

EXE, OCX, DLL és CAB fájlok aláírása SingCode alkalmazással

Windows tanúsítványtárban és kriptográfia eszközökön található
tanúsítványok esetén

1. Tartalomjegyzék

1.	Tartalomjegyzék	2
2.	Bevezető	3
3.	A dokumentációról	3
4.	A korlátozások.....	3
5.	Döntés a kód időbélyegzéséről	4
6.	Példák biztonsági figyelmeztetésekre	4
6.1.	A kódot aláíró tanúsítvány még érvényes, időbélyegzés nem volt.....	4
6.2.	A kódot aláíró tanúsítvány már nem érvényes (pl. lejárt) és időbélyegzés nem volt.....	5
6.3.	A kódot aláíró tanúsítvány már nem érvényes, de volt időbélyegzés	5
7.	Az EXE, OCX és DLL fájlok aláírása	6
8.	Minősített tanúsítvány használata céges kód aláírásra.....	8
9.	Függelék A – Programvédelmek együttműködése az kódaláírással.....	9

2. Bevezető

Ennek a tájékoztatónak az a célja, hogy az OCX, DLL, EXE kódot a biztonság érdekében minél zökkenő mentesebben láthassa el elektronikus aláírással és szükség esetén időbélyeggel.

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. A dokumentációról

A dokumentáció Windows XP rendszeren készült, nem érinti a Vista esetleg megváltozott tanúsítvány kezelését.

A Vista tesztelése jelenleg folyamatban van.

4. A korlátozások

Jelenleg Code Signing tanúsítvány csak minősített osztályban adható ki, ennek megfelelően az aláíró tanúsítvány elsősorban személyhez köthető.

Figyelem!

Code Signing tanúsítványok jelenleg nem elérhetők Java kódok aláírásához.

5. Döntés a kód időbélyegzéséről

Egy kód aláírásakor javasolt eldöntenünk, hogy kívánjuk-e időbélyegezni azt vagy sem.

Amennyiben időbélyegezzük, úgy a kódon lévő aláírás a tanúsítvány lejáta után is érvényes lesz, míg időbélyeg nélkül csak a tanúsítvány időtartamán belül.

Az időbélyegzett kód hasznos lehet „magára hagyott” kód esetében, mely az „örökkévalóságig” érvényben lesz, míg időbélyeg nélkül a fájl a tanúsítvány lejáta után „lejár”.

A következőkben biztonsági figyelmeztetéseken keresztül ezt is megvizsgáljuk.

6. Példák biztonsági figyelmeztetésekre

A következőkben az látható, hogy miképp jelenik meg a biztonsági figyelmeztetés egyes esetekben.

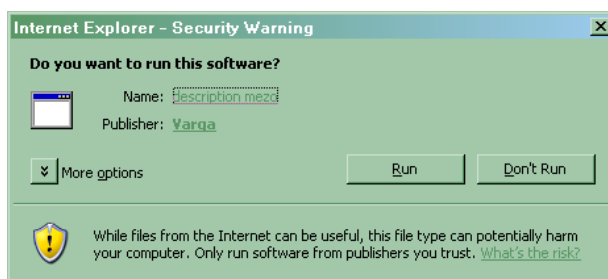
6.1. A kódot aláíró tanúsítvány még érvényes, időbélyegzés nem volt

Ez a figyelmeztetés tekinthető normálisnak, figyelemben tartva, hogy az időbélyegzés nélkül a tanúsítvány lejáta után már a következő fejezetben látható figyelmeztetés jelenik meg.

