

# Lotus Notes alkalmazás beállítása tanúsítványok használatához

---

Windows tanúsítványtárban és kriptográfia eszközökön található  
tanúsítványok esetén

## 1. Tartalomjegyzék

1.	Tartalomjegyzék .....	2
2.	Bevezető .....	3
3.	A Lotus Notes R6/R7 alkalmazás beállítása tanúsítványok használatához .....	3
4.	A szoftver korlátozásai .....	3
5.	Ajánlások a szoftverrel kapcsolatosan .....	3
5.1.	A gyökértanúsítványok telepítése .....	4
5.2.	A gyökértanúsítványok telepítése Administrator felületen Notes domain szintre .....	4
5.3.	A gyökértanúsítványok telepítése egyéni felhasználóknak .....	4
5.3.1.	Előkészítés - A Notes beállítása böngészőként .....	4
5.3.2.	A gyökértanúsítványok telepítésének lépései .....	5
5.4.	A visszavonási listák letöltésének beállítása .....	7
5.5.	Fájlban található tanúsítvány telepítése .....	8
5.5.1.	Tanúsítvány exportálása Internet Explorerből a Lotus Notes programba történő telepítéshez .....	9
5.6.	Tanúsítvány telepítése, ha a tanúsítványa kriptográfiai eszközön (Smart kártya, USB token) található .....	10
5.6.1.	Az ID fájl biztonsági mentése .....	10
5.6.2.	A kártyás/tokenes bejelentkezés beállítása .....	10
5.7.	Tanúsítvány importálása kriptográfiai eszközről .....	13
5.8.	Aláírt és/vagy titkosított levelek küldése .....	14
6.	Aláírt levelekkel kapcsolatos műveletek megjelenítése .....	15
7.	Egyes alkalmazások együttes futtatásával kapcsolatos lehetséges problémák .....	16
8.	Függelék A – Az e-mail címek beállításnak lehetőségei .....	17

## 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 tanúsítványokkal kapcsolatos bármilyen kérdése van vagy problémája támad, Ügyfélszolgálatunk az (40) 22-55-22 telefonszámon, az info@netlock.net e-mail címen vagy személyesen a 1023 Budapest, Zsigmond tér 10. szám alatt munkanapokon 9 és 17 óra között készséggel áll rendelkezésére.

A Lotus Notes rendszerek tesztelését partnerünkkel, az UNIOFFICE Rendszerházzal végeztük, Lotus Notes specifikus kérdésekre igazán ők tudnak választ adni.

Elérhetőségük:      telefon      (1) 372-7575  
                                 e-mail      info@unioffice.hu

## 3. A Lotus Notes R6/R7 alkalmazás beállítása tanúsítványok használatához

---

A következő fejezetek a Lotus Notes R6/R7 alkalmazás beállítását mutatják be, ahhoz, hogy tanúsítványait, el tudja érni, illetve használni tudja levelező programjából.

A telepítés lépései a Windows rendszereken történő beállításokat írják le, Lotus Notes R6/R7 program esetében. Korábbi verziók használatát nem javasoljuk, a későbbi verziók beállításai kis mértékben eltérhetnek a leírtaktól.

## 4. A szoftver korlátozásai

---

A Lotus Notes R6/R7 esetében a következő korlátozások érvényesek:

- Jelenlegi teszteredményeink alapján minősített tanúsítvánnyal nem működik.
- A visszavonási információk kezelése jelenlegi teszteredményeink alapján hiányos.
- A Single Login funkció kártya/token használata során nem használható.

## 5. Ajánlások a szoftverrel kapcsolatosan

---

A Lotus Notes R6/R7 esetében a következő korlátozások érvényesek:

- Szoftveresen tárolt tanúsítványok esetében a szoftver működőképessége megfelelő.
- Kriptográfiai eszközök közül a leginkább ajánlható eszköz a Rainbow/Safenet iKey 2032 kriptográfiai token.

### 5.1. A gyökértanúsítványok telepítése

A Lotus Notes R6/R7 verzióban még nem találhatóak meg a Netlock gyökértanúsítványai ezért telepítésük szükséges. Legalább a saját tanúsítványunknak megfelelő telepítése szükséges, de javasolt minden tanúsítványkiadót telepíteni.

A telepítés történhet felhasználói, illetve Notes adminisztrátori szinten (ez utóbbi esetben teljes Notes domainre)

### 5.2. A gyökértanúsítványok telepítése Administrator felületen Notes domain szintre

Amennyiben a Notes rendszerükben várhatóan többen is használnak majd Netlock Kft. Által kibocsátott tanúsítványt elektronikus aláírásra, titkosításra, javasolt a rendszer szintű telepítés.

