Thunderbird levelező program beállítása tanúsítványok használatához

Windows tanúsítványtárban, PFX fájlban, vagy kriptográfia eszközökön található tanúsítványok esetén

(Windows és Linux operációs rendszereken)

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

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, 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.hu e-mail címen vagy személyesen a 1101 Budapest, Expo tér 5-7. szám alatt, munkanapokon 9 és 17 óra között készséggel áll rendelkezésére.

3. 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 16.0.1. 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.

4. A Thunderbird szoftver tanúsítványkezelésnek hibái

Az elvégzett működési tesztek alapján a következő hibák kerültek feltárásra.

(A problémák a fejlesztő felé bejelentésre kerültek.)

1. A szoftverbe más személy tanúsítványát importálni nem lehetséges, ezért nehézkessé válhat a tikosított levelek küldése, fogadása.
2. A kriptográfiai eszközön tárolt tanúsítványok közül csak az első aláíró és titkosító tanúsítvány használható, a szoftver nem kezeli megfelelően az ilyen tanúsítványokat.
3. A beimportált szoftveres tanúsítványok közül csak az első aláíró és titkosító tanúsítvány használható, a szoftver nem kezeli megfelelően az ilyen tanúsítványokat.
4. A kriptográfiai eszközön tárolt tanúsítványok esetén a szoftverből ne töröljük a tanúsítványt, mert a program a kártyáról is törli azt!

5. 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.

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. A 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:

SHA1 algoritmusú kiadók:

http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.cer
http://www.netlock.hu/index.cgi?ca=mkozig
http://www.netlock.hu/index.cgi?ca=bkozig

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 lépései a következők:

1. Indítsa el böngészőjét.
2. Nyissa meg a böngészővel a fent látható linkek egyikét.
3. A fájt mentse le a gépére.
4. Indítsa el a Thunderbird programot, majd navigáljon el a gyökértanúsítványokig. Eszközök > Beállítások > Speciális (vagy Haladó) > Tanúsítványok fül > Tanúsítványok megjelenítése > Hitelesítésszolgáltatók fül (Tools > Options > Advanced > Certificates fül > View certificates gomb > Authorities fül)
5. Kattintson az Import 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.

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. Rövid áttekintés a tanúsítványigénylési - és tárolási megoldásokról

A tanúsítványok létrehozása és tárolása többféleképpen történhet. Ezek különségeiről 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.

7.1. Tanúsítvány igénylése Mozilla böngészőn keresztül

A Mozilla böngészők, levelezők a több operációs rendszeren használhatóság érdekében a tanúsítványokat alkalmazásonként 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 P12) fájlformátumban jön létre. A mentés készítéséhez vegye igénybe az adott szoftver beállítási útmutatóját.

Fontos megjegyezni, hogy a levelező 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.

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.

Mivel minden egyes Mozilla termék külön tanúsítványtárral rendelkezik, ha másik Mozilla termékből kívánja használni szoftveresen tárolt tanúsítványát, arról itt mentést kell készítenie, és oda is telepítenie kell azt.

7.2. Tanúsítvány igénylése Internet Exploreren keresztül

A Windows operációs rendszer biztosít egy központi tanúsítvány tárat, amelyet az alkalmazások – amelyeket erre megprogramoztak – 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. A később kiadott tanúsítványt az Internet Explorer böngészővel, az ügyfélmenü importálás pontját választva helyezheti 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.

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

Fontos! A tanúsítványkérelem beadása (kulcsgenerálás) és az elkészült tanúsítvány importálása közötti időszakban, ne telepítse újra operációs rendszerét, böngészőjét, mivel ezzel helyreállíthatatlanul törli a tanúsítványához tartozó privát kulcsot is, e nélkül pedig az használhatatlan lesz.

Mivel a Mozilla termékek nem férnek hozzá ehhez a közös tanúsítványtárolóhoz ezért mindenféleképp exportálni kell a Windows tanúsítvány tárból az ilyen tanúsítványát.

