FIRA Elektronikus Aláírás Termék v1.5

Támogató dokumentáció
Support Guide
SG

Verzió:	1.5.0
Dátum:	2015.05.05.
Készítette:	Juhász Ágnes

Copyright 2015, Polysys Kft, Budapest, Hungary. All rights reserved. Minden jog fenntartva.

Ezen dokumentumot a Polysys kifejezett engedélye nélkül sem egészében, sem részleteiben, semmilyen eszközzel nem lehet többszörözni, módosítani, használatba vagy kölcsön adni, eladni, terjeszteni, másolatot készíteni, vagy egyéb származékos művet létrehozni belőle.

polysys®
A polysys® védjegyet a Szellemi Tulajdon Nemzeti Hivatala (korábban Országos Találmányi Hivatal) a 129230/1989 szám alatt lajstromozta.

Java™
A Java™, valamint minden olyan védjegy, amely a Java szót tartalmazza az Oracle védjegye vagy bejegyzett védjegye az Egyesült Államokban és egyéb országokban..

Ez a dokumentum a „JAVA” szóval szintén a Java védjegyre utal.

Változás kezelés

verzió	dátum	leírás	készítette
0.9	2007-06-08	kiinduló verzió	Juhász Ágnes
1.0	2007-06-13	1.0 verzió	Juhász Ágnes
1.0.1	2007-07-02	1.0.1 verzió: az aláírás SignaturePolicyIdentifier elemében a legújabb, 1.04 verziószámú Educatio aláíráspolitika követése	Juhász Ágnes
1.0.2	2007-07-11	1.0.2 verzió: az aláírás SignaturePolicyIdentifier elemében a legújabb, 2.0 verziószámú Educatio aláíráspolitika követése	Juhász Ágnes
1.0.3	2007-07-17	1.0.3 verzió: - új input paraméter (upload-filename) a PHP feltöltés támogatására - Netlock (Class B) Közigazgatási Tanúsítványkiadó által kiadott aláírói tanúsítványok is használhatók	Juhász Ágnes
1.0.4	2007-07-25	1.0.4 verzió: - új input paraméterek (*keystore-type, keystore-value, stb*) az aláíró kulcsot tartalmazó kulcstároló előválasztáshoz - Microsec e-Szigno CA6 tanúsítványkiadó által kiadott aláírói tanúsítványok is használhatók - Netlock (Class A) Közigazgatási Tanúsítványkiadó által kiadott aláírói tanúsítványok is használhatók	Juhász Ágnes
1.0.5	2007-08-03	1.0.5 verzió: - Máv Informatika Trust&Sign ACA v2.0 tanúsítványkiadó által kiadott aláírói tanúsítványok is használhatók - Máv Informatika Trust&Sign QCA v2.1 tanúsítványkiadó által kiadott aláírói tanúsítványok is használhatók - új látvány téma a színek csoportban: szürke-rózsaszín	Juhász Ágnes
1.0.6	2007-09-11	1.0.6 verzió: - Magyar Telekom Minositett KET CA tanúsítványkiadó által kiadott aláírói tanúsítványok is használhatók	Juhász Ágnes
1.0.7	2007-11-14	1.0.7 verzió: - Microsec Giesecke kártyán „üres_KE”, „üres_AUT” tulajdonos és kiállítóval szereplő, nem értelmezhető tanúsítványok miatti workaround - új látvány téma a színek csoportban: sötétkék - egy menetben, egymás után, több kiválasztott adatszolgáltatás írható alá	Juhász Ágnes
1.0.8	2008-05-22	1.0.8 verzió: - Máv Informatika Trust&Sign ACA v2.0 tanúsítványkiadót lecserélték, új tanúsítványa: Trust&CA NQKET v2.0 - Educatio EDUCA-2 tanúsítványkiadó által kiadott aláírói tanúsítványok is használhatók	Juhász Ágnes

1.0.9	2008-07-15	1.0.9 verzió: - Máv Informatika Trust&Sign QCA v2.1 tanúsítványkiadót lecserélték, új tanúsítványa: Trust&CA QKET v2.0	Juhász Ágnes
1.0.10	2008-09-29	1.0.10 verzió: - CryptoSigno Interop API legújabb tanúsított v2.1.0 verzió beépítése	Juhász Ágnes
1.0.11	2009-06-29	1.0.11 verzió: - Substance Look and Feel beépítése	Juhász Ágnes
1.1.1	2011-03-10	1.1.1 verzió: - CryptoSigno Interop API legújabb tanúsított v2.2.1b140 verzió beépítése - Windows tanúsítványtár támogatás - Gemalto Classic V3 (GemP15-1) kártya támogatás - új látvány: piros-fekete	Juhász Ágnes
1.2.0	2012-02-22	1.2.0 verzió: - CryptoSigno Interop API legújabb tanúsított v2.3.0b141 verzió beépítése - MELASZ Ready v2.0 aláírási formátum használata SHA256withRSA algoritmussal - az alábbi tanúsítványkiadók által kibocsátott tanúsítványok is használhatók: • Info&CA NQKET v3.0 • Qualified KET e-Szigno CA 2009 • Signature Class 3 KET e-Szigno CA 2009	Juhász Ágnes
1.3.0	2013-04-08	1.3.0 verzió: - CryptoSigno Interop API legújabb tanúsított v2.4.0b142 verzió beépítése - minden, a magyar Bizalmi Listán szereplő tanúsítványkiadó használható (bővebb információ: www.polysys.eu/tledit)	Juhász Ágnes
1.3.2	2014-01-08	1.3.2 verzió: - workaround a Java7 u45+ verzió alatt jelentkező "lefagyás" probléma(100 % processzorfoglaltsággal az alkalmazás percekig nem reagál az eseményekre) megoldására	Juhász Ágnes
1.3.3	2014-01-27	1.3.3 verzió: - Java7 u51 kompatibilitás	Juhász Ágnes
1.4.0	2014-02-24	1.4.0 verzió: - Bizalmi Lista új szabványának követése (ETSI TS 119 612 V1.1.1 (2013-06))	Juhász Ágnes
1.5.0	2015-05-05	1.5.0 verzió: - CryptoSigno Interop API legújabb tanúsított v2.4.1b143 verzió beépítése	Juhász Ágnes

Tartalomjegyzék

Tartalomjegyzék 5
1 Bevezetés 7
1.1 Azonosítás 7
1.2 Ismertetés 7
1.3 Licenc kezelés 8
1.3.1 Első licenc igénylése 8
1.3.2 Licenc igénylése az aláíró tanúsítvány cseréje esetén 9
1.4 Látvány testreszabása 10
1.5 Input paraméterek 10
1.5.1 Működést befolyásoló input paraméterek 11
1.5.2 Látványt befolyásoló input paraméterek 12
1.6 FIRA integrációja Java alkalmazásba 14
1.6.1 Rendelkezésre álló beállítások 14
1.6.2 FIRA példány létrehozása 16
1.6.3 FIRA befejeződésének észlelése 16
1.6.4 Elkészült aláírás visszaadása 17
1.7 Elkészült aláírás feltöltése szerver oldali komponensnek 17
2 Előfeltételek 18
2.1 Az informatikai környezetre vonatkozó követelmények 18
2.1.1 Hardver 18
2.1.2 Operációs rendszer 18
2.1.3 Java környezet 18
2.1.4 Web szerver 18
2.1.5 Ant telepítése 18
2.1.6 További követelmények 18
3 FIRA készlet telepítése 19
3.1 Telepítéshez szükséges fájl 19
3.1.1 fira-{verziószám}.zip fájl kifejtése 19
3.1.1.1 A doc könyvtár 19
3.1.1.2 Az src könyvtár 20
3.1.1.3 A test könyvtár 20
3.1.1.4 A trial könyvtár 20
3.1.1.5 A web könyvtár 20
3.1.1.6 További fájlok 20
4 FIRA indítópult segédprogram 22
4.1 A segédprogram futtatása 22
4.2 A segédprogram használata 22
5 FIRA kipróbálása 24
5.1 Aláíró tanúsítvány és kulcs kiválasztása 24
5.2 Adatszolgáltatást tartalmazó fájl kiválasztása 26
5.3 Aláírandó adatszolgáltatás megtekintése 27
5.4 Aláírás 28
6 FIRA, mint web alkalmazás üzembe helyezése 30
6.1.1 Előkészítés 30