Ennek módja a következő:

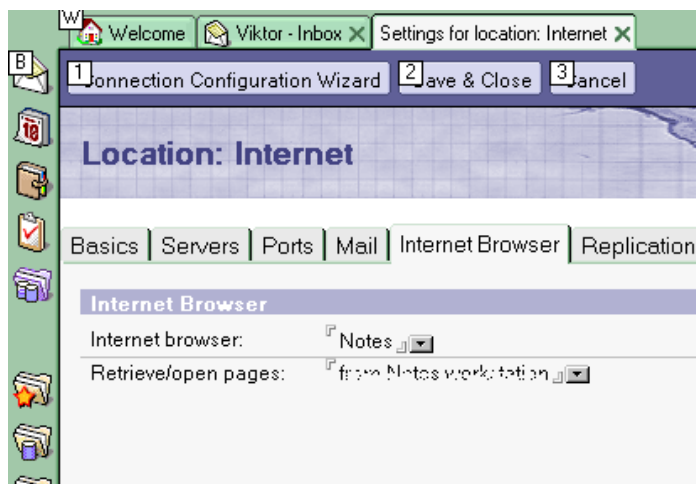
1. A megfelelő jogosultsággal rendelkező kolléga töltsse le a <http://www.netlock.hu/html/cacrl.html> oldalról a "Tanúsítványkiadók letöltése böngészőbe" menüpontban található tanúsítványkiadói tanúsítványokat.
2. Az Administrator felületen a központi címtárba importálja be ezeket a tanúsítványokat. Configuration > Certificates > Certificates Actions menüpont > Import Internet Certificate (cer/der állományok kiválasztása)

### 5.3. A gyökértanúsítványok telepítése egyéni felhasználóknak

#### 5.3.1. Előkészítés - A Notes beállítása böngészőként

Ahhoz, hogy a gyökértanúsítványokat be tudja állítani, az Internet kapcsolattal is rendelkező profilban be kell állítania a Notes böngészőt mint használandó böngészőt.

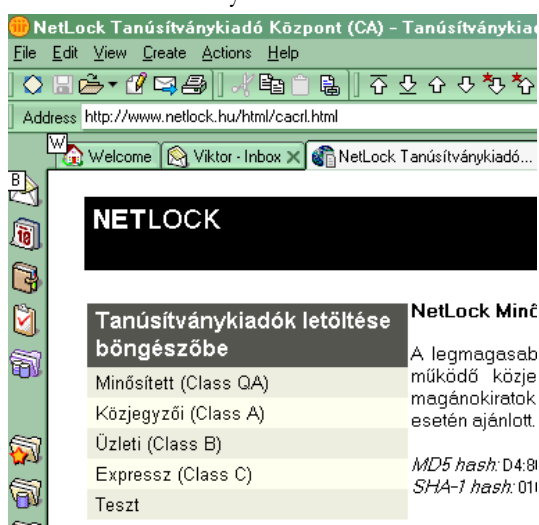
1. Menjen el a böngésző beállításokig. (Fájl > Beállítások > Hely beállítások > Internet böngésző fül) (File > Preferences > Location preferences > Internet browser fül)
2. Állítsa be Internet böngészőnek a Notes alkalmazást, majd nyomjon a Mentés és Bezárás (Save & Close) gombra.



### 5.3.2. A gyökértanúsítványok telepítésének lépései

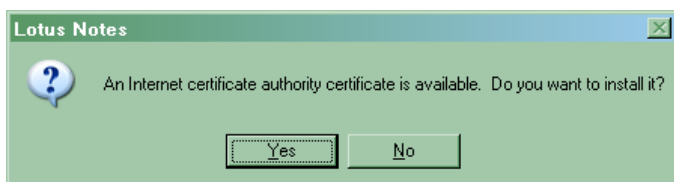
A gyökértanúsítványok telepítése a következőképpen lehetséges.

