

Tanúsítvány és hozzá tartozó kulcsok telepítése szoftveresen tárolt tanúsítványok esetén

Windows XP és Vista rendszeren,
PFX fájlban található tanúsítvány és kulcsok esetében

1. Tartalomjegyzék

1.	Tartalomjegyzék	2
2.	Bevezető	3
3.	A szoftver/hardver korlátozásai	3
4.	Rövid áttekintés a tanúsítvány igénylési - és tárolási megoldásokról.....	4
4.1.	Tanúsítvány igénylése Internet Exploreren keresztül.....	4
4.2.	Tanúsítvány igénylése Mozilla böngészőn keresztül.....	4
5.	A tanúsítványok tárolása és kezelése Windows és Firefox 3+ tanúsítványtár esetén.....	6
5.1.	Biztonsági másolat, avagy PFX állomány készítése tanúsítványairól és kulcsairól Internet Explorer böngészőből.....	6
5.2.	Biztonsági másolat készítése tanúsítványairól és kulcsairól Firefox 3+ böngészőből.....	8
6.	PFX állományban lévő tanúsítványok telepítése	9
6.1.	PKCS12 (PFX) fájlban található tanúsítvány telepítése Windows tanúsítványtárba.....	9
6.2.	PKCS12 (PFX) fájlban található tanúsítvány telepítése Firefox 3+ böngésző tanúsítvány tárába.....	10
7.	A közigazgatási gyökértanúsítványok telepítése	11
7.1.	A közigazgatási gyökértanúsítványok telepítésének Windows XP esetén	11
7.2.	A közigazgatási gyökértanúsítvány telepítése Windows Vista esetén.....	12
7.3.	A közigazgatási gyökértanúsítvány telepítése Firefox 3+ esetén.....	13
8.	Függelék A – Hibalehetőségek és javításuk.....	14
9.	Függelék B - Visszavonási listák első letöltése.....	15
9.1.	Visszavonási lista Internet Explorer böngészőben	15
9.2.	Visszavonási lista Firefox 3+ böngészőben.....	16
9.2.1.	KGYHSZ visszavonási lista letöltése Firefox 3+ böngészőbe	17

2. Bevezető

Ennek a tájékoztatónak az a célja, hogy az elektronikus aláíráshoz és titkosításhoz szükséges tanúsítványok telepítése és használata minél zökkenő mentesebben történjen meg. 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 szoftver/hardver korlátozásai

A szoftveresen tárolt tanúsítványok használatához ajánlott minimum operációs rendszer követelmény:

Windows XP SP3

Windows Vista SP1

A leggyakrabban használt böngészők esetében:

Internet Explorer 7

Firefox 3+

Kérjük, hogy mindig a legfrissebb böngésző verziót használja, annak frissítését a tanúsítvány igénylés megkezdése előtt végezze el!

Figyelem!

A Windows 98 SE, Windows ME, Windows NT és Windows 2000 rendszerek Microsoft támogatása megszűnt ezért azok nem támogatottak.

A szoftver 64 bites rendszereken (XP, Vista) nem került tesztelésre.

4. 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.

4.1. 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.

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.

4.2. 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, vagy a Windows tanúsítvány tárába is telepíteni kívánja (javasolt) azt, 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.

5. A tanúsítványok tárolása és kezelése Windows és Firefox 3+ tanúsítványtár esetén

Az Ön által igényelt szoftveresen tárolt aláírói tanúsítványának kulcsai vagy a Windows tanúsítvány tárában vagy annak a böngészőnek a tanúsítvány tárában vannak, melyben a tanúsítványt igényelte, majd letöltötte.

Annak érdekében, hogy tanúsítványáról biztonsági másolatot tudjon készíteni, illetve egy másik számítógépre, vagy böngészőbe tudja telepíteni, szükséges a tanúsítványról és a hozzá tartozó kulcsokról mentést készítenie.

Aszerint, hogy tanúsítványát mely böngésző tanúsítvány tárában tárolja, ezek a lépések eltérőek lehetnek.

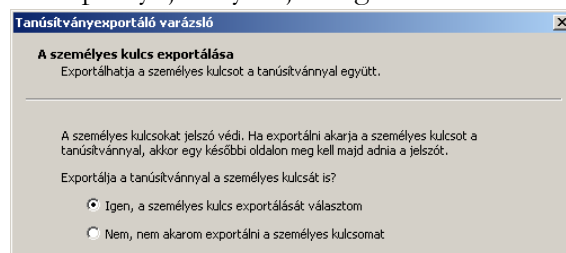
Útmutatónk a két leggyakrabban használt böngészőt mutatja be.

Amennyiben ettől eltérő böngészőt használ, kérjük, keresse az arra vonatkozó leírásunkat!

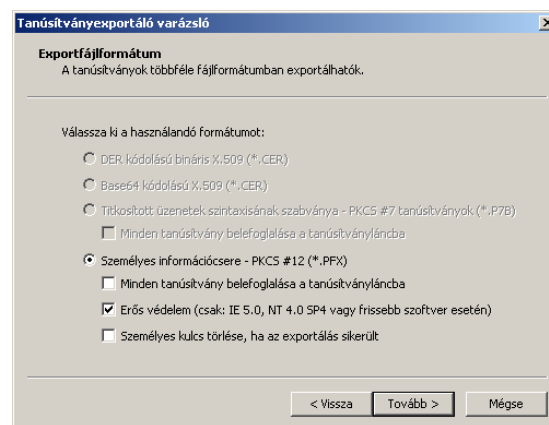
5.1. Biztonsági másolat, avagy PFX állomány készítése tanúsítványairól és kulcsairól Internet Explorer böngészőből

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. Továbbá így lehetősége nyílik azt más számítógépre, vagy böngészőbe telepíteni.

1. A kulcs és tanúsítvány exportálásához indítson Internet Explorer böngészőt.
2. Navigáljon el a tanúsítványok menüponthoz. (Eszközök > Internet beállítások > Tartalom fül > Tanúsítványok gomb) (Tools > Internet Settings > Content fül > Certificates gomb)
3. Válassza ki a Saját (Personal) lapon a tanúsítványok közül az exportálandót, majd nyomja meg az Export gombot.
4. A megjelenő tanúsítvány exportáló varázsló üdvözlő képernyőjén nyomja meg a Tovább (Next) gombot.
5. A következő ablakban válassza a privát kulcs exportálását is (Yes, export the private...), majd kattintson a Tovább (Next) gombra.



6. 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.



7. 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.

8. A következő ablakban kiválaszthatjuk a fájlnevet, és a helyet, ahol a fájlt létre szeretnénk hozni.

9. 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.

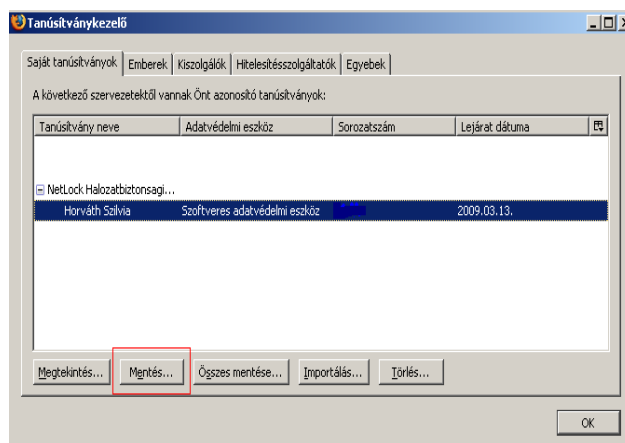
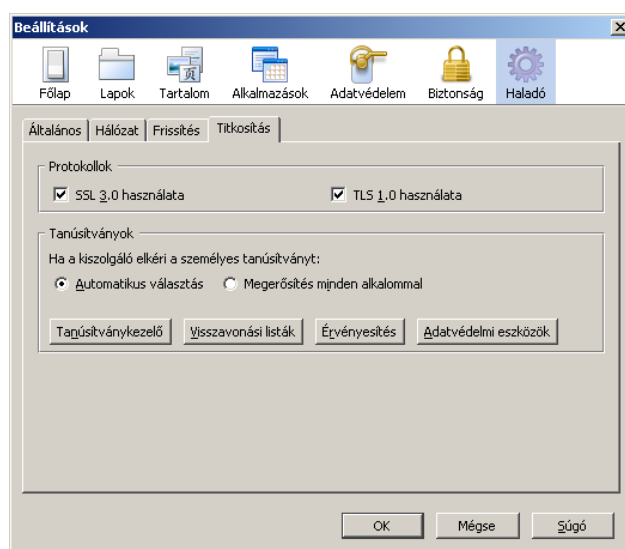
Ezt az állományt érdemes biztonságos helyen elzárni valamilyen adathordozón.

