Tanúsítványok használata XPS fájl aláírására

Windows operációs rendszeren tanúsítványtárban, PFX fájlban, vagy kriptográfia eszközökön található 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

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/vagy titkosításhoz használható szoftverek beállítása minél zökkenő mentesebben megtörténjen, illetve hogy a használat könnyen elsajátítható legyen.

Amennyiben bármilyen kérdése van vagy problémája támad, 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.

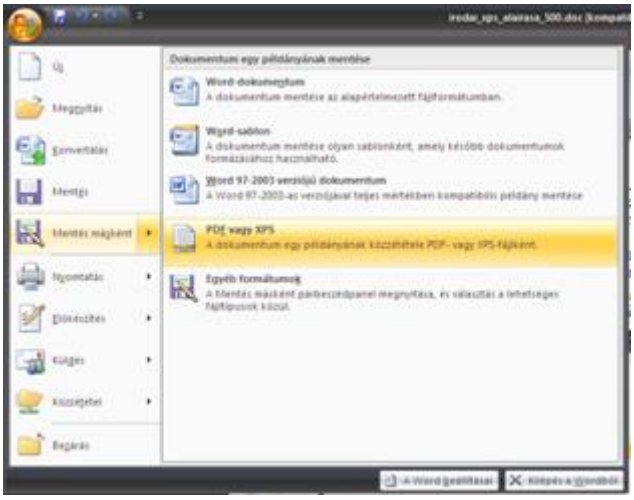
3. Az XPS fájl létrehozásról

Ahhoz, hogy XPS fájlt hozzon létre, telepítenie kell a megfelelő 2007-es Microsoft Office-bővítményt. Ez lehetővé teszi a PDF és XPS formátumban való exportálást és mentést. A bővítmény letölthető innen:

http://www.microsoft.com/downloads/details.aspx?displaylang=hu&FamilyID=4d951911-3e7e-4ae6-b059-a2e79ed87041#QuickInfoContainer

A modul telepítése után, az adott Office-dokumentumot a következőképp tudjuk XPS kiterjesztéssel elmenteni: Office gomb > Mentés másként > PDF vagy XPS opció.

(A következő ablakban a fájltípusnál válasszuk ki a *.xps opciót.)



Az XPS dokumentumok megtekintéséhez szükségünk lesz még a Microsoft XPS Viewer alkalmazás telepítésére is, ez elérhető innen:
http://www.microsoft.com/whdc/xps/viewxps.mspx

Ezek után az Internet Explorer alkalmas lesz ezeknek a dokumentumoknak a megjelenítésére, ill. kezelésére.

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. 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.

4.1. 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.

4.2. 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

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

helyreállíthatatlanul törli a tanúsítványához tartozó privát kulcsot is, e nélkül pedig az használhatatlan lesz.

4.3. 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.

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

Mint az előbbiekben 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.

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 tanúsítványok telepítése

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

5.1. 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, hajtsa végre az ott leírtakat.

5.2. 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 létrehoznia.

5.3. 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.

5.3.1. 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 menüpontig. 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.

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. 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.

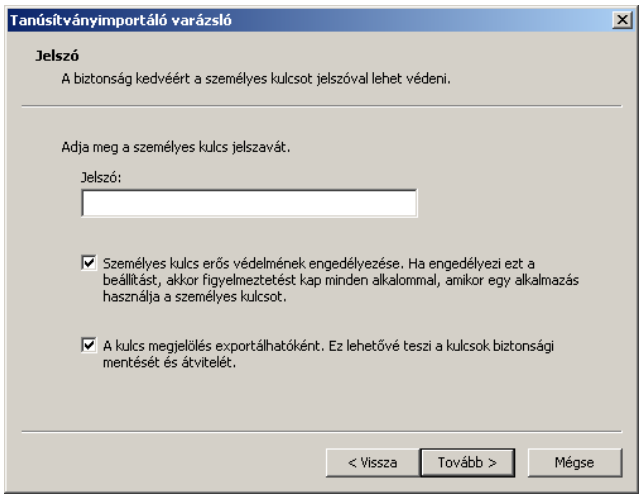
A következő fejezet ismerteti a PKCS#12 állományok telepítését.

5.4. 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 tanúsítványtárban 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 tartózó jelszót. Itt állíthatja be a tanúsítvány erős védelmét és későbbi exportálhatóságát. Javasoljuk mindkét opciót kipipálni és ezután a Tovább (Next) gombot megnyomni.



