

A Netscape 9 alkalmazáscsomag beállítása tanúsítványok használatához

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

**A termék támogatásának befejezése miatt
a dokumentáció nem kerül frissítésre a továbbiakban.**

1. Tartalomjegyzék

| | | |
|----------|---|----|
| 1. | Tartalomjegyzék | 2 |
| 2. | Bevezető | 3 |
| 3. | A Netscape 9 böngésző beállítása tanúsítványok használatához | 3 |
| 4. | A Linux rendszerek korlátozásai..... | 3 |
| 4.1. | A közigazgatási gyökértanúsítványok telepítése | 4 |
| 5. | Rövid áttekintés a tanúsítvány igénylési és tárolási megoldásokról | 5 |
| 5.1.1. | Tanúsítvány igénylése Mozilla böngészőn keresztül..... | 5 |
| 5.1.2. | Tanúsítvány igénylése Internet Exploreren keresztül..... | 6 |
| 5.1.3. | Tanúsítvány és kulcsok PKCS#12 (PFX) állományban..... | 7 |
| 5.1.4. | Tanúsítvány és kulcsok kriptográfiai eszközön (kártyán, tokenen)..... | 7 |
| 6. | A tanúsítványok beállítása..... | 8 |
| 6.1. | Kártyán, tokenen tárolt tanúsítvány beállítása | 8 |
| 6.2. | Tanúsítványkérelem beadása Mozilla böngészőn keresztül történt..... | 8 |
| 6.3. | Tanúsítványkérelem beadása Internet Explorer böngészőn keresztül történt | 8 |
| 6.3.1. | Tanúsítvány exportálása Internet Explorerből a Netscape böngészőbe történő telepítéshez..... | 8 |
| 6.3.2. | PKCS12 (PFX) fájlban található tanúsítvány telepítése..... | 9 |
| 6.3.3. | PIN kód megadása az alkalmazásban, ha kriptográfiai eszközt (Smart kártya, USB token) használ..... | 10 |
| 6.3.3.1. | Micardo kártya esetén..... | 10 |
| 6.3.3.2. | Oberthur eszköz esetén..... | 11 |
| 6.3.3.3. | Rainbow Ikey 2032 token esetén | 11 |
| 7. | Függelék A - Egyes alkalmazások együttes futtatásával kapcsolatos lehetséges problémák..... | 12 |
| 8. | Függelék B – Biztonsági mentés készítése tanúsítványairól és kulcsairól Netscape 9 böngészőből..... | 13 |
| 9. | Függelék C – A visszavonási listák letöltése..... | 14 |
| 10. | Függelék D – Dokumentáció információk..... | 15 |

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 Netscape 9 böngésző beállítása tanúsítványok használatához

A következő fejezetek a Netscape 9 alkalmazáscsomag beállítását mutatják be.

A Netscape 9 böngészőben már nem elérhető a korábban a szoftver részének tekintett levelező program, így annak beállítása nem lehetséges.

A telepítés lépései a Netscape 9 verzió esetén történő beállításokat írják le, kis eltérésekkel korábbi verziók esetében is felhasználhatók.

A Netscape 9 fejlesztése megszűnt, javasolt átállni egy újabb böngészőre (Firefox, Seamonkey).

A KGYHSZ visszavonási lista nem importálható a szoftverbe, így közigazgatási tanúsítvánnyal a Netscape nem használható.

4. A Linux rendszerek korlátozásai

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

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

4.1. A közigazgatási gyökértanúsítványok telepítése

A Netscape 9.0 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 a következő linkeken érhetők el:

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

kgyhsz root menteni kell!!!!

authorities / import ugyanaz

Hitelesítésszolgáltatók / Importálás

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

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

A közigazgatási gyökértanúsítványok telepítésének lépései a következők:

1. Indítsa el a Netscape böngészőt.
2. Nyissa meg a böngészővel a fent látható linkek egyikét.
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 két linkre is a fentieket.

Ezzel a közigazgatási tanúsítványok telepítése megtörtént.

5. 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.

5.1.1. 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, 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.

5.1.2. 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 a 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 mindenféleképp exportálni kell a Windows tanúsítvány tárból az ilyen tanúsítványát.

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

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

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

Igen népszerű igénylési mód a tanúsítványok kártyán vagy tokenen 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, mely 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.

6. A tanúsítványok beállítása

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

6.1. Kártyán, tokenen tárolt tanúsítvány beállítása

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

Javasoljuk a hardvereszköz telepítőcsomagjának és útmutatójának megtekintését.

6.2. Tanúsítványkérelem beadása Mozilla böngészőn keresztül történt

Amennyiben a kérelmet Mozilla böngészőn keresztül adta be, a később kiadott tanúsítványt a Mozilla böngészővel az ügyfélmenü importálás pontját választva helyezze be véglegesen Mozilla saját tanúsítványtárolójába, 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.

6.3. 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.

6.3.1. Tanúsítvány exportálása Internet Explorerből a Netscape böngészőbe történő telepítéshez

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 nyomjon rá az Export gombra.
4. A megjelenő tanúsítvány exportáló 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 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.

6.3.2. 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 tanúsítvány és kulcs importálásának folyamata a következő:

1. Navigáljon el a Tanúsítvány beállítások beállítások menüpontra. (Eszközök > Beállítások > Speciális > Titkosítás > Tanúsítványok megtekintése) (Tools > Options > Advanced > Encryption > View Certificates)
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 Netscape-en belüli tanúsítványvédelmi jelszót. (mester jelszó /master password) (Software Security Device jelszó) Ez az első tanúsítvány importálás előtt nincs beállítva, ekkor kétszer kell begépelnie, és a későbbiek során ez után fog rendszeresen érdeklődni a Netscape a tanúsítványok kezelésekor.
5. Ezután adja meg a PKCS #12 (.pfx .p12) fájl jelszavát, amelyet Ön adott meg. (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.

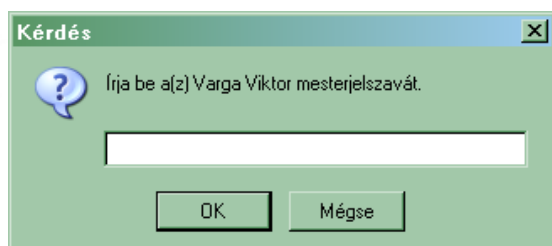
6.3.3. PIN kód megadása az alkalmazásban, ha kriptográfiai eszközt (Smart kártya, USB token) használ.

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

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

6.3.3.1. Micardo kártya esetén

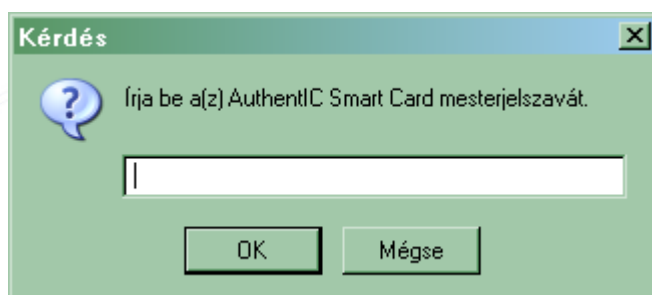
A megnevezés (mint a példában is látható), megegyezik a Micardo PKI programban látható megnevezéssel, ami alapértelmezésben a tanúsítvány tulajdonos neve szokott lenni.



Tehát ebben az esetben a kártya PIN kódját kell megadnia.

6.3.3.2. Oberthur eszköz esetén

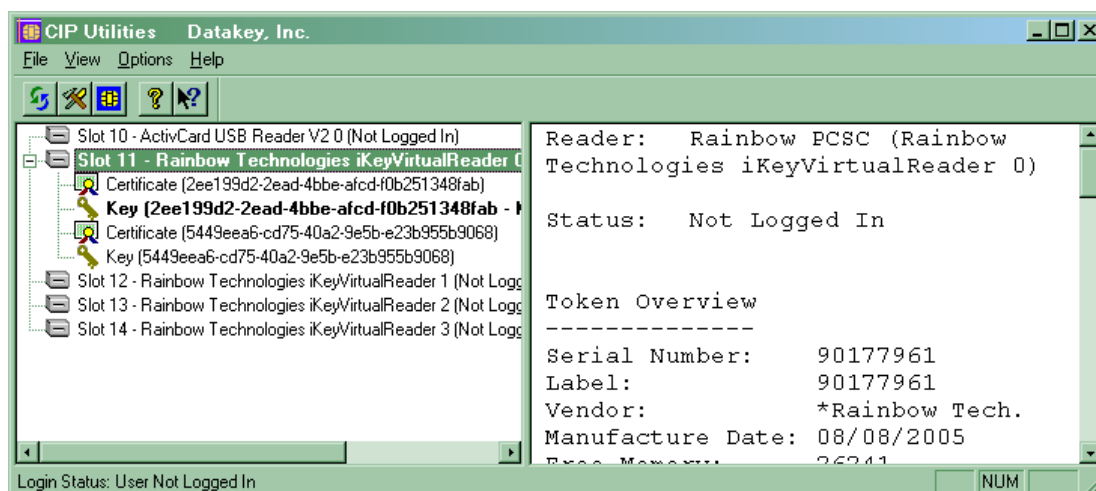
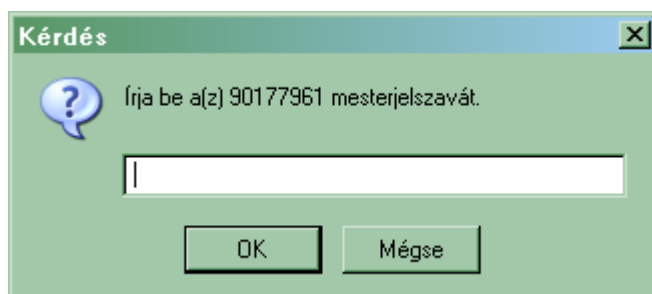
A megnevezés „AuthentIC Smart Card”.



Tehát ebben az esetben a kártya PIN kódját kell megadnia.

6.3.3.3. 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

7. 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

8. Függelék B – Biztonsági mentés készítése tanúsítványairól és kulcsairól Netscape 9 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.

1. Indítsa el a böngészőt
2. Navigáljon el a Tanúsítványok menüpontra. Eszközök > Beállítások > Haladó fül> Tanúsítvány megtekintés gomb gomb (Tools > Options > Advanced > View certificates gomb).
3. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön nyomja meg a Mentés (Backup) 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.

9. Függelék C – A visszavonási listák letöltése

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

A visszavonási listák letöltése a következő módon történik:

1. Indítsa el a Netscape 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.

A KGYHSZ visszavonási lista jelenleg nem importálható a szoftverbe.

10. Függelék D – Dokumentáció információk

A dokumentációt készítette:
Varga Viktor, Netlock Kft.

Felhasználása tetszőleges, a szerző megjelölésével.