1. Indítsa el a Lotus Notes böngészőjét, és látogasson el vele a <http://www.netlock.hu/html/cacrl.html> oldalra.
2. A bal oldalt található "Tanúsítványkiadók letöltése böngészőbe" menüpontban kattintson az első tanúsítványkiadóra

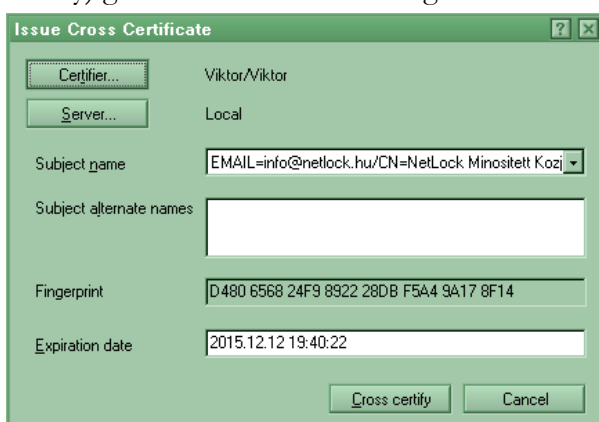


3. A megjelenő figyelmeztetés megkérdezi, hogy az elérhető gyökértanúsítványt kívánja-e telepíteni. Kattintson az Igen (Yes) gombra.





4. A következő megjelenő ablakban lehetőség van arra, hogy Kereszt hitelesítés (Cross-certify) gombra kattintva lehetősége van az adott kiadót elfogadni.



5. Ezzel az adott kiadót telepítette, javasolt a Teszt kivételével az összes kiadó telepítésére elvégezni a fenti lépéseket.

#### *5.4. A visszavonási listák letöltésének beállítása*

---

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

**A Lotus Notes esetében külön a visszavonási listák beállítási lehetősége opció nem található.**

**A Netlock tanúsítványai tartalmazzák a CDP bejegyzést, mely alapvetően a különböző szoftvereknek szól, hogy hol érhetik el ezeket a listákat. Amennyiben a Lotus Notes ezt kezeli, képes lehet a tanúsítvány visszavonását értelmezni, azonban tesztelni ezt a képességét nem tudtuk.**

## 5.5. Fájlban található tanúsítvány telepítése

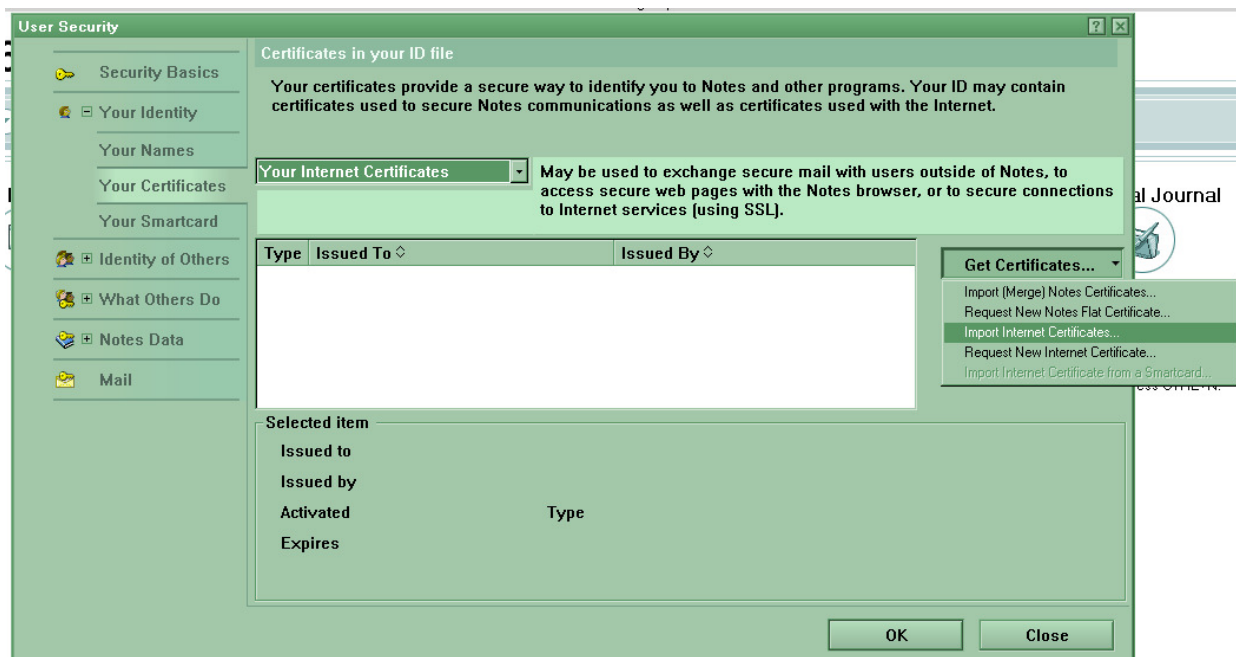
Abban az esetben, ha tanúsítványát nem kriptográfiai eszközön szerezte be, akkor az arról készült PKCS#12 (.pfx) formátumú mentett állomány segítségével tudja tanúsítványát a Lotus Notes alkalmazásba beállítani.