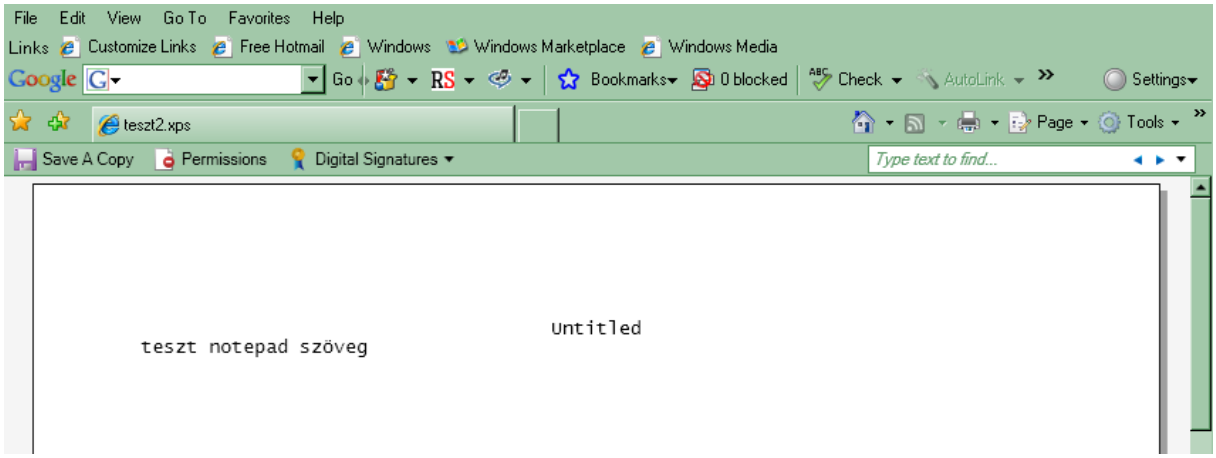
5. A következő képernyő megkérdezi, hogy automatikus vagy kézzel történő elhelyezést kíván a megfelelő tanúsítványtárolóban. Itt válassza az Automatikus kiválasztást (Automatically...), majd kattintson a Tovább (Next) gombra.
6. Az utolsó képernyőn kattintson a Befejezés (Finish) gombra.

A tanúsítvány telepítése ezzel megtörtént.

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. Dokumentumok aláírása

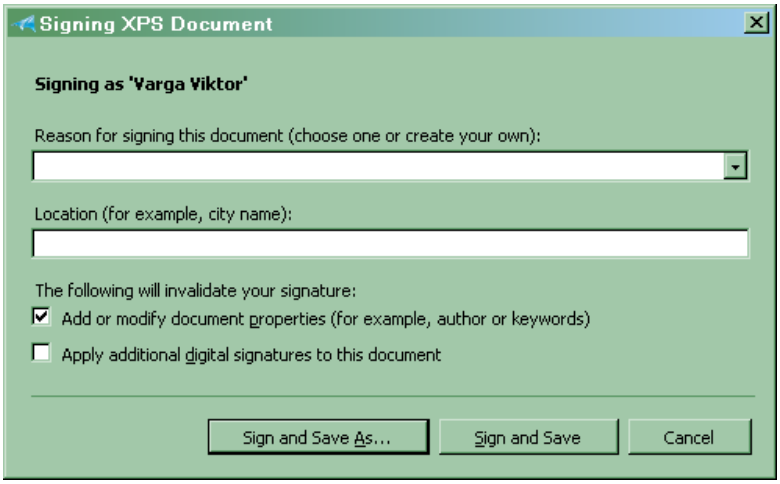
1. Nyissa meg az XPS dokumentumot az Internet Explorer böngészőben (verzió: 6.0 vagy magasabb). Legegyszerűbb megoldás, ha egyszerűen rádobja a dokumentumot a böngészőre.
2. A következő ablak jelenik meg:



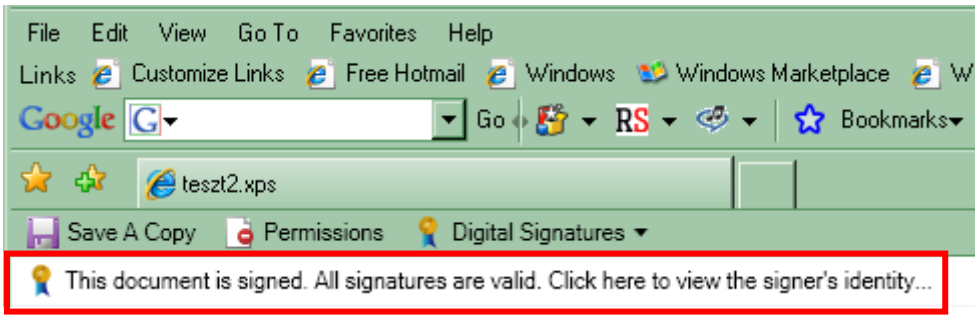
3. Itt a Digitális aláírások > Dokumentum aláírása (Digital signatures > Sign this document) opciót kiválasztva tudja azt aláírni.
4. Először egy figyelmeztető ablakot kapunk, hogy a dokumentum még nem volt aláírva, illetve, hogy további aláírás mezők hozzáadása lehetséges. (Erről részletesen később olvashat az Aláírás kérelmezése, Aláírás kérelmezett aláírás esetén c. fejezetekben olvashat.)
5. A következő megjelenő ablakban ki kell választania a tanúsítványát, majd az ezt követő ablakban megadandó az aláírás oka (reason) (Például, „Egyetértek a tartalommal”), illetve az aláírás helye is (location).

   Ezek az aláírás után tk. nyilatkozatoknak tekintendők.

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. Nyomjuk meg az „Aláírás és mentés” (Sign adn Save) vagy ha más néven kívánjuk menteni „Aláírás és mentés másként” (Sign and Save as...) gombot.
7. Amennyiben a számítógépünkre kriptográfiai eszközön tárolt (smart kártya, USB token) tanúsítvány már korábban telepítésre került, az operációs rendszer kéri az eszköz behelyezést, csatlakoztatását, majd a PIN kód megadását. Ezután az aláírt fájl lementésre kerül a megfelelő módon.
8. Az aláírás és érvényessége mindig a felső sorban látszik.

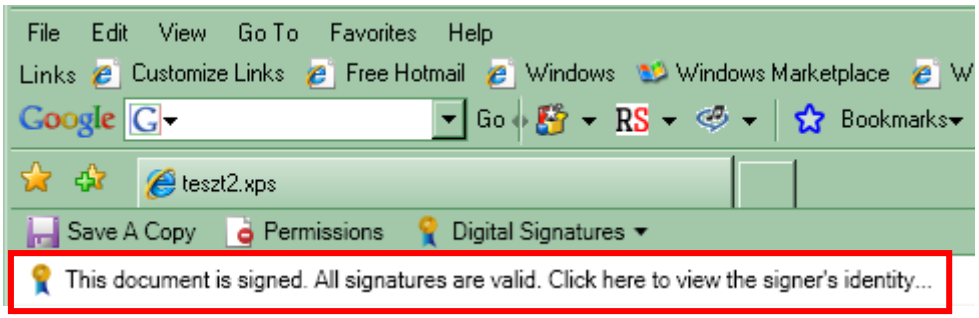


9. Természetesen a dokumentumra több aláírás is elhelyezhető, a „Digitális aláírások” (Digital signatures) menüt lenyitva és az „Aláírások részletei” (View signature details) menüpontot választva megtekinthetjük az összeset.

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. Dokumentumok aláírásának megtekintése, ellenőrzése

Az aláírt XPS dokumentum ellenőrzése böngészőben megnyitva automatikus, a felső sorban láhatjuk az aláírás ellenőrzésének eredményet.



Természetesen a dokumentumra több aláírás is elhelyezhető, a „Digitális aláírások” (Digital signatures) menüt lenyitva és az „Aláírások részletei” (View signature details) menüpontot választva megtekinthetjük az összest.

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

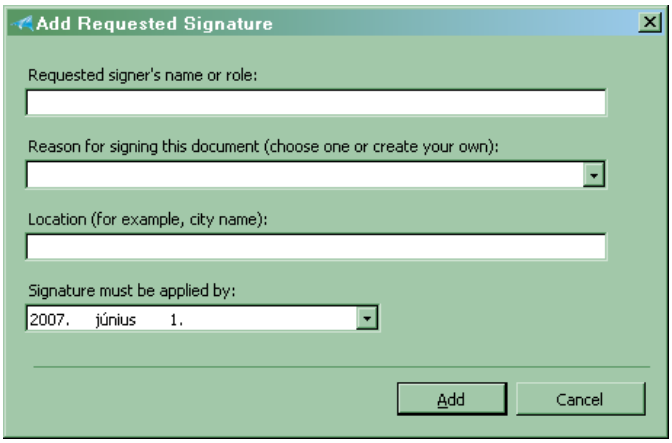
8. Aláírás kérelmezése

Az XPS dokumentumok rendelkeznek egy hasznos új funkcióval, amelyet aláírások kérelmezésének neveznek.

Ez esetben, mielőtt aláírnánk a dokumentumunkat, elhelyezhetünk rajta aláírás mezőket, melyen mások elhelyezhetik az aláírásokat.

Ilyen mező elhelyezésének lépései a következők:

1. Nyissuk meg az XPS állományt.
2. Válaszuk a Digitális aláírások > Aláírás kérelmezés (Digital Signatures > Request signature) menüpontot.
3. A megjelenő ablakban nyomjuk meg a Hozzáadás (Add) gombot.

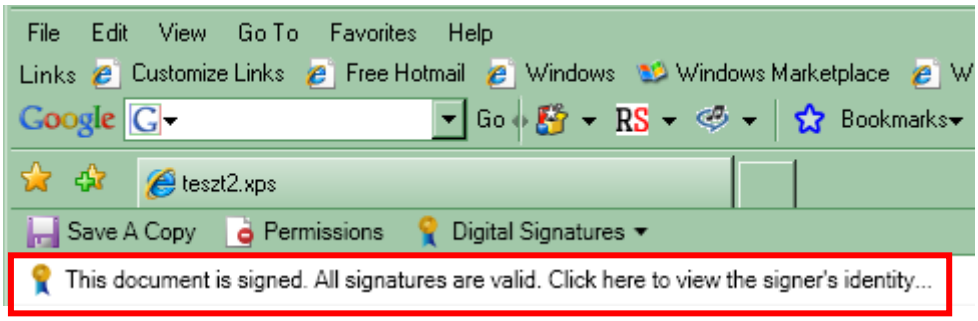


4. Töltsük ki értelemszerűen a megjelenő ablak mezőit.
5. Ha végeztünk a mezők hozzáadásával nyomjuk meg a Kész (Done) gombot.
6. Ezután a korábban már látottak alapján írjuk alá a dokumentumot. (lásd Dokumentumok aláírása)

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

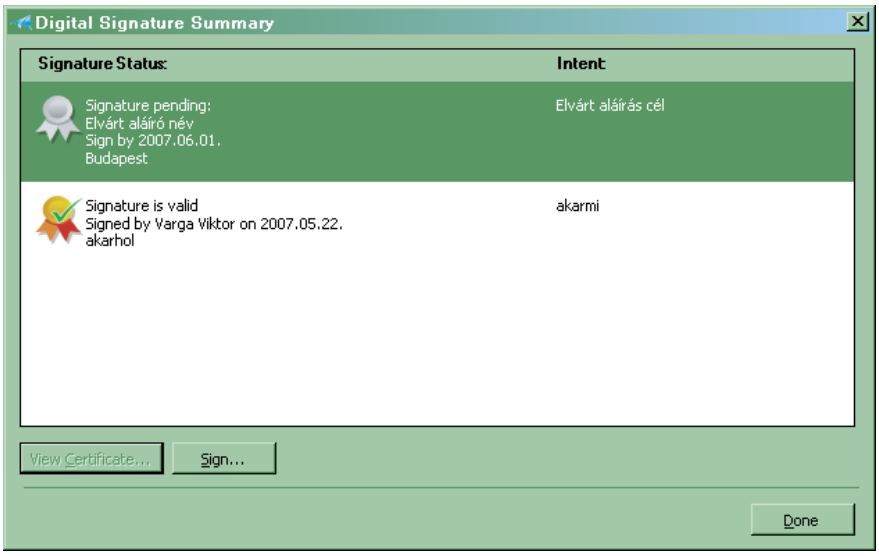
9. Aláírás kérelmezett aláírás esetén

Ha kérelmezett aláírás mező tartozik egy aláírt dokumentumhoz, azt az aláírás ellenőrző mezőre kattintva írhatjuk alá.



Lépései a következők:

1. Kattintsunk az jelzett területre.
2. A megjelenő ablakban látható, hogy a szürke jelzésű hely egy elvárt aláírás, ehol a megadott elvárt aláíró személy és az elvárt aláírási cél (ok) is látható.



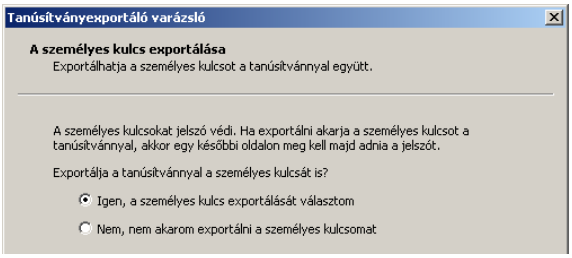
3. Ezt kijelölve kattintsunk az Aláírás (Sign) gombra. Innentől az aláírás lépései a korábban látottakkal megegyeznek. (Lásd Dokumentumok aláírása)

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

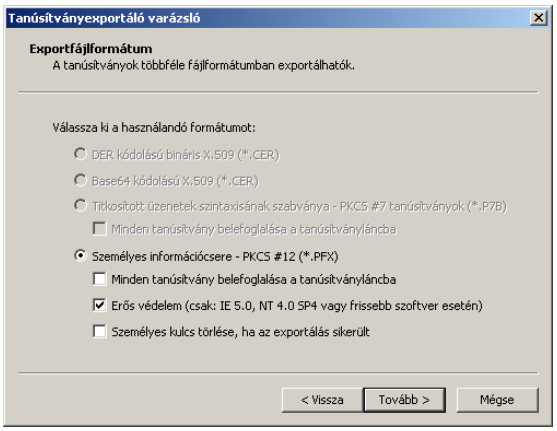
10. Függelék A – Biztonsági másolat készítése tanúsítványairól és kulcsairól

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 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