Evolution levelező program beállítása tanúsítványok használatához

Linux operációs rendszeren, szoftveresen tárolt tanúsítványok esetén

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

1. Tartalomjegyzék

1. Tartalomjegyzék 2
2. Bevezető 3
3. Az Evolution szoftver korlátozásai 3
4. Az Evolution levelező program beállítása tanúsítványok használatához 3
4.1. A gyökértanúsítványok telepítése 3
4.2. A visszavonási listák kezelése 3
4.3. Fájlban található (PFX állomány) tanúsítvány telepítése 4
5. Tanúsítványok és kulcsok beállítása levelezéshez és titkosításhoz 5
6. Aláírt és/vagy titkosított levelek küldése 6
7. Függelék A – Aláírás érvényességének megtekintése 7
8. Függelék B - Tanúsítvány (PKCS#12 fájl) exportálása Firefox böngészőből 8
9. Függelék C - Tanúsítvány (PFX fájl) exportálása Seamonkey alkalmazásból 8
10. Függelék D – Tanúsítvány (PFX fájl) exportálása Internet Explorer böngészőből 9

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

2. Bevezető

Ennek a tájékoztatónak az a célja, hogy az elektronikus aláíráshoz és titkosításhoz szükséges kriptográfiai eszközök (intelligens kártya, USB token) 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 1101 Budapest, Expo tér 5-7. szám alatt munkanapokon 9 és 17 óra között készséggel áll rendelkezésére.

3. Az Evolution szoftver korlátozásai

Az Evolution levelező program jelenleg nem támogatja az intelligens kártya használatát.

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

Az Evolution levelező program előzetes tesztjeink alapján nem támogat visszavonási listákat, tehát használata valamilyen szintű biztonsági kockázatot rejt, a tanúsítványok esetleges visszavonása nem derül ki a szoftver számára.

4. Az Evolution levelező program beállítása tanúsítványok használatához

A következő fejezetek az Evolution levelező program beállítását mutatják be, ahhoz, hogy tanúsítványait, el tudja érni, illetve használni tudja levelező programjából.

A beállítási útmutató a 2.4.0 verzió alapján készült, korábbi verziók használatát nem javasoljuk.

4.1. A gyökértanúsítványok telepítése

Az Evolution szoftverben a Netlock A, B, C osztályú gyökértanúsítványai megtalálhatók, telepítésük nem szükséges. Amennyiben mégis szükségesek a gyökértanúsítványok, az alábbi oldalon megtalálja őket: https://www.netlock.hu/html/cacrl.html

4.2. A visszavonási listák kezelése

Az előzetes tesztek alapján a az Evolution levelező program nem kezel visszavonási listákat.

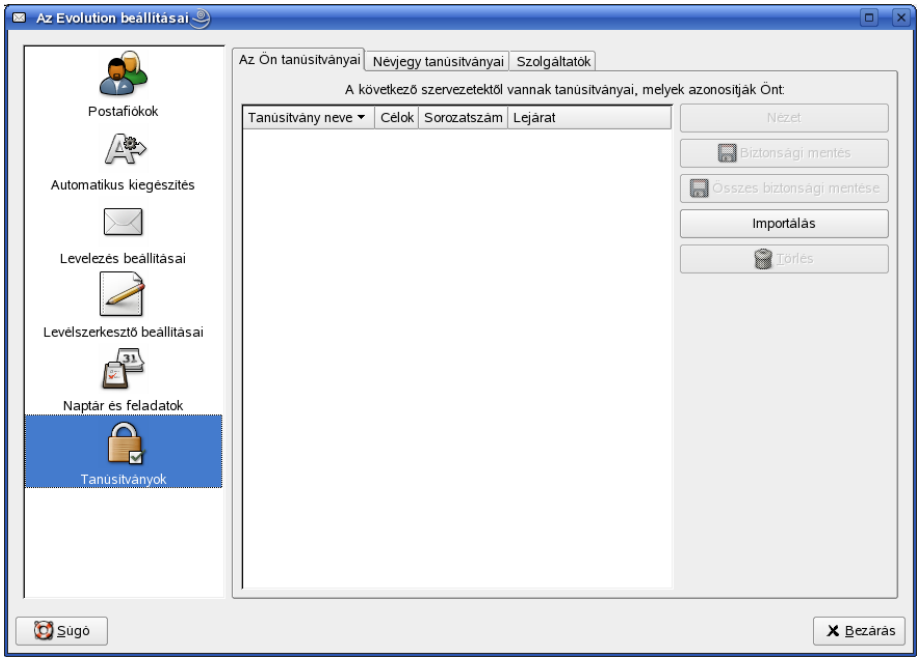
NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

4.3. Fájlban található (PFX állomány) tanúsítvány telepítése

1. Navigáljon el a tanúsítvány beállítások ablakig.

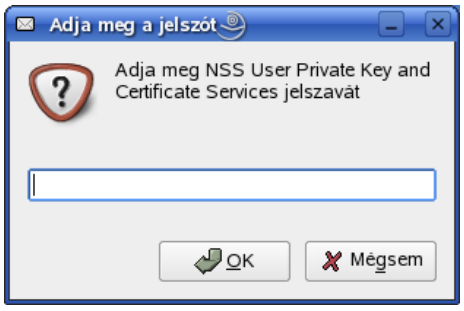
   Eszközök > Beállítások > Tanúsítványok > Az Ön tanúsítványai fül

   (Tools > Options > Certificates > Your certificates fül)

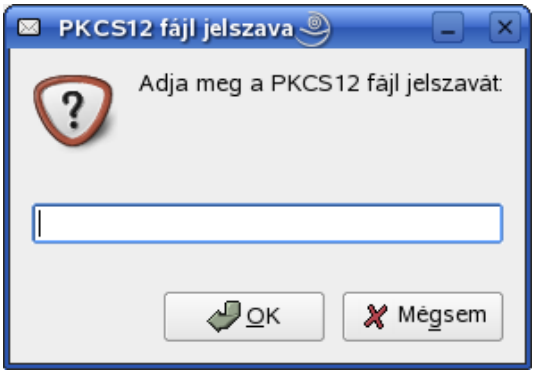


2. Nyomja meg az Importálás (Import) gombot, majd tallózza ki a PKCS#12 (.PFX vagy .P12) fájlt.
3. A megjelenő ablakban adja meg a tanúsítvány védelmi jelszót.

   Figyelem! Az első alkalommal megadott jelszóra lesz később is szüksége, jegyezze azt fel.



4. Ezután adja meg a PFX fájl jelszavát.



A tanúsítvány telepítése ezzel megtörtént.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

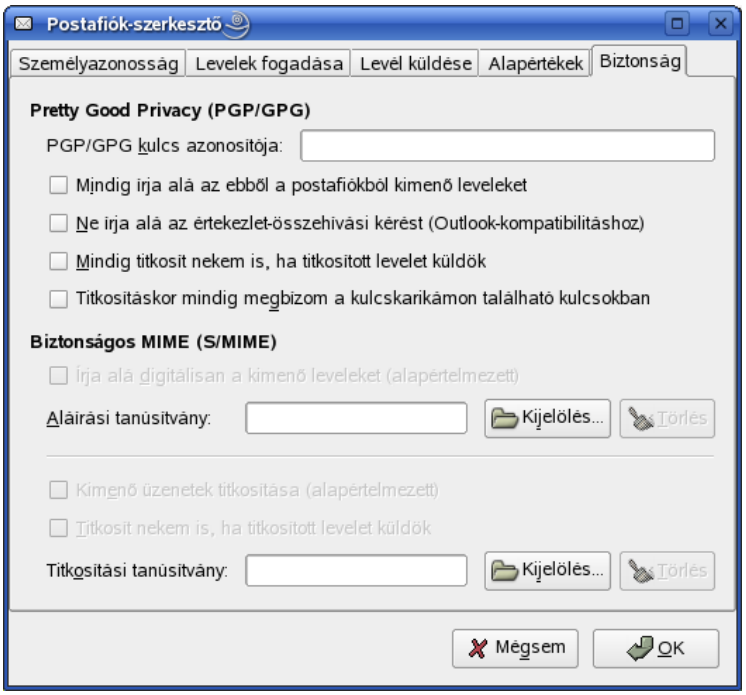
5. Tanúsítványok és kulcsok beállítása levelezéshez és titkosításhoz

Ahhoz, hogy az Evolution levelező programban tanúsítvánnyal aláírva és titkosítva is küldhessen levelet a következő lépéseket kell végrehajtania.

1. Navigáljon el a Postafiók szerkesztő (Account editor) menüpontba, azon belül a Biztonság fülre

   Eszközök > Beállítások > Postafiókok > beállítandó fiók kiválasztása > Szerkesztés Biztonság fül)

   (Tools > Options > Certificates > Accounts > beállítandó fiók kiválasztása > Properties > Security)



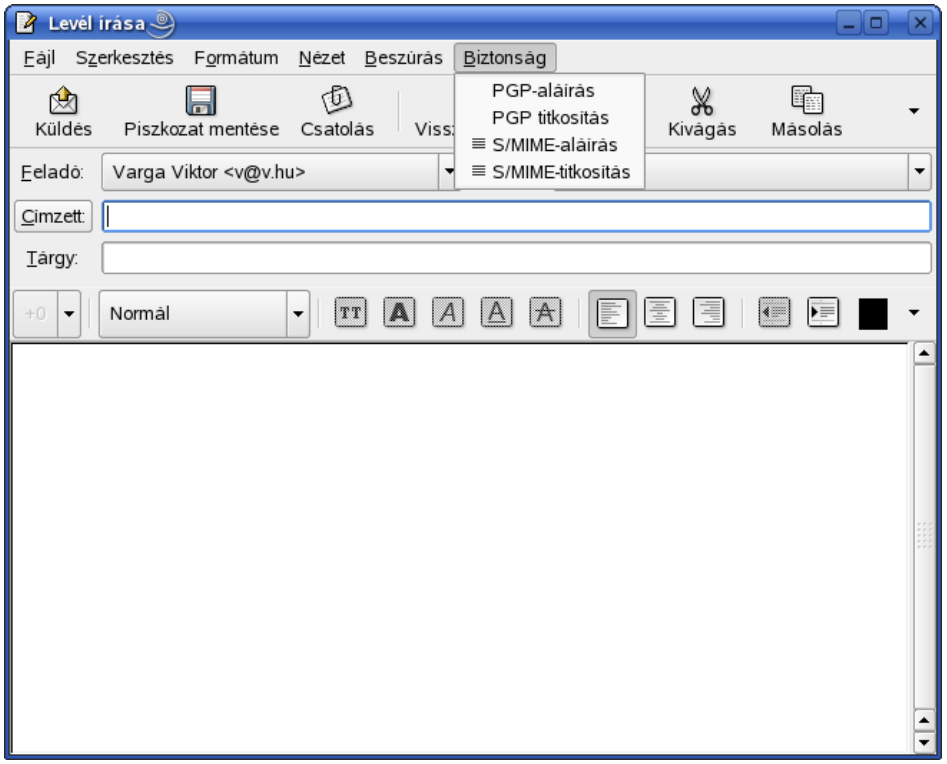
2. Biztonságos MIME (S/MIME) szekcióban állítsa be az aláíró és titkosító tanúsítványokat.
3. Amennyiben alapértelmezettként aláírni illetve titkosítani szeretne, akkor az itt található jelölő négyzetekkel az is beállíthatja.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

6. *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) menüpontot.
2. A lenyíló menüben kiválaszthatja, hogy digitálisan aláírja (S/MIME-aláírás) és/vagy titkosítja (S/MIME-titkosítás) a levelet.



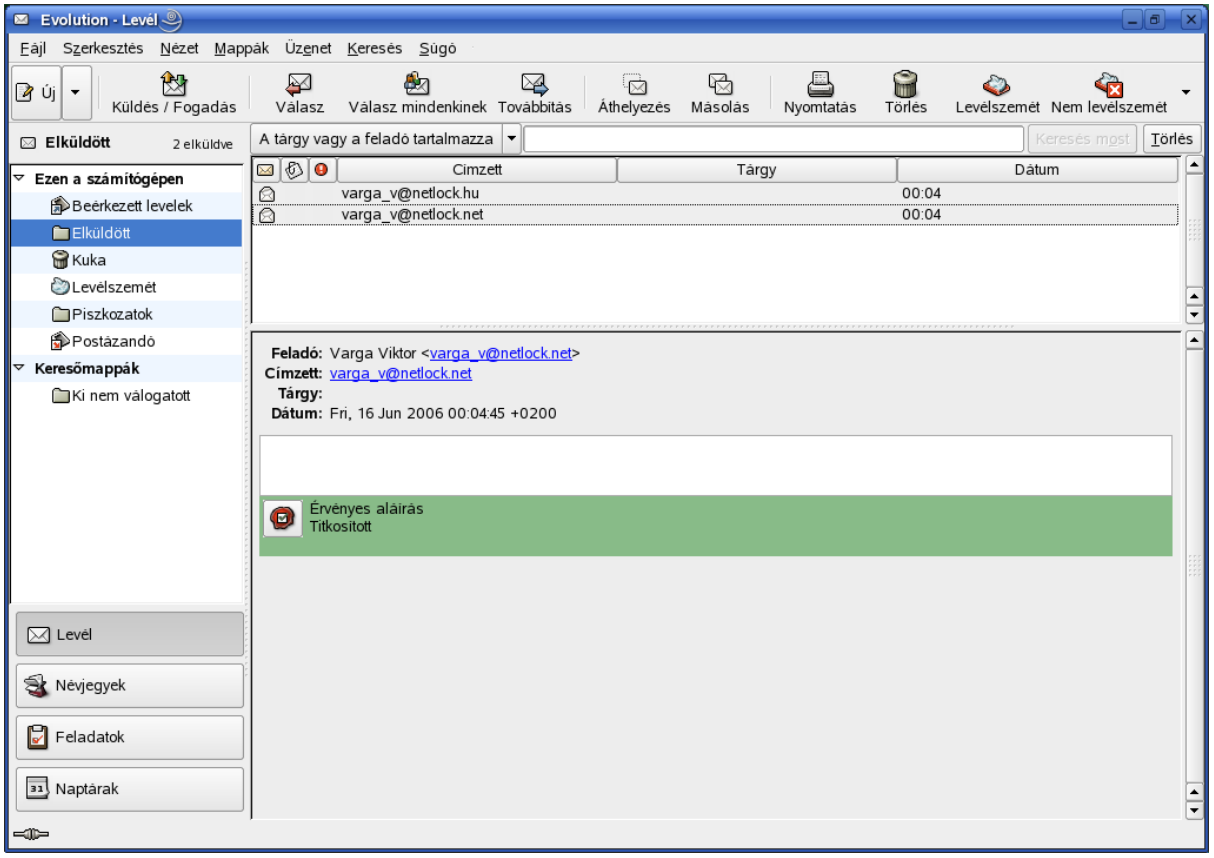
Fontos, hogy tudja, hogy ahhoz, hogy titkosított levelet küldjön valakinek, rendelkeznie kell a levelezőpartner nyilvános kulcsával. Ennek feltétele, hogy szerepeljen partnere a címjegyzékben, partnere névjegyében pedig a tanúsítványa nyilvános kulcsa.

Ha ez a feltétel nem teljesül, 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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

7. Függelék A – Aláírás érvényességének megtekintése

Az aláírt/titkosított levelekről a betekintő ablakban kaphatunk információt, mint a következő ábrán is látható.



NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

8. Függelék B - Tanúsítvány (PKCS#12 fájl) exportálása Firefox böngészőből

Az exportálás lépései a következők:

1. Indítsa el a Firefox böngészőt.
2. Navigáljon el a Tanúsítványok menüpontig. Eszközök > Beállítások > Haladó (vagy Speciális) > Titkosítás fül > Tanúsítványkezelő gomb (Tools > Options > Advanced > Security fül > Certificates gomb)
3. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön válassza ki tanúsítványát, majd nyomja meg a Mentés (Backup) gombot.
4. Adja meg a PKCS#12 fájl fájlnevét és a helyet, ahova menteni szeretné.
5. Adja meg a PKCS#12 fájl jelszavát. Ez a jelszó lesz az, amivel a PKCS#12 fájl titkosításra fog kerülni, hogy illetéktelenek a jelszó ismerete nélkül a tanúsítványt más gépbe, programba ne importálhassák.
6. Az OK gomb megnyomása után a tanúsítvány mentésre kerül a privát kulccsal együtt.

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

9. Függelék C - Tanúsítvány (PFX fájl) exportálása Seamonkey alkalmazásból

1. Navigáljon el a biztonsági beállítások menüpontig. (Szerkesztés > Beállítások > Adatvédelem & Biztonság > Tanúsítványok) (Edit > Preferences > Privacy & Security > Certificates)
2. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön válassza ki tanúsítványát, majd nyomja meg az Backup (Mentés) gombot.
3. Adja meg a a PKCS #12 fájl fájlnevét.
4. Adja meg a böngésző belső tanúsítványvédelmi jelszavát. (Ha volt ilyen beállítva.)
5. Adja meg a PKCS #12 fájl jelszavát. Ez a jelszó lesz az amivel a PKCS #12 fájl titkosításra fog kerülni, hogy illetéktelenek a jelszó ismerete nélkül a tanúsítványt más gépbe, programba ne importálhassák.

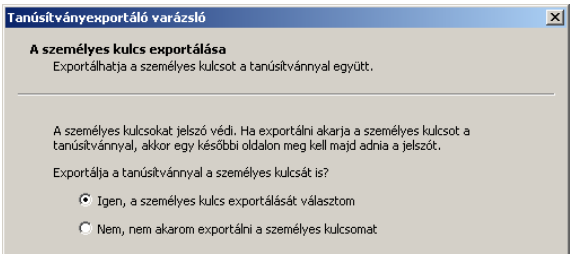
A tanúsítvány exportálása ezzel megtörtént. Javasolt az exportált állományt a telepítés után, mint biztonsági másolatot biztonságos helyen tárolni.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

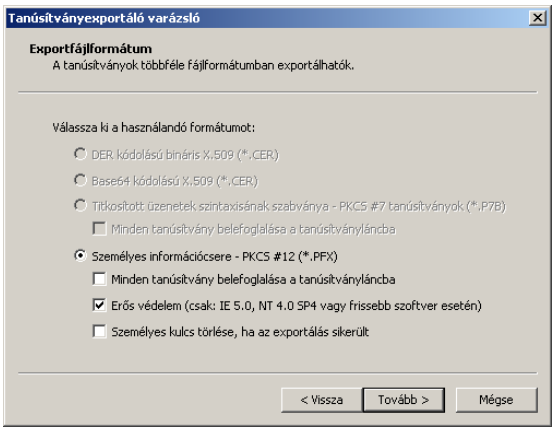
10. Függelék D – Tanúsítvány (PFX fájl) exportálása Internet Explorer böngészőből

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. 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 fájlt 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.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu