

# A Seamonkey alkalmazáscsomag beállítása tanúsítványok használatához

---

**Böngészővel igényelt vagy 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 Seamonkey alkalmazáscsomag beállítása tanúsítványok használatához.....	4
4.	A Linux rendszerek korlátozásai.....	4
5.	A Seamonkey szoftver tanúsítványkezelésnek hibái.....	4
6.	A gyökértanúsítványok telepítése.....	5
7.	Rövid áttekintés a tanúsítvány igénylési és tárolási megoldásokról .....	6
7.1.	Tanúsítvány igénylése Seamonkey alkalmazáson keresztül.....	6
7.2.	Tanúsítvány igénylése Internet Exploreren keresztül.....	7
7.3.	Tanúsítvány és kulcsok PKCS#12 (PFX) állományban.....	8
7.4.	Tanúsítvány és kulcsok kriptográfiai eszközön (kártyán, tokenen).....	8
8.	A tanúsítványok beállítása.....	9
8.1.	Kártyán, tokenen tárolt tanúsítvány beállítása .....	9
8.2.	Tanúsítványkérelem beadása Mozilla böngészőn keresztül történt.....	9
8.3.	Tanúsítványkérelem beadása Internet Explorer böngészőn keresztül történt .....	9
8.3.1.	Tanúsítvány exportálása Internet Explorerből a Seamonkey alkalmazásba történő telepítéshez.....	9
8.3.2.	PKCS12 (PFX) fájlban található tanúsítvány telepítése.....	10
8.3.3.	Hardvereszközön található tanúsítvány használatának beállítása.....	12
9.	PIN kód megadása az alkalmazásban, ha kriptográfiai eszközt (Smart kártya, USB token) használ.....	13
9.1.	Micardo kártya esetén.....	13
9.2.	Oberthur kártya esetén.....	14
9.3.	Rainbow Ikey 2032 token esetén.....	14
10.	Tanúsítványok és kulcsok beállítása levezéshez és titkosításhoz.....	15
11.	Aláírt és/vagy titkosított levelek küldése.....	16

12.	Függelék A - Egyes alkalmazások együttes futtatásával kapcsolatos lehetséges problémák.....	17
13.	Függelék B - A visszavonási listák letöltése .....	18
13.1.	KGYSZ visszavonási lista letöltése.....	19
14.	Függelék C – Tanúsítvány biztonsági mentése Seamonkey alkalmazásból .....	21

## *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 zökkenőmentesebben 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 Seamonkey alkalmazáscsomag beállítása tanúsítványok használatához*

---

A következő fejezetek a Seamonkey alkalmazáscsomag beállítását mutatják be.

A Seamonkey alkalmazáscsomag egy közös tanúsítványtárat használ, azaz a tanúsítványok beállítása a böngészőben (Seamonkey) és a levelezőprogramban (News & Mailgroups) tulajdonképpen egyszerre, egy lépésben beállíthatók.

## *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.

## *5. A Seamonkey 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.

## 6. A gyökértanúsítványok telepítése

---

A Seamonkey 1.0 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.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 Seamonkey 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](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 böngészőben a Szerkesztés menühez, majd válassza a Beállítások menüpontot. Az Adatvédelem és biztonság alatt válassz a Tanúsítványok menüt, majd a megjelenő ablakban a Tanúsítványok kezelése opciót (KGYHSZ tanúsítvány esetén).
11. A Hitelesítés szolgáltatók fülre kattintva tudja importálni a tanúsítványt (KGYHSZ tanúsítvány esetén).
12. A megjelenő ablakban pipálja ki a mind a három opciót.
13. 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, de amennyiben új digitális aláírás használó, javasoljuk elolvasni.

### 7.1. Tanúsítvány igénylése Seamonkey alkalmazáson 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.

Esetünkben a Seamonkey két komponense, a levelező és a böngésző egy saját, de közös tanúsítványtáron osztozik tehát nem kell a két komponens miatt több műveletet végezni.