7.2.1. Tanúsítvány és kulcsok PKCS#12 (PFX) állományban

Mint az előbbiekben olvashatta (lásd Tanúsítvány igénylése Mozilla böngészőn keresztül és Tanúsítvány igénylése Internet Exploreren keresztül fejezetek), a PKCS#12 (vagy másik nevén PFX) fájlformátum alapvetően biztonsági mentés, illetve kulcsok és tanúsítványok együttes mozgatása gépek között céjára szolgálhat. Ilyen formában tanúsítványt nem tud igényelni, hanem csak létrehozni tudja azokat, melyeket helyreállítási céllal egyébként is lényeges megtennie.

A Thunderbird esetében, ha NEM kriptográfiai eszközön kapta, ez a mentés feltétlenül szükséges.

7.2.2. Tanúsítvány és kulcsok kriptográfiai eszközön (kártyán, tokenen)

Igen népszerű igénylési mód a tanúsítványok kártyán vagy tokenen való igénylése, melyek az eszközök és a hozzá tartozó PIN kód miatt egy fokkal magasabb biztonságot is nyújtanak.

Az ilyen eszközön a privát kulcs biztonságosan tárolódik, az egyes aláírási műveletek közben sem kerül ki az eszközből, hanem az kapja meg a feladatot, és a PIN kód megadása 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.

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. A tanúsítványok beállítása

Az előző fejezetekben áttekinteteknek megfelelően a következők leírják, hogyan tudja a tanúsítványát beállítani a használathoz.

8.1. 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. Ezt egy későbbi fejezet ismerteti.

8.2. PKCS12 (PFX) 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 Thunderbird 2.0 levelező programban beállítani.

Ha nincs ilyen PKCS#12 (.PFX) állományba készült mentése, akkor az elkészült tanúsítványt vagy a Mozilla böngészőjéből, vagy a Windows tanúsítvány tárából exportálnia kell. (Lásd Tanúsítvány exportálása

Amennyiben nem rendelkezik a szükséges PKCS#12 mentéssel, azt létre kell hoznia.

A következőkben a két legelterjedtebb böngésző ilyen lépéseit olvashatja, más böngészők esetén tekintse meg a vonatkozó útmutatókat.

Tanúsítvány exportálása Internet Explorerből és Firefoxból fejezeteket.)

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

1. Navigáljon el a Tanúsítványok menüpontig.
   Eszközök > Beállítások > Haladó > Tanúsítványok > Tanúsítványok megjelenítése
   (Tools > Options > Advanced > Certificates fül > View certificates gomb)
2. A megjelenő ablakban a Saját tanúsítványok (Your certificates) fülön nyomja meg az Import gombot.
3. Ezután tallózza ki a PKCS #12 fájlt, amely a tanúsítványát és a hozzá tartozó kulcsot tartalmazza.
4. Adja meg Thunderbird-en belüli tanúsítványvédelmi jelszót. (mester jelszó / master password) (Ez az első tanúsítványimportálás előtt még nincs beállítva (ekkor kétszer kell begépelnie) és a későbbiek során ez után fog rendszeresen érdeklődni a Thunderbird levelező program.)
5. Ezután adja meg a .pfx fájl jelszavát, amelyet exportálásakor kapott. (Ha adott neki ilyen jelszót.)
6. Az importálás után tájékoztatást kap arról, hogy az importálás sikeresen megtörtént, majd nyomjon Ok gombot az összes ablak bezáródásáig.
7. Ezzel a tanúsítványa és a hozzá tartozó kulcs importálásra került. Ezt természetesen javasolt a birtokában lévő többi kulcs esetén is elvégezni.

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

8.2.1. Tanúsítvány exportálása

Amennyiben nem rendelkezik a szükséges PKCS#12 mentéssel, azt létre kell hoznia.

A következőkben a két legelterjedtebb böngésző ilyen lépéseit olvashatja, más böngészők esetén tekintse meg a vonatkozó útmutatókat.

8.2.1.1. Tanúsítvány exportálása Internet Explorerből

Az exportálás lépései a következők:

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 Exportálás gombra.
4. A megjelenő tanúsítványexportáló 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 bezárnunk.

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

8.2.1.2. Tanúsítvány exportálása Firefox 3+ 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. Hardvereszközön található tanúsítvány használatának beállítása

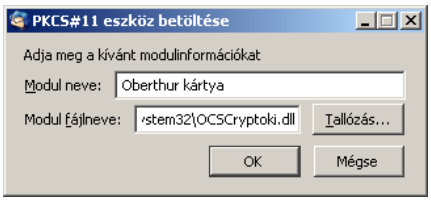
Amennyiben tanúsítványa kriptográfiai eszközön található, akkor első lépésként el kell végeznie azokat a beállításokat, melyek az eszköz telepítéséről szóltak. Az ott található beállítások között természetesen találhatóak olyan lépések is, melyek a Thunderbird levelező programból történő használathoz nem szükségesek, de az optimális használathoz érdemes elvégezni az ott szereplő beállítások mindegyikét.

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 menüpontig. Eszközök > Beállítások > Haladó (vagy Speciális) > 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 név (Modul name) mezőben adja meg az eszköz nevét. Javasoljuk, hogy a kriptográfiai eszköz típusát adja meg névnek (vagyis "Oberthur kártya").

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. A Modul fájlnév (module filename) ablakban tallózza ki a megfelelő kártyakezelő fájtl, vagy másolja be a vágólapon keresztül a következő útvonalat pontosan.



   Oberthur eszközöknél (AuthentIC Manager 4.4.4. és 4.4.5. verziók esetén):

   32 bites operációs rendszer esetében a betöltendő fájl elérési útvonala:
   C:\Program Files\Oberthur Technologies\AuthentIC Webpack\DLLs\OCSCryptoki.dll
   64 bites operációs rendszer esetében:
   C:\Program Files\Oberthur Technologies\AuthentIC Webpack\DLLs\OCSCryptoki_P11.dll

   Ha 64 bites az operációs rendszer, és létrejött a Program Files(x86) mappában a NetLock Eszközszolgáltatás program telepítésével egy Oberthur Technologies mappa, akkor azon belül az AuthentIC Webpack -> DLLs mappában is célszerű keresni az OCSCryptoki.dll vagy az OCSCryptoki_P11.dll fájlokat.
   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.

9.1. PIN kód megadása az alkalmazásban, ha kriptográfiai eszközt (Smart kártya, USB token) használ.

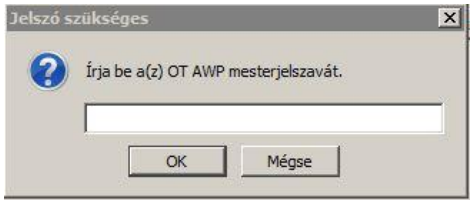
Kriptográfiai eszközön tárolt tanúsítványok esetében a rendszer megtévesztő módon „mesterjelszót" kér be, azonban ebben az esetben mindig az eszköz PIN kódja kell hogy megadásra kerüljön.

9.1.1. Oberthur eszközök esetén

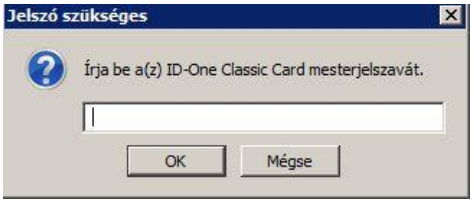
A megnevezés eszközönként eltérő lehet, de minden esetben az eszköz PIN kódját kell megadni.

Néhány példa:

Oberthur Token esetében:



Oberthur Chipkártya esetében:



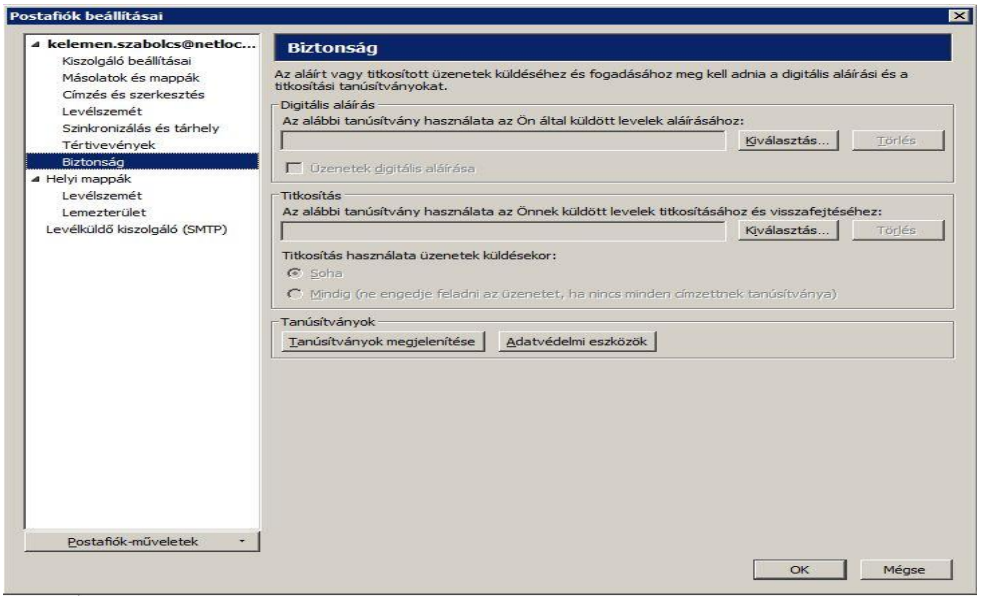
Egyes esetekben előfordulhat, hogy az eszköz sorszámának (pl. kártyaszám) utolsó 8 számjegye jelenik meg megnevezésként.

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. Tanúsítványok és kulcsok beállítása levelezéshez és titkosításhoz

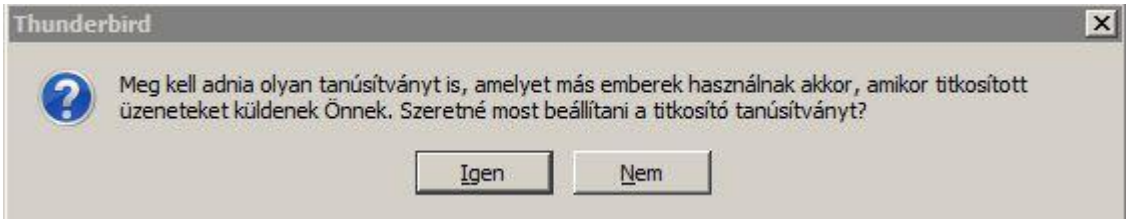
Ahhoz, hogy a Thunderbird levelező programban tanúsítvánnyal aláírva és titkosítva is küldhessen levelet a következő lépéseket kell végrehajtania.

1. Navigáljon el a Fiók beállítások (Account settings) menüpontba.
   (Eszközök> Postafiókok beállításai)/Tools > Account Settings/
2. Válassza ki az e-mail címét, majd nyissa le a hozzá tartozó fastruktúrát, és válassza ki az ez alatt található Biztonság (Security) menüpontot.



3. A jobb oldalon a Digitális aláírás (Digital singing) szekcióban nyomja meg Kiválasztás (Select) gombot, és válassza ki az aláíró tanúsítványát. Az ez alatt található opcióval bekapcsolhatja, hogy alapértelmezetten minden kimenő levél alá legyen írva digitálisan. (Általában a program automatikusan eldönti, hogy adott tanúsítvány aláírásra vagy titkosításra jó.)

   Esetenként előfordulhat, hogy a program automatikusan kezdeményezi, hogy az aláíró tanúsítvány kiválasztását követően egy titkosító tanúsítvány is beállításra kerüljön:



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. A Titkosítás (Encryption) szekcióban nyomja meg Kiválasztás (Select) gombot, és válassza ki a titkosító tanúsítványát. Csak titkosító tanúsítványokat fog megjeleníteni a program kiválasztható tanúsítványként.

   Az alatta lévő opciók a titkosítás alapértelmezett viselkedését adják meg; a Soha (Never) opció alapértelmezetten soha nem titkosít, a Mindig opció esetében addig nem megy el a levél, amíg nincs minden címzettnek tanúsítványa.
5. Miután ezeket beállította, nyomjon Ok gombot, amíg vissza nem jut a főképernyőig.

Ezzel a tanúsítványok beállítása megtörtént.

11. 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) gomb melletti háromszöget.
2. A lenyíló menüben kiválaszthatja, hogy digitálisan aláírja (Digitaly sign) és/vagy titkosítja (Encrypt this message) a levelet.

Ha a Fiók beállításkor 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, 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

12. Függelék A - 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

13. Függelék B - Hibaelhárítás

Tanúsítványomat nem látom a programból…

Ellenőrizze, hogy a fiókhoz beállított e-mail cím egyezik-e a tanúsítványban találhatóval.
A kettőnek egyeznie kell.