Ha nincs ilyen PKCS#12 (.pfx) állományba készült mentése, de a tanúsítványa a Windows tanúsítványtárban megtalálható, akkor onnan azt ki tudja exportálni, és azt be fogja tudni importálni. Lapozzon egy kicsit tovább, a következő bekezdése ennek elvégzését tárgyalja.

A Lotus Notes R6/R7 alkalmazásba a tanúsítvány és kulcs importálásának folyamata a következő:

1. Navigáljon el az **Your Internet certificate** (Az Ön Internet tanúsítványai) menüpontra.  
File > Security > User Security > Your Identity lenyíló > Your Certificates lenyíló > Your Internet certificates listaelem  
(Fájl > Biztonság > Felhasználói biztonság > Személyazonosság > Az Ön tanúsítványai lenyíló > Internet tanúsítványok listaelem)
2. Válassza ki a **Get certificates** (Tanúsítványok beszerzése) gomb alatt elérhető listából az **Import Internet Certificates...** (Internet tanúsítványok importálása) menüpontot.

A következő ábrán az 1-2. lépések képernyőjét láthatja.



3. Tallózza ki a tanúsítványt és kulcsokat tartalmazó PKCS#12 fájlt, majd nyomjon az **Open** (Megnyitás) gombra



4. A megjelenő formátum kérdés során válassza a következőt: PKCS 12 titkosított. (PKCS 12 encoded), majd nyomjon a Continue (Folytatás) gombra.
5. Adja meg a PKCS #12 fájl jelszavát.
6. Az utolsó megerősítést kérő ablakban fogadja el az Accept All (Mindent elfogad) gombbal a megjelenő tanúsítványokat.

Ezzel az adott gépen a fájlban található tanúsítványát telepítette az adott Notes felhasználói ID-hez, aki a Notes esetén be volt jelentkezve.

Ha több gépen szeretné elektronikus aláírást ugyanígy használni, több gépen is telepítenie kell.

#### *5.5.1. Tanúsítvány exportálása Internet Explorerből a Lotus Notes programba 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.
11. A tanúsítvány exportálása ezzel megtörtént. Javasolt az exportált állományt a telepítés után, mint biztonsági másolatot biztonságos helyre eltenni.

## *5.6. Tanúsítvány telepítése, ha a tanúsítványa kriptográfiai eszközön (Smart kártya, USB token) található*

---

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 Lotus Notes programból történő használathoz nem szükségesek, de az optimális használathoz érdemes elvégezni az ott szereplő beállítások mindegyikét.

### *5.6.1. Az ID fájl biztonsági mentése*

---

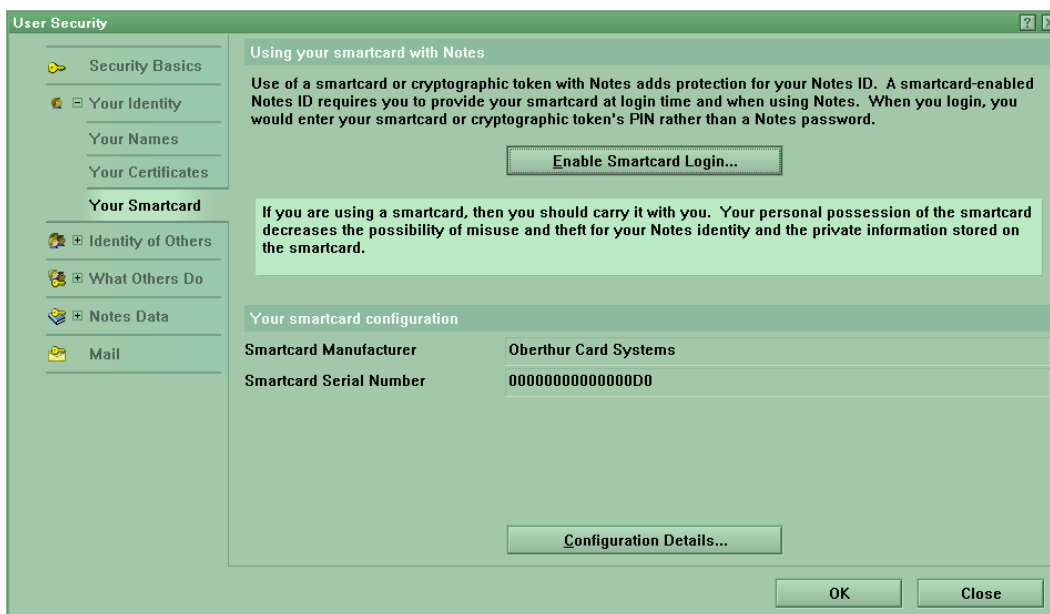
A kriptográfiai eszköz beállítása előtt mindenféleképpen javasolt a felhasználó ID fájljáról egy biztonsági mentést készíteni, mert az ID fájl a művelet során módosul, és a felhasználónak, akik kriptográfiai eszközt vesz igénybe aláíráshoz a bejelentkezésre csak az eszköz birtokában lesz lehetősége.

### *5.6.2. A kártyás/tokenes bejelentkezés beállítása*

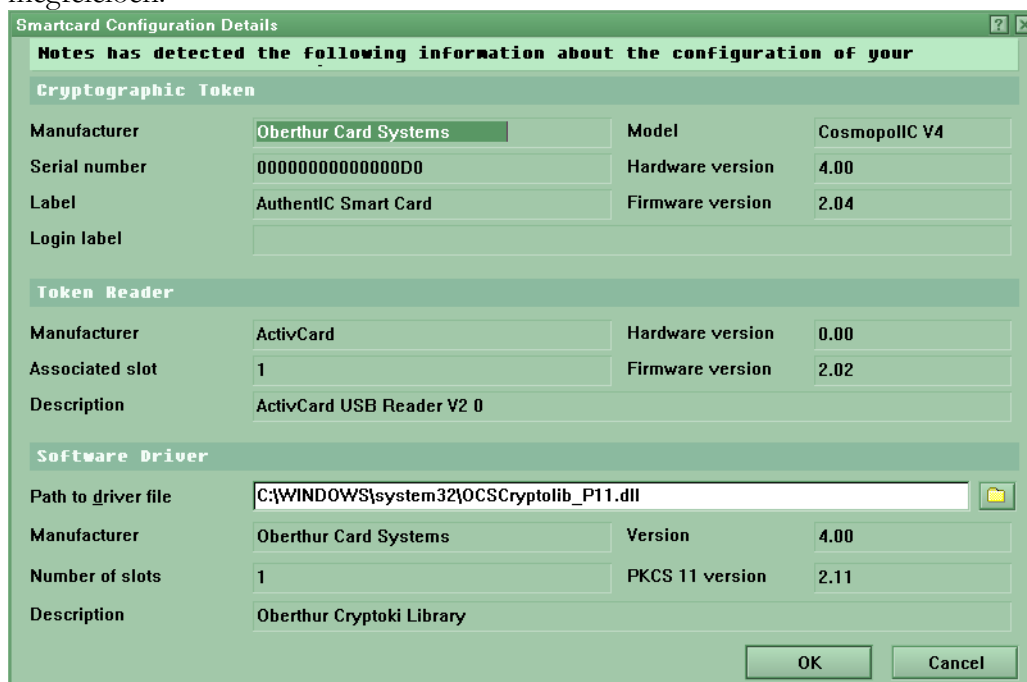
---

A Lotus Notes programban 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 az Your Smart Card (Az Ön Smart kártyája) menüpontra.  
File > Security > User Security > Your Identity lenyíló > Your Certificates lenyíló > Your Internet certificates listaelem  
(Fájl > Biztonság > Felhasználói biztonság > Személyazonosság > Az Ön tanúsítványai lenyíló > Internet tanúsítványok listaelem)



3. Nyomja meg a Configuration Details (Beállítási részletek) gombot.
4. A megjelenő ablakban a Path... (Útvonal...) mezőt töltsé ki a kriptográfiai eszközének megfelelően.



Tallózza ki a megfelelő kártyakezelő fájlt, vagy másolja be a vágólapon keresztül a következő útvonalat pontosan.

*Micardo kártya esetében:*

*C:\WINDOWS\system32\MicardoPKCS11.dll - ez itt nem megy*

Oberthur kártya esetében:

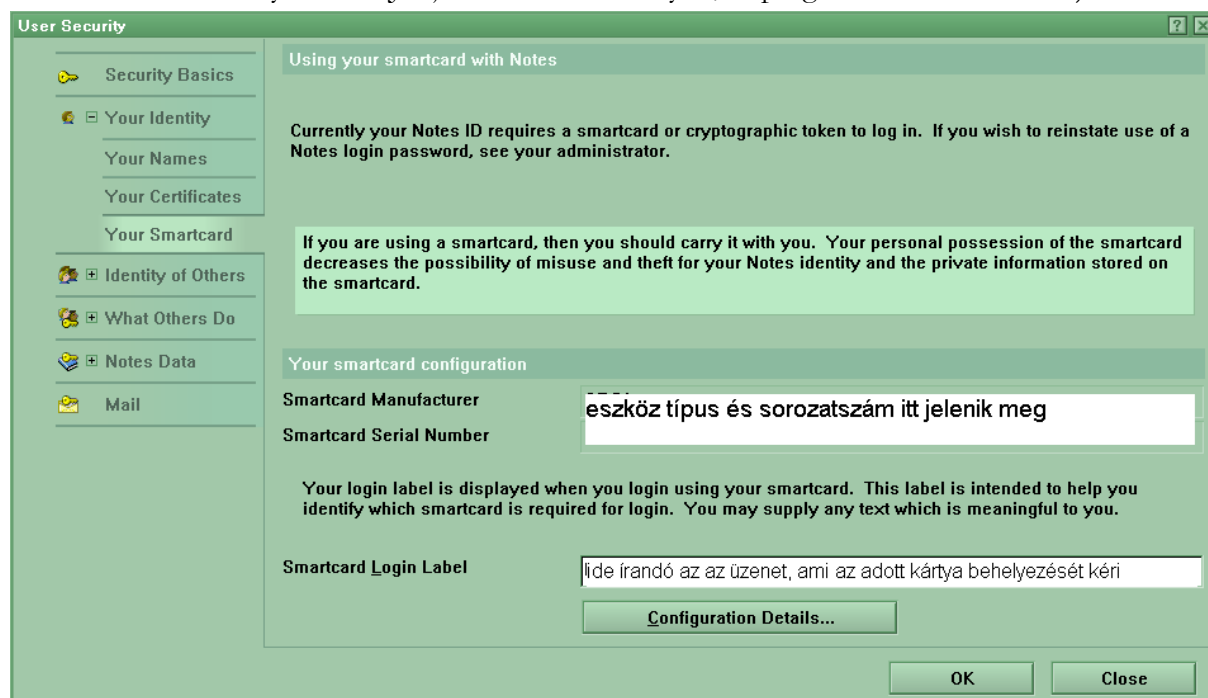
C:\WINDOWS\system32\OCSCryptolib\_P11.dll

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.)

5. Ezután nyomja meg az Enable Smart Card Login (Smart kártyás bejelentkezés engedélyezése) gombot. A program ezután jelzi, hogy a rendszergazda az internet jelszót nem tudja majd a Notes-ban megadottra módosítani, majd az eszköz PIN kódjának helyes megadása után végrehajta a beállításokat.
6. Ez után a következő képernyőt kapjuk. Az eszköz típusa megjelenik a képen, illetve megadható a Smartcard Login label opciónál, hogy milyen üzenetet írjon ki számunkra, amikor a kártyát kéri. (Jól jöhet ha több kártyánk, kriptográfiai eszközünk van.)



### 5.7. Tanúsítvány importálása kriptográfiai eszköztől

---

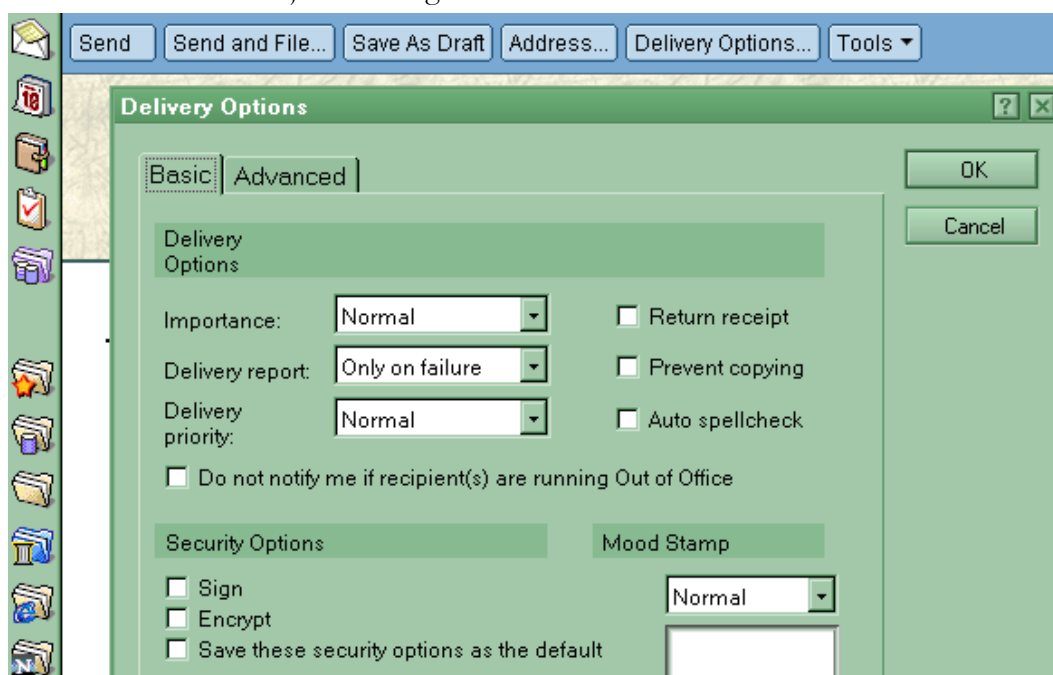
1. Navigáljon el az Your Internet certificate (Az Ön Internet tanúsítványai) menüpontra.  
File > Security > User Security > Your Identity lenyíló > Your Certificates lenyíló > Your Internet certificates listaelem  
(Fájl > Biztonság > Felhasználói biztonság > Személyazonosság > Az Ön tanúsítványai lenyíló > Internet tanúsítványok listaelem)
2. Válassza ki a Get certificates (Tanúsítványok beszerzése) gomb alatt elérhető listából az Import Internet Certificates from a Smart Card (Internet tanúsítványok importálása smart kártyáról) menüpontot.
3. A szoftver pillanatok múlva sikeres importálásról tudósít, azonban az új tanúsítvány csak akkor látszik, ha ismételten a menü elejétől elnavigálunk a Your Internet certificates (Az Ön Internet tanúsítványai) menüpontra.



## 5.8. 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 Kézbesítési beállítások (Delivery options) gombot.
2. Az Alap (Basic) fülön jelölje be az Aláír (Sign) és/vagy Titkosít (Encrypt) jelölő négyzeteket., majd nyomjon Ok gombot.
3. A levél küldésekor a kijelöltek megtörténnek.



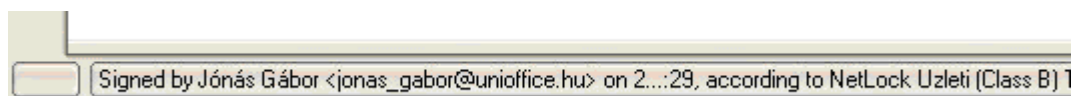
Fontos, hogy tudja, hogy ahhoz, hogy titkosított levelet küldjön valakinek, rendelkeznie kell a levelezőpartner nyilvános kulcsával.

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.



## 6. Aláírt levelekkel kapcsolatos műveletek megjelenítése

Az aláírt levelekkel kapcsolatos műveleteket, mint elvégzett aláírást, kapott levelek aláírásának ellenőrzését a Lotus Notes nem feltűnően végzi, ezeket az információkat mindig a státusz sorban találhatjuk meg.



## 7. 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:

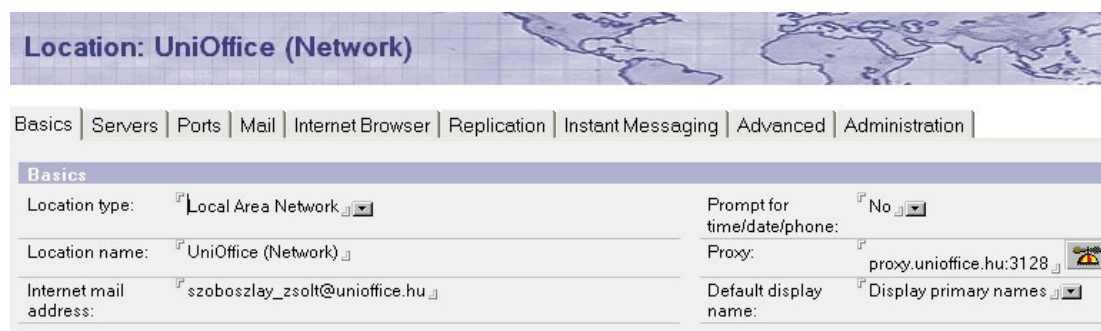
- Micardo PKI User kártyakezelő szoftver
- Mozilla Suite alkalmazáscsomag
- Netscape alkalmazáscsomag
- Firefox böngésző
- Thunderbird levelező program
- Lotus Notes R6/R7 alkalmazás

## 8. Függelék A – Az e-mail címek beállításának lehetőségei

Alapkövetelmény, hogy a tanúsítványokban található e-mail címnek levelezés esetén meg kell egyeznie a levelezésben beállítható e-mail címmel.

Ez a Lotus Notes estében viszonylag sok helyen beállítható, mégpedig a következő helyeken:

- Szerver címtár személy dokumentum
- Location > Basics > Internet mail address



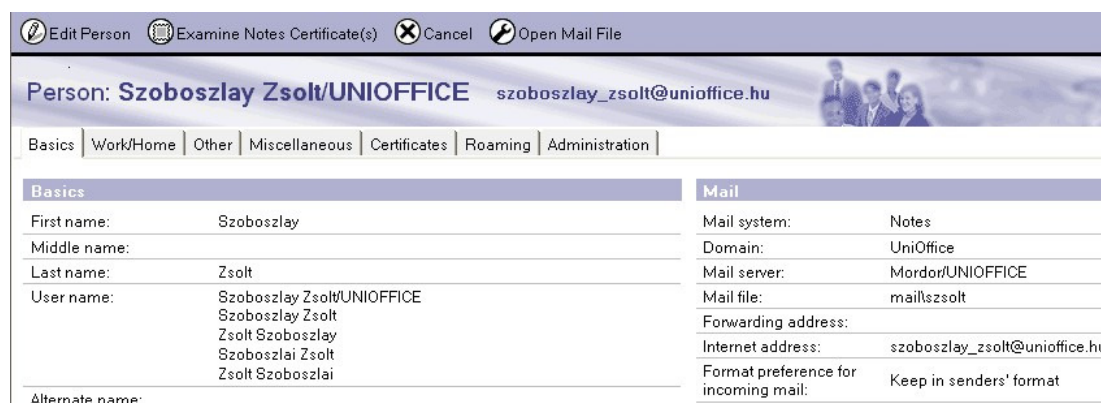
**Location: UniOffice (Network)**

Basics | Servers | Ports | Mail | Internet Browser | Replication | Instant Messaging | Advanced | Administration

**Basics**

Location type:	Local Area Network	Prompt for time/date/phone:	No
Location name:	UniOffice (Network)	Proxy:	proxy.unioffice.hu:3128
Internet mail address:	szoboszlay_zsolt@unioffice.hu	Default display name:	Display primary names

- Person > Basics > Internet address



**Person: Szoboszlay Zsolt/UNIOFFICE** szoboszlay\_zsolt@unioffice.hu

Basics | Work/Home | Other | Miscellaneous | Certificates | Roaming | Administration

Basics		Mail	
First name:	Szoboszlay	Mail system:	Notes
Middle name:		Domain:	UniOffice
Last name:	Zsolt	Mail server:	Mordor/UNIOFFICE
User name:	Szoboszlay Zsolt/UNIOFFICE Szoboszlay Zsolt Zsolt Szoboszlay Szoboszlay Zsolt Zsolt Szoboszlay	Mail file:	mailszsolt
Alternate name:		Forwarding address:	
		Internet address:	szoboszlay_zsolt@unioffice.hu
		Format preference for incoming mail:	Keep in senders' format

- Messaging > Domains > Global Domains > Conversions

Domain Uniinternet	
Basics   Restrictions   <b>Conversions</b>   Comments   Administration	
<b>SMTP Address Conversion</b>	
Local primary Internet domain:	<input type="text" value="unioffice.hu"/>
Alternate Internet domain aliases:	<input type="text"/>
Internet address lookup:	<input type="text" value="Enabled"/>
<i>If disabled or no match, convert as follows:</i>	
Local part formed from:	<input type="text" value="Short name"/>
Domino domain(s) included:	<input type="text" value="None"/>
Domino domain(s) position:	<input type="text" value="Left of '@'"/>
Domino domain separator:	<input type="text" value="% - percent sign"/>
Address example:	JMD@acme.com
NOTE: The following settings are not used in R5, R6, or R7. They only apply to R4.x SMTP MTAs	
Outbound mail restriction:	<input type="text" value="Unrestricted"/>
Address format:	<input type="text" value="Address only"/>