

Eudora levelező program beállítása tanúsítványok használatához

Windows tanúsítványtárban és kriptográfia eszközökön található
tanúsítványok esetén

1. Tartalomjegyzék

1.	Tartalomjegyzék	2
2.	Bevezető	3
3.	Az Eudora levelező program beállítása tanúsítványok használatához	3
4.	Operációs rendszer követelmények.....	3
5.	Korlátozások.....	3
6.	Az Eudora tanúsítványt kezelő plug-in telepítése, beállítása	4
7.	Az Eudora alkalmazás tanúsítványkezelése.....	5
7.1.	Rövid áttekintés a tanúsítvány igénylési - és tárolási megoldásokról.....	5
7.1.1.	Tanúsítvány igénylése Mozilla böngészőn keresztül.....	5
7.1.2.	Tanúsítvány igénylése Internet Exploreren keresztül.....	5
7.1.3.	Tanúsítvány és kulcsok kriptográfiai eszközön (kártyán, tokenen).....	7
7.1.4.	Tanúsítvány és kulcsok PKCS#12 (PFX) állományban.....	7
7.2.	A tanúsítványok telepítése	7
7.2.1.	Ha a tanúsítvány kártyán, tokenen található.....	7
7.2.2.	Ha a tanúsítvány már a gépen található	8
7.2.3.	Ha a tanúsítványkérelem beadása Mozilla böngészőn keresztül történt.....	8
7.2.3.1.	Tanúsítvány exportálása Firefox böngészőből Windows tanúsítványtárba telepítéshez.....	8
7.3.	PKCS12 (PFX) fájlban található tanúsítvány telepítése Windows tanúsítványtárba.....	9
8.	Aláírt és/vagy titkosított levelek küldése:.....	10
9.	Függelék A – Biztonsági másolat készítése tanúsítványairól és kulcsairól.....	11

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 vagy problémája támad, 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. Az Eudora levelező program beállítása tanúsítványok használatához

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

A telepítés lépései a Windows rendszereken történő beállításokat írják le, Eudora 7.x levelező program esetében. Korábbi verziók használatát nem javasoljuk.

4. Operációs rendszer követelmények

A tanúsítványok használatához ajánlott minimum operációs rendszer követelmény:

Windows XP SP3

Jelen útmutató az Eudora 7.1.0.9. verziója alapján készült, a különböző verzióknál eltéréseket tapasztalhat a menüpontok elnevezésében és felépítésében!

A szoftver 64 bites rendszereken (XP, Vista) nem került tesztelésre.

5. Korlátozások

A program a következő ismert problémákkal rendelkezik, melyek miatt használata nem javasolt, helyette javasolt az Outlook 2007 / Thunderbird / Seamonkey használata

- A program kezelőfelületén aláírásra használandó tanúsítvány kiválasztására külön nincs lehetőség, ezt a program automatikusan választja, ezért több tanúsítvány esetén beállítása nehézséget okozhat.
- A plug-in működése instabil, alkalmanként üzenet feldolgozása közben hibaüzenettel leáll.
- Tesztjeink során a titkosító üzenet küldése az Eudora programmal nem volt lehetséges, ezért használatát nem javasoljuk.

6. Az Eudora tanúsítványt kezelő plug-in telepítése, beállítása

Az Eudora levelező program alapértelmezésben nem támogatja az S/MIME tanúsítványok használatát, azonban a plug-in struktúrája lehetővé teszi, hogy ilyen kiegészítést telepítsünk.

1. A programhoz elérhető plug-in a következő címről tölthető le:
http://www.eudora.com/cgi-bin/export.cgi?productid=EUDORA_win_smime_70
2. A letöltött állományban található .dll-t a program telepítési könyvtárán belül található plug-in könyvtárba kell helyezni.

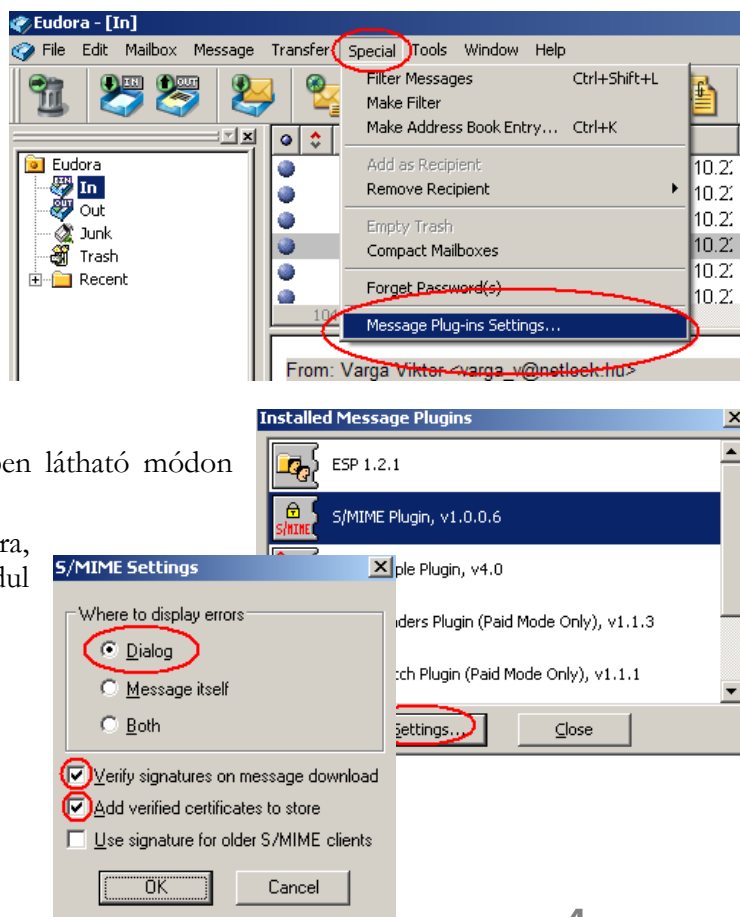
Figyelem!

A beépülő modul telepítése nélkül a szoftver nem használható tanúsítványokkal!

A plug-in beszerzése és telepítése után az Eudora levelező program képes a tanúsítványok kezelésére.

Ennek beállításai az alábbiak szerint történjenek meg:

1. A főmenüben a Special menüpontra kattintva, válasszuk a „Message Plug-ins Settings...” opciót.
2. A megjelenő „Installed Message Plugins” ablakban jelöljük ki a S/MIME Plugin kezdetű sort, majd kattintsunk a Settings gombra.
3. Az S/MIME Settings ablakban képen látható módon jelöljük be a választható opciókat.
4. Végül kattintsunk az OK gombra, ezzel beállítottuk a beépülő modul működését.



7. Az Eudora alkalmazás tanúsítványkezelése

7.1. 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.

7.1.1. 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.

7.1.2. 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.

7.1.3. 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.

7.1.4. 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.

7.2. A tanúsítványok telepítése

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

7.2.1. 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, hajtva végre az ott leírtakat.

7.2.2. 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 létrehozni.

7.2.3. 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.

7.2.3.1. 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.

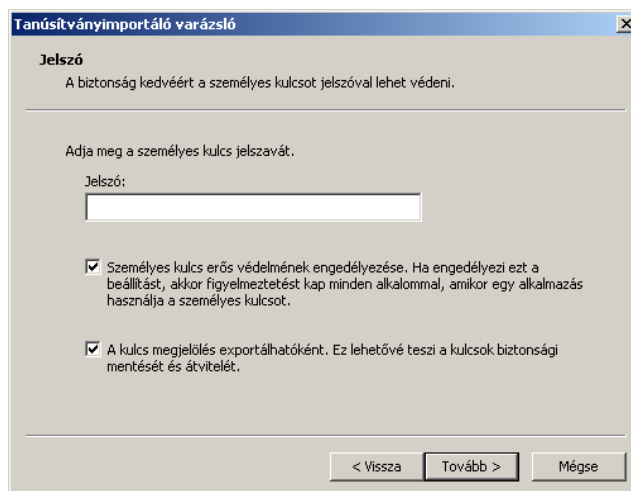
7.3. PKCS12 (PFX) fájlban található tanúsítvány telepítése Windows tanúsítványtárba

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.

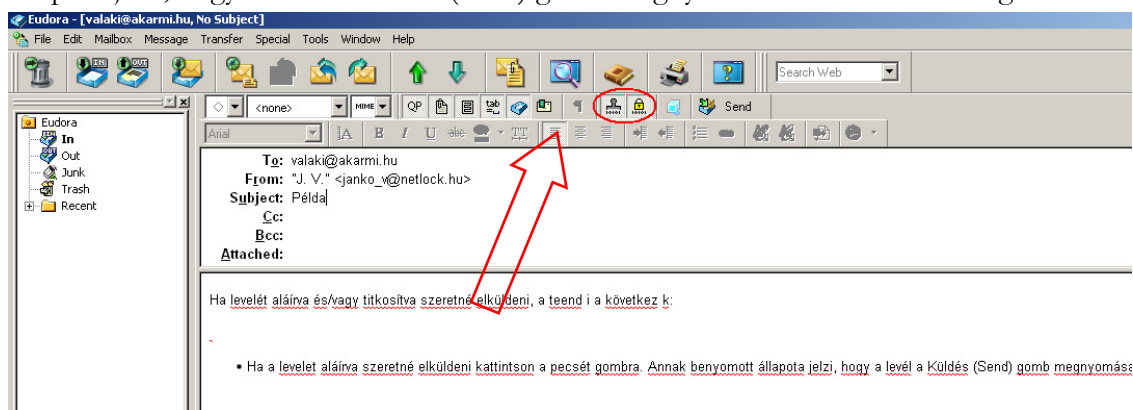
A tanúsítvány telepítése ezzel megtörtént.



8. Aláírt és/vagy titkosított levelek küldése:

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

1. Ha a levelet aláírva szeretné elküldeni kattintson a pecsét gombra. Annak benyomott állapota jelzi, hogy a levél a Küldés (Send) gomb megnyomásakor alá lesz írva digitálisan.
2. Ha a levelet titkosítva szeretné elküldeni kattintson a lakat gombra. Annak benyomott állapota jelzi, hogy a levél a Küldés (Send) gomb megnyomásakor alá lesz írva digitálisan.



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

9. 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 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 bezárni.

A tanúsítvány exportálása ezzel megtörtént.

Ezt az állományt érdemes biztonságos helyen elzárni valamilyen adathordozón.