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.**

## 7.2. 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 mindenféleképp exportálni kell a Windows tanúsítvány tárból az ilyen tanúsítványát.**

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

Mint az előbbiekben olvashatta (Lásd Tanúsítvány igénylése Seamonkey alkalmazáson 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.

### 7.4. Tanúsítvány és kulcsok kriptográfiai eszközön (kártyán, tokenen)

Igen népszerű igénylési mód a tanúsítványok kártyán vagy tokenen történő 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.

## ***8. A tanúsítványok beállítása***

---

Az előző fejezetekben áttekinteteknek 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 legtöbb szoftver esetében végre lehet hajtani a hardvereszköz telepítő csomagjában található segédprogrammal, azonban a Seamonkey ezt NEM TÁMOGATJA, tehát KÉZI beállítás szükséges. Ezt egy későbbi fejezet ismerteti.

(Lásd Hardvereszközön található tanúsítvány használatának beállítása)

### ***8.2. 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, ez után az használható lesz.

**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. 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.

#### ***8.3.1. Tanúsítvány exportálása Internet Explorerből a Seamonkey alkalmazásba 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 fájlnévet, 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.

### 8.3.2. PKCS12 (PFX) fájlban található tanúsítvány telepítése

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

A tanúsítvány és kulcs importálásának folyamata a következő:

1. Navigáljon el a biztonsági beállítások menüpontig. (Szerkesztés > Beállítások > Adatvédelem & Biztonság > Tanúsítványok) (Edit > Preferences > Privacy & Security > Certificates)
2. A jobb oldali panelen a Tanúsítványkezelő (Manage Certificates) szekcióban nyomja meg Tanúsítványok kezelése (Manage Certificates) gombot.
3. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön nyomja meg az Import gombot.
4. Ezután az Importálás gomb segítségével tallózza ki a PKCS #12 fájlt, amely a tanúsítványt és a hozzá tartozó kulcsot tartalmazza.
5. Adja meg Seamonkey alkalmazáson belüli tanúsítványvédelmi jelszót. (Ez az első tanúsítvány importálás előtt nincs beállítva, ekkor kétszer kell begépelnie, és a későbbiek során ez után fog rendszeresen érdeklődni a Seamonkey alkalmazás.)
6. Ezután adja meg a .pfx fájl jelszavát, amelyet exportálásakor adott meg. (Ha adott neki ilyen jelszót.)



7. 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.

### 8.3.3. Hardvereszközön található tanúsítvány használatának beállítása

Amennyiben tanúsítványa kriptográfiai eszközön található, akkor első lépésként el kell végeznie azokat a beállításokat, melyek az eszköz telepítéséről szóltak. Az ott található beállítások között természetesen találhatóak olyan lépések is, melyek a Seamonkey alkalmazásból történő használathoz nem szükségesek, de az optimális használathoz érdemes elvégezni az ott szereplő beállítások mindegyikét.

A Seamonkey alkalmazásban a kriptográfiai eszköz használatának beállítása a következő:

1. Vizsgálja meg, hogy telepítette-e a kártyaolvasó, és a kártyakezelő szoftvereket, ezek telepítése nélkül nem lehetséges a kártya használata.
2. Navigáljon el a biztonsági beállítások menüpontig. (Szerkesztés > Beállítások > Adatvédelem & Biztonság > Tanúsítványok) (Edit > Preferences > Privacy & Security > Certificates)
3. Nyomja meg a Biztonsági eszközök kezelése (Manage Security Devices) gombot.
4. A megjelenő ablakban nyomja meg a Betöltés (Load) gombot.
5. Az előugró ablakban a Modul név (Modul name) mezőben adja meg az eszköz nevét. Javasoljuk, hogy a kriptográfiai eszköz típusát adja meg névnek. (Vagyis "Oberthur eszkozok" , "Micardo kartya" vagy „Rainbow token” nevet adjon neki, a kriptográfiai eszköztől függően.)
6. A Modul fájlnev (module filename) ablakban tallózza ki a megfelelő kártyakezelő fájlt, vagy másolja be a vágólapon keresztül a következő útvonalat pontosan.

Ez Micardo kártya esetében:

C:\WINDOWS\system32\MicardoPKCS11.dll

Ez Oberthur eszközök esetében: (Authentic Manager 3.3.0.0 verzió esetén)

C:\WINDOWS\system32\OCSCryptoki.dll

Ez Safenet (Rainbow) Ikey 2032 USB token esetében:

C:\WINDOWS\system32\dkck201.dll

(Ez az útvonal természetesen az alapértelmezett helyre történő telepítéskor érvényes, ha más helyre telepítette, ennek megfelelően állítsa be.)

7. Nyomjon Ok gombot addig, amíg nem jut vissza a kezdő képernyőhöz.
8. Indítsa újra a szoftvert a beállítások életbe lépéséhez.

Ezzel a kriptográfiai eszköz használata Seamonkey alkalmazásból beállításra került.

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

---

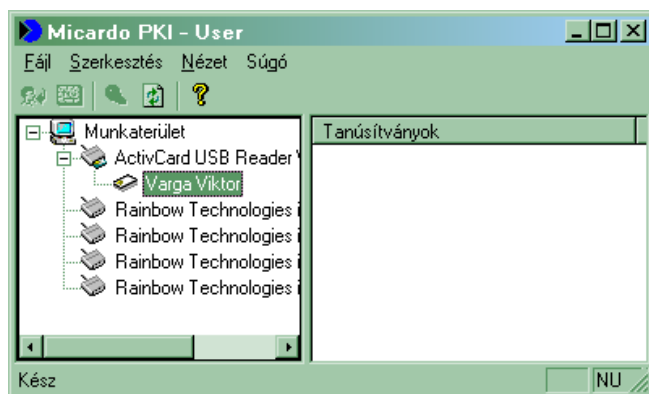
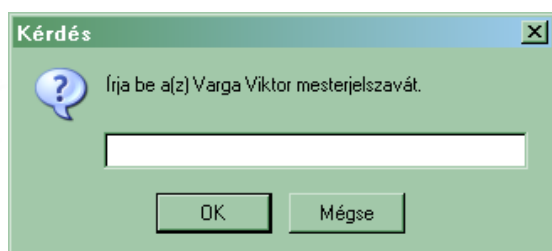
Amennyiben kriptográfiai eszközön tárolt tanúsítványt használ, abban az esetben a rendszer, amikor PIN kódot kell megadni, megtevesztően „mester jelszó” (master password) után érdeklődik.

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

### 9.1. Micardo kártya esetén

---

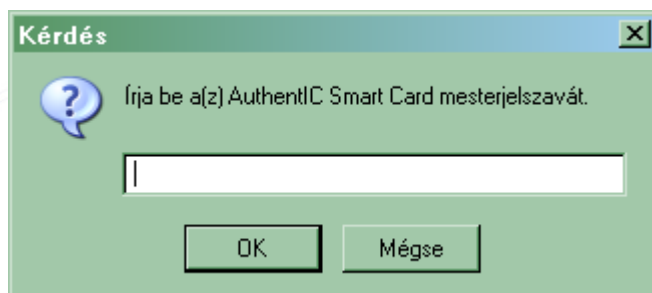
A megnevezés (mint a példában is látható), megegyezik a Micardo PKI programban látható megnevezéssel, ami alapértelmezésben a tanúsítvány tulajdonos neve szokott lenni.



Tehát ebben az esetben a kártya PIN kódját kell megadnia.

### 9.2. Oberthur kártya esetén

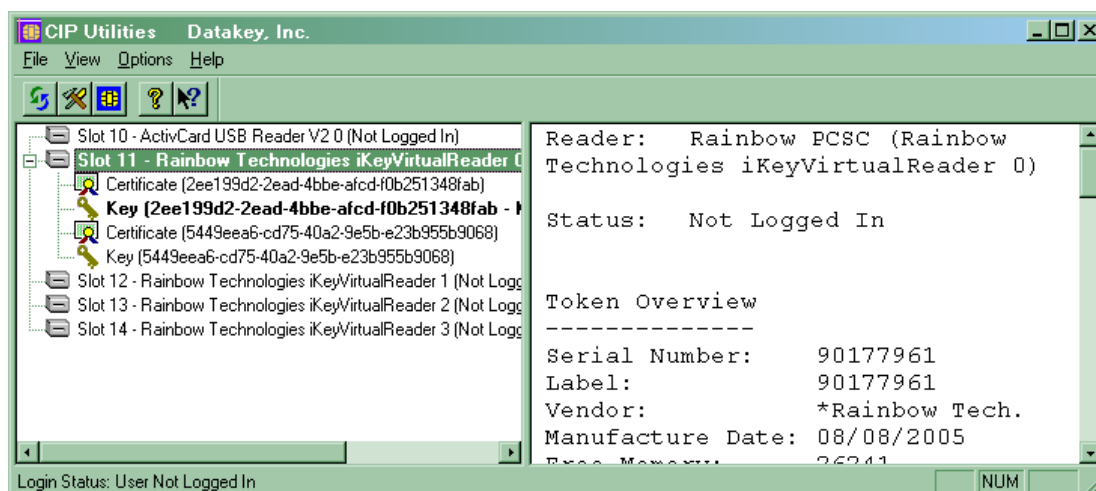
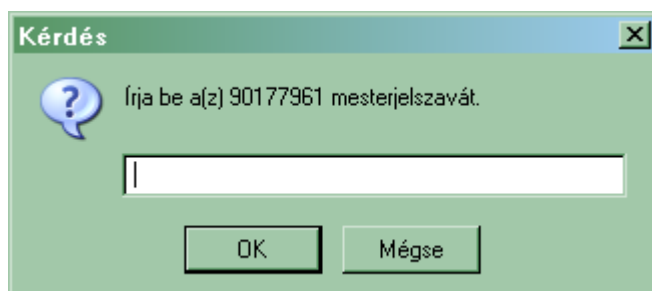
A megnevezés „AuthentIC Smart Card”.



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. Tanúsítványok és kulcsok beállítása levezéshez és titkosításhoz

Ahhoz, hogy a Seamonkey alkalmazáscsomagból tanúsítvánnyal aláírva és titkosítva is küldhessen levelet a következő lépéseket kell végrehajtania.

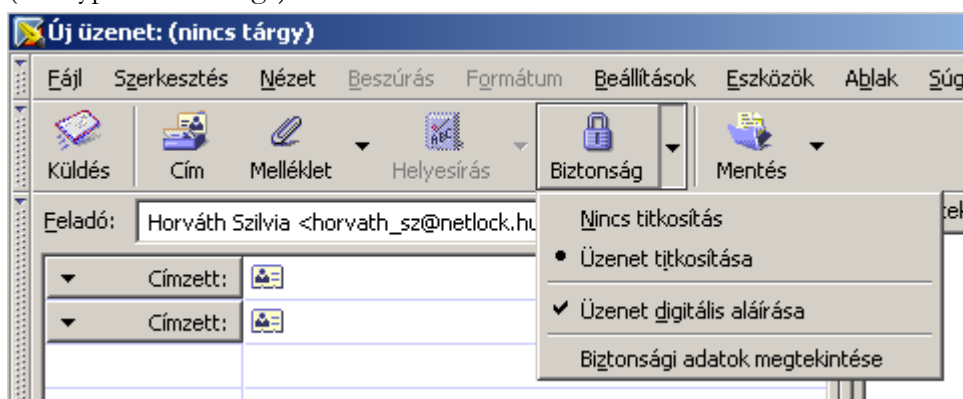
1. Indítsa el a Mail & Newsgroups alprogramot.
2. Navigáljon el a Fiók beállítások (Account settings) menüpontba.  
(Szerkesztés > Postafiókok beállításai)  
(Edit > Mail & Newsgroups Account Settings)
3. Válassza ki az e-mail címét, majd nyissa le a hozzá tartozó fastruktúrát, és válassza ki az ez alatt található Biztonság (Security) menüpontot.
4. A jobb oldalon a Digitális aláírás (Digital signing) szekcióban nyomja meg Kiválasztás (Select) gombot, és válassza ki az aláíró tanúsítványát. Az ez alatt található opcióval bekapcsolhatja, hogy alapértelmezetten minden kimenő levél alá legyen írva digitálisan. (Általában a program automatikusan eldönti, hogy adott tanúsítvány aláírásra vagy titkosításra jó.)
5. A Titkosítás (Encryption) szekcióban a nyomja meg a Kiválasztás (Select) gombot, és válassza ki a titkosító tanúsítványát. Az alatta lévő opciók a titkosítás alapértelmezett viselkedését adják meg, a Soha (Never) opció alapértelmezetten soha nem titkosít, a Mindig (Required) opció esetében addig nem megy el a levél, amíg nincs minden címzettnek tanúsítványa.
6. Miután ezeket beállította, nyomjon Ok gombot, amíg vissza nem jut a főképernyőig.

Ezzel a tanúsítványok beállítása megtörtént.

## 11. Aláírt és/vagy titkosított levelek küldése

Ha levelét aláírva és/vagy titkosítva szeretné elküldeni, a teendői a következők:

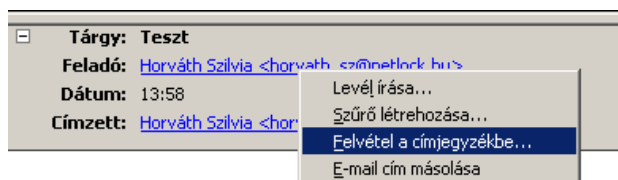
1. Amikor megírta a levelét, még a küldés előtt válassza ki a Biztonság (Security) gomb melletti háromszöget.
2. A lenyíló menüben kiválaszthatja, hogy digitálisan aláírja (Digitaly sign) és/vagy titkosítja (Encrypt this message) a levelet.



Fontos, hogy tudja, hogy ahhoz, hogy titkosított levelet küldjön valakinek, rendelkeznie kell a levelezőpartner nyilvános kulcsával.

Ha ez megvan a címjegyzékében, akkor nem okozhat problémát.

Ha nincs, kérje meg a levelező partnerét, hogy küldjön Önnek egy aláírt levelet, amelyet mikor Ön megkap, mentenie kell belőle a feladó címét saját címjegyzékébe, és akkor a titkosításhoz szükséges nyilvános kulcs is tárolásra kerül a bejegyzéssel együtt.



## *12. 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:

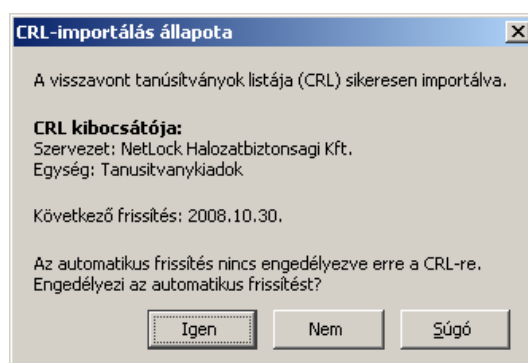
- Micardo PKI User kártyakezelő szoftver
- Seamonkey alkalmazáscsomag
- Mozilla Suite alkalmazáscsomag
- Netscape alkalmazáscsomag
- Firefox böngésző
- Thunderbird levelező program
- Lotus Notes alkalmazás
- Pénztár 5 alkalmazás

### 13. Függelék B - A visszavonási listák letöltése

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

A visszavonási listák letöltése a következő módon történik:

1. Indítsa el a Seamonkey 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.

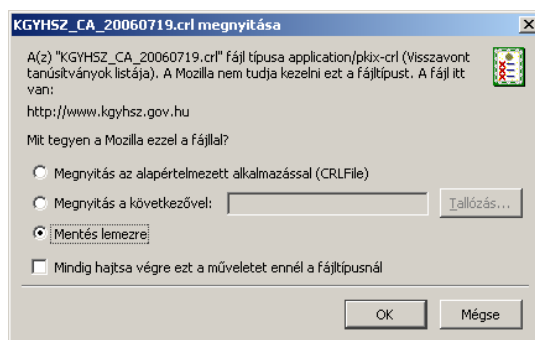
Ha sürgősen a legfrissebb listára van szüksége, akkor az itt leírtak alapján azt bármikor megismételheti.

### 13.1.KGYHSZ visszavonási lista letöltése

1. A Seamonkey böngészőben nyissa meg az alábbi linkeket:

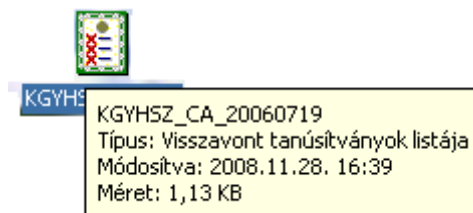
[http://www.kgyhsz.gov.hu/KGYHSZ\\_CA\\_20060719.crl](http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.crl)

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.

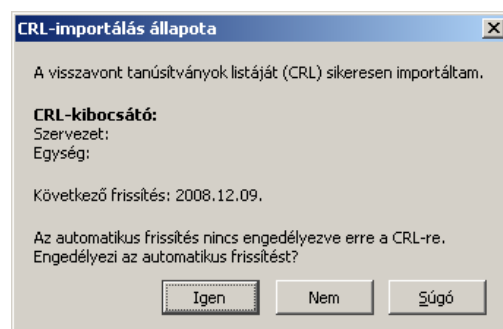


4. A Seamonkey böngésző File menüjéből válassza a File megnyitása (Open) lehetőséget.

5. Ekkor tallózó ablakot kap, ahol meg tudja keresni a korábban elmentett file-t.

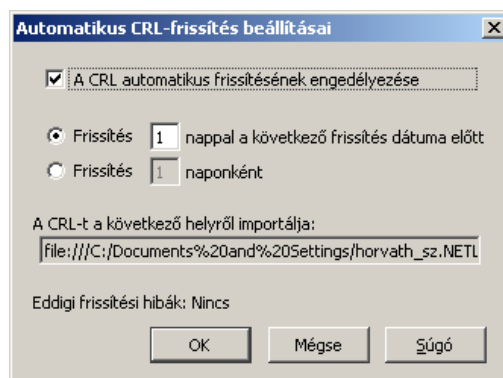


6. A file kiválasztását követően az alábbi ablak fog megjelenni.



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.

#### *14. Függelék C – Tanúsítvány biztonsági mentése Seamonkey alkalmazásból*

---

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. A kulcs és tanúsítvány exportálásához indítson Seamonkey böngészőt.
2. Navigáljon el a tanúsítványok menüponthoz. (Szerkesztés > Beállítások > Adatvédelem és biztonság > Tanúsítványok) (Edit > Preferences > Privacy and Security > Certificates)
3. Kattintson a Tanúsítványok kezelése (Manage certificates) gombra
4. Válassza ki a Saját tanúsítványok (Your certificates) lapon a tanúsítványok közül az exportálandót, majd nyomjon rá a Biztonsági mentés (Backup) gombra.
5. A Tallózó ablakban ki tudja választani, a megfelelő könyvtárat, ahova menteni szeretné a tanúsítványt, valamint itt adhat neki egy tetszőleges nevet.
6. Ha szüksége van arra, hogy a tanúsítvánnyal együtt a hozzá tartozó gyökértanúsítványt is exportálja, akkor jelölje ki a Biztonsági mentés mindenről opciót (Backup all).
7. A következő ablakban gépeljük be a jelszót, amit szeretnénk a fájlnak adni.
8. Az OK gomb megnyomása után a tanúsítvány mentésre kerül a privát kulccsal együtt.

Ezt az állományt érdemes biztonságos helyen elzárni valamilyen adathordozón.