6.1.2 Üzembe helyezés lépései..... 30
7 FIRA, mint helyi gépen futó Java alkalmazás üzembe helyezése..... 31
8 Tanúsítványok, kriptográfiai eszközök kezelése, hibaelhárítása..... 32
8.1 Aláírói tanúsítvány..... 32
8.2 Kriptográfiai eszközök és aláíró kulcsok kezelése..... 32
8.2.1 Teendők, ha a kriptográfiai eszközökben talált aláírói tanúsítványok listája üres.....33
8.2.2 Teendők „nincs jelen közigazgatási, ügyfélhez kapcsolódó aláíró tanúsítvány” hibajelzés esetén..... 34
Táblázatok jegyzéke..... 36
Hivatkozott dokumentumok..... 37

1 Bevezetés

1.1 Azonosítás

Jelen dokumentum a *FIRA Elektronikus Aláírás Termék* üzembe helyezési és üzemeltetési útmutatója.
A *FIRA Elektronikus Aláírás Termék*et a FIRA készlet tartalmazza, amely a http://www.polysys.eu/hu/FIRA lapon található linkről tölthető le. Jelen dokumentum legfrissebb változata az említett lapról szintén letölthető.

A FIRA készlet tartalma:

- *FIRA Elektronikus Aláírás Termék* üzembe helyezéséhez szükséges fájlok
- *FIRA indítópult*: - egy segédprogram, amelynek célja, hogy az üzemeltetőket, fejlesztőket támogassa a FIRA üzembe helyezését megelőző és kísérő tevékenységekben.
- teszt aláíró tanúsítvány és kulcs a kipróbáláshoz

Jelen dokumentumban a FIRA rövidített megnevezés a *FIRA Elektronikus Aláírás Termék*et jelenti.

1.2 Ismertetés

A *FIRA Elektronikus Aláírás Termék* egy dobozos jellegű aláíró alkalmazás, amellyel a Felsőoktatási Információs Rendszer (FIR) adatszolgáltatás elektronikus aláírásával kapcsolatos követelmények gyorsan és hatékonyan kielégíthetők. Teljes mértékben megfelel az Educatio Kht. által kiadott aláíráspolitikában (OID: 1.3.6.1.4.1.27537.3.1) rögzített követelményeknek.

Meghívható:

- web lapba ágyazva appletként
- paraméterezett linkkel appletként
- parancssorból scripttel
- Java WebStart alkalmazásként
- asztali Java alkalmazásként
- más Java alkalmazásba integrálva (panelként)

A FIRA az elektronikus aláírás létrehozásához a tanúsított *A2 CryptoSigno Interop JAVA API* fejlesztőkészletet használja fel. Az *A2 CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz* fejlesztőkészletről további információk a www.polysys.eu weblapon találhatók.

A FIRA számára input paraméterekkel lehet átadni az aláírandó tartalmat, amely lehet:

- XML-t tartalmazó string
- XML-t tartalmazó fájl
- URL, amelyről az XML letölthető

FIRA főbb funkciói:

- A FIRA aláírás előtt megjeleníti az aláíró számára az aláírandó tartalmat, az input paraméterezéstől függően vagy XSL-el formázva, vagy XML szövegként és XML fában.
- Az aláírónak az aláírandó tartalom megtekintését követően ki kell nyilvánítania aláírási szándékát.
- A FIRA automatikusan felismeri a telepített kriptográfiai eszközöket (ALE/BALE, pl. Axalto, Gemalto, stb). Az aláíró számára megjeleníti a felismert (PKCS#11 szabványnak megfelelő) kriptográfiai eszközök listáját, amelyből az aláíró kiválaszthatja a használni kívánt aláíró kulcsot.
- A FIRA képes az aláírás létrehozására abban az esetben is, amikor az aláíró kulcs PKCS#12 szabványnak megfelelő kulcstároló fájlban áll rendelkezésre.

A FIRA az elektronikus aláírást a közigazgatási egységes aláírási formátumnak, valamint az Educatio Kht. EDUAP-1 elektronikus aláírás politikájának megfelelően hozza létre.

Az elkészített elektronikus aláírás az input paraméterezéstől függően a következő módokon kerül visszaadásra:

- stringként
- fájlba mentve
- megadott http címre feltöltve

1.3 Licenc kezelés

1.3.1 Első licenc igénylése

A FIRA használatához egy megfelelő licenc fájl megléte szükséges. A licenc az aláíró tanúsítványhoz kapcsolódik, az aláíró tanúsítvány érvényességi időtartamán belül az alkalmazással tetszőleges számú elektronikus aláírás hozható létre.

A FIRA használatba vételével megkezdődik az úgynevezett „megrendelési időszak”, amely alatt engedélyezett az alkalmazás licenc fájl nélküli használata. A megrendelési időszak célja, hogy a felhasználó cég, intézmény vagy magánszemély számára lehetőség nyíljon a Termék kipróbálására, megrendelésére, a licenc igénylési eljárás lefolytatására.

A megrendelési időszakban, elektronikus aláírás készítésekor minden esetben megjelenik egy ablak, amely visszajelzi a licenc és megrendelés állapotával kapcsolatos információkat. Itt rendelkezésre áll a „megrendelés készítése” szolgáltatás, amellyel onlájn módon lehet a megrendelést elkészíteni és elküldeni. A megrendelést elküldését és visszaigazolását, majd a kézhez vett számla kifizetését követően lehetőség nyílik a licenc fájl onlájn letöltésére.

A megrendelési időszak lejártával, amennyiben megfelelő licenc fájl továbbra sem található meg, a FIRA további használata már nem engedélyezett, az információs ablakban egyedül a „kilép” nyomógomb jelenik meg.

A licenc igénylés lépései az üzembe helyezés és üzemeltetés szempontjából:

- A felhasználó gépén telepíteni kell az aláíró tanúsítványt és kulcsot hordozó kriptográfiai eszközt, általában az Axalto kártyát és a kártyaolvasóval ellátott billentyűzetet. Meg kell győződni arról, hogy a kriptográfiai eszköz megfelelően működik.
- A telepített *FIRA Elektronikus Aláírás Termék*kel meg kell kezdeni egy tetszőleges adatszolgáltatás aláírását (kész adatszolgáltatás hiányában tetszőleges XML fájl használható).
- Az aláíró kulcshoz történt sikeres bejelentkezést követően a képernyőn megjelenik az információs ablak, amelyben a licenc és megrendelés állapotával kapcsolatos információk visszajelzésre kerülnek. Itt a *megrendelés készítés* nyomógombbal lehet indítani a FIRA onlájn megrendelését. Amennyiben a számítógép rendelkezik élő Internet kapcsolattal, elindul az *Onlájn megrendelés* alkalmazás.
- Amennyiben a FIRA-t futtató számítógép nem rendelkezik Internet eléréssel (oflájn megrendelés esete), az aláíró tanúsítványt elektronikus levélben kell elküldeni a fira@polysys.eu címre. A tanúsítvány megküldése a levél csatolmányaként történjen. A tanúsítványnak az elektronikus levél csatolmányként történő megküldéséhez, a FIRA a felhasználó által aláírásra utoljára kiválasztott tanúsítványt eltárolja a FIRA-t futtató számítógép helyi fájlrendszerében. Az elérési útvonal a következő:

{felhasználó alapkönyvtára}/.fira/pkidata/personalcerts/SignerCertificate.cer

Oflájn megrendelés esetén egy további megrendelő adatlap kitöltése lesz majd szükséges.

