

A Firefox 3+ böngésző program beállítása tanúsítványok használatához

Böngészővel igényelt, Windows tanúsítványtárban, vagy PFX fájlban, vagy
kriptográfia eszközökön található tanúsítványok esetén
(Windows és Linux operációs rendszereken)

1. Tartalomjegyzék

1.	Tartalomjegyzék	2
2.	Bevezető	4
3.	A Firefox böngésző beállítása tanúsítványok használatához	4
4.	A Firefox szoftver tanúsítványkezelésnek hibái	4
5.	A Linux rendszerek korlátozásai.....	4
6.	A közigazgatási gyökértanúsítványok telepítése	5
7.	Rövid áttekintés a tanúsítvány igénylési - és tárolási megoldásokról.....	6
7.1.1.	Tanúsítvány igénylése Mozilla böngészőn keresztül.....	6
7.1.2.	Tanúsítvány igénylése Internet Exploreren keresztül.....	7
7.1.3.	Tanúsítvány és kulcsok PKCS#12 (PFX) állományban.....	7
7.1.4.	Tanúsítvány és kulcsok kriptográfiai eszközön (kártyán, tokenen).....	7
8.	A tanúsítványok beállítása.....	9
8.1.	Kártyán, tokenen tárolt tanúsítvány beállítása	9
8.2.	Tanúsítványkérelem beadása Mozilla böngészőn keresztül történt.....	9
8.3.	PKCS#12 mentés készítése tanúsítványairól és kulcsairól Firefox 3+ böngészőből.....	9
8.4.	Tanúsítványkérelem beadása Internet Explorer böngészőn keresztül történt	10
8.4.1.	Tanúsítvány PKCS#12 mentése Internet Explorerből.....	10
8.4.1.	PKCS12 (PFX) fájlban található tanúsítvány telepítése.....	11
9.	PIN kód megadása az alkalmazásban, ha kriptográfiai eszközt (Smart kártya, USB token) használ.....	12
9.1.	Micardo kártya esetén.....	12
9.2.	Oberthur kártya esetén.....	13
9.3.	Rainbow Ikey 2032 token esetén.....	13
10.	Függelék A - Egyes alkalmazások együttes futtatásával kapcsolatos lehetséges problémák.....	14
11.	Függelék B - A visszavonási listák letöltése	15

11.1.	KGYSZ visszavonási lista letöltése.....	16
12.	Függelék C – Biztonsági másolat készítése tanúsítványairól és kulcsairól Firefox 3+ böngészőből.....	18

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 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 Firefox böngésző beállítása tanúsítványok használatához

A következő fejezetek a Firefox 3.0+ böngésző beállítását mutatják be ahhoz, hogy tanúsítványait el tudja érni, illetve használni tudja böngészőjéből.

Javasolt, hogy a Firefox böngészőből mindig a legfrissebb verziót használja.

4. A Firefox szoftver tanúsítványkezelésnek hibái

Az elvégzett működési tesztek alapján a következő hibák kerültek feltárássra.

(A problémák a fejlesztő felé bejelentésre kerültek.)

1. A szoftverbe más személy tanúsítványát importálni nem lehetséges, ezért nehézkessé válhat a titkosított levelek küldése, fogadása.
2. A kriptográfiai eszközön tárolt tanúsítványok közül csak az első aláíró és titkosító tanúsítvány használható, a szoftver nem kezeli megfelelően az ilyen tanúsítványokat.
3. A beimportált szoftveres tanúsítványok közül csak az első aláíró és titkosító tanúsítvány használható, a szoftver nem kezeli megfelelően az ilyen tanúsítványokat.
4. A kriptográfiai eszközön tárolt tanúsítványok esetén a szoftverből ne töröljük a tanúsítványt, mert az a kártyáról is törli azt.

5. A Linux rendszerek korlátozásai

Az útmutató lépései Linux esetén megegyeznek a Windows verzió megoldásaival, a képernyő képek azonban kissé eltérhetnek.

Tesztjeink alapján jelenleg a Linux rendszerek smart kártya kezelésre nem alkalmasak, de a PFX fájlban található tanúsítványok, illetve a web felületen keresztüli tanúsítvány igénylések megfelelően működnek.

6. A közigazgatási gyökértanúsítványok telepítése

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.

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 is, de amennyiben új digitális aláírás használó, javasoljuk elolvasni.

7.1.1. 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.

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.

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.

Amennyiben abban a Mozilla termékben igényeltük a tanúsítványt, amelyikből használni kívánjuk, akkor a tanúsítvány már használható.

Ha nem így történt, akkor az adott Mozilla termékből PKCS#12 mentést kell készíteni, majd a használandó termékbe telepíteni azt.

A mentés készítéséhez vegye igénybe az adott szoftver beállítási útmutatóját.

7.1.2. 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.

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

Mivel a Mozilla termékek nem férnek hozzá ehhez a közös tanúsítványtárolóhoz ezért mindenfélekképp exportálni kell a Windows tanúsítvány tárból az ilyen tanúsítványát.

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

Mint az előbbieken 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.

7.1.4. 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 nyújtanak.

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.

8. A tanúsítványok beállítása

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

8.1. Kártyán, tokenen tárolt tanúsítvány beállítása

A kártyán, tokenen tárolt tanúsítvány beállítását a hardvereszköz telepítő csomagjának „Bongeszo” könyvtárában található a böngésző firefox.bat elindításával tudja megtenni.

Javasoljuk a hardvereszköz telepítő csomagjának és útmutatójának megtekintését.

8.2. 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, ezután lesz az használható.

Amennyiben abban a Mozilla termékben igényeltük a tanúsítványt, amelyikből használni kívánjuk, akkor a tanúsítvány már használható.

Ha nem így történt, akkor az adott Mozilla termékből PKCS#12 mentést kell készíteni, majd a használandó termékbe telepíteni azt.

A mentés készítéséhez vegye igénybe az adott szoftver beállítási útmutatóját.

8.3. PKCS#12 mentés készítése tanúsítványairól és kulcsairól Firefox 3+ böngészőből

Az egyik leggyakoribb böngésző, amit a Thunderbird-del együtt használnak a Firefox böngésző, így itt ismertetjük a PKCS#12 mentés készítését Firefox böngészőből, egyéb böngészőkhöz az adott böngészők útmutatóiban talál segítséget.

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.

1. Indítsa el a Firefox böngészőt
2. Navigáljon el a Tanúsítványok menüpontra. 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.
1. A következő ablakban gépeljük be a jelszót, amit szeretnénk a fájlhoz adni. Ez a jelszó lesz az, amivel a PKCS#12 fájl titkosításra fog kerülni, hogy illetéktelenek a jelszó ismerete nélkül a tanúsítványt más gépbe, programba ne importálhassák.
5. Az OK gomb megnyomása után a tanúsítvány mentésre kerül a privát kulccsal együtt.

Ezt az állományt érdemes biztonságos helyen elzárni valamilyen adathordozón.

8.4. Tanúsítványkérelem beadása Internet Explorer böngészőn keresztül történt

Amennyiben a kérelmet Internet Explorer böngészőn keresztül adta be, a később kiadott tanúsítványt az Internet Explorer böngészővel az ügyfélmenü importálás pontját választva helyezze be véglegesen a Windows tanúsítvány tárolóba, ahonnan majd exportálnia kell azt PKCS#12 (vagy másik nevén PFX) fájlként.

8.4.1. Tanúsítvány PKCS#12 mentése Internet Explorerből

1. A kulcs és tanúsítvány exportálásához indítson Internet Explorer böngészőt.
2. Navigáljon el a tanúsítványok menüpontra. (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 nyomjon rá az Export gombra.
4. A megjelenő tanúsítványexportáló varázsló üdvözlő képernyőjén nyomjon a Tovább (Next) gombra.
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 állítsuk be az Erős titkosítást (Enable strong protection).