5.2. Biztonsági másolat készítése tanúsítványairól és kulcsairól Firefox 3+ böngészőből

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.

Továbbá így lehetősége nyílik azt más számítógépre, vagy böngészőbe telepíteni.

1. Indítsa el a Firefox böngészőt
2. Navigáljon el a Tanúsítványok menüpontig. Eszközök > Beállítások > Haladó > Titkosítás fül > Tanúsítványkezelő gomb (Tools > Options > Advanced > Encryption fül > Manage certificates gomb).
3. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön nyomja meg a Mentés (Save) gombot.
4. A Tallózó ablakban ki tudja választani, a megfelelő könyvtárat, ahova menteni szeretné a tanúsítványt, valamint itt adhat neki egy tetszőleges nevet.
5. A következő ablakban gépeljük be a jelszót, amit szeretnénk a fájlnak adni.
6. Az OK gomb megnyomása után a tanúsítvány mentésre kerül a privát kulccsal együtt.



Ezt az állományt érdemes biztonságos helyen elzárni valamilyen adathordozón.

6. PFX állományban lévő tanúsítványok telepítése

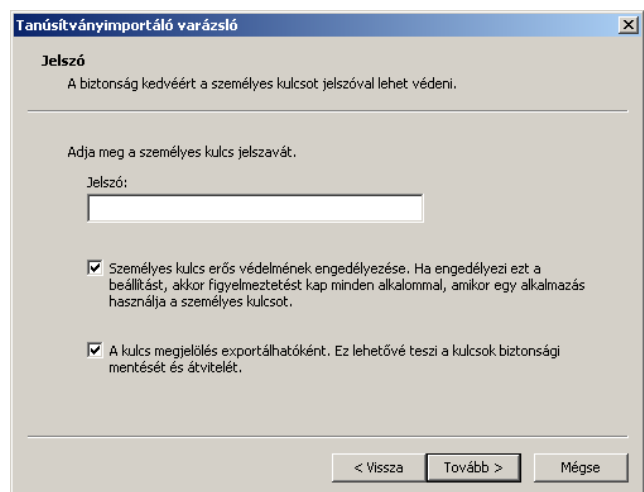
Az elkészített PFX állományokat telepítenünk kell. Ennek lépései különböznek Windows és Mozilla böngésző (pl. Firefox 3+) tanúsítvány tár esetében.

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

A Windows tanúsítványtárba a tanúsítvány és kulcs importálásának folyamata a következő:

1. Ahhoz, hogy a gépen 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 tartozó 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.



6.2. PKCS12 (PFX) fájlban található tanúsítvány telepítése Firefox 3+ böngésző tanúsítvány tárába

A Firefox böngészőbe tanúsítvány és kulcs importálásának folyamata a következő:

1. Navigáljon el a Tanúsítványok menüpontra. Eszközök > Beállítások > Haladó > Titkosítás fül > Tanúsítványkezelő gomb (Tools > Options > Advanced > Encryption fül > Manage certificates gomb).
2. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön nyomja meg az Import gombot.
3. Ezután tallózza ki a PKCS #12 fájlt, amely a tanúsítványát és a hozzá tartozó kulcsot tartalmazza.
4. Adja meg Firefox-on belüli tanúsítványvédelmi jelszót. (mesterjelszó / master password) (Ez az első tanúsítványimportálás előtt nincs beállítva, ekkor kétszer kell begépelnie, és a későbbiek során ez után fog rendszeresen érdeklődni a Firefox böngésző.)
5. Ezután adja meg a .pfx fájl jelszavát, amelyet exportálásakor megadott. (Ha adott neki ilyen jelszót.)
6. Az importálás után tájékoztatást kap arról, hogy az importálás sikeresen megtörtént, majd nyomjon Ok gombot az összes ablak bezáródásáig.

Ezzel a tanúsítványa és a hozzá tartozó kulcs importálásra került.

7. A közigazgatási gyökértanúsítványok telepítése

A Netlock A, B, C, QA osztályú gyökértanúsítványai már megtalálhatók a Windows operációs rendszerben, de

a közigazgatási gyökértanúsítványokat azok használatához telepítenie kell.

A közigazgatási gyökértanúsítványok a következő linkeken érhetők el:

http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.cer

<http://www.netlock.hu/index.cgi?minositett&raw&ca=mkozig>

<http://www.netlock.hu/index.cgi?raw&ca=bkozig>

7.1. 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.

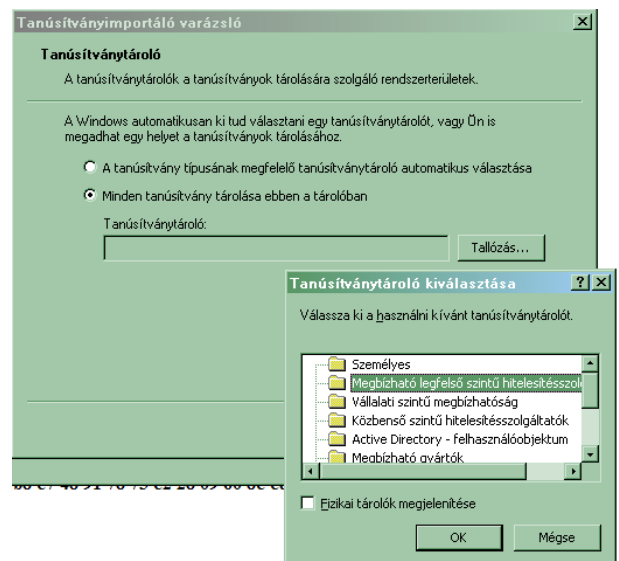
7.2. A közigazgatási gyökértanúsítvány telepítése Windows Vista esetén

A KGYHSZ gyökértanúsítvány telepítése Vista rendszeren eltér a többitől.

A lépései a következők:

1. Indítsa el az Internet Explorer böngészőt.
2. Nyissa meg a böngészővel a következő linket:
http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.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.
- 9.

Ezzel a közigazgatási gyökértanúsítvány telepítése Windows Vista rendszerre megtörtént.



A másik két tanúsítvány telepítéséhez használható a Windows XP rendszerénél található telepítési módszer.

<http://www.netlock.hu/index.cgi?minositett&raw&ca=mkozig>

<http://www.netlock.hu/index.cgi?raw&ca=bkozig>

7.3. A közigazgatási gyökértanúsítvány telepítése Firefox 3+ esetén

A Firefox 2.0+ verziótól kezdve a NetLock A, B, C, QA osztályú gyökértanúsítványai már megtalálhatók az alkalmazásban, de a **közigazgatási gyökértanúsítványokat – azok használatához – telepítenie kell.**

A közigazgatási gyökértanúsítványok több helyen érhetők el.

A közigazgatási gyökértanúsítványok telepítésének lépései a következők:

1. Indítsa el a Firefox böngészőt.
2. Nyissa meg a böngészővel az alábbi linkek egyikét:
<http://www.netlock.hu/index.cgi?minositett&raw&ca=mkozig>
<http://www.netlock.hu/index.cgi?raw&ca=bkozig>
3. A linket megnyitva előugrik a Tanúsítvány letöltése (Downloading Certificate) ablak.
4. Ebben az ablakban pipálja ki a mind a három opciót.
5. Miután kipipálta az összes opciót kattintson az Ok gombra.
6. Hajtsa végre a másik linkre is a fentieket.

7. Nyissa meg a böngészővel az alábbi linket:
http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.cer
8. A linket megnyitva előugrik a Letöltés (Downloading...) ablak.
9. A megjelenő ablakban válassza a Fájl mentése... (Save) opciót, és mentse olyan helyre, ahol később megtalálja azt.
10. Navigáljon el a Tanúsítványok menüpontra.
Eszközök > Beállítások > Haladó > Titkosítás fül > Tanúsítványkezelő gomb
(Tools > Options > Advanced > Encryption fül > Manage certificates gomb).
11. Válassza ki a Hitelesítés szolgáltatók (Trusted root...) fület, majd nyomja meg az Importálás (Import) gombot és tallózza ki az imént lementett tanúsítványt.
12. Ebben az ablakban pipálja ki a mind a három opciót. Miután kipipálta az összes opciót kattintson az Ok gombra.

Ezzel a közigazgatási tanúsítványok telepítése megtörtént.

8. Függelék A – Hibalehetőségek és javításuk

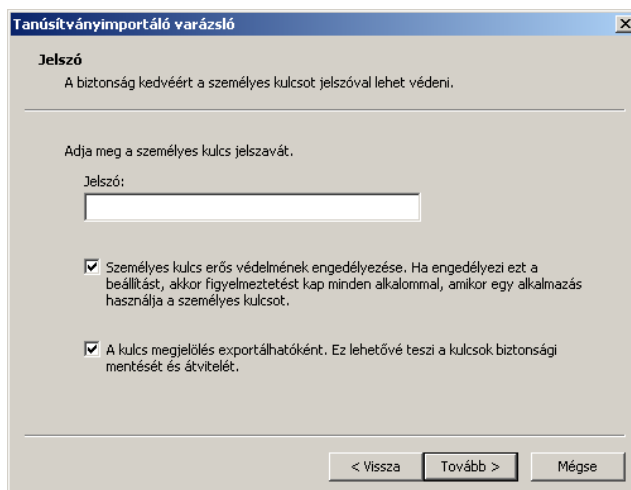
- **Nem tudok telepíteni, mert a gép azt mondja, hogy adminisztrátori jogosultság szükséges hozzá.**

Valószínűleg nem rendszergazdaként van belépve a gépre, és nincs jogosultsága jelenleg a telepítéshez. Ebben az esetben lépjen be rendszergazdaként és így próbálja meg a telepítést, vagy szóljon a rendszergazdájának.

- **Nem tudok biztonsági másolatot készíteni, mert nem engedi kiválasztani a személyes kulcs importálása lehetőséget Windows tanúsítványtárból.**

A PFX állomány telepítésekor a személyes kulcs importálása lehetőségét ki kell választani annak érdekében, hogy a későbbiekben a tanúsítványról mentést készíthessünk (pl. megújítást követően).

Ha nem választottuk ezt a lehetőséget, a meglévő PFX állományból újra tudjuk telepíteni azt (eltávolítás, majd újra telepítés), amikor is a személyes kulcs importálását ki tudjuk választani.



9. Függelék B - Visszavonási listák első letöltése

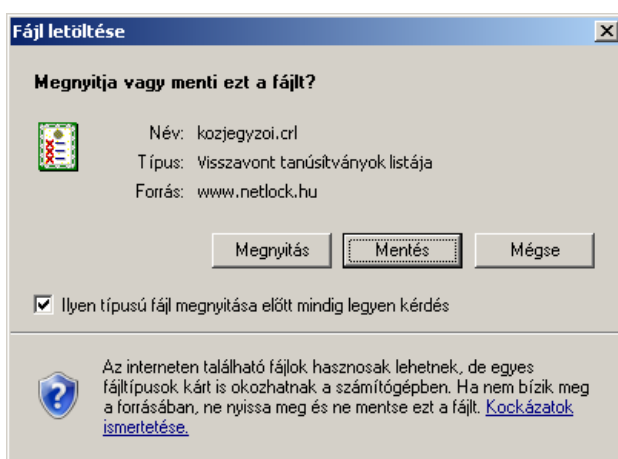
A visszavonási listák azokat a tanúsítványokat tartalmazzák, amelyeket valamilyen okból (elveszett a kártya, stb.) a tulajdonosok visszavontak. Ezeket az Ön biztonsága érdekében javasolt letölteni.

9.1. Visszavonási lista Internet Explorer böngészőben

Ezt a következőképpen tudja megtenni:

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

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



Ezután az Asztra 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.



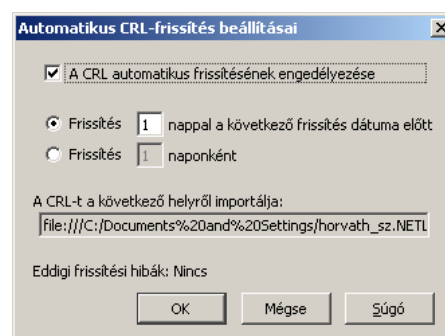
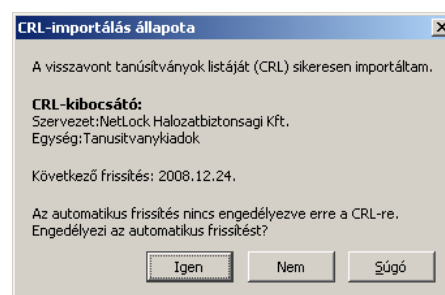
Az előugró ablakban kétszer a Tovább (Next), majd a Befejezés (Finish) gombot kell megnyomnia.

A visszavonási listák telepítését minden (QA, A, B, C, KQA, KB) osztályra érdemes első alkalommal elvégeznie.

9.2. Visszavonási lista Firefox 3+ böngészőben

A visszavonási listák letöltése az Firefox böngészőbe a következő módon történik:

1. Indítsa el a Firefox böngészőt, és látogasson el vele a <http://www.netlock.hu/html/cacrl.html> oldalra.
2. A bal oldalt található "Visszavonási listák letöltése böngészőbe" menüpontban található az egyes tanúsítványkiadók visszavonási listái, melyekre kattintva egyesével letöltheti őket.
3. Rákattintva valamelyikre, előugrik egy „CRL-importálás állapota” (CRL Import State) ablak.
4. Ebben az ablakban a program tájékoztat arról, hogy az importálás sikeresen megtörtént, és megtekinthetjük a CRL listák automatikus frissítésének beállításait az Igen (Yes) gomb megnyomásával. Ezt nyomjuk is meg.
5. A megjelenő ablakban az automatikus frissítést kapcsolhatjuk be a "CRL automatikus frissítésének engedélyezése" opció kipipálásával. (Automatic update for this CRL)
6. A többi opcióval a frissítés gyakoriságát állíthatjuk be, ami lehet x nappal a következő frissítés dátuma előtt (első opció), vagy x naponként (második opció). Ezt javasolt alapértelmezetten hagyni (vagyis 1 nappal a következő frissítés dátuma előtt)
7. A fenti folyamatot érdemes a többi visszavonási listára is elvégeznie.



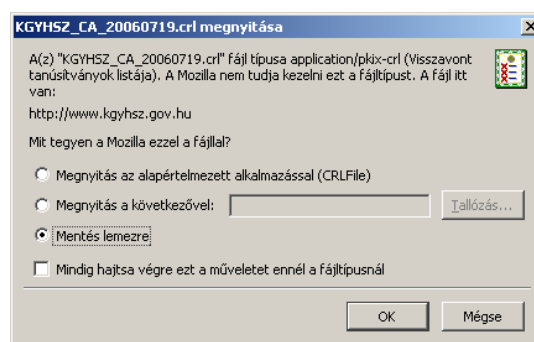
Amennyiben a visszavonási listák automatikus letöltését beállította, a továbbiakban ez a böngésző indulásakor automatikusan megtörténik, a szokásos, visszavonási listákban megadott időközönként.

Ha sürgősen a legfrissebb listára van szüksége, akkor az itt leírtak alapján azt bármikor megismételheti.

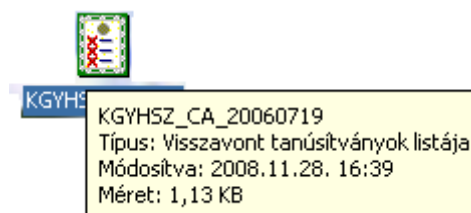
9.2.1. KGYHSZ visszavonási lista letöltése Firefox 3+ böngészőbe

1. A Firefox böngészőben nyissa meg az alábbi linkeket:
http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.crl

2. A linket megnyitva előugrik a Letöltés (Downloading...) ablak.
3. A megjelenő ablakban válassza a Fájl mentése... (Save) opciót, és mentse olyan helyre, ahol később megtalálja azt.



4. A Firefox böngésző File menüjéből válassza a File megnyitása (Open) lehetőséget.
5. Ekkor tallózó ablakot kap, ahol meg tudja keresni a korábban elmentett file-t.



6. A file kiválasztását követően az alábbi ablak fog megjelenni.

