

www.netlock.hu

1(9)

Evolution levelező program beállítása tanúsítványok használatához

Linux operációs rendszeren, szoftveresen tárolt tanúsítványok esetén





www.netlock.hu

2(9)

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





www.netlock.hu

3(9)

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 színtű 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.





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.

🛛 PKCS12 fájl jelszava 🎱 📃 🗙					
?	Adja meg a PKCS12 fájl jelszavát:				
]			

4(9)



www.netlock.hu

5(9)

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)

Postafiók-szerkesztő	×						
Személyazonosság Levelek fogadása Levél küldése Alapértékek Biztonság							
Pretty Good Privacy (PGP/GPG)							
PGP/GPG <u>k</u> ulcs azonositója:							
🗌 Mindig irja alá az ebből a postafiókból kimenő leveleket							
Ne irja alá az értekezlet-összehívási kérést (Outlook-kompatibilitáshoz)							
☐ <u>M</u> indig titkosit nekem is, ha titkositott levelet küldök							
🗌 Títkosításkor mindig megbizom a kulcskarikámon található kulcsokban							
Biztonságos MIME (S/MIME)							
🔲 Írja alá digitálisan a kimenő leveleket (alapértelmezett)							
Aláirási tanúsitvány:	5						
🔲 Titkosit nekem is, ha titkositott levelet küldök							
Titkositási tanúsitvány: 🕒 Kijelölés) 🔪 Törlé	5						
🗶 Mégsem 🥥 OK							

- 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.





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.

🕜 Levél írása 🎱 💶 🗖	×
<u>F</u> ájl S <u>z</u> erkesztés F <u>o</u> rmátum <u>N</u> ézet <u>B</u> eszúrás <u>Biztonság</u>	
Image: Wight with the second seco	•
Eeladó: Varga Viktor <v@v.hu></v@v.hu>	-
Cimzett:	
Iárgy:	
	•
	÷

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.





www.netlock.hu

7. Függelék A – Aláírás érvényességének megtekintése

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

🗵 Evolution - Levél 🎱								
Eájl Szerkesztés <u>N</u> ézet <u>M</u> appák Üz <u>e</u> net <u>K</u> eresés <u>S</u> úgó								
🕑 Új 🝷 🕅 Küldés / Fogadás	Válasz Válasz mindenkinek Tovább	itás Áthelyezés Másolás Nyomtatás	Törlés Levélszemét Nem levélszemét					
Elküldött 2 elküldve	A târgy vagy a feladô tartalmazza 🔻		Keresës m <u>o</u> st <u>T</u> örlës					
 ▼ Ezen a számítógépen Beérkezett levelek ■ Elküldött ♥ Kuka ♥ Levélszemét ● Piszkozatok ♥ Postázandó ▼ Keresőmappák ♥ Ki nem válogatott 	Cimzett Cimzett Cimzett Cimzett Cimzett Cimzett Varga_v@netlock.hu Cimzett Varga_v@netlock.net Varga_v@ne	<net></net>	Dâtum 00:04 00:04 					
Level Level Level Feladatok			•					





www.netlock.hu

8(9)

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

Az exportálás lépései a következők:

- 1. Indítsa el a Firefox böngészőt.
- 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
 - 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.



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.
- 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.
- 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.
- 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.
- × A személyes kulcs exportálása Exportálhatja a személyes kulcsot a tanúsítvánnyal együtt A személyes kulcsokat jelszó védi. Ha exportálni akarja a személyes kulcsot a tanúsítvánnyal, akkor egy későbbi oldalon meg kell majd adnia a jelszót. Exportálja a tanúsítvánnyal a személyes kulcsát is? Igen, a személyes kulcs exportálását választor 🔿 Nem, nem akarom exportálni a személyes kulcsoma usítványexportáló varázsló × Exportfájlformátum A tanúsítványok többféle fájlformátumban exportálhatók Válassza ki a használandó formátumot: C DER kódolású bináris X.509 (*.CER) C Base64 kódolású X.509 (*.CER) C Titkosított üzenetek szintaxisának szabványa - PKCS #7 tanúsítványok (*.P7B) 📕 Minden tanúsítvány belefoglalása a tanúsítványláncba Személyes információcsere - PKCS #12 (*.PFX) 🦳 Minden tanúsítvány belefoglalása a tanúsítványláncba 🗹 Erős védelem (csak: IE 5.0, NT 4.0 SP4 vagy frissebb szoftver esetén) 🔲 Személyes kulcs törlése, ha az exportálás sikerült < Vissza Tovább > Mégse

 $\mathbf{9}_{(9)}$

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.