Az alábbi figyelmeztetés jelenik meg egy fájl használatakor:

Az aláírásakor megadott opciók a következők voltak:

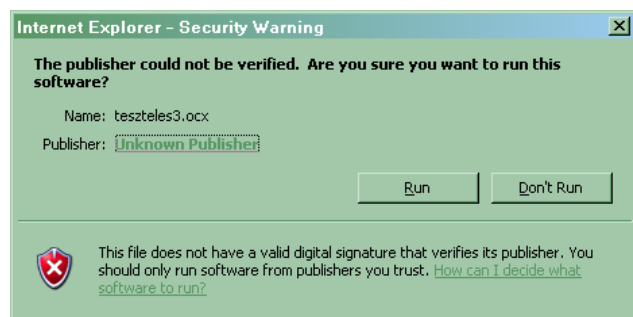
- description = „description mező”
ez a szöveg látszik
- web location = <http://www.index.hu>
a „description mező” sorra kattintva rögtön el is visz kedvenc híroldalunkra ☺
- az aláíró tanúsítvány CN mezője = „Varga”
igen ez a Publisher (fejlesztő, kiadó) sorban látszik is, rákattintva mind az aláírás érvényességéről, mind a tanúsítványról meggyőződhetünk.



6.2. A kódot aláíró tanúsítvány már nem érvényes (pl. lejárt) és időbélyegzés nem volt

Az alábbi figyelmeztetés jelenik meg a tanúsítvány lejártá után ugyanarra a kódra, aminek az előbb is láttuk a figyelmeztetését, mert ez a kód nem volt ez esetben aláírva.

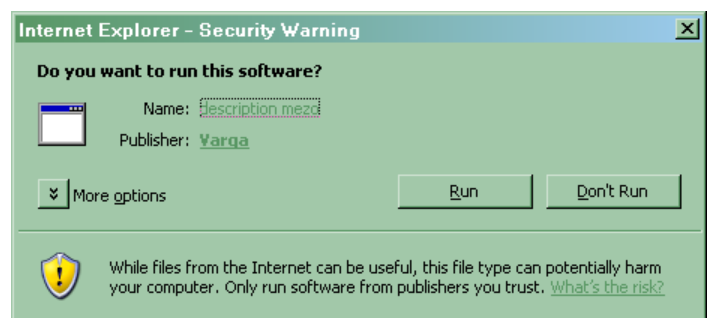
Mint látható, semmilyen aláíráskor meglévő információt nem vesz át a fájlról az operációs rendszer, Name (név) mezőnek a fájl nevét, aláírónak meg Ismeretlen (Unknown) opciót jelez.



6.3. A kódot aláíró tanúsítvány már nem érvényes, de volt időbélyegzés

Ez a figyelmeztetés megegyezik az első példában láthatóval, a különbség annyi, hogy mivel volt időbélyegzés, a tanúsítvány lejártá után sem változik a figyelmeztetés módja, ugyanez az ablak jelenik meg.

Az alábbi figyelmeztetés jelenik meg a tanúsítvány lejáratá után ugyanarra az aláírt és időbélyegzett kódra.



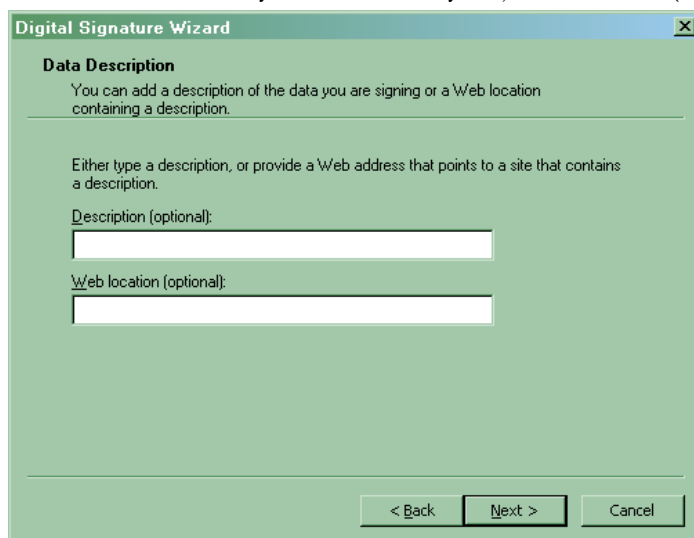
Az aláíráskor megadott opciók a következők voltak:

- description = „description mező”
ez a szöveg látszik
- web location = <http://www.index.hu>
a „description mező” sorra kattintva rögtön el is visz a kedvenc híroldalunkra ☺
- az aláíró tanúsítvány CN mezője = „Varga”
igen ez a Publisher (fejlesztő, kiadó) sorban látszik is, rákattintva mind az aláírás érvényességéről, mind a tanúsítványról meggyőződhetünk

Az aláírt, időbélyegzett kód abban az esetben érvényes, ha az aláírás időpontjában a tanúsítvány érvényes volt.

7. Az EXE, OCX és DLL fájlok aláírása

1. Indítsuk el a SignCode alkalmazást, majd nyomjunk Tovább (Next) gombot.
2. Tallózzuk ki az aláírni kívánt exe, ocx, dll állományunkat.
3. Válasszuk az aláírási opciók közül a Tipikus (Typical) opciót, majd nyomjunk tovább gombot.
4. Nyomjuk meg a Tanúsítványtárból (Select from Store) gombot, majd válasszuk ki kódaláíró tanúsítványunkat, utána nyomjunk Tovább (Next) gombot.



The screenshot shows a dialog box titled "Digital Signature Wizard" with a close button (X) in the top right corner. The main heading is "Data Description". Below it, the text reads: "You can add a description of the data you are signing or a Web location containing a description." A horizontal line separates this text from the instructions below: "Either type a description, or provide a Web address that points to a site that contains a description." There are two input fields: "Description (optional):" and "Web location (optional):". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

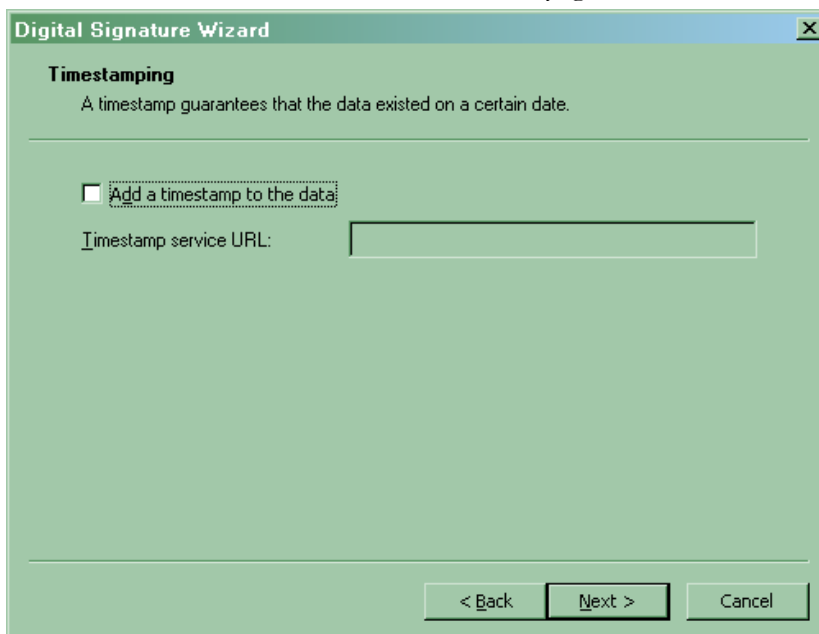
A megjelenő ablakban következők adhatóak meg:

- description (leírás)
a biztonsági figyelmeztetés Name (név) sorának tartalma adandó itt meg
- web location (webhely)
a biztonsági figyelmeztetés Name (név) sora egy link lesz, melynek felirata a korábban megadott, és amely link az itt megadott weboldalra mutat.

Figyelem!

A http:// vagy https:// előtag kötelező ennek megadásakor!

5. A következő ablakban választhatunk időbélyegzést is



Ha a kódot időbélyegezzük, akkor az érvényes lesz a tanúsítvány lejárta után is, egyébként problémát jelez. (lásd Példák biztonsági figyelmeztetésekre fejezetet)

Ha időbélyegezni szeretnénk, az időbélyeg szabványtól való eltérése miatt a következők egyikét tudjuk egyelőre csak használni:

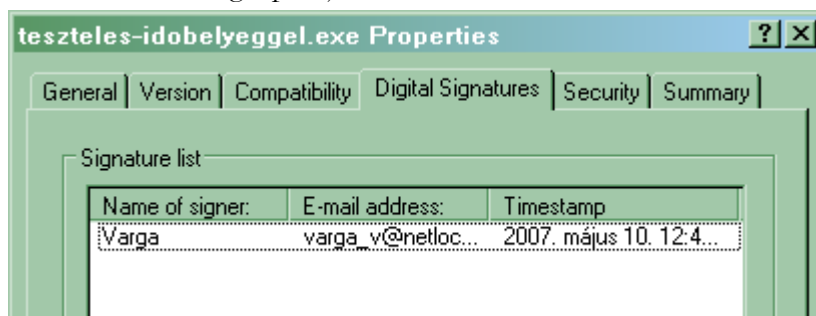
(ha valamelyik nem működik, próbáljuk a másikkal)

`http://timestamp.verisign.com/scripts/timestamp.dll`

`http://timestamp.comodoca.com/authenticode`

6. Az utolsó képernyőn nyomjuk meg a Befejezés (Finish) gombot.

A sikeres aláírásról egy üzenet tudósít, illetve a fájlra jobb gombbal kattintva, Tulajdonságok (Properties) gombot nyomva és Digitális aláírások (Digital Signatures) fület választva megkaphatjuk az aláírás információit.



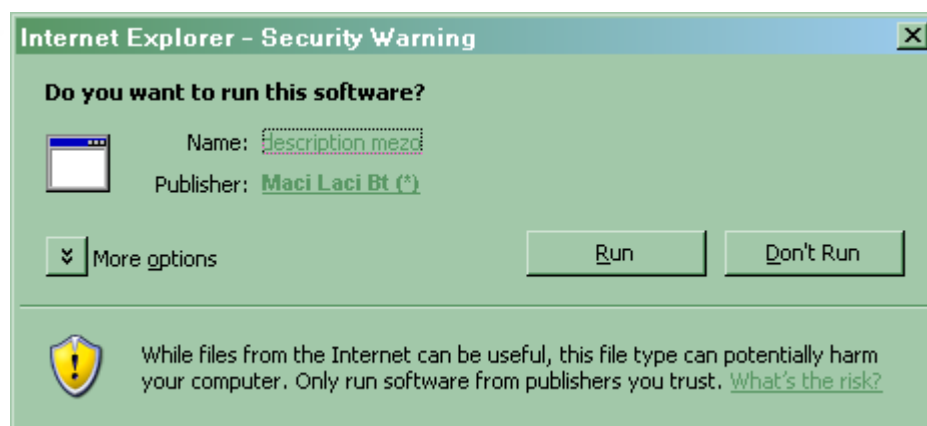
Az ábrán aláírt és időbélyegzett kód fenti módon megtekinthető tulajdonságai láthatók.

8. Minősített tanúsítvány használata céges kód aláírásra

A minősített tanúsítvány elsősorban személy nevére szól, ami az aláírt kód használata során megjelenő ablakban a Publisher (Fejlesztő, kiadó) sorban megjelenő személynevet mutat.

Az ilyen problémák elkerülésére kérhető, ún. álneves tanúsítvány, mely esetben a szervezet adatai kerülnek a személy által igényelt tanúsítványba, így a tanúsítvány szervezeti tanúsítványnak látszik a „(*)” kiegészítéssel.

A kód aláírása egy ilyen tanúsítvány esetén ugyanúgy működik, az egyetlen különbség az alábbi képen látszik, miszerint a Publisher mezőben a cégnév található a „(*)” kiegészítéssel.



9. Függelék A – Programvédelmek együttműködése az kódaláírással

Az aláírás és az időbélyeg a fájlban tárolódik, így felmerülhet a kérdés, hogy érinti-e ez a fájljaink fájlkódoláson, vagy egyéb megoldáson alapuló további védelmét.

A következő védelmi megoldások kerültek tesztelésre, és került megállapításra, hogy nem érinti:

- EXECryptor
- Codemeter

A fentiek alapján megjósolható, hogy várhatóan más védelmi rendszereket sem érint.