Az Internet Explorer 7+ böngésző program beállítása tanúsítványok használatához

Windows tanúsítványtárban és kriptográfia eszközökön található tanúsítványok esetén

Windows XP és Vista operációsrendszer esetén

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

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

Ennek a tájékoztatónak az a célja, hogy az elektronikus aláíráshoz és titkosításhoz szükséges kriptográfiai eszközök (intelligens kártya, kártyaolvasó) telepítése, üzembe helyezése és használata minél zökkenő mentesebben történjen meg. 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 rendelkezésére.

3. Az Internet Explorer 7 böngésző beállítása tanúsítványok használatához

A következő fejezetek az Internet Explorer 7 böngésző beállítását mutatják be, ahhoz, hogy tanúsítványait, el tudja érni, illetve használni tudja böngészőjéből.

A telepítés lépései a Windows rendszereken történő beállításokat írják le, Internet Explorer 7 böngésző esetében. A leírás kisebb eltérésekkel a korábbi verziók esetén is használható.

Javasolt, hogy az Internet Explorer böngészőből legalább 7-es vagy későbbi verziót használjon, és hogy böngészőjét rendszeresen frissítse.

4. Operációs rendszer követelmények

A tanúsítványok használatához ajánlott minimum operációs rendszer követelmény:

Windows XP SP3

Windows Vista SP1

Windows 7

5. A Windows Vista rendszerről

A Windows Vista rendszer biztonsági felépítésében új elemeket hozott be az XP-hez képest. Ahol a rendszer az XP-től eltér, külön említésre kerül a dokumentációban.

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. A közigazgatási gyökértanúsítványok telepítése

A Netlock gyökértanúsítványai már megtalálhatók a Windows operációs rendszerben, de **a közigazgatási gyökértanúsítványokat, azok használatához, telepítenie kell.**

A közigazgatási gyökértanúsítványok a következő linkeken érhetők el:

SHA1 algoritmusú kiadók:

http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.cer
http://www.netlock.hu/index.cgi?ca=mkozig
http://www.netlock.hu/index.cgi?ca=bkozig

SHA256 algoritmusú kiadók:

http://www.kgyhsz.gov.hu/KGYHSZ_CA_20091210.cer
http://www.netlock.hu/index.cgi?ca=mkozig256
http://www.netlock.hu/index.cgi?ca=bkozig256

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

6.1. A közigazgatási gyökértanúsítványok telepítésének Windows XP esetén

A lépések a következők:

1. Indítsa el az Internet Explorer böngészőt.
2. Nyissa meg a böngészővel a fent látható linkek egyikét.
3. A linket megnyitva előugrik a Tanúsítvány letöltése (Downloading Certificate) ablak.
4. A megjelenő ablakban válassza a Megnyitás (Open) opciót.
5. A következő megjelenő ablakban válassza a Tanúsítvány telepítése (Install certificate) gombot.
6. Nyomja meg kétszer a Tovább (Next) gombot.
7. Nyomja meg a Befejezés (Finish) gombot, és a megjelenő tájékoztató üzenetre nyomja meg az OK gombot.
8. Hajtsa végre a másik két linkre is a fentieket.

Ezzel a közigazgatási tanúsítványok telepítése Windows XP rendszerre megtörtént.

Figyelem!

Ha nincs telepítve a Root Update komponens vagy régi operációs rendszert használ, további gyökértanúsítvány telepítésekre lesz szüksége.

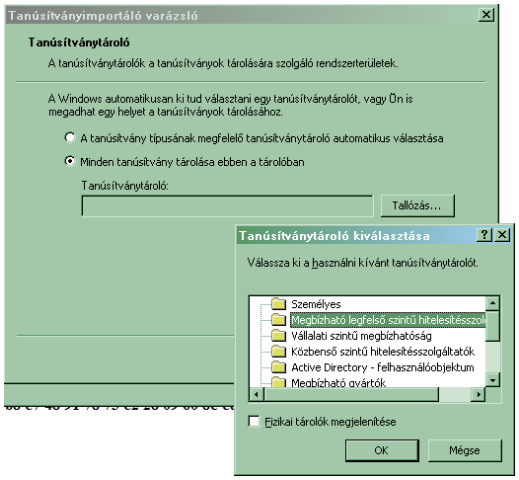
NetLock Kft. cím: 1101 Budapest, Expo tér 5-7. postacím: 1439 Budapest, Pf. 663.
telefon: +36 1 437 6655 telefax: +36 1 700 2828 e-mail: info@netlock.hu web: www.netlock.hu

6.2. A közigazgatási gyökértanúsítvány telepítése Windows Vista esetén

A KGYHSZ gyökértanúsítvány telepítése Windows Vista rendszeren a fentiekhez képest eltér.

A lépései a következők:

1. Indítsa el az Internet Explorer böngészőt.
2. Nyissa meg a böngészővel a következő linkek egyikét:
   (SHA1-SHA256 kiadóknak megfelelően)
   SHA1: http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.cer
   SHA256: http://www.kgyhsz.gov.hu/KGYHSZ_CA_20091210.cer
3. .A megjelenő ablakban válassza a Megnyitás (Open) opciót.
4. A következő megjelenő ablakban válassza a Tanúsítvány telepítése (Install certificate) gombot.
5. Nyomja meg egyszer a Tovább (Next) gombot.
6. A következő ablakban válassza a második opciót, majd „Megbízható legfelső szintű… ” opciót. (Trusted root…)
7. Az ablakot Ok gombbal hagyja jóvá, majd nyomja meg a Tovább (Next) gombot.
8. Nyomja meg a Befejezés (Finish) gombot, és a megjelenő tájékoztató üzenetre nyomja meg az OK gombot.



Ezzel a közigazgatási gyökértanúsítvány telepítése Windows Vista rendszerre megtörtént.

A másik két tanúsítvány telepítéséhez használható a Windows XP rendszernél található telepítési módszer. (SHA1-SHA256 kiadóknak megfelelően):

SHA1: http://www.netlock.hu/index.cgi?ca=mkozig
http://www.netlock.hu/index.cgi?ca=bkozig

SHA256: http://www.netlock.hu/index.cgi?ca=mkozig256
http://www.netlock.hu/index.cgi?ca=bkozig256

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. Rövid áttekintés a tanúsítvány igénylési - és tárolási megoldásokról

A tanúsítványok létrehozása és tárolása többféleképpen történhet. Ezek különbségeiről olvashat a következőkben, amely hasznos lehet a beállításhoz. Természetesen a beállítás elvégezhető ezen rövid áttekintés elolvasása nélkül, de amennyiben új digitális aláírás használó, javasoljuk elolvasni.

7.1. Tanúsítvány igénylése Mozilla böngészőn keresztül

A Mozilla böngészők, levelezők a több operációs rendszeren használhatóság érdekében a tanúsítványokat egy-egy saját védett tárolóban tárolják, melyhez csak az adott, illetve az ezt megfelelően kezelni tudó alkalmazás fér hozzá, az operációs rendszer irányából nem látszik.

Amikor Mozilla böngészővel hoz létre weboldalunkon egy kérelmet, akkor a privát kulcs a böngésző saját tárában jön létre, ott tárolódik, és a később kiadott tanúsítványt a Mozilla böngészővel az ügyfélmenü importálás pontját választva helyezi be véglegesen a tárolóba, ez után lesz az használható.

Ekkor készíthet róla biztonsági mentést, mely a szabványos PKCS#12 (vagy másik nevén PFX) fájlformátumban jön létre.

Fontos megjegyezni, hogy a böngésző is védi ezt a kulcsot (Mesterjelszó), amit első alkalommal Ön állít be, amennyiben ezt a jelszót elfelejti, nincs lehetőség a későbbiekben sem a tanúsítvány használatára, ezért a böngésző védelmi jelszavát biztonságosan tárolja.

Mivel minden egyes Mozilla termék, külön tanúsítványtárral rendelkezik, ha másik Mozilla termékből kívánja használni tanúsítványát, arról itt mentést kell készítenie, és oda is telepítenie kell azt.

Fontos! A tanúsítványkérelem beadása (kulcsgenerálás) és az elkészült tanúsítvány importálása közötti időszakban, **ne telepítse újra operációs rendszerét, se böngészőjét**, mivel ezzel helyreállíthatatlanul törli a tanúsítványához tartozó privát kulcsot is; e nélkül pedig az használhatatlan lesz.

7.2. Tanúsítvány igénylése Internet Exploreren keresztül

A Windows operációs rendszer biztosít egy központi tanúsítvány tárat, amelyet az alkalmazások, amelyeket erre felkészítettek, elérhetnek. Ehhez a tárhoz fér hozzá a teljesség igénye nélkül a Microsoft Internet Explorer, az Outlook és Outlook Express programok, illetve a digitális aláírásra képes Office alkalmazások is.

Amikor Internet Explorer böngészővel hoz létre weboldalunkon egy kérelmet, akkor a privát kulcs a Windows operációs rendszer tanúsítványtárában jön létre, ott tárolódik, és a később kiadott tanúsítványt az Internet Explorer böngészővel, az ügyfélmenü importálás pontját választva helyezi be véglegesen a tárolóba, ez után lesz az használható.

Ekkor készíthet róla biztonsági mentést, mely a szabványos PKCS#12 (vagy másik nevén PFX) fájlformátumban jön létre.

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

Fontos! A tanúsítványkérelem beadása (kulcsgenerálás) és az kiadott tanúsítvány importálása közötti időszakban **ne telepítse újra operációs rendszerét, se böngészőjét**, mivel ezzel helyreállíthatatlanul törli a tanúsítványához tartozó privát kulcsot is, e nélkül pedig az használhatatlan lesz.

7.3. Tanúsítvány és kulcsok kriptográfiai eszközön (kártyán, tokenen)

Igen népszerű igénylési mód a tanúsítványok kártyán vagy tokenen való igénylése, mely az eszközök és a hozzá tartozó PIN kód miatt egy fokkal magasabb biztonságot is nyújt.

Az ilyen eszközökben a privát kulcs biztonságosan tárolódik, az egyes aláírási műveletek közben sem kerül ki az eszközből, hanem az kapja meg a feladatot, és PIN kód kérés után adja vissza az eredményt.

Amikor egy ilyen eszközt használ, akkor előtte természetesen a meghajtó (driver) programokat telepítenie kell a gépre, melyek telepítése során az eszköz a Windows tanúsítványtárával magas fokon integrálódik, tehát Windows tanúsítványtárat használó alkalmazások (a teljesség igénye nélkül: a Microsoft Internet Explorer, az Outlook és Outlook Express programok, illetve a digitális aláírásra képes Office alkalmazások) rögtön használni tudják.

Amennyiben az alkalmazás NEM használja a Windows tanúsítvány tárat (például Mozilla programok) természetesen meg kell mondani az alkalmazásnak, hogy hogyan éri el az eszközt. Ezért bonyolultabb például a Mozilla programok beállítása.

Az ilyen eszközön kiadott tanúsítványokról egyébként nem tud PKCS#12 (vagy másik nevén PFX) mentést csinálni, mert a kártyáról a privát kulcs nem szedhető ki.

7.4. Tanúsítvány és kulcsok PKCS#12 (PFX) állományban

Mint az előbbiekben olvashatta, a PKCS#12 (vagy másik nevén PFX) fájlformátum alapvetően biztonsági mentés, illetve kulcsok és tanúsítványok együttes mozgatása gépek között céljára szolgálhat. Ilyen formában tanúsítványt nem tud igényelni, hanem csak létrehozni tudja azokat, melyeket helyreállítási céllal egyébként is lényeges megtennie.

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

8. A tanúsítványok telepítése

Az előző fejezetekben áttekintetteknek megfelelően, a következők leírják, hogyan tudja a tanúsítványát beállítani a használathoz.

8.1. Ha a tanúsítvány kártyán, tokenen található

Amennyiben tanúsítványát kriptográfiai eszközön kapta meg, akkor a kriptográfiai eszköz telepítési útmutatója leírja, hogyan importálható a tanúsítvány a Windows tanúsítványtárba. Kérjük, hajtsa végre az ott leírtakat.

8.2. Ha a tanúsítvány már a gépen található

Ha a tanúsítvány igénylését (fokozott biztonságú tanúsítvány esetén) Internet Explorerből intézte, a tanúsítvány kiadási folyamat végén a tanúsítvány és a kulcsok megtalálhatók az Ön gépén.

Ekkor nincs szükség a tanúsítvány telepítésére, azonban biztonsági másolatot érdemes létrehoznia.

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

8.3. Ha a tanúsítványkérelem beadása Mozilla böngészőn keresztül történt

Amennyiben a kérelmet Mozilla böngészőn keresztül adta be, a később kiadott tanúsítványt a Mozilla böngészővel, a NetLock ügyfélmenüjébe belépve (itt: Tanúsítványok menüpont> Kiadott tanúsítványok) az importálás pontot választva tudja véglegesen Mozilla saját tanúsítványtárolójába behelyezni, majd ezt importálnia kell, és a Windows tanúsítvány tárba telepítenie.

8.3.1. Tanúsítvány exportálása Firefox böngészőből Windows tanúsítványtárba telepítéshez

A Firefox böngésző az egyik leggyakoribb Mozilla böngésző, ezért a PKCS#12 mentés készítését ezen mutatjuk be, a többi Mozilla termék PKCS#12 mentés készítését az adott termékhez készült dokumentáció mutatja be.

1. Indítsa el a Firefox böngészőt.
2. Navigáljon el a Tanúsítványok menüpontig. Eszközök > Beállítások > Speciális (Haladó) > Titkosítás fül > Tanúsítványkezelő gomb (Tools > Options > Advanced > Encryption fül > Manage certificates gomb).
3. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön válassza ki mentendő tanúsítványt, majd nyomja meg a Mentés (Backup) gombot.
4. A következő ablakban adja meg a mentés helyét.
5. Ezt követően adja meg Firefox-on belüli tanúsítványvédelmi jelszót. (mesterjelszó / master password) (Ez az első tanúsítvány export-import előtt nincs beállítva, ekkor kétszer kell begépelnie, és a későbbiek során ez után fog rendszeresen érdeklődni a Firefox böngésző.)
6. Ezután adja meg a .pfx fájl jelszavát, amellyel védeni kívánja, ezt a jelszót jegyezze is fel.
7. A mentés után tájékoztatást kap, hogy az sikeresen megtörtént, majd nyomjon Ok gombot az összes ablak bezáródásáig.

A tanúsítvány exportálása ezzel megtörtént. Javasolt az exportált állományt a telepítés után, mint biztonsági másolatot biztonságos helyre eltenni (külső adathordozón).

A következő fejezet ismerteti a PKCS#12 állományok telepítését.

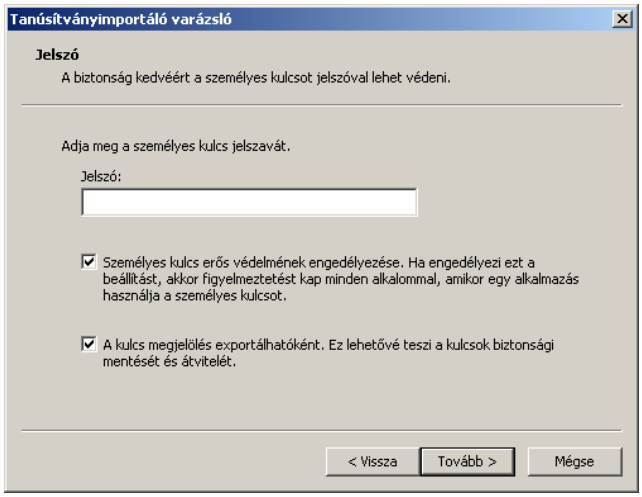
8.4. PKCS12 (PFX) fájlban található tanúsítvány telepítése Windows tanúsítványtárba

Abban az esetben, ha tanúsítványát nem kriptográfiai eszközön szerezte be, és nem Internet Explorer böngészőn keresztül igényelte, akkor az arról készült PKCS#12 (.pfx) formátumú mentett állomány segítségével is tudja tanúsítványát a Windows tanúsítványtárban beállítani.

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 Windows tanúsítványtárba a tanúsítvány és kulcs importálásának folyamata a következő:

1. Ahhoz, hogy a gépén található PKCS#12 állományt telepítse, kattintson kétszer az Intézőből (Explorer) a *.pfx, (*.p12) kiterjesztésű fájlra. Ekkor a tanúsítvány telepítése varázsló indul el.
2. Az üdvözlő képernyőn nyomja meg a Tovább (Next) gombot.
3. A második képernyőn az importálandó fájl nevét látja. Itt nincs semmi teendő, lépjen tovább a Tovább (Next) gomb segítségével.
4. A következő képernyőn adja meg a PKCS#12 fájlhoz tartózó jelszót. Itt állíthatja be a tanúsítvány erős védelmét és későbbi exportálhatóságát. Javasoljuk mindkét opciót kipipálni és ezután a Tovább (Next) gombot megnyomni.



5. 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.
6. Az utolsó képernyőn kattintson a Befejezés (Finish) gombra.

A tanúsítvány telepítése ezzel megtörtént.

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

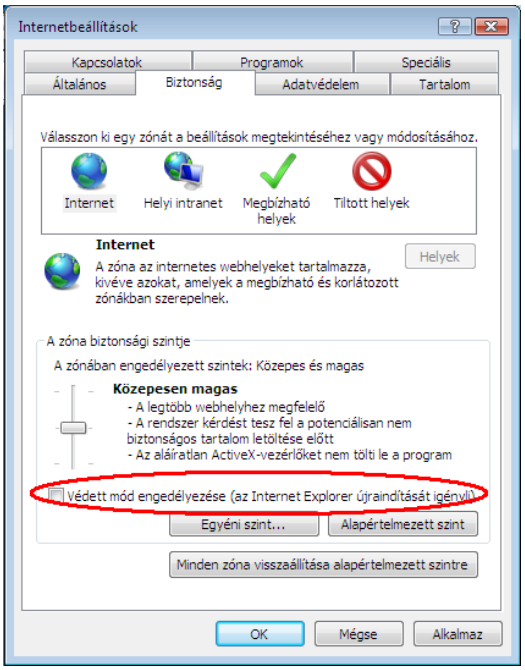
9. Tanúsítvány használat Windows Vista rendszeren

A Windows Vista rendszer alapértelmezés szerint az Internet Explorert egy ún. sandbox-ban futtatja, azaz a böngésző nem fér hozzá a számítógépen található szenzitív adatokhoz, többek között a tanúsítványokhoz SEM.

Ezért a böngészőben, ha tanúsítványt akarunk használni, a **Védett módot** ki kell kapcsolni.

Ezt a következőképp tehetjük meg:

1. Indítsa el az Internet Explorer böngészőt.
2. Navigáljon el a Biztonság menüponthoz.
   (Eszközök > Internet beállítások > Biztonság fül)
   (Tools > Internet Settings > Security fül)
3. A megjelenő ablakban szedjük ki a pipát a Védett mód… (Protected mode…) opció mellől, majd a böngésző újraindítása szükséges.



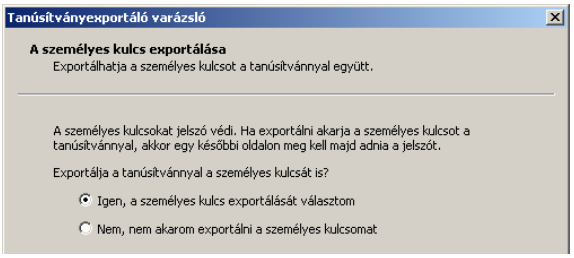
Ezzel a tanúsítványaink használhatóvá válnak Internet Explorer böngészőből Vista rendszer alól is.

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

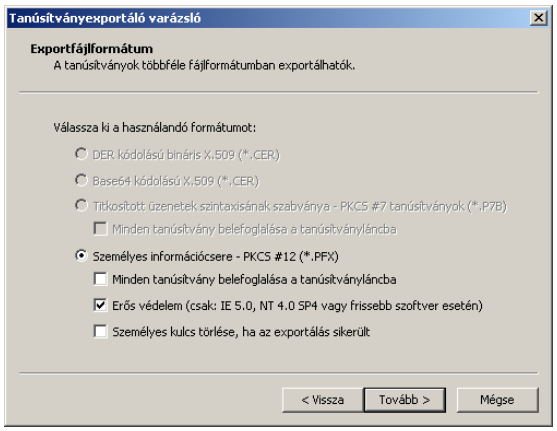
10. Függelék A – Biztonsági másolat készítése tanúsítványairól és kulcsairól

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

4. A kulcs és tanúsítvány exportálásához indítson Internet Explorer böngészőt.
5. Navigáljon el a tanúsítványok menüponthoz. (Eszközök > Internet beállítások > Tartalom fül > Tanúsítványok gomb) (Tools > Internet Settings > Content fül > Certificates gomb)
6. Válassza ki a Saját (Personal) lapon a tanúsítványok közül az exportálandót, majd nyomja meg az Export gombot.
7. A megjelenő tanúsítvány exportáló varázsló üdvözlő képernyőjén nyomja meg a Tovább (Next) gombot.



8. A következő ablakban válassza a privát kulcs exportálását is (Yes, export the private...), majd kattintson a Tovább (Next) gombra.
9. 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.



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

A tanúsítvány exportálása ezzel megtörtént.

Ezt az állományt érdemes biztonságos helyen elzárni valamilyen adathordozón.

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

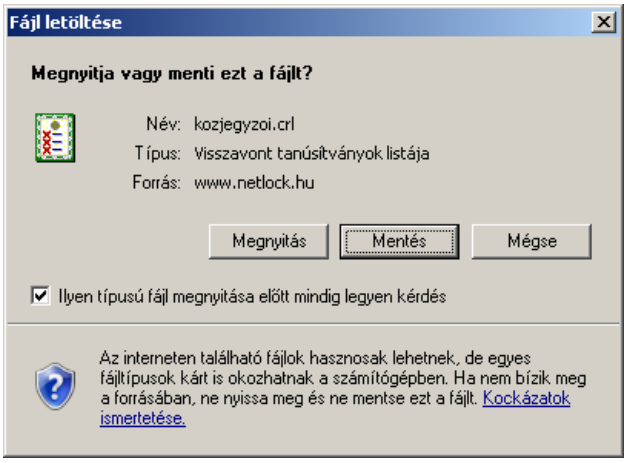
11. Függelék B - Visszavonási listák első letöltése

A visszavonási listák azokat a tanúsítványokat tartalmazzák, amelyeket valamilyen okból (elveszett a kártya, stb.) a tulajdonosok visszavontak. Ezeket az Ön biztonsága érdekében javasolt letölteni.

Ezt a következőképpen tudja megtenni:

Látogasson el az Internet Explorer böngészővel a http://www.netlock.hu/html/cacrl.html weboldalra, a Visszavonási listák menüpontok alatt kattintson rá minden egyes visszavonási listára. (Teszt nem szükséges.)

A linkre kattintva válassza a Mentés (Save) gombot, majd mentse le a számítógép munkaasztalára.



Ezután az Asztalra visszatérve egy új ikont találhatunk.

Ezen az ikonon jobb gombbal kattintva és a Tanúsítvány telepítése (Install certificate) opciót választva kezdheti meg a visszavonási lista telepítését.

Az előugró ablakban kétszer a Tovább (Next), majd a Befejezés (Finish) gombot kell megnyomnia.

A visszavonási listák telepítését minden osztályra érdemes első alkalommal elvégeznie.

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