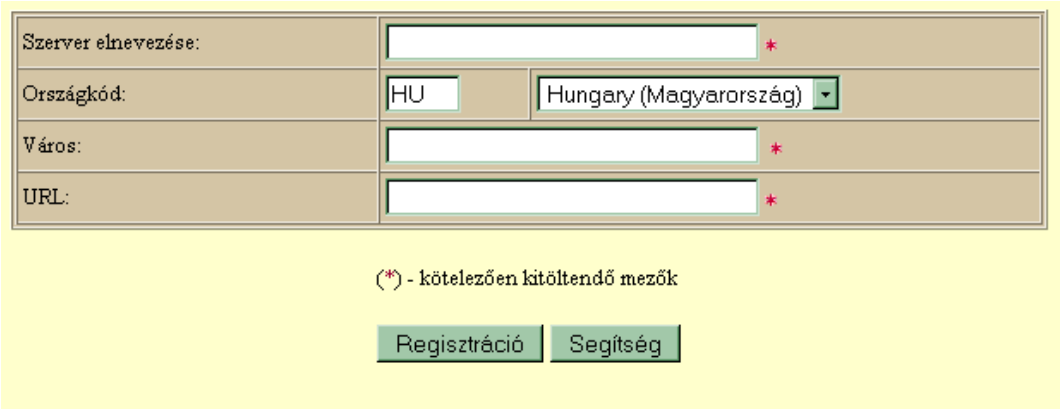
  – saját domain és szolgáltatás nevekkel
- -Keysize 2048 – a 2048 bites kulcshossz a minimum.
- SubjectName, O=cégnév, L=székhely szerinti város
- A –PrivateKeyExportable $true opció csak akkor adandó meg, ha később ki szeretné exportálni a kulcsokat.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 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, akkor a függelékben találhatóak alapján regisztráljon.
2. Bejelentkezve a rendszerbe válassza az Új szerver regisztrációja gombot. A megjelenő ablakban töltse ki az adatokat a következő táblázatnak megfelelően.



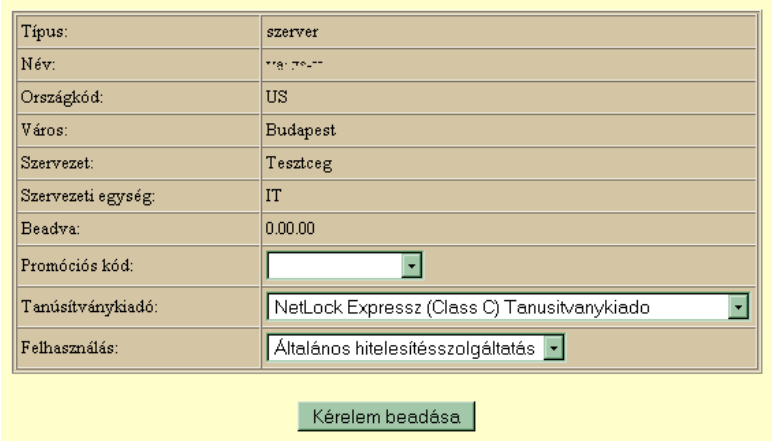
Szerver elnevezése	Szerver elnevezése, valamilyen beszédes név
Országkód	A személy vagy szervezet igazolt székhelye/lakhelye alapján (cégkivonat, lakcímkártya), Cég számára beszerzendő tanúsítvány esetén szervezeti adatok, magánszemély által beszerzendő esetén a személy adatai alapján.
Város	
URL	A szerver URL https nélkül, meg kell egyeznie a később tanúsítvány kérelemben lévő URL-lel.

3. Ezután válassza az Új kérelem beadása > Szerver tanúsítványok > Web szerver (SSL) > menüpontot, 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. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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

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



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

10. Kiadott tanúsítvány telepítése

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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

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

Az Exchange Managament 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.

11. A köztes kiadó tanúsítványának telepítése

Amennyiben a tanúsítvány kiadója közbenső (Intermediate) tanúsítványú kiadó, és nem települt automatikusan a 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 szükség lehet az Exchange szerver újraindítására.

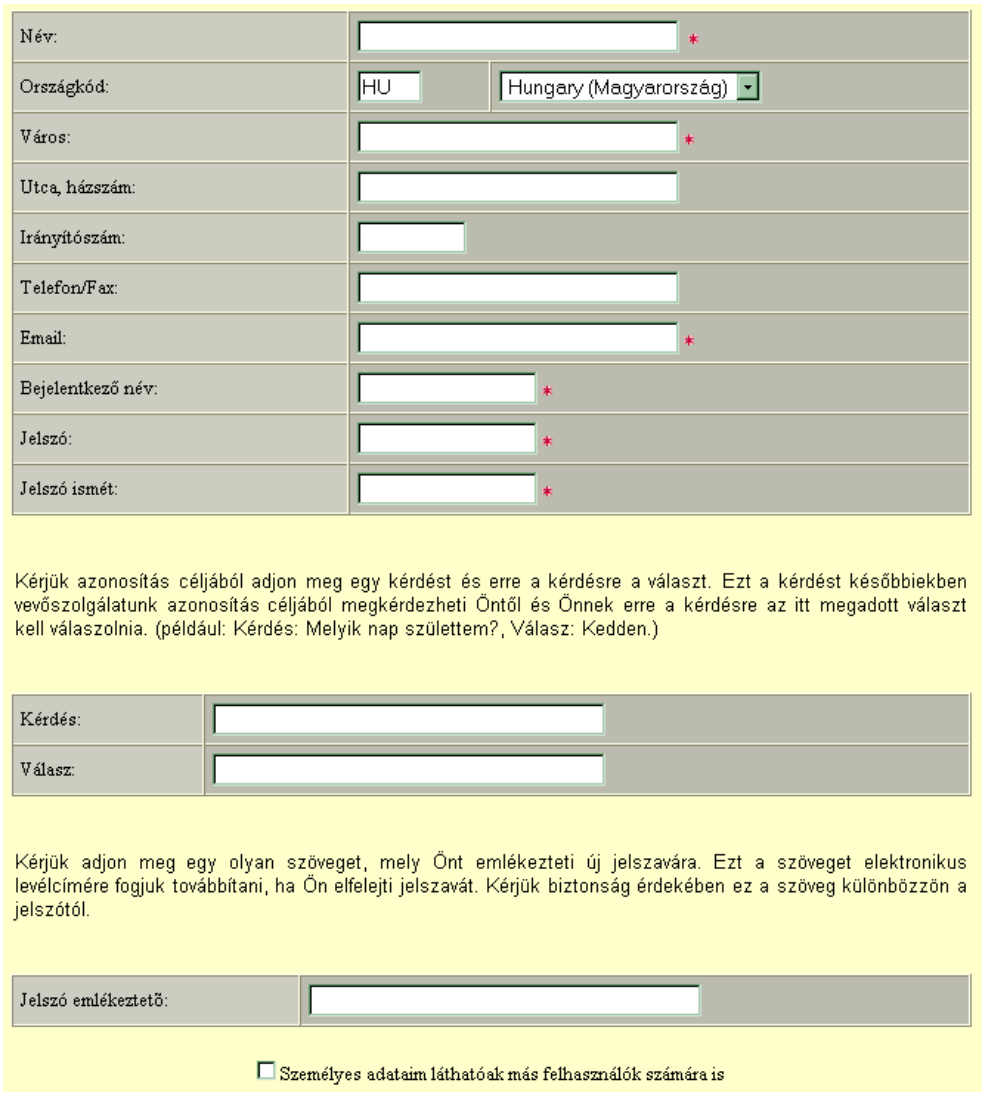
NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

12. Függelék A – Regisztráció ügyfélmenübe

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

A felhasználó regisztrációjának lépései a következők

1. Látogasson el a www.netlock.hu oldalra, és ott válassza a „Fokozott biztonságú tanúsítvány igénylése” menüpontot, majd a megjelenő oldalon válassza a Regisztráció menüpontot.
2. A megjelenő adatlapon töltse ki személyes adatait az igazolványainak (személyi igazolvány, lakcímkártya) megfelelő adatokkal (ahol ez értelmezhető).



A kitöltendő adatok a következők:

Név	

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

Országkód	Az érvényes személyes adatok igazolványok alapján.
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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

13. 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. Ezt 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. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

14. Függelék C – Tanúsítvánnyal kapcsolatos ügyintézés

Figyelem!

A fejezetben leírtakra csak akkor van szüksége, ha tanúsítványát megújítja, vagy valamilyen okból a felfüggesztése, visszavonása mellett dönt.

14.1. Az ügyfélmenü használata

Tanúsítvány kérelmeinek létrehozása és beadása során ügyfélmenü jött létre az Ön számára a NetLock Kft. honlapján. Itt tekintheti meg a saját és mások tanúsítványait, innen intézheti a tanúsítványokkal kapcsolatos ügyeit.

14.2. 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 bal oldalon és középen is megtalálható menüpontok közül választhat.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

14.3. A tanúsítvány felfüggesztése

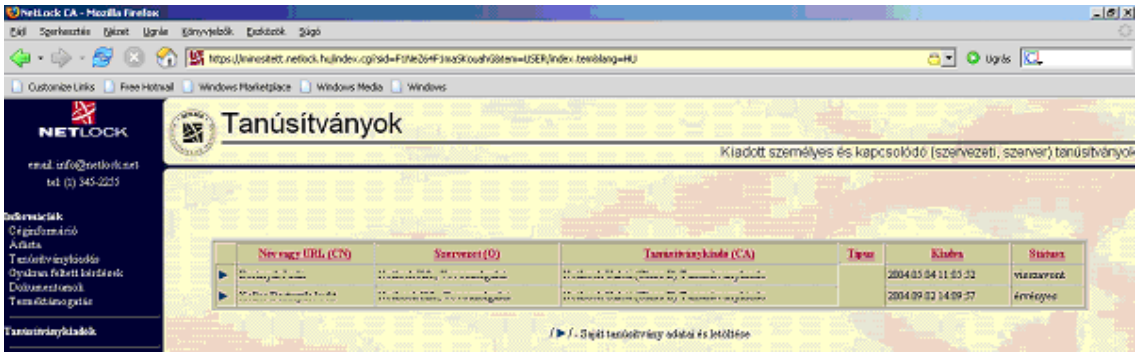
Elektronikus tanúsítványait - akárcsak bankkártyáját - gondosan kell kezelnie és őriznie, hiszen a tanúsítványával az Ön nevében végezhetnek elektronikus aláírást és ezáltal az Ön nevében tehetnek joghatással bíró nyilatkozatot.

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

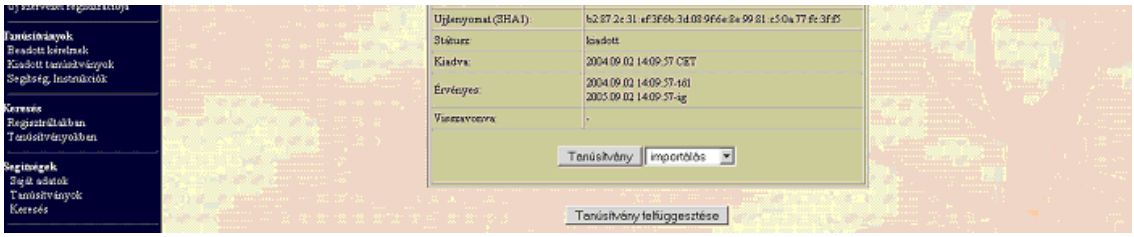
Ha nem tud minden kétséget kizáróan meggyőződni arról, hogy időközben a magánkulcsot nem használta illetéktelen személy, intézkedjen a tanúsítvány végleges visszavonásáról. A felfüggesztési, visszavonási lépéseket a NetLock Kft. Szolgáltatási Szabályzatában szereplő módon (Internetes ügyfélmenün keresztül,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

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

1. Jelentkezzen be az ügyfélmenüjébe, és válassza ki a bal oldali menüsorban a **Kiadott tanúsítványok** menüpontot.
2. A megjelenő ablakban láthatja 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.

14.3.1. 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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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

14.4. 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 ügyfélmenüjébe
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. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

14.4.1. 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.

Fokozott biztonságú „C" osztályú tanúsítvány esetén:

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

Fokozott biztonságú „B" osztályú tanúsítvány esetén:

A 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 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. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

14.4.2. Megújított tanúsítványok letöltése

Amennyiben tanúsítványait megújította és a tanúsítvány kiadásra került, az új tanúsítványokat cserélni kell 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 tanúsítványtárában megtalálható legyen. Amennyiben nincs ott, telepítse a Függelék D fejezet 14.2 pontja alapján.

14.4.3. A régi tanúsítvány cseréje 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 telepítheti szerverére, melynek lépései a következők:

Figyelem!

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

Az Exchange Managament 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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

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

15.1. 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 <a tanúsítvány thumprintje szóközök
nélkül> -BinaryEncoded:$true -Path
c:\mentett.pfx -Password:(Get-Credential).password
```

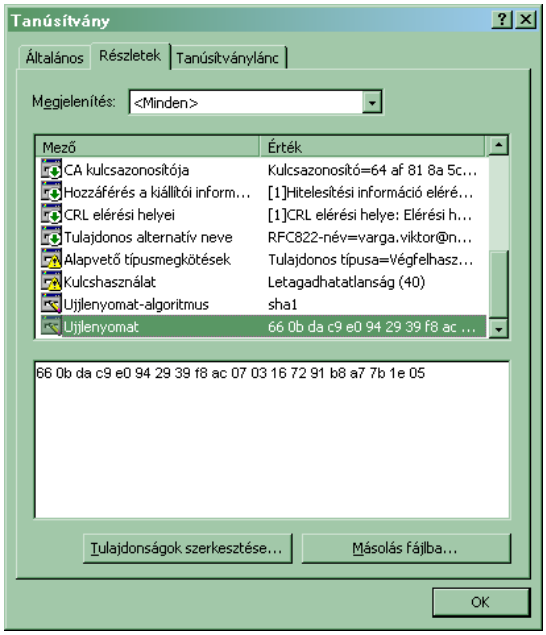
Az exportálás során meg kell adnunk a fájl jelszavát.

Értelemszerűen a <c:\mentett.pfx> helyettesítendő az aktuális fájlnévvel, azonban a fájlnévnek kötelezően .pfx kiterjesztéssel kell rendelkeznie.

15.1.1. A tanúsítvány Thumbprint-jének kiderítése az exporthoz

Lépések:

1. Nyissuk meg a tanúsítvány adatlapját, majd váltsunk a Részletek fülre
2. Gördítsünk le az ujjlenyomatig, majd az alsó mezőből tegyük vágólapra.
3. A jegyzettömbbe beszúrva szedjük ki a szóközöket.
4. Illesszük be a parancsba.



A fenti példa esetében:

A thumbprint: 66 0b da c9 e0 94 29 39 f8 ac 07 03 16 72 91 b8 a7 7b 1e 05

Ebből a szóközöket kivéve a paraméter megadási módja:

–Thumbprint 660bdac9e0942939f8ac0703167291b8a77b1e05 lesz a paraméter.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

15.2. 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 fájlnévvel.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

16. Függelék E – 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 (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, megismeri belőle a belső nevet.
3. A támadó a hitelesítés szolgáltató felé bead 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 a 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 ilyen tanúsítvány - mely e 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.

17. Függelék F – Regisztrált domain név használata a belső domain név helyett Exchange 2007 és Exchange 2010 szerveren

Windows szerverek esetén évekig a belső domain nevek használatát javasolták a belső hálózatok kiépítéséhez. Mivel belső domain névre nem adható ki tanúsítvány, ez az ajánlás megváltozott.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

Amennyiben Exchange szerverét még belső domain névvel telepítette, a tanúsítvány beszerzése után szükséges lehet ezt átállítani.

17.1.Az Exchange szerver átirányítása a külső név használatához

Az alábbi parancsok beállítják az EWS, az OAB és az Autodiscovery szolgáltatásokat:

```
Set-ClientAccessServer -Identity gepnev -AutodiscoverServiceInternalUri
https:// vargaviktor.hu /autodiscover/autodiscover.xml

Set-WebServicesVirtualDirectory -Identity "gepnev\EWS (Default Web Site)"
-InternalUrl https:// vargaviktor.hu /ews/exchange.asmx

Set-OABVirtualDirectory -Identity "gepnev\oab (Default Web Site)"
-InternalUrl https://vargaviktor.hu/oab
```

A parancsokban a **vargaviktor.hu** és a **gepnev** paramétereket saját értékeinkkel kell helyettesítenünk.

A beállítások elvégzése után szükséges a beállítások életbe lépéséhez az IIS alkalmazás pool frissítése, ennek lépései a következők:

1. Indítsuk el az IIS Manager-t! (Start > Futtatás > inetmgr)
2. Nyissuk le a szervert és azon belül az Application Pools mappát.
3. Keressük meg az **MSExchangeAutodiscoverAppPool –t és kattintsunk rajta jobb gombbal, majd válasszuk a Recycle opciót.**

A végrehajtás után az új beállítások az Exchange -ben életbe lépnek.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

18. Kulcs helyreállítása

Ha a tanúsítvány importálásakor az alábbi hibaüzenetet kapjuk, akkor a kulcsunk megsérült, elveszett, de jó eséllyel helyreállítható, ha ez nem törlés következménye volt.

A hibaüzenet:

```
xxxxxx was found but is not valid for use with Exchange Server
(reason: PrivateKeyMissing).
At line:1 char:27
+ Enable-ExchangeCertificate <<<< -Services "SMTP,POP,IMAP,IIS"
```

Ezt a tanúsítvány adatlapját megnyitva is ellenőrizhetjük, ha nem tartalmaz kis kulcsot, a rendszer nem találja a hozzá tartozó privát kulcsot.

A helyreállításhoz az alábbi lépéseket kell végrehajtania:

1. Start > Futtatás > cmd
2. A megjelenő ablakba írja be a következő parancsot:

   ```
   certutil –repairstore my ”xxxxxx”
   ```

   Ahol az ”xxxxxx” a tanúsítvány thumbprintje, az eredeti szóközökkel tagolt formában.

   A thumprint meghatározásának módját korábbi fejezet tartalmazza.

3. A fentiek után a tanúsítvány adatlapon az FRISSÍTVE vagy ÚJRA MEGNYITVA látni fogja, hogy a kis kulcs megjelent, és ezek után a tanúsítvány használható.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu