

Thunderbird levelező program beállítása tanúsítványok használatához

Windows tanúsítványtárban, PFX fájlban, vagy kriptográfia eszközökön
található tanúsítványok esetén
(Windows és Linux operációs rendszereken)

Tartalomjegyzék

1.	Bevezető	3
2.	A Thunderbird levelező program beállítása tanúsítványok használatához	3
3.	A Linux rendszerek korlátozásai.....	3
3.1.	A Közigazgatási gyökértanúsítványok telepítése	3
4.	A tanúsítványok beállítása Windows rendszeren.....	4
4.1.	Kártyán, tokenen tárolt tanúsítvány beállítása	4
4.2.	PKCS12 (PFX) fájlban található tanúsítvány telepítése.....	4
4.3.	Kártya vagy token beállítása Thunderbird programba.....	5
5.	Tanúsítványok és kulcsok beállítása levelezéshez és titkosításhoz.....	7
6.	Levelek küldése Aláírva és/vagy Titkosítva	8
	Függelék - Egyes alkalmazások együttes futtatásával kapcsolatos problémák.....	9

1. Bevezető

Ennek a tájékoztatónak az a célja, hogy az elektronikus aláíráshoz és titkosításhoz szükséges beállítás és üzembe helyezés minél zökkenő mentesebben történjen meg. Kérjük, olvassa el figyelmesen, és kövesse a leírtakat.

Amennyiben bármilyen kérdése van vagy problémája támad, ügyfélszolgálatunk készséggel áll az Ön rendelkezésére az alábbi elérhetőségeken és időpontokban.

Telefonszám: (1) 437 6655

E-mail cím: info@netlock.hu vagy support@netlock.hu

2. A Thunderbird levelező program beállítása tanúsítványok használatához

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

Javasolt mindig a legfrissebb verzió használata (a leíráshoz a Thunderbird 52.8.0 verzióját alkalmaztuk).

Fontos!

Az elektronikus aláírást csak azon e-mail postafiókon tudja beállítani, melynek az e-mail címe szerepel a kiadott tanúsítványban!

A beállítás megkezdése előtt, kérjük, ellenőrizze a megfelelő postafiók beállítást.

3. 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.

3.1. A Közigazgatási gyökértanúsítványok telepítése

A Thunderbird 2.0 verziótól kezdve a Netlock gyökértanúsítványai már megtalálhatók az alkalmazásban, de **a közigazgatási gyökértanúsítványokat azok használatához telepítenie kell.**

A közigazgatási gyökértanúsítványok a következő linkeken érhetők el:

SHA256 algoritmusú kiadók:

http://www.kgyhsz.gov.hu/KGYHSZ_CA_20091210.cer

<http://www.netlock.hu/index.cgi?ca=mkozig256>

<http://www.netlock.hu/index.cgi?ca=bkozig256>

A közigazgatási gyökértanúsítványok telepítésének egyszerűsített lépései a következők:

1. Indítsa el böngészőjét.
2. Nyissa meg a böngészővel a fent látható linkek egyikét.
3. A fájlt mentse le a gépére.
4. Indítsa el a Thunderbird programot, majd navigáljon el a gyökértanúsítványokig. Eszközök > Beállítások > Speciális (vagy Haladó) > Tanúsítványok fül > Tanúsítványok kezelése > Hitelesítésszolgáltatók fül (Tools > Options > Advanced > Certificates fül > View certificates gomb > Authorities fül)
5. Kattintson az Importálás... gombra.
6. Tallózza ki az imént lementett fájlt.
7. A megjelenő ablakban pipálja ki mindhárom opciót.
8. Miután kipipálta kattintson az Ok gombra.
9. Hajtsa végre a másik két linkre is a fentieket.

Ezzel a közigazgatási tanúsítványok telepítése megtörtént.

4. A tanúsítványok beállítása Windows rendszeren

A tanúsítványok beállítása és használata vételéhez kövesse a leírtakat!

4.1. 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 Thunderbird ezt NEM TÁMOGATJA, tehát KÉZI beállítás szükséges.

4.2. PKCS12 (PFX) fájlban található tanúsítvány telepítése

Abban az esetben, ha tanúsítványát nem kriptográfiai eszközön szerezte be (hanem szoftveresen), akkor az arról készült PKCS#12 (.PFX) formátumú mentett állomány segítségével tudja tanúsítványát a Thunderbird 58-as verziójú levelező programban beállítani.

Ha nincs ilyen PKCS#12 (.PFX) állományba készült mentése, akkor az elkészült tanúsítványát a Mozilla böngészőjéből, vagy a Windows tanúsítvány tárából exportálnia kell. A tanúsítvány exportálásának lépéseit [Ide kattintva találja](#) attól függően, hogy milyen típusú tanúsítvánnyal rendelkezik.

A Thunderbird levelező programba a tanúsítvány és kulcs importálásának folyamata a következő:

1. Navigáljon el a Tanúsítványok menüpontra.
Eszközök > Beállítások > Haladó > Tanúsítványok > Tanúsítványok kezelése
(Tools > Options > Advanced > Certificates fül > View certificates gomb)
2. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön nyomja meg az „Importálás...” gombot.
3. Ezután tallózza ki a PKCS #12 fájlt, amely a tanúsítványát és a hozzá tartozó kulcsot tartalmazza.
4. Ezután adja meg a .pfx fájl jelszavát, amelyet exportálásakor kapott. (Ha adott neki ilyen jelszót.)
5. Az importálás után tájékoztatást kap arról, hogy az importálás sikeresen megtörtént, majd nyomjon Ok gombot az összes ablak bezáródásáig.
6. Ezzel a tanúsítványa és a hozzá tartozó kulcs importálásra került. Ezt természetesen javasolt a birtokában lévő tanúsítvány esetén is elvégezni.

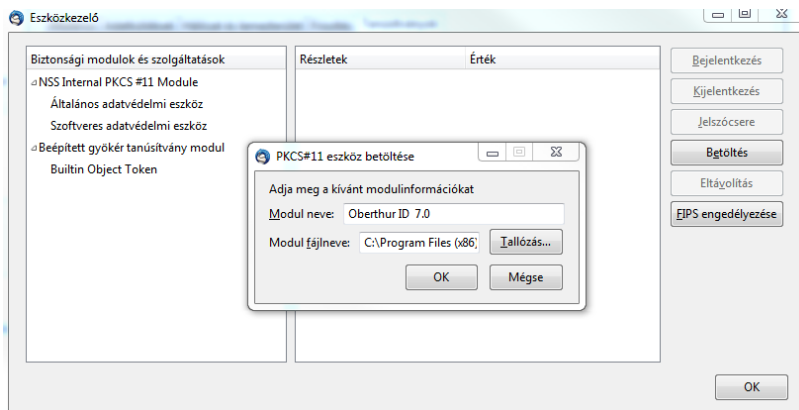
4.3. Kártya vagy token beállítása Thunderbird programba

Amennyiben tanúsítványa kriptográfiai eszközön található, akkor első lépésként el kell végeznie azokat a beállításokat, melyek az eszköz telepítéséről szólnak. Az ott található beállítások között természetesen találhatóak olyan lépések is, melyek a Thunderbird levelező programból történő használathoz nem szükségesek, de az optimális használathoz érdemes elvégezni az ott szereplő beállítások mindegyikét. [Itt töltheti le a kártyájához és tokenéhez az útmutatót a "Chipkártyán, tokenen tárolt tanúsítványok" menüpontban!](#)

A Thunderbird levelező programban a kriptográfiai eszköz használatának beállítása a következő:

1. Vizsgálja meg, hogy telepítette-e a kártyaolvasó, és a kártyakezelő szoftvereket, ezek telepítése nélkül ugyanis nem lehetséges a kártya használata.
2. Navigáljon el az Adatvédelmi eszközök kezelése menüpontra.
Eszközök > Beállítások > Speciális fül > Tanúsítványok > Adatvédelmi eszközök gomb
(Tools > Options > Advanced > Certificates fül > Security Devices gomb)
3. A megjelenő ablakban nyomja meg a Betöltés (Load) gombot.
4. Az előugró ablakban a Modul neve (Modul name) mezőben adja meg az eszköz nevét. Javasoljuk, hogy a kriptográfiai eszköz típusát adja meg névnek (pl: "Oberthur kártya").

5. A Modul fájlneve (module filename) ablakban tallózza ki a megfelelő kártyakezelő fájlt, vagy másolja be a vágólapon keresztül a következő útvonalat.
Oberthur eszközöknél (AWP Manager 4.5. verzió esetén):



32 bites operációs rendszer esetében a betöltendő fájl elérési útvonala:

C:\Program Files\ Oberthur Technologies\AWP\DLLs\OCSCryptolib_P11.dll

64 bites operációs rendszer esetében:

C:\Program Files (x86)\Oberthur Technologies\AWP\DLLs\OCSCryptolib_P11.dll

Vagy

C:\Program Files (x86)\Oberthur Technologies\ Authentic IC Webpack
\DLLs\OCSCryptolib_P11.dll

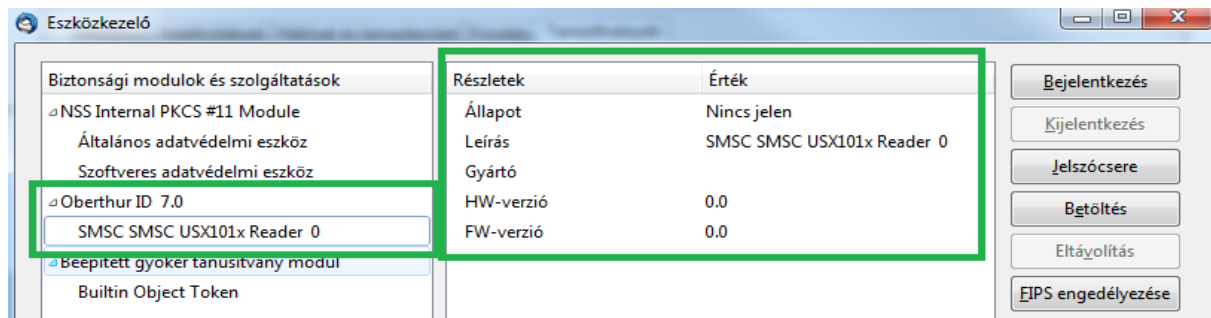
Gemalto Classic esetén:

C:\Program Files (x86)\Gemalto\Classic Client\BIN

A művelet végrehajtásához rendszergazdai jogosultsággal kell rendelkeznie.

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

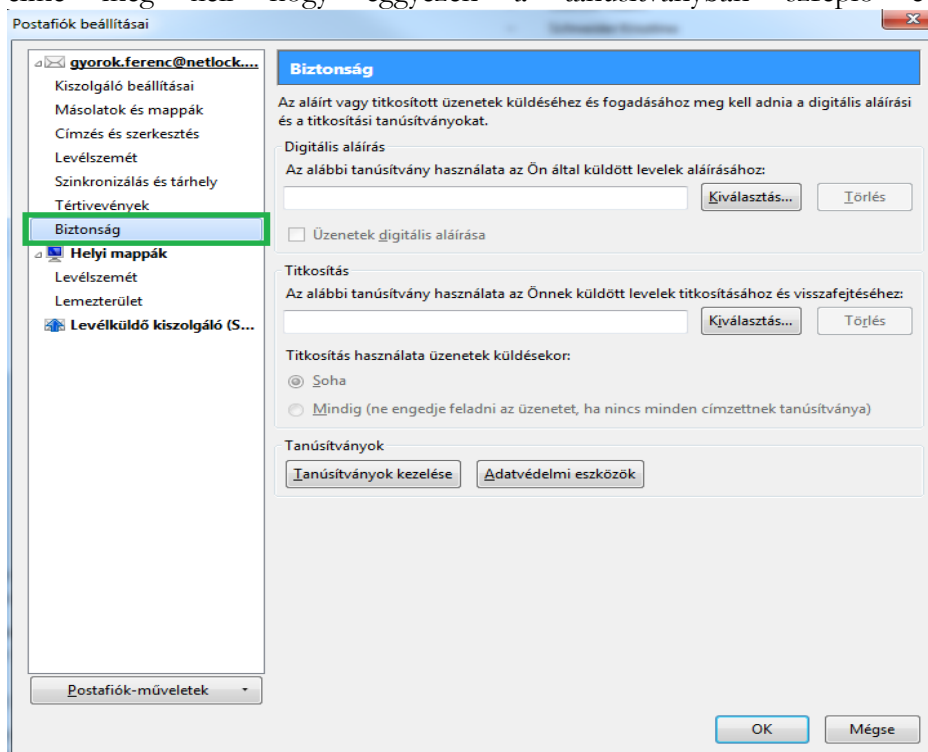
Ezzel a kriptográfiai eszköz használata a Thunderbird levelező programból beállításra került.



5. Tanúsítványok és kulcsok beállítása levelezéshez és titkosításhoz

Ahhoz, hogy a Thunderbird levelező programban tanúsítványával aláírva és titkosítva is küldhessen levelet, a következő lépéseket kell végrehajtania.

1. Navigáljon el a Fiók beállítások (Account settings) menüpontba.
(Eszközök > Postafiókok beállításai)/Tools > Account Settings/
2. Kattintson az e-mail cím előtt lévő nyílra, és válassza ki az ez alatt található Biztonság (Security) menüpontot. **Figyelem! Csak arra az e-mail címre tudja beállítani a tanúsítványát, amely e-mail cím a tanúsítványban is szerepel.** Tehát az e-mail fiók címe meg kell hogy egyezzen a tanúsítványban szereplő e-mail címmel.



3. Tanúsítványok beállítása

Digitális aláírás beállítása:

A jobb oldalon a Digitális aláírás (Digital signing) szekcióban nyomja meg „Kiválasztás...” (Select) gombot, és válassza ki az aláíró tanúsítványát.

Az alatta lévő jelölő négyzettel bekapcsolhatja, hogy alapértelmezetten minden kimenő levél legyen digitálisan aláírva.

Titkosító tanúsítvány beállítása:

Digitális aláírás alatt található szekcióban nyomja meg „Kiválasztás...” (Select) gombot, és válassza ki a titkosító tanúsítványát.

Az alatta lévő rádió gombbal bekapcsolhatja, hogy alapértelmezetten minden kimenő levél legyen titkosítva.

(Általában a program automatikusan eldönti, hogy adott tanúsítvány aláírásra vagy titkosításra jó.)

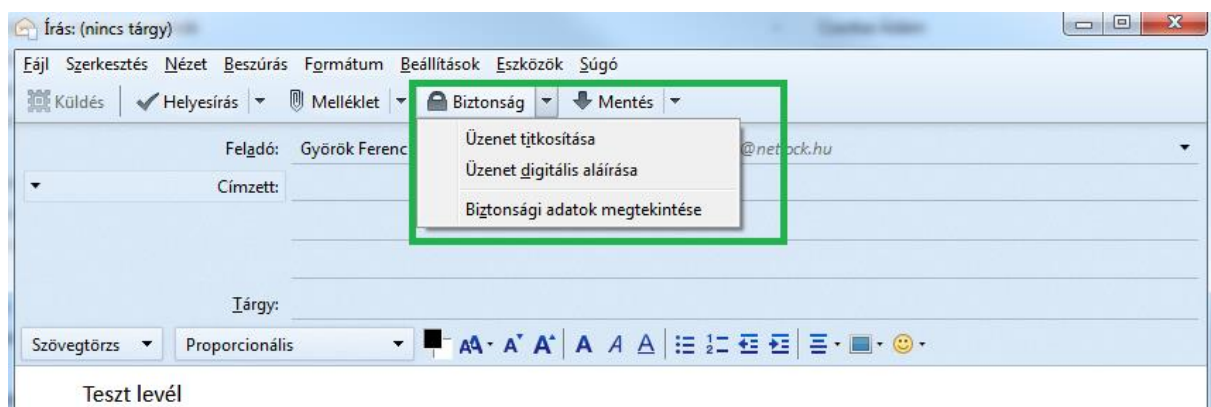
4. Miután ezeket beállította, nyomjon Ok gombot, amíg vissza nem jut a főképernyőig.

Ezzel a tanúsítványok beállítása megtörtént.

6. Levelek küldése Aláírva és/vagy Titkosítva

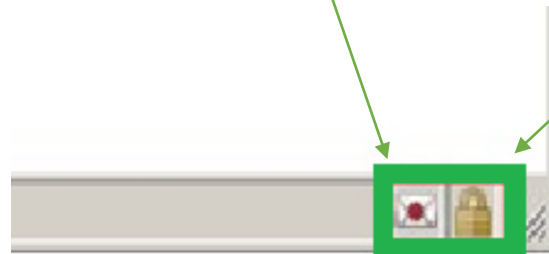
Ha levelét aláírva és/vagy titkosítva szeretné elküldeni, a teendői a következők:

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



Ha a Fiók beállításakor bejelölte az Üzenetek digitális aláírása és/vagy Titkosítás használata opciókat, akkor automatikusan be van pipálva az aláírás és/vagy titkosítás.

Az aláírás és/vagy titkosítás kiválasztásának megtörténtéről az ablak jobb alsó sarkában lévő piktogramokról is meggyőződhet (bal oldalon az aláírást jelző, jobb oldalon a titkosítást):



Fontos, hogy tudja: 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. A kapott levélből mentse el a feladó címét a saját névjegyzékébe és akkor a titkosításhoz szükséges nyilvános kulcs is tárolásra kerül, a bejegyzéssel együtt.

Függelék -

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