

# Novell GroupWise alkalmazás tanúsítványok használatához

---

Windows tanúsítványtárban és kriptográfia eszközökön található  
tanúsítványok esetén

## 1. Tartalomjegyzék

---

1.	Tartalomjegyzék .....	2
2.	Bevezető .....	3
3.	A Novell GroupWise alkalmazás beállítása tanúsítványok használatához.....	3
4.	A szoftver specifikus tulajdonságok.....	3
5.	A közigazgatási gyökértanúsítványok telepítése .....	4
5.1.	A közigazgatási gyökértanúsítványok telepítése Windows XP esetén.....	4
5.2.	A közigazgatási gyökértanúsítvány telepítése Windows Vista esetén.....	5
6.	Rövid áttekintés a tanúsítvány igénylési - és tárolási megoldásokról.....	6
6.1.	Tanúsítvány igénylése Mozilla böngészőn keresztül.....	6
6.2.	Tanúsítvány igénylése Internet Exploreren keresztül.....	6
6.3.	Tanúsítvány és kulcsok kriptográfiai eszközön (kártyán, tokenen).....	7
6.4.	Tanúsítvány és kulcsok PKCS#12 (PFX) állományban.....	7
7.	A tanúsítványok telepítése .....	8
7.1.	Ha a tanúsítvány kártyán, tokenen található.....	8
7.2.	Ha a tanúsítvány már a gépen található .....	8
7.3.	Ha a tanúsítványkérelem beadása Mozilla böngészőn keresztül történt.....	8
7.3.1.	Tanúsítvány exportálása Firefox böngészőből Windows tanúsítványtárba telepítéshez.....	8
7.4.	PKCS12 (PFX) fájlban található tanúsítvány telepítése Windows tanúsítványtárba.....	9
7.5.	A Netlock gyökértanúsítványainak elfogadása.....	10
7.6.	A visszavonási listák beállítása .....	11
8.	A tanúsítványok elérésének meghatározása, használatának beállítása .....	12
9.	Aláírt és/vagy titkosított levelek küldése.....	14
10.	Egyes alkalmazások együttes futtatásával kapcsolatos lehetséges problémák.....	15
11.	Hibaelhárítás .....	16
12.	Függelék A - Biztonsági másolat készítése tanúsítványairól és kulcsairól.....	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 zökkenő mentesebben történjen meg. Kérjük, olvassa el figyelmesen, és kövesse a leírtakat.

Amennyiben bármilyen kérdése van, 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.

## *3. A Novell GroupWise alkalmazás beállítása tanúsítványok használatához*

---

A következő fejezetek a Novell GroupWise csopormunka alkalmazás beállítását mutatják be, ahhoz, hogy tanúsítványait, el tudja érni, illetve használni tudja szoftveréből.

A telepítés lépései a Windows rendszereken történő beállításokat írják le.

A működés tesztelése és a dokumentáció Novell GroupWise 7 verzió használatával történt, javasolt lehetőség szerint legalább ezt a verziót használni.

Korábbi verziók beállításához kérjük, tekintse át a GroupWise felhasználói kézikönyvét vagy konzultáljon a Novell hazai képviselőjével (Novell Kft, 1125 Budapest Csörsz utca 45. 7. emelet, Tel: (1) 489-4600).

A dokumentáció elsősorban a Novell levező kliens beállításnak lépéseit mutatja be, más beállítások kapcsán kérjük, tekintse át a GroupWise felhasználói kézikönyvét vagy konzultáljon a Novell vevőszolgálatával.

## *4. A szoftver specifikus tulajdonságok*

---

A Novell GroupWise kliens a tanúsítványok használatához mindenféleképpen igényli egy titkosító és egy aláíró tanúsítvány jelenlétét, ezért mindkét tanúsítványtípus beszerzése szükséges, melyet egy kriptográfiai eszközön kell tárolni. (Tehát vagy mind ugyanazon eszközön, vagy mind szoftveresen.)

## 5. A közigazgatási gyökértanúsítványok telepítése

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

**a közigazgatási gyökértanúsítványokat azok használatához telepítenie kell.**

A közigazgatási gyökértanúsítványok a következő linkeken érhetők el:

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

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

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

### 5.1. A közigazgatási gyökértanúsítványok telepítése Windows XP esetén

A lépések a következők:

1. Indítsa el az Internet Explorer böngészőt.
2. Nyissa meg a böngészővel a fent látható linkek egyikét.
3. A linket megnyitva előugrik a Tanúsítvány letöltése (Downloading Certificate) ablak.
4. A megjelenő ablakban válassza a Megnyitás (Open) opciót.
5. A következő megjelenő ablakban válassza a Tanúsítvány telepítése (Install certificate) gombot.
6. Nyomja meg kétszer a Tovább (Next) gombot.
7. Nyomja meg a Befejezés (Finish) gombot, és a megjelenő tájékoztató üzenetre nyomja meg az OK gombot.
8. Hajtsa végre a másik két linkre is a fentieket.

Ezzel a közigazgatási tanúsítványok telepítése Windows XP rendszerre megtörtént.

#### **Figyelem!**

**Ha nincs telepítve a Root Update komponens vagy régi operációs rendszert használ, további gyökértanúsítvány telepítésekre lesz szüksége.**

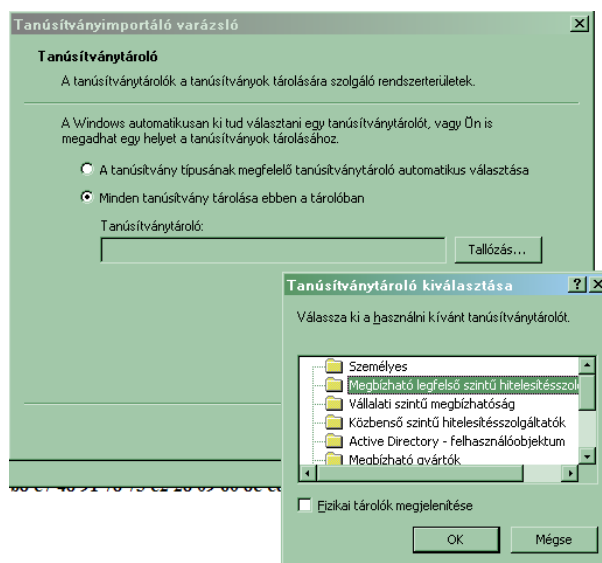
## 5.2. A közigazgatási gyökértanúsítvány telepítése Windows Vista esetén

A KGYHSZ gyökértanúsítvány telepítése Vista rendszeren eltér a többitől.

A lépései a következők:

1. Indítsa el az Internet Explorer böngészőt.
2. Nyissa meg a böngészővel a következő linket:  
[http://www.kgyhsz.gov.hu/KGYHSZ\\_CA\\_20060719.cer](http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.cer)
3. A megjelenő ablakban válassza a Megnyitás (Open) opciót.
4. A következő megjelenő ablakban válassza a Tanúsítvány telepítése (Install certificate) gombot.
5. Nyomja meg egyszer a Tovább (Next) gombot.
6. A következő ablakban válassza a második opciót, majd „Megbízható legfelső szintű...” opciót. (Trusted root...)
7. Az ablakot Ok gombbal hagyja jóvá, majd nyomja meg a Tovább (Next) gombot.
8. Nyomja meg a Befejezés (Finish) gombot, és a megjelenő tájékoztató üzenetre nyomja meg az OK gombot.
- 9.

Ezzel a közigazgatási gyökértanúsítvány telepítése Windows Vista rendszerre megtörtént.



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

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

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

## 6. 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.

### 6.1. 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.

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.

**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.

### 6.2. 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, se böngészőjét**, mivel ezzel helyreállíthatatlanul törli a tanúsítványához tartozó privát kulcsot is, e nélkül pedig az használhatatlan lesz.

### 6.3. 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 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, 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.

### 6.4. 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. A tanúsítványok telepítése

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

### 7.1. Ha a tanúsítvány kártyán, tokenen található

Amennyiben tanúsítványát kriptográfiai eszközön kapta meg, akkor a kriptográfiai eszköz telepítési útmutatója leírja, hogyan importálható a tanúsítvány a Windows tanúsítványtárba. Kérjük, hajtja végre az ott leírtakat.

### 7.2. Ha a tanúsítvány már a gépen található

Ha a tanúsítvány a tanúsítvány igénylését (fokozott biztonságú tanúsítvány esetén) Internet Explorerből intézte, a tanúsítvány kiadási folyamat végén a tanúsítvány és a kulcsok megtalálhatók az Ön gépén.

Ekkor nincs szükség a tanúsítvány telepítésére, azonban biztonsági másolatot érdemes létrehoznia.

### 7.3. Ha a 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, majd ezt importálnia kell, és a Windows tanúsítvány tárba telepítenie.

#### 7.3.1. Tanúsítvány exportálása Firefox böngészőből Windows tanúsítványtárba telepítéshez

A Firefox böngésző az egyik leggyakoribb Mozilla böngésző, ezért a PKCS#12 mentés készítését ezen mutatjuk be, a többi Mozilla termék PKCS#12 mentés készítését az adott termékhez készült dokumentáció mutatja be.

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 válassza ki mentendő tanúsítványt, majd nyomja meg a Mentés (Backup) gombot.
4. A következő ablakban adja meg a mentés helyét.

5. Ezt követően adja meg Firefox-on belüli tanúsítványvédelmi jelszót. (mesterjelszó / master password) (Ez az első tanúsítvány export-import előtt nincs beállítva, ekkor kétszer kell begépelnie, és a későbbiek során ez után fog rendszeresen érdeklődni a Firefox böngésző.)
6. Ezután adja meg a .pfx fájl jelszavát, amellyel védeni kívánja, ezt a jelszót jegyezze is fel.
7. A mentés után tájékoztatást kap, hogy az sikeresen megtörtént, majd nyomjon Ok gombot az összes ablak bezáródásáig.

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

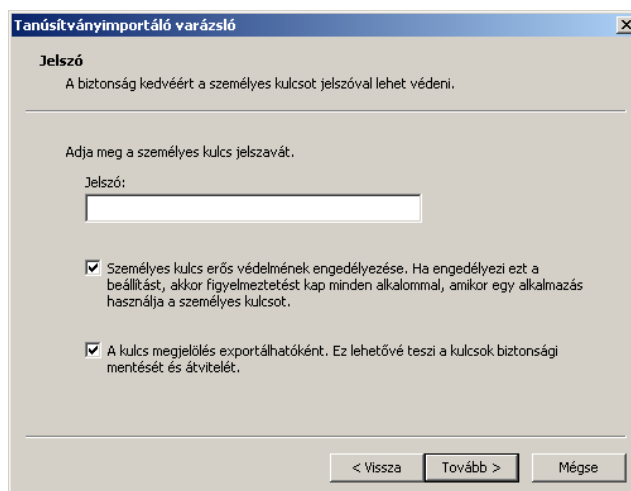
A következő fejezet ismerteti a PKCS#12 állományok telepítését.

#### 7.4. PKCS12 (PFX) fájlban található tanúsítvány telepítése Windows tanúsítványtárba

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

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

1. Ahhoz, hogy a gépén található PKCS#12 állományt telepítse, kattintson kétszer az Intézőből (Explorer) a \*.pfx, (\*.p12) kiterjesztésű fájlra. Ekkor a tanúsítvány telepítése varázsló indul el.
2. Az üdvözlő képernyőn nyomja meg a Tovább (Next) gombot.
3. A második képernyőn az importálandó fájl nevét látja. Itt nincs semmi teendő, lépjen tovább a Tovább (Next) gomb segítségével.
4. A következő képernyőn adja meg a PKCS#12 fájlhoz tartozó jelszót. Itt állíthatja be a tanúsítvány erős védelmét és későbbi exportálhatóságát. Javasoljuk mindkét opciót kipipálni és ezután a Tovább (Next) gombot megnyomni.
5. A következő képernyő megkérdezi, hogy automatikus vagy kézzel történő elhelyezést kíván a megfelelő tanúsítványtárolóban. Itt válassza az



- Automatikus kiválasztást (Automatically...), majd kattintson a Tovább (Next) gombra.  
6. Az utolsó képernyőn kattintson a Befejezés (Finish) gombra.

A tanúsítvány telepítése ezzel megtörtént.

### 7.5. A Netlock gyökértanúsítványainak elfogadása

A tanúsítvány kiadója minden tanúsítványt aláír saját privát kulcsával annak szavatolása érdekében, hogy a tanúsítvány tartalma garantált legyen. A tanúsítvány valódiságának biztosítására a felhasználók a tanúsítványhatóság nyilvános kulcsával ellenőrzik aláírását. Első lépésként a GroupWise kliensen be kell állítani azt, hogy az a NetLock által aláírt tanúsítványokban megbízzon, azokat valódiaknak fogadja el.

Ennek lépései a következők:

1. Kriptográfiai szolgáltató (CSP) megadása

A Eszközök | Beállítások | Adatvédelem | Küldési beállítások (GroupWise Tools | Option | Security | Send Options) menüpont alatt a „Biztonsági szolgáltató kiválasztása” („Select a security service provider”) legördülő menüben válasszuk ki az „Microsoft Enhanced Cryptographic Provider v1.0”-t, majd nyomjuk meg az Ok gombot.

Erre a lépésre azért van szükség, hogy a belső hitelesítő tanúsítvány biztosan a gépen, véletlenül se a kártyára jöjjön létre.

2. A tanúsítványhatóság hitelesnek minősítése

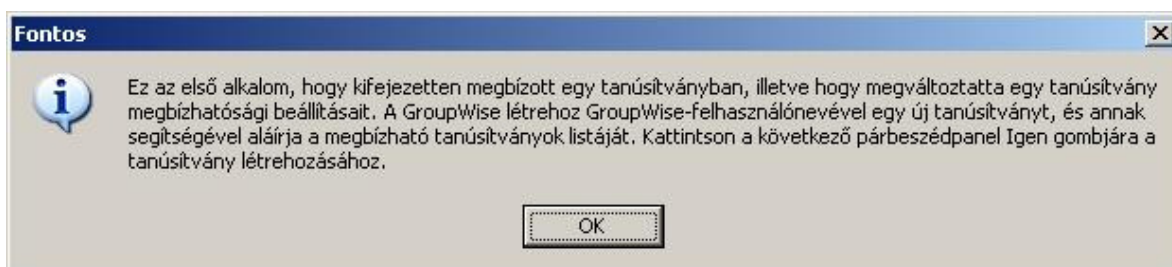
Az Eszközök | Beállítások | Tanúsítványok | Hitelesítésszolgáltatók tanúsítványai | Gyökér-hitelesítésszolgáltatók tanúsítványai (Tools | Option | Certificates | Certificate Authorities' Certificates | Root Certificate Authorities' Certificates) menüpont alatt válasszuk ki a listából a „NetLock CA” bejegyzést.

Kattintsunk rá a „Megbízhatóság módosítása” („Modify Trust”) gombra.

Válasszuk ki a legfelső pontot, az „Ezen hitelesítésszolgáltató által aláírt tanúsítványok elfogadása (Összes)” („Trust all certificates signed by this Certificate Authority (All)”), majd nyomjuk meg az Ok gombot, majd még egyszer az Ok gombot a Tanúsítványok (Certificates) ablakban.

Ha ez az első alkalom, hogy megváltoztattuk a GroupWise kliensben valamely tanúsítvány bizalmassági státuszát, egy figyelmeztetést kapunk arról, hogy a kliens egy új tanúsítványt

készít a használt GroupWise azonosítóval a megbízható tanúsítványok listájának aláírásához. A figyelmeztetés ablakban nyomjuk meg az Ok gombot.



**A figyelmeztető üzenet**

A következő dialógusablakban a Windows rákérdez, hogy hozzá szeretnénk-e adni a létrehozott tanúsítványt a tanúsítványkiadókat tartalmazó listához. Lépünk tovább igennel.

Ezzel a beállítások megtörténtek.

## ***7.6. A visszavonási listák beállítása***

---

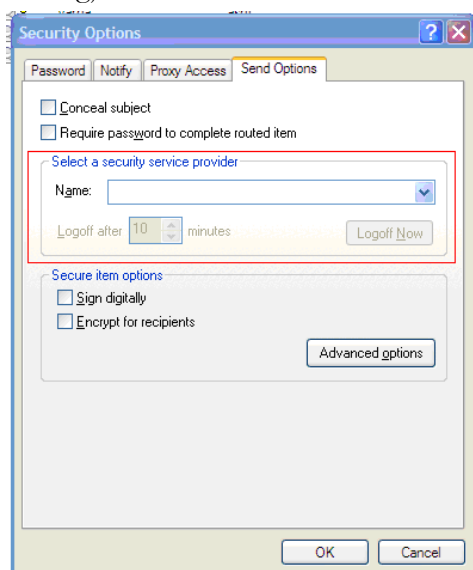
A Novell kliens a tanúsítványokban található CDP mező alapján automatikusan ellenőrzi a tanúsítványok szereplését visszavonási listákon, ezért e-téren nincs szükség semmilyen külön beállításra.

## 8. A tanúsítványok elérésének meghatározása, használatának beállítása

Az előző fejezet alapján telepített tanúsítványok elérési módját a Novell GroupWise számára meg kell határozni.

Ezt a következőképpen teheti meg:

1. Navigáljon el a Küldési beállítások (Send options) menüpontig.  
Eszközök > Beállítások > Biztonság > Küldési beállítások  
(Tools > Options > Security > Send options)
2. A megjelenő ablakban válassza ki a megfelelő kriptográfiai szolgáltatót.



Ez a következő lehet:

**Szoftveresen tárolt tanúsítvány**  
**Rainbow Ikey 2032 token**  
**Oberthur kártya**  
**Micardo kártya**

**Microsoft Enhanced Cryptographic Provider**  
**DAakey RSA CSP**  
**OCS Cryptographic Service Provider**  
**Orga Micardo Card CSP**

Ugyanezen ablak Biztonságos elem beállítások (Secure item options) pontja alatt beállítható, az alapértelmezett aláírás (sign digitally) és titkosítás (encrypt) is, vagyis ezeket bepipálva alapértelmezetten mindenkinek aláírva és/vagy titkosítva kerül kézbesítésre a levél.

3. Ez után be kell állítania az adott helyen elérhető tanúsítványokat, mint alapértelmezett tanúsítványokat.
4. Navigáljon el a Tanúsítványok (Certificates) menüpontra.  
Eszközök > Beállítások > Tanúsítványok  
(Tools > Options > Certificates)
5. Az elérhető tanúsítványok közül válasszon ki egy aláírókat majd nyomja meg az Alapértelmezés (Set as default) gombot.
6. Az elérhető tanúsítványok közül ezután válasszon ki egy titkosítót majd nyomja meg az Alapértelmezés (Set as default) gombot.

Ezzel a tanúsítványok elérhetősége, és levelezésre történő használatuk beállításra került.

## *9. Aláírt és/vagy titkosított levelek küldése*

---

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

Amikor megírta a levelét, még a küldés előtt válassza nyomja meg az Aláírás (pecsét) és/vagy a Titkosítás (lakat) gombokat, majd küldje el 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.

### 10. 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. Hibaelhárítás*

---

### **Tanúsítványomat nem látom a programból**

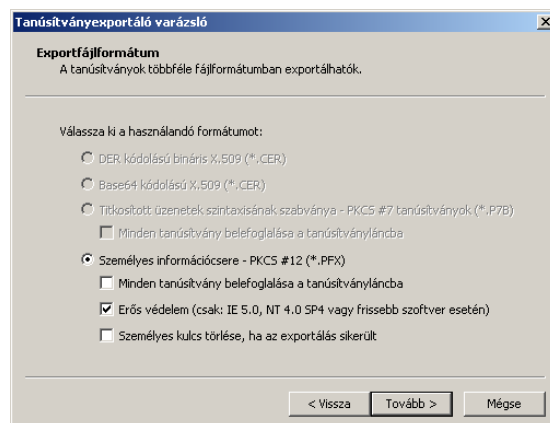
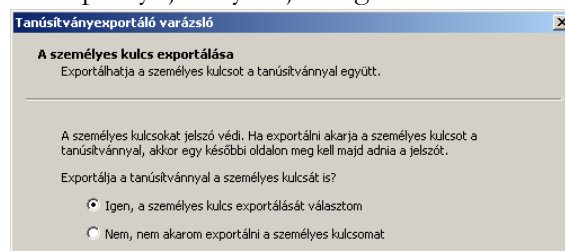
Ellenőrizze, hogy a fiókhöz beállított e-mail cím egyezik-e a tanúsítványban találhatóval.

A kettőnek egyeznie kell.

## 12. Függelék A - Biztonsági másolat készítése tanúsítványairól és kulcsairól

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 Internet Explorer böngészőt.
2. Navigáljon el a tanúsítványok menüponthoz. (Eszközök > Internet beállítások > Tartalom fül > Tanúsítványok gomb) (Tools > Internet Settings > Content fül > Certificates gomb)
3. Válassza ki a Saját (Personal) lapon a tanúsítványok közül az exportálandót, majd nyomja meg az Export gombot.
4. A megjelenő tanúsítvány exportáló varázsló üdvözlő képernyőjén nyomja meg a Tovább (Next) gombot.
5. A következő ablakban válassza a privát kulcs exportálását is (Yes, export the private...), majd kattintson a Tovább (Next) gombra.
6. A következő ablakban a második rádiógombhoz tartozó szekció érhető csak el. Itt állítson be Erős titkosítást (Enable strong protection). Ha szüksége van arra, hogy a tanúsítvánnyal együtt a hozzá tartozó gyökértanúsítványt is exportálja, akkor jelölje ki a Minden tanúsítvány exportálása opciót (Include all certificates...) is. Ha a privát kulcsot törölni akarja az exportálás után erről a gépről, akkor jelölje be a privát kulcs törlése (Delete the Private...) opciót is.
7. A következő ablakban adja meg kétszer azt a jelszót, amelyet szeretne a fájlnak adni. Ez jegyezze meg jól, mert ennek ismeretében tudja telepíteni másik gépen tanúsítványát.
8. A következő ablakban kiválaszthatjuk a fájlnevet, és a helyet, ahol a fájl létre szeretnénk hozni.
9. Miután ezt beállította, már csak a Tovább (Next) és végül a Befejezés (Finish) gombot kell megnyomnia, valamint a megnyitott ablakokat OK gombbal bezárnia.



A tanúsítvány exportálása ezzel megtörtént.

Ezt az állományt érdemes biztonságos helyen elzárni valamilyen adathordozón.