Kártyán, tokenen található tanúsítványomat nem tudom beállítani…

Előfordulhat, hogy a beállítás nehézségbe ütközik, mert a Thunderbird levelező nem találja a tanúsítványt.
Ez esetben a következő javasolt:

1. Indítsa újra gépét, szükség esetén jelentkezzen be.
2. Helyezze be kártyáját az olvasóba.
3. Indítsa el a Thunderbird programot. (Ez legyen az első program, amit a gépen indít.)
4. Próbálkozzon a beállítással.

Ez a lépéssorozat azért szükséges, mert ha nem sikerül beállítani a tanúsítványt, az többnyire arra vezethető vissza, hogy valamilyen másik alkalmazás már zárolja saját részére a kártyát, és az első beállítás során a Thunderbird szoftver nem fér hozzá a kártyához.

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

14. Függelék C - A visszavonási listák beállítása

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

A Thunderbird 1.5 verziójától van lehetőség erre, a következő módon:

1. Indítsa el a Thunderbird programot és navigáljon el a Visszavonási listák menüpontig. Eszközök > Beállítások > Haladó > Tanúsítványok > Visszavonási listák gomb (Tools > Options > Advanced > Certificates > Revocation lists gomb)
2. A megjelenő ablakban nyomja meg az Import gombot, majd az előugró ablakba illessze be a visszavonási listák linkjét (javasolt az összest hozzáadni):

SHA-1 kiadók visszavonási listái:

https://www.netlock.hu/index.cgi?minositett&crl=mshea	(Class QA)
https://www.netlock.hu/index.cgi?crl=kozjegyzoi	(Class A)
https://www.netlock.hu/index.cgi?crl=uzleti	(Class B)
https://www.netlock.hu/index.cgi?crl=expressz	(Class C)
https://www.netlock.hu/index.cgi?minositett&crl=mkozig	(Class QA)
https://www.netlock.hu/index.cgi?crl=bkozig	(B közig.)
https://www.netlock.hu/index.cgi?crl=olsslca1	(OnlineSSL)

SHA-256 kiadók visszavonási listái:

https://www.netlock.hu/index.cgi?crl=gold	(Class Gold)
https://www.netlock.hu/index.cgi?crl=cqlca	(Class Q Legal)
https://www.netlock.hu/index.cgi?crl=cqlsca	(Class Q Legal S)
https://www.netlock.hu/index.cgi?crl=caca	(Class A)
https://www.netlock.hu/index.cgi?crl=calca	(Class A Legal)
https://www.netlock.hu/index.cgi?crl=cblca	(Class B Legal)
https://www.netlock.hu/index.cgi?crl=cbca	(Class B)
https://www.netlock.hu/index.cgi?crl=cclca	(Class C Legal)
https://www.netlock.hu/index.cgi?crl=ccca	(Class C)
https://www.netlock.hu/index.cgi?crl=mkozig256	(Class QA)
https://www.netlock.hu/index.cgi?crl=bkozig256	(Class B közig.)
https://www.netlock.hu/index.cgi?crl=teszt3	(Teszt tan.)

3. Ezt követően megjelenő ablak érdeklődik arról, hogy kívánjuk-e a visszavonási listákat automatikusan frissíteni. Erre válaszoljunk Igen (Yes) gombbal.

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. A megjelenő ablakban az automatikus frissítést kapcsolhatjuk be a "A CRL automatikus frissítésének engedélyezése" opció kipipálásával. (Automatic update for this CRL)
5. A többi opcióval a frissítés gyakoriságát állíthatjuk be, ami lehet x nappal a következő frissítés dátuma előtt (első opció), vagy x naponként (második opció). Ezt javasolt alapértelmezetten hagyni (vagyis 1 nappal a következő frissítés dátuma előtt)
6. A fenti folyamatot érdemes a többi visszavonási listára is elvégeznie.

Amennyiben a visszavonási listák automatikus letöltését beállította, a továbbiakban ez a levelező program indulásakor automatikusan megtörténik, a szokásos, visszavonási listákban megadott időközönként.

Ha sürgősen a legfrissebb listára van szüksége, akkor az itt leírtak alapján azt bármikor megismételheti.

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