7. Ha szükségünk van arra, hogy a tanúsítvánnyal együtt a hozzá tartozó gyökértanúsítványt is exportáljuk, akkor jelöljük ki a „Minden tanúsítvány exportálása” opciót (Include all certificates...) is.
8. Ha a privát kulcsot törölni akarjuk az exportálás után erről a gépről, akkor jelöljük be a privát kulcs törlése (Delete the Private...) opciót is. A következő ablakban gépeljük be azt a jelszót kétszer, amit szeretnénk a fájlnak adni.
9. A következő ablakban kiválaszthatjuk a fájlnevet, és a helyet, ahol a fájlt létre szeretnénk hozni.
10. Miután ezt beállítottuk, már csak a Tovább (Next) és végül Befejezés (Finish) gombokat kell nyomkodnunk, valamint a megnyitott ablakokat Ok gombokkal bezárunk.

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

8.4.1. PKCS12 (PFX) fájlban található tanúsítvány telepítése

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

A Firefox böngészőbe tanúsítvány és kulcs importálásának folyamata a következő:

6. Navigáljon el a Tanúsítványok menüpontra. Eszközök > Beállítások > Haladó > Titkosítás fül > Tanúsítványkezelő gomb (Tools > Options > Advanced > Encryption fül > Manage certificates gomb).
7. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön nyomja meg az Import gombot.
8. Ezután tallózza ki a PKCS #12 fájlt, amely a tanúsítványát és a hozzá tartozó kulcsot tartalmazza.
9. 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.)
10. Ezután adja meg a .pfx fájl jelszavát, amelyet exportálásakor megadott. (Ha adott neki ilyen jelszót.)
11. 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.

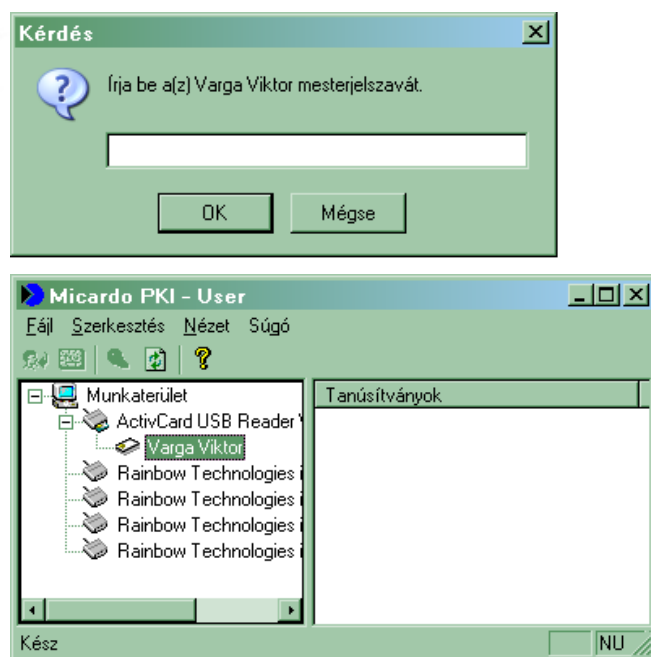
9. PIN kód megadása az alkalmazásban, ha kriptográfiai eszközt (Smart kártya, USB token) használ.

Amennyiben kriptográfiai eszközön tárolt tanúsítványt használ, abban az esetben a rendszer, amikor PIN kódot kell megadni, megtevesztően „mester jelszó” (master password) után érdeklődik.

Tehát amennyiben a következő ablakok valamelyikét látja (kriptográfiai eszköztől függően) akkor az eszköz PIN kódját kell megadnia.

9.1. Micardo kártya esetén

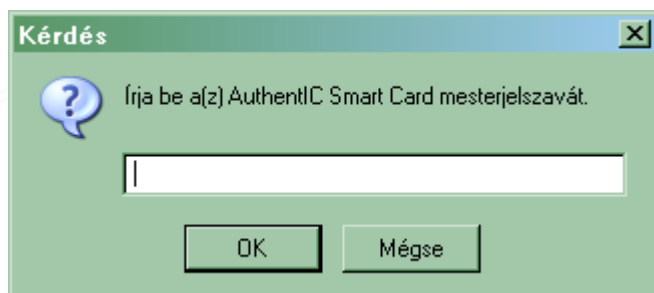
A megnevezés (mint a példában is látható), megegyezik a Micardo PKI programban látható megnevezéssel, ami alapértelmezésben a tanúsítvány tulajdonos neve szokott lenni.



Tehát ebben az esetben a kártya PIN kódját kell megadnia.

9.2. Oberthur kártya esetén

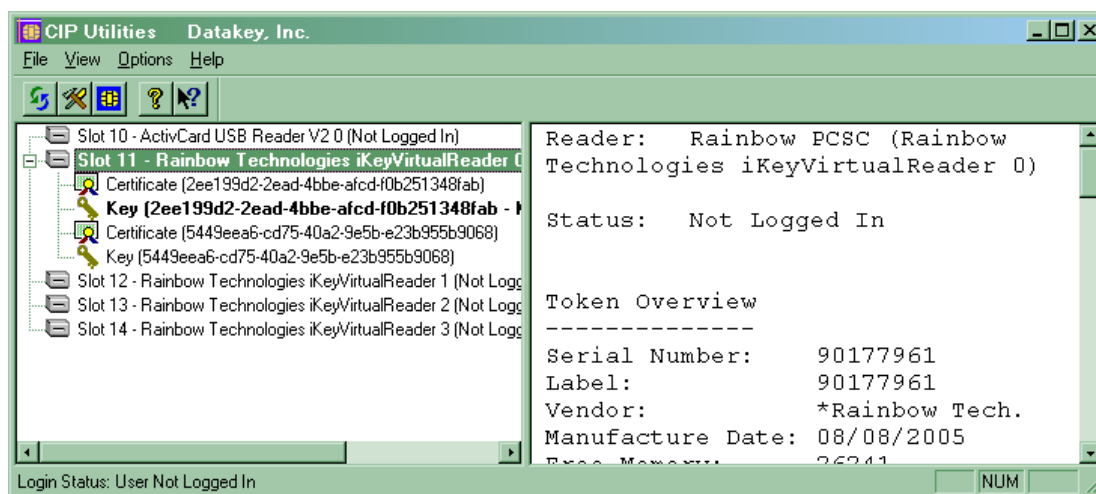
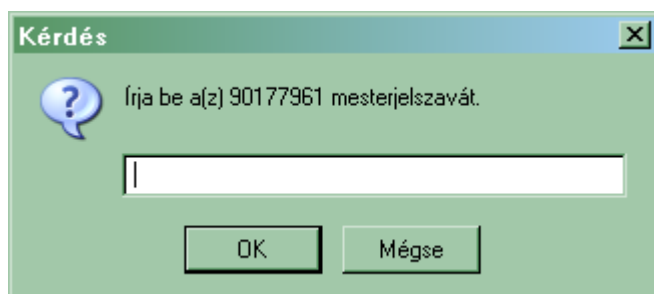
A megnevezés „AuthentIC Smart Card”.



Tehát ebben az esetben a kártya PIN kódját kell megadnia.

9.3. Rainbow Ikey 2032 token esetén

A megnevezés (mint a példában is látható), megegyezik a CIP Utilities programban látható sorozatszámmal (serial number). Ez egyébként az eszköz sorozatszáma is.



Tehát ebben az esetben a token PIN kódját kell megadnia

10. Függelék A - Egyes alkalmazások együttes futtatásával kapcsolatos lehetséges problémák

Ha kriptográfiai eszközön tárolódik tanúsítványa, előfordulhat, hogy egyes alkalmazások együttes futtatása során nem mindegyik alkalmazásból érik el a tanúsítványokat.

Ennek oka, hogy a PKCS#11 felületet használó alkalmazások közül az első megnyitott alkalmazás a kezelésre használt programot kizárólagosan futtatja, ezért a később indított alkalmazások nem férnek hozzá. Ebben az esetben az ilyen programok közül egyszerre csak egyet futtasson, az egyik alkalmazás bezárása után indítsa csak a másikat.

Ilyen egyszerre nem biztosan futtatható alkalmazások lehetnek (a teljesség igénye nélkül) a következők:

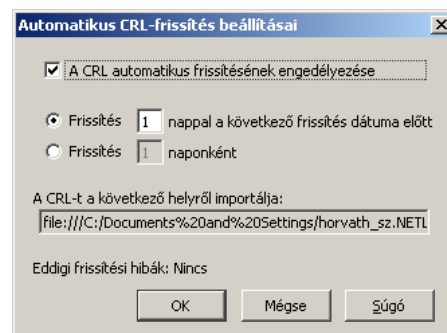
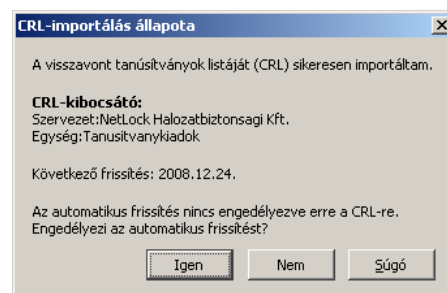
- Micardo PKI User kártyakezelő szoftver
- Mozilla Suite alkalmazáscsomag
- Netscape alkalmazáscsomag
- Firefox böngésző
- Thunderbird levelező program
- Lotus Notes alkalmazás
- Pénztár 5 alkalmazás

11. Függelék B - A visszavonási listák letöltése

A visszavonási listák rendszeres letöltése azért fontos, mert ezek a listák tartalmazzák azokat az elektronikus aláírásokat, melyek még lejáratú határidejük előtt érvénytelenné váltak.

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.



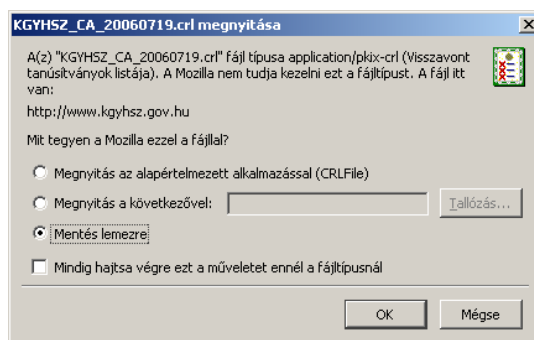
Amennyiben a visszavonási listák automatikus letöltését beállította, a továbbiakban ez a böngésző indulásakor automatikusan megtörténik, a szokásos, visszavonási listákban megadott időközönként.

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

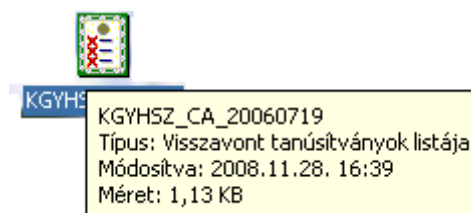
11.1. KGYHSZ visszavonási lista letöltése

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

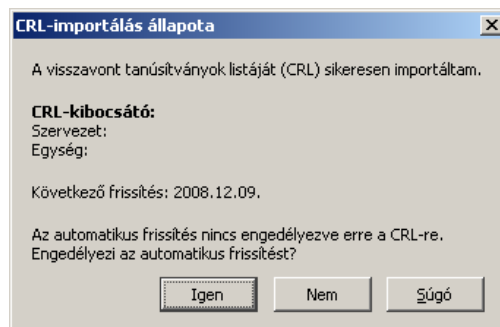
2. A linket megnyitva előugrik a Letöltés (Downloading...) ablak.
3. A megjelenő ablakban válassza a Fájl mentése... (Save) opciót, és mentse olyan helyre, ahol később megtalálja azt.



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.

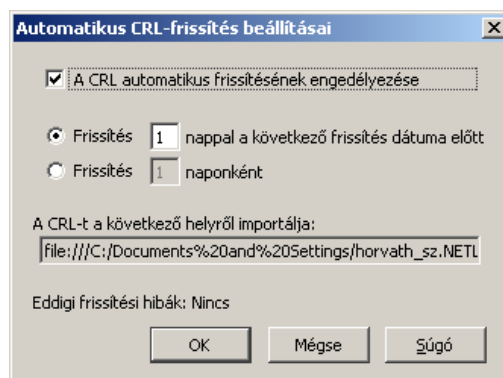


6. A file kiválasztását követően az alábbi ablak fog megjelenni.



7. A CRL automatikus frissítéséhez az alábbi lépéseket kövesse:

- a. Az Igen (Yes) gombra kattintva beállíthatja a frissítés gyakoriságát.
- b. Pipálja ki „A CRL automatikus frissítésének engedélyezése” (Automatic update for this CRL) mezőt.
- c. 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)
- d. Kattintson az OK gombra.



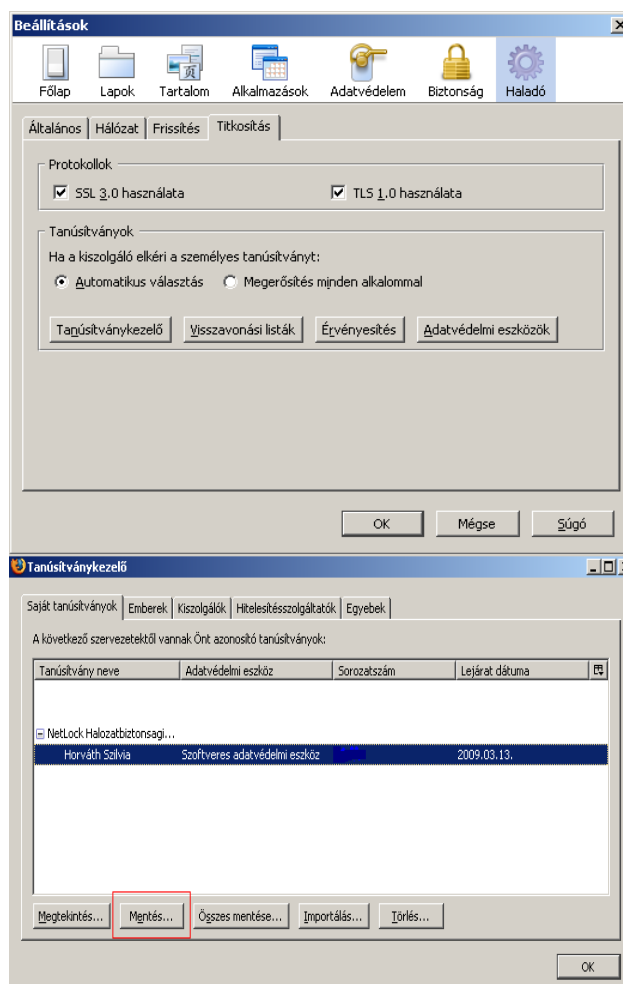
Ezzel a közigazgatási visszavonási lista telepítése megtörtént.

12. Függelék C – Biztonsági másolat készítése tanúsítványairól és kulcsairól Firefox 3+ böngészőből

Az egyik leggyakoribb böngésző, amit a Thunderbird-del együtt használnak a Firefox böngésző, így itt ismertetjük a PKCS#12 mentés készítését Firefox böngészőből, egyéb böngészőkhöz az adott böngészők útmutatóiban talál segítséget.

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.

1. Indítsa el a Firefox böngészőt
2. Navigáljon el a Tanúsítványok menüpontra. 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.