- A Polysys az onlájn módon vagy elektronikus levélben megküldött megrendeléshez kiállítja és megküldi a számlát, amelynek kifizetése után az aláírói tanúsítványhoz kiállítja a licencet és elektronikus levélben értesítést küld.

- Onlájn megrendelés esetén, az elkészült licenc fájl az információs ablakban található *licenc fájl letöltése* nyomógombbal tölthető le. Oflájn megrendelés esetén, a Polysys által elektronikus levélben megküldött licenc fájlt el kell helyezni a FIRA konfigurációs könyvtárában, amely a következő: *{felhasználó alapkönyvtára}/.fira.*
- Ezt követően, az aláírás létrehozása, az adott aláíró tanúsítvánnyal engedélyezésre kerül.
- Az aláíró tanúsítvány érvényességi időtartamán belül, tetszőleges számú elektronikus aláírás hozható létre.
- A tanúsítvány lejáratát megelőző 30 napos időszakban a FIRA figyelmeztet a tanúsítvány érvényességének közelgő lejáratára, lásd részletesen az 1.3.2 fejezetben.

Megjegyzés: a FIRA készlet tartalmaz egy tesztelési célra használható aláíró tanúsítványt és az ahhoz tartozó licenc fájlt, lásd részletesen a 3.1.1.4 fejezetben.

Figyelem: egy számítógépen egy adott felhasználói névvel bejelentkezve, a FIRA-nak egy példánya, egy aláíró részére használható. A FIRA az első futáskor létrehoz egy könyvtárat, amelyben a beállításokat, adatokat tárolja. Ez a könyvtár a következő: *{felhasználó alapkönyvtára}/.fira*, ahol a *{felhasználó alapkönyvtára}* a felhasználó alap könyvtárát jelenti az adott számítógépen. Ez Windows környezetben pl. c:/Documents and Settings/Rendszergazda, Linux környezetben pl. /home/username. Ebből következően, ha ugyanazon a számítógépen ugyanazon felhasználói névvel bejelentkezve, egy újabb aláíró kezdi meg a FIRA használatát, akkor az eredeti beállítások, adatok felülírásra kerülnek.

1.3.2 Licenc igénylése az aláíró tanúsítvány cseréje esetén

A tanúsítvány lejáratát megelőző 30 napos időszakban a FIRA tájékoztató üzenetet jelenít meg a felhasználó számára, hogy ne feledjen el időben gondoskodni új aláírói tanúsítványról és licencről.

A tanúsítvány cseréjét, megújítását kezdeményezze hitelesítés-szolgáltatójánál !

Az új tanúsítvány használatához új licenc beszerzése is szükséges. Ennek lépései a következők:

- Helyezze üzembe az új tanúsítványt tartalmazó kulcstárolót.
- Indítsa el a FIRA alkalmazást.
- Az *Aláíró tanúsítvány és kulcs kiválasztása* képernyőn válassza az új tanúsítványt tartalmazó kulcstárolót. Amennyiben „*A jövőben ezt a kulcstároló kívánom használni*” jelölőnégyzet be van kapcsolva, a *vissza* nyomógombbal léphet vissza erre a képernyőre.
- Kezdje meg egy tetszőleges adatszolgáltatás aláírását, a *Bejelentkezés elektronikus aláírás készítéséhez* ablakban az új tanúsítványhoz tartozó PIN kódot adja meg.
- A megjelenő, *FIRA Elektronikus Aláírás Termék licenc információk* ablak tájékoztat arról, hogy a licenc fájl nem a most kiválasztott aláírói tanúsítványhoz tartozik. Kattintson a *megrendelés készítése* nyomógombra. Hamarosan megjelenik az „Onlájn megrendelés” alkalmazás képernyője. Töltse ki az adatlapot, majd kattintson a *megrendelés elküldése* nyomógombra.
- A Polysys az onlájn módon megküldött megrendeléshez kiállítja és megküldi a számlát, amelynek kifizetése után az új aláírói tanúsítványhoz kiállítja a licencet és elektronikus levélben értesítést küld.
- Onlájn megrendelés esetén, az elkészült licenc fájl az információs ablakban található „licenc fájl letöltése” nyomógombbal tölthető le. Oflájn megrendelés esetén, a Polysys által elektronikus levélben megküldött licenc fájlt el kell helyezni a FIRA konfigurációs könyvtárában, amely a következő: *{felhasználó alapkönyvtára}/.fira.*
- Ezt követően, az aláírás létrehozása, az új aláírói tanúsítvánnyal engedélyezésre kerül.
- Az új tanúsítvány érvényességi időtartamán belül, ismét, tetszőleges számú elektronikus aláírás hozható létre.

Amennyiben az új tanúsítvány beszerzése még azt megelőzően megtörténik, hogy a régi tanúsítvány lejárt volna, abban az időszakban, amikor a régi tanúsítvány még érvényes, de az új tanúsítványhoz tartozó licenc fájl még nem érkezett meg, vissza lehet kapcsolni a régi tanúsítvánnyal történő aláírásra.

Visszakapcsolás a régi tanúsítványra és licencre:

- Helyezze üzembe a régi tanúsítványt tartalmazó kulcstárolót.
- Indítsa el a FIRA alkalmazást.
- Az *Aláíró tanúsítvány és kulcs kiválasztása* képernyőn válassza a régi tanúsítványt tartalmazó kulcstárolót. Amennyiben „*A jövőben ezt a kulcstároló kívánom használni*” jelölőnégyzet be van kapcsolva, a *vissza* nyomógombbal léphet vissza erre a képernyőre.
- A régi tanúsítvány és licenc érvényességi időszakában a szokásos módon használhatja a FIRA alkalmazást.

Teendők, amikor az új tanúsítványhoz tartozó licencről az értesítés megérkezett:

- Helyezze üzembe az új tanúsítványt tartalmazó kulcstárolót.
- Indítsa el a FIRA alkalmazást.
- Az *Aláíró tanúsítvány és kulcs kiválasztása* képernyőn válassza az új tanúsítványt tartalmazó kulcstárolót. Amennyiben „*A jövőben ezt a kulcstároló kívánom használni*” jelölőnégyzet be van kapcsolva, a *vissza* nyomógombbal léphet vissza erre a képernyőre.
- Kezdje meg egy tetszőleges adatszolgáltatás aláírását, a *Bejelentkezés elektronikus aláírás készítéséhez* ablakban az új tanúsítványhoz tartozó PIN kódot adja meg.
- A megjelenő, *FIRA Elektronikus Aláírás Termék licenc információk* ablak tájékoztat arról, hogy a licenc fájl nem a most kiválasztott aláírói tanúsítványhoz tartozik. Kattintson a *megrendelés készítése* nyomógombra. Hamarosan megjelenik az „Onlájn megrendelés” alkalmazás képernyője. A megjelenő „*Ehhez az aláírói tanúsítványhoz már van ismert megrendelés. Letölti a megrendelés adatokat?*” kérdésre válaszoljon igennel. A letöltést követően lépjen ki mind az „Onlájn megrendelés”, mind a FIRA alkalmazásból.
- Indítsa el ismét a FIRA alkalmazást,kezdje meg egy tetszőleges adatszolgáltatás aláírását az új tanúsítvánnyal.
- A megjelenő, *FIRA Elektronikus Aláírás Termék licenc információk* ablak tájékoztat arról, hogy a licenc fájl nem a most kiválasztott aláírói tanúsítványhoz tartozik. Kattintson a *licenc fájl letöltése* nyomógombra. A licenc fájl sikeres letöltését követően, a *tovább* gombbal folytathatja az aláírás létrehozását.

1.4 Látvány testreszabása

A FIRA látványa, kinézete, az adott felhasználási környezet jellegének, kívánalmainak megfelelően testre szabható, vagy paraméterezett módon (lásd 1.5 fejezet), vagy a felhasználó beállításainak megfelelően. Amennyiben a menü megjelenítése engedélyezett, a felhasználó a *Látvány* menüben az alkalmazás látványát és témáját szabadon beállíthatja. A FIRA az első futáskor létrehoz a felhasználó számítógépen egy könyvtárat, amelyben a beállításokat tárolja. Ez a könyvtár a következő: *{felhasználó alapkönyvtára}/.fira*, ahol a *{felhasználó alapkönyvtára}* a felhasználó alap könyvtárát jelenti az adott számítógépen. Ez Windows környezetben pl. c:/Documents and Settings/Rendszergazda, Linux környezetben pl. /home/username.
A *FIRA Elektronikus Aláírás Termék* a következő futáskor a felhasználó által beállított látvánnyal és témával fog megjelenni.

1.5 Input paraméterek

Ez a fejezet ismerteti a *FIRA Elektronikus Aláírás Termék* input paramétereit.

Az input paraméterek két csoportba sorolhatók:

- működést befolyásoló paraméterek, amelyek meghatározzák és befolyásolják a FIRA működését
- látvánnyal kapcsolatos paraméterek, amelyek a FIRA megjelenését határozzák meg

1.5.1 Működést befolyásoló input paraméterek

- **help-url**: az URL, amelyről a súgó fájl letölthető
  - ha nincs megadva, akkor az alapértelmezett súgó fájl kerül megjelenítésre
  - ha meg van adva, akkor az erről a címről letöltött html tartalommal lesz súgó támogatás megjelenítve
  - a „none” speciális érték megadásával nem lesz súgó támogatás
- **xml-url**: az URL, amelyről az aláírandó XML fájl letölthető
  - Ha nincs megadva, és a FIRA statikus *SetXmlText* metódusával sincs XML közölve, akkor a felhasználó az alkalmazásban utólag választhatja ki a az aláírandó XML-t tartalmazó fájlt. Ekkor egy adatszolgáltatás aláírását követően, az utolsó képernyőn a „befejezés” nyomógomb mellett megjelenik az „elejére” nyomógomb is, amelyre kattintva lehetőség nyílik egy program behívással több adatszolgáltatás egymás utáni aláírására.
  - ha meg van adva, és értelmezhető URL-ként, akkor az aláírandó XML adat erről a címről kerül letöltésre
  - ha meg van adva, de nem értelmezhető URL-ként, akkor a felhasználó az alkalmazásban utólag választhatja ki az aláírandó XML-t tartalmazó fájlt
- **xsl-url**: az URL, amelyről az XML megjelenítéséhez az XSL letölthető
  - ha nincs megadva, akkor az aláírandó adatok formázott megjelenítésre kimarad, az aláírandó XML szöveg és fa nézetben kerül az aláíró számára megjelenítésre
  - ha meg van adva, akkor az aláírandó XML a megadott XSL-el formázva HTML-ként kerül az aláíró számára megjelenítésre
  - ha aláírandó XML nincs átadva, akkor ez a paraméter nem lesz figyelembe véve
- **upload-url**: az URL, amelyre az aláírás állomány feltöltésre kerül
  - ha nincs megadva, akkor a feltöltés kimarad, a felhasználó kiválaszthatja a fájlt, amelybe az elkészült aláírás mentésre kerül
  - ha meg van adva, akkor az elkészült aláírás erre a címre lesz feltöltve (POST), „application/octet-stream” tartalom típussal
  - a „none” speciális érték megadásával a feltöltés és a fájlba mentés kimarad
- **upload-filename**: az aláírt állomány feltöltéséhez a fájl név
  - ez a paraméter csak akkor lesz figyelembe véve, ha az **upload-url** paraméter nem üres és nem a „none” speciális érték.
  - ha nem üres, akkor a feltöltés (POST) „multipart/form-data” tartalom típussal fog történni, és ennek a paraméternek az értéke lesz a küldött fájl neveként megadva.
- **keystore-type**: aláírói kulcsot tároló kulcstároló típusa, lehetséges értékei: „file”, „device”
  - ha nincs megadva, akkor az *Aláírói tanúsítvány és kulcs kiválasztása* képernyő a szokásos módon működik, azaz ha az alkalmazás még soha nem futott, akkor nincs kiajánlás a kulcstároló típusára, ha az alkalmazás már futott megelezően, akkor a felhasználó által az utolsó futásnál kiválasztott kulcstároló típus kerül kiajánlásra.
  - ha meg van adva, és értéke a megengedett „file”, „device” értékek valamelyike, akkor a kulcstároló típusa az *Aláírói tanúsítvány és kulcs kiválasztása* képernyőn ezen paraméter szerint kerül kiajánlásra.
- **keystore-value**: csak akkor lesz figyelembe véve, ha a **keystore-type** meg van adva
  - ha a **keystore-type** paraméter értéke „file”, akkor az *Aláírói tanúsítvány és kulcs kiválasztása* képernyőn a kulcstárolót tartalmazó fájl elérési útja szövegmező ezen paraméter értékével kerül kitöltésre, felülírva a felhasználó által az utolsó futásnál megadott értéket.
  - ha a **keystore-type** paraméter értéke „device”, akkor az *Aláírói tanúsítvány és kulcs kiválasztása* képernyőn a kriptográfiai eszköz választólistában ezen

paraméter értékével kiválasztás történik, felülírva a felhasználó által az utolsó futásnál megadott értéket.

- **pass-signerkeychooser**: csak akkor jut érvényre, ha a **keystore-type** és **keystore-value** paraméter egyaránt meg van adva, lehetséges értékei: „true”, „false”.
  - „true” értéke esetén az alkalmazás, amennyiben az lehetséges automatikusan kihagyja az *Aláírói tanúsítvány és kulcs kiválasztása* képernyőt.
  - „false” értéke esetén az alkalmazás az *Aláírói tanúsítvány és kulcs kiválasztása* képernyőt megjeleníti, azon a „tovább” gomb választásával lehet tovább lépni.

1.5.2 Látványt befolyásoló input paraméterek

- **_EnableSplashWindow**: opcionális, megengedett értékei: „true” vagy „false”.
  Azt határozza meg, hogy az alkalmazás indulásakor megjelenítésre kerüljön-e a splash ablak.
  - alapértelmezett értéke: „true”
  - „true” értéke esetén az alkalmazás indulásakor a splash ablak megjelenik
  - „false” értéke esetén az alkalmazás indulásakor splash ablak nem jelenik meg
- **_EnableMenu**: opcionális, megengedett értékei: „true” vagy „false”.
  Azt határozza meg, hogy az alkalmazásnak legyen-e főmenüje, *Fájl*, *Látvány* és *Segítség* menükkel.
  - alapértelmezett értéke: „true”
  - „true” értéke esetén az alkalmazásnak lesz főmenüje, benne *Fájl*, *Látvány* és *Segítség* menükkel
  - „false” értéke esetén az alkalmazásnak nem lesz főmenüje
- **_EnableShowConfirmExitDialog**: opcionális, megengedett értékei: „true” vagy „false”.
  Azt határozza meg, hogy amennyiben az alkalmazásnak van főmenüje, akkor a *Fájl* menüből a *Kilép* menüpont választásával, vagy amennyiben az alkalmazás önálló ablakban fut, az ablak bezárásakor megjelenjen-e a kilépési szándékot megerősítő kérdés.
  - alapértelmezett értéke: „true”
  - „true” értéke esetén az alkalmazásból történő kilépéshez megerősítés szükséges
  - „false” értéke esetén az alaklamzásból történő kilépéshez megerősítés nem szükséges
  - amennyiben az alkalmazásnak nincs főmenüje, és nincs önálló ablaka, ez a paraméter lesz figyelembe véve
- **_IconSize**: opcionális, megengedett értékei: „16”, „24”, „32” vagy „48”.
  Azt határozza meg, hogy az alkalmazás a nyomógombok ikonjait mekkora mérettel hozza létre.
  - alapértelmezett értéke: „32”
  - bármely megengedett érték esetén az alkalmazás az ikonokat ezzel a mérettel hozza létre
  - nem megengedett érték esetén az alapértelmezett érték jut érvényre
- **_EnableIconSizeMenu**: opcionális, megengedett értékei: „true” vagy „false”.
  Azt határozza meg, hogy amennyiben az alkalmazásnak van főmenüje, akkor annak *Látvány* menüjében szerepeljen-e az ikonok méretét beállító almenü. Ennek az almenünek a segítségével a felhasználó dinamikusan állíthatja be a nyomógombok méretét.
  - alapértelmezett értéke: „true”
  - „true” értéke esetén a *Látvány* menüben szerepelni fog az *Ikonok mérete* menüpont
  - „false” értéke esetén a *Látvány* menüben az *Ikonok mérete* menüpont nem fog szerepelni
  - amennyiben az alkalmazásnak nincs főmenüje, ez a paraméter nem lesz figyelembe véve
- **_ShowUseThisKeyStoreInTheFuture**: opcionális, megengedett értékei: „true” vagy „false”.
  Azt határozza meg, hogy amennyiben az alkalmazásnak van főmenüje, akkor annak

Látvány menüjében szerepeljen-e az ikonok méretét beállító almenü. Ennek az almenünek a segítségével a felhasználó dinamikusan állíthatja be a nyomógombok méretét.
    - alapértelmezett értéke: „true”
    - „true” értéke esetén az *Aláírói tanúsítvány és kulcs kiválasztása* képernyőn látható lesz „A jövőben ezt a kulcstárolót kívánom használni” jelölőnégyzet
    - „false” értéke esetén az *Aláírói tanúsítvány és kulcs kiválasztása* képernyőn nem lesz látható „A jövőben ezt a kulcstárolót kívánom használni” jelölőnégyzet
- amennyiben az alkalmazásnak nincs főmenüje, ez a paraméter nem lesz figyelembe véve
_LAF: opcionális, megengedett értékei „Windows”, „Motif”, „Metal”, „Kunststoff”, „Ocean”, „Macintosh”. Az alkalmazás kezdeti látványát (LookAndFeel – LAF) határozza meg. Ennek a paraméternek a megadása esetén a felhasználó által utoljára használt (konfigurációs könyvtárban tárolt) beállítás nem jut érvényre.
    - alapértelmezett értéke: a konfigurációs könyvtárban tárolt beállítás, annak hiányában „Kunststoff”
    - bármely megengedett érték esetén az alkalmazás ezzel a kezdeti látvánnyal jelenik meg
    - nem megengedett érték esetén az alapértelmezett érték jut érvényre
- **_Theme**: opcionális, megengedett értékeit lásd az 1. táblázat: Témák táblázatban.
Az alkalmazás látványnak kezdeti témáját határozza meg. A témákat a következő látványok támogatják: „Metal”, „Kunststoff”. A többi látvány esetében a téma nem támogatott. Ennek a paraméternek a megadása esetén a felhasználó által utoljára használt (konfigurációs könyvtárban tárolt) beállítás nem jut érvényre.
    - alapértelmezett értéke: a konfigurációs könyvtárban tárolt beállítás, annak hiányában „SnowLimit”
    - bármely megengedett érték esetén, amennyiben az aktuális látvány téma alkalmazását lehetővé teszi, az alkalmazás ezzel a kezdeti témával jelenik meg
    - nem megengedett érték esetén, amennyiben az aktuális látvány téma alkalmazását lehetővé teszi, az alapértelmezett téma jut érvényre

1. táblázat: Témák

csoport	***_Theme* paraméter értéke**	**vizuális azonosítást segítő megnevezés**
alap	JAVA default	szokásos
	Presentation	bemutató
	BigContrast	nincs kéznél a szemüvegem
	Projector800x800	projektor (800x600)
hangulatok	Capuccino	capuccino
	BlackCoffe	erős kávé cukor nélkül
	Jaffa	jaffa
	BlueSky	bárányfelhő
	Punch	puncsfagylalt
	Spectrum	spektrum
	SnowLimit	hóhatár
	Carib	karib tenger
	Uranium	uránium
	RainForest	esőerdő
	Pepita	pepita
	Pool	medence
	EU	EU
	YellowtailDamselfish	sárga farkú korallsügér
kunststoff	Kunststoff desktop	asztal
	Kunststoff notebook	notebook
	Kunststoff presentation	prezentáció
színek	Contrast	fekete-fehér

	Auburn	Ó-arany
	Gold	arany
	Steel	acél
	PastelGreen	pasztellzöld
	Bourdon	bordó (nagy betűméret)
	BlackAndRed	piros-fekete
	GrayAndPink	szürke-rózsaszín
	DarkBlue	sötétkék

Megjegyzés: a *_Theme* paraméter megadásánál a kis- és nagybetűk különbözőnek számítanak.

1.6 FIRA integrációja Java alkalmazásba

A *FIRA Elektronikus Aláírás Termék* tetszőleges, GUI felülettel rendelkező Java alkalmazásba integrálható. Használata rendkívül egyszerű, a használó alkalmazás valamely paneljéhez mint kész komponens hozzáadható.

Az integráció lépései:

- FIRA statikus változók beállítása (opcionális)
- aláírandó XML adat átadás a statikus *SetXmlText* metódussal (opcionális)
- FIRA objektum példány létrehozása
- figyelők hozzáadása a FIRA példányhoz (opcionális)
- a FIRA komponens hozzáadása a Java alkalmazás valamely paneljéhez
- input paraméterek átadása (opcionális)
- FIRA indítása

Az integrációt forráskódban rendelkezésre álló példa segíti, lásd a 3.1.1.2 fejezetben.

1.6.1 Rendelkezésre álló beállítások

A FIRA-t integráló Java alkalmazás, a FIRA példány létrehozását megelőzően, statikus változók értékadásával meghívásával képes a FIRA látványát meghatározó beállítások elvégzésére, valamint az aláírandó adatszolgáltatás átadására.

String **hu.polysys.epa.client.Main_._CurrentUI**

Tetszőleges nem *null* érték megadása a FIRA számára azt jelenti, hogy a hívó Java alkalmazás a látvánnyal kapcsolatos beállításokat elvégezte. Ebben az esetben a FIRA semmilyen látvánnyal és témával kapcsolatos beállítást nem végez, a hívó alkalmazás egyedül vezérli a látvány és téma kezelést. A felhasználó által utoljára kiválasztott (konfigurációs könyvtárban tárolt) látvány és téma e beállítás esetén szintén nem jut érvényre.
Figyelem: a *_LAF* és *_Theme* input paraméter megadása felülbírálja ezt a beállítást.

Példa a használatra:
hu.polysys.epa.client.Main_._CurrentUI = „Windows";

boolean **hu.polysys.epa.client.Main_._EnableSplashWindow**

Jelentése és alapértelemzése azonos, mint az *_EnableSplashWindow* input paraméteré.
Figyelem: az említett input paraméter megadása felülbírálja ezt a beállítást.
Példa a használatra:
hu.polysys.epa.client.Main_._EnableSplashWindow = false;

boolean **hu.polysys.epa.client.Main_._EnableMenu**
Jelentése és alapértelemzése azonos, mint az *_EnableMenu* input paraméteré.
Figyelem: az említett input paraméter megadása felülbírálja ezt a beállítást.

Példa a használatra:
hu.polysys.epa.client.Main_._EnableMenu = false;

boolean **hu.polysys.epa.client.Main_._EnableShowConfirmExitDialog**
Jelentése és alapértelemzése azonos, mint az *_EnableShowConfirmExitDialog* input paraméteré.
Figyelem: az említett input paraméter megadása felülbírálja ezt a beállítást.

Példa a használatra:
hu.polysys.epa.client.Main_._EnableShowConfirmExitDialog = false;

int **hu.polysys.epa.client.Main_._IconSize**
Jelentése és alapértelemzése azonos, mint az *_IconSize* input paraméteré.
Figyelem: az említett input paraméter megadása felülbírálja ezt a beállítást.

Példa a használatra:
hu.polysys.epa.client.Main_._IconSize = 48;

boolean **hu.polysys.epa.client.Main_._EnableIconSizeMenu**
Jelentése és alapértelemzése azonos, mint az *_EnableIconSizeMenu* input paraméteré.
Figyelem: az említett input paraméter megadása felülbírálja ezt a beállítást.

Példa a használatra:
hu.polysys.epa.client.Main_._EnableIconSizeMenu = false;

void **hu.polysys.epa.client.fir.sign.Main.SetXmlText**(String text)
Ennek a statikus metódusnak a meghívásával a FIRA-t integráló Java alkalmazás képes átadni az aláírandó adatszolgáltatást, XML-t tartalmazó UTF-8 kódolású stringben.
Figyelem: ahhoz, hogy ez a beállítás érvényre jusson, nem szabad megadni az *xml-url* input paramétert. Ha a a stringben átadott adat XML dokumentumként nem értelmezhető, akkor a FIRA az *Aláírandó adatszolgáltatás megtekintése* képernyőn hibaüzenetet jelenít meg, a felhasználó számára egyedül az alkalmazásból történő kilépés lehetőségét hagyva meg.

Példa a használatra:
hu.polysys.epa.client.fir.sign.Main.SetXmlText(…);

boolean **hu.polysys.epa.client.fir.sign.Main._ShowUseThisKeyStoreInTheFuture**
Jelentése és alapértelemzése azonos, mint a *_ShowUseThisKeyStoreInTheFuture* input paraméteré.
Figyelem: az említett input paraméter megadása felülbírálja ezt a beállítást.

Példa a használatra:
hu.polysys.epa.client.fir.sign.Main._ShowUseThisKeyStoreInTheFuture = false;

1.6.2 FIRA példány létrehozása

A FIRA példány létrehozása az azt integráló Java alkalmazásból következő módon történik:

```
import hu.polysys.epa.client.fir.sign.Main;
…
// statikus beállítások
…
// statikus paraméter átadása
…
// példány létrehozása
Main main = new Main(false,Main.CreateSplashWindow());
// figyelők hozzáadása
main.addAppExitListener(new PropertyChangeListener()
{
  public void propertyChange(PropertyChangeEvent e)
  {
    …
  }
});
main.addXmlSignatureReadyListener(new PropertyChangeListener()
{
  public void propertyChange(PropertyChangeEvent e)
  {
    …
  }
});
// hozzáadás az integráló alkalmazás egy meglevő paneljéhez
panel.add(main,BorderLayout.CENTER);
// automatikus méretezés tiltása
main.enableSizingToLastKnown(false);
// indítás az input paraméterek átadásával
Hashtable args = new Hashtable();
hashtable.put(”help-url”,”none”);
…
main.initialize(args);
```

1.6.3 FIRA befejeződésének észlelése

A *FIRA Elektronikus Aláírás Termék* futása befejeződik az alábbi esetekben:

- a felhasználó létrehozta az elektronikus aláírást, és megnyomta a *befejezés* gombot
- a *Fájl* menüből a *Kilépés* menüpontot használta (amennyiben a menü megjelenítése engedélyezett)
- a FIRA ablakát bezárta (amennyiben a FIRA külön ablakban jelenik meg)

Ha szükséges, hogy a FIRA komponenst az integráló Java alkalmazás a fenti esetekben eltüntesse, ezt egy megfelelő figyelő hozzáadásával, az *addAppExitListener (PropertyChangeListener listener)* metódus segítségével teheti meg. Így az integráló Java alkalmazás értesítést kap a FIRA befejeződéséről, és gondoskodhat a komponens eltüntetéséről.

1.6.4 Elkészült aláírás visszaadása

A FIRA képes arról a tényről értesíteni az integráló Java alkalmazást, hogy az elektronikus aláírás elkészült, a FIRA objektum példányhoz egy megfelelő figyelő hozzáadásával, az *addXmlSignatureReadyListener(PropertyChangeListener listener)* metódus segítségével.

String **hu.polysys.epa.client.fir.sign.Main.GetXMLSignature**()

Ennek a statikus metódusnak a meghívásával a FIRA-t integráló Java alkalmazás képes a felhasználó által létrehozott elektronikus aláírás megszerzésére. A visszaadott string UTF-8 kódolt stringként tartalmazza az XML aláírást. Amennyiben a felhasználó még nem hozta létre az aláírást, akkor a metódus *null*-t ad vissza.

1.7 Elkészült aláírás feltöltése szerver oldali komponensnek

A FIRA képes a felhasználó által létrehozott elektronikus aláírást egy szerver oldali komponensnek továbbítani. Ezt az *upload-url* input paraméter megadásával lehet kezdeményezni. A szerver oldali komponens tetszőleges olyan komponens lehet, amely képes binárisan feltöltött adat fogadására, pl. egy Java szervlet. Amennyiben a szerver oldalon PHP komponens fogadja a feltöltött állományt, javasolt az *upload-filename* input paraméter megadása, amelynek hatása az, hogy a feltöltés tartalom típusa „multipart/form-data” lesz, lásd http://www.php.net/manual/hu/features.file-upload.php. Ha az *upload-filename* input paraméter nincs megadva, akkor a feltöltés tartalom típusa „application/octet-stream” lesz.

A FIRA a felhasználó által létrehozott aláírást minden esetben elmenti a saját könyvtárába, amely a következő *{felhasználó alapkönyvtára}/.fira/outbox/{időből képzett alkönyvtár név}, XMLSignature.xml* fájl néven.

Ezt követően a fájl tartalmát feltölti az *upload-url* megadott címre, ha az *upload-filename* input paraméter nincs megadva, akkor a következő módon:

```
URL url = new URL(uploadurl);
connection = (HttpURLConnection)url.openConnection();
connection.setDoInput(true);
connection.setDoOutput(true);
connection.setUseCaches(false);
connection.setRequestMethod("POST");
connection.setRequestProperty("Content-Type","application/octet-stream");
```

…

2 Előfeltételek

Ez a fejezet leírja a *FIRA Elektronikus Aláírás Termék* üzemeltetéséhez szükséges informatikai környezeti előfeltételeket.

2.1 Az informatikai környezetre vonatkozó követelmények

2.1.1 Hardver

- bármely hardver, amelyhez Java futtató környezet rendelkezésre áll

2.1.2 Operációs rendszer

- bármely operációs rendszer, amelyhez Java futtató környezet rendelkezésre áll
- minden aláíró külön bejelentkezési nevet kell, hogy használjon

Figyelmeztetés: egy számítógépen egy adott felhasználói névvel bejelentkezve, a FIRA-nak egy példánya, egy aláíró részére használható. A FIRA az első futáskor létrehoz egy könyvtárat, amelyben a beállításokat, adatokat tárolja. Ez a könyvtár a következő: *{felhasználó alapkönyvtára}/.fira*, ahol a *{felhasználó alapkönyvtára}* a felhasználó alap könyvtárát jelenti az adott számítógépen. Ez Windows környezetben pl. c:/Documents and Settings/Rendszergazda, Linux környezetben pl. /home/username. Ebből következően, ha ugyanazon a számítógépen ugyanazon felhasználói névvel bejelentkezve, egy újabb aláíró kezdi meg a FIRA használatát, akkor az eredeti beállítások, adatok felülírásra kerülnek.

2.1.3 Java környezet

- 1.5.0 vagy magasabb verzió számú Java futtató környezet

2.1.4 Web szerver

Amennyiben a *FIRA Elektronikus Aláírás Termék* web alkalmazásként (Java applet/Java WebStart alkalmazás) kerül majd felhasználásra, az üzembe helyezéséhez szükséges egy olyan web szerver, amely alkalmas Java appletek, valamint Java WebStart alkalmazások hosztolásához. Javasolt az Apache Tomcat használata, amely a http://tomcat.apache.org címről letölthető.

2.1.5 Ant telepítése

Amennyiben a *FIRA Elektronikus Aláírás Termék* web alkalmazásként (Java applet/Java WebStart alkalmazás) kerül majd felhasználásra, a web alkalmazás elkészítéséhez az Ant segédeszköz szükséges, amely a http://ant.apache.org/ címről letölthető. Legalább 1.6.0 verzió szükséges.

2.1.6 További követelmények

- aláíró kulcs és tanúsítvány rendelkezésre állása PKCS#12 formátumú fájlban vagy PKCS#11 szabványt támogató ALE/BALE kriptográfiai eszközben
- kriptográfiai eszköz meghajtók (kártyaolvasó driver, smartcard driver) megfelelően telepítettek és megfelelően működnek
- kriptográfiai eszköz PKCS#11 interfésze engedélyezett és az megfelelően működik

3 FIRA készlet telepítése

Ez a fejezet lépésenként leírja a FIRA készlet telepítését.

A jelen dokumentumban szereplő konkrét példák a Windows operációs rendszerre vonatkoznak. Más operációs rendszer használata esetén a megadott példákat értelemszerűen módosítani kell, az adott operációs rendszernek megfelelően. A példák módosításához az adott operációs rendszer általános adminisztrátori ismerete elégséges.

3.1 Telepítéshez szükséges fájl

A telepítéshez a következő fájl szükséges:

- *fira-{verziószám}.zip,* ahol a verziószám pl. 1_0_0

3.1.1 *fira-{verziószám}.zip* fájl kifejtése

A *fira-{verziószám}.zip* fájl a tartalmazza a *FIRA Elektronikus Aláírás Termék* üzembe helyezéséhez szükséges fájlokat, valamit a *FIRA indítópult* segédprogramot.

A fájl kifejtéséhez használja az adott operációs rendszer megfelelő segédprogramját.
Jelen dokumentum feltételezi, hogy a kifejtés a következő könyvtárba történik:

c:\FIRA

A kifejtés után a következő könyvtárszerkezet jön létre:

doc	dokumentáció
src	*FIRA indítópult* segédprogram forrása
test	teszteléshez: aláírható XML fájlok, XSL fájl
trial	teszteléshez: kulcstároló, tanúsítvány, licenc
web	webes alkalmazáshoz fájlok
build.xml	Ant script
fira.jar	*FIRA Elektronikus Aláírás Termék* jar fájl
fira2.jar	*FIRA Elektronikus Aláírás Termék* jar fájl
firastarter.jar	*FIRA indítópult* segédprogram jar fájl
serializer.jar	Apache Serializer 2.7.1
xalan.jar	Apache Xalan 2.7.1
xercesImpl.jar	Apache Xerces 2.9.0

Megjegyzés: a jar fájlok mindegyikét a Polysys egy olyan megfelelő elektronikus aláírással ellátta, amely biztosítja megbízható Java appletként és Java WebStart alkalmazásként való futtathatóságot.

Megjegyzés: a *xalan.jar* és *xercesImpl.jar* használata erősen javasolt, mivel a Java futtató környezetekben ezekből rendelkezésre álló, előtelepített változatok verziója túlságosan régi.

3.1.1.1 A doc könyvtár

A *doc* könyvtár tartalmazza jelen dokumentumot.

3.1.1.2 Az src könyvtár

Az *src* könyvtár tartalmazza a *FIRA indítópult* segédprogram forrását: *FIRAStarter.java*. Ennek tanulmányozása azoknak a fejlesztőknek a számára hasznos és javasolt, akik a FIRA-t integrálni szeretnék meglevő, GUI felülettel rendelkező, általuk fejlesztett Java alkalmazásba.

A forráskód bemutatja az 1.6, FIRA integrációja Java alkalmazásba fejezetben leírt lépések megvalósítását.

3.1.1.3 A test könyvtár

A *test* könyvtár tartalmazza a *FIRA Elektronikus Aláírás Termék* kipróbálása során aláírható XML és XSL fájlokat tartalmaz.

2. táblázat: A test könyvtár tartalma

fájlnév	leírás
order.xml	megrendelést tartalmazó XML fálj
order.xsl	az *order.xml* formázásához alkalmas XSL fájl
OSZE_001-1.xml	példa adatszolgáltatást tartalmazó XML fájl

3.1.1.4 A trial könyvtár

A *trial* könyvtár tartalmazza a *FIRA Elektronikus Aláírás Termék* kipróbálásához alkalmas a teszt aláírói tanúsítványt és kulcstárolót, valamint a teszt aláíró tanúsítványhoz tartozó licenc fájlt.

3. táblázat: A trial könyvtár tartalma

fájlnév	leírás
test.cer	teszt aláíró tanúsítvány
test.pfx	a *test.cer* aláíró tanúsítványt és ahhoz tartozó magánkulcsot tartalmazó kulcstároló (PKCS#12) fájl
a2-licence.xml	a *test.cer* tanúsítványhoz tartozó licenc fájl

Megjegyzés: a *test.pfx* kulcstároló jelszava: 12345. A teszt aláírói tanúsítvánnyal történő kipróbáláshoz az alkalmazás indítása előtt a *trial* könyvtárban található *a2-licence.xml* licenc fájlt be kell másolni a FIRA konfigurációs könyvtárába, amely a következő: *{felhasználó alapkönyvtára}/.fira,* ahol a *{felhasználó alapkönyvtára}* a felhasználó alap könyvtárát jelenti az adott számítógépen. Ez Windows környezetben pl. c:/Documents and Settings/Rendszergazda, Linux környezetben pl. /home/username.

3.1.1.5 A web könyvtár

A *web* könyvtár tartalmazza azokat a html, jnlp és kép fájlokat, amelyek a web alkalmazás elkészítéséhez szükségesek.

3.1.1.6 További fájlok

build.xml
Egy Ant script, amely támogatja a FIRA web alkalmazásnak egy adott cél környezetben történő bevetését.

fira.jar

FIRA Elektronikus Aláírás Termék futtatható jar fájl, Polysys által aláírva.

fira2.jar
FIRA Elektronikus Aláírás Termék futásához szükséges jar fájl, Polysys által aláírva.

firastarter.jar
FIRA indítópult segédprogram futtatható jar fájl, Polysys által aláírva.

serializer.jar
FIRA Elektronikus Aláírás Termék futásához szükséges Apache Serializer 2.7.1, Polysys által aláírva.

xalan.jar
FIRA Elektronikus Aláírás Termék futásához szükséges Apache Xalan 2.7.1, Polysys által aláírva.

xercesImpl.jar
FIRA Elektronikus Aláírás Termék futásához szükséges Apache Xerces 2.9.0, Polysys által aláírva.

4 FIRA indítópult segédprogram

A *FIRA indítópult* egy segédprogram, amelynek célja, hogy az üzemeltetőket, fejlesztőket támogassa a FIRA üzembe helyezését megelőző és kísérő tevékenységekben.

Használható a FIRA megfelelő paraméterezésének kialakításában, az indító html vagy jnlp fájl elkészítéséhez.

A *FIRA indítópult* egyben egy FIRA-t integráló Java alkalmazás, amely forráskódban rendelkezésre áll.

4.1 A segédprogram futtatása

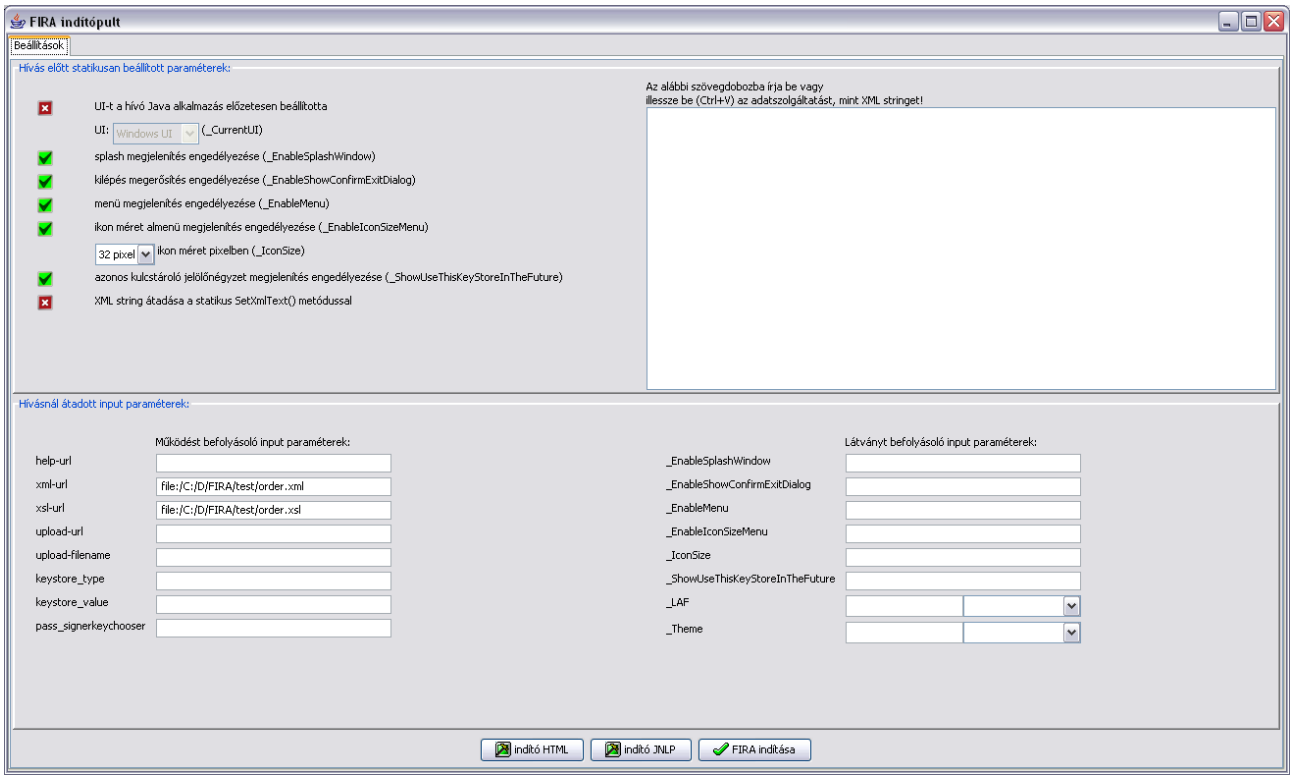
A *FIRA indítópult* segédprogram futtatásához szükséges a 2. és 3. fejezetben leírt előkészületek elvégzése.

A futtatás több módon történhet:

- parancssorból:
  1. parancssor vagy konzol nyitása
  2. a *c:\FIRA* könyvtár legyen az aktuális könyvtár.
  3. a következő parancs kiadása:
     java –jar firastarter.jar
- fájl böngészőből a *firastarter.jar* fájlon történő dupla kattintással

4.2 A segédprogram használata

A képernyő felső részén a FIRA-t integráló Java alkalmazások számára rendelkezésre álló beállítási és paraméterátadási lehetőségek láthatók:



A beállítási lehetőségeket részletesen az 1.6.1 fejezet ismerteti.

Megjegyzés: a *_CurrentUI* legördülő lista engedélyezéséhez be kell kattintani az „*UI-t a hívó Java alkalmazás előzetesen beállította”* jelölőnégyzetet, a bal oldalon látható szövegdoboz szerkeszthetőségéhez be kell kattintani az „*XML string átadása a statikus SetXmlText() metódussal*” jelölőnégyzetet.

A képernyő alsó részén az összes alkalmazási lehetőség esetére rendelkezésre álló input paraméterek állíthatók be, amelyeket részletesen az 1.5 fejezet ismertet.

Megjegyzés: a *_LAF* és *_Theme* input paraméter választható legördülő listából, vagy beírható szövegesen. A legördülő listában a vizuális azonosítást segítő téma megnevezések magyarul szerepelnek, azonban a szöveg mezőben az angol megnevezést kell megadni, az 1. táblázat: Témák táblázat szerint.

Megjegyzés: csak a „Metal” és a „Kunststoff” látvány támogatja a vizuális témák használatát, a többi látvány esetében a *_Theme* paraméter nem lesz figyelembe véve.

FIRA indítása nyomógomb:

A *Hívás előtt statikusan beállított paraméterek* szekcióban és a *Hívásnál átadott input paraméterek* szekcióban beállított értékekkel elindítja a *FIRA Elektronikus Aláírás Termék*t. Megjelenik egy újabb fül, amelyen a FIRA látható és fut, teljes értékűen.

indító JNLP nyomógomb:

A *Hívás előtt statikusan beállított paraméterek* szekcióban és a *Hívásnál átadott input paraméterek* szekcióban beállított értékekkel elkészíti a Java WebStart JNLP fájl tartalmát, amelyet egy szerkeszthető szövegdobozban jelenít meg.
A *codebase* a http://localhost:8080/fira értékkel kerül kitöltésre, azonban az átírható az adott környezetben szükséges címre.
A *mentés* nyomógombbal a JNLP fájl tetszőleges helyre menthető.
Tipp: a JNLP indítás web szerver nélkül is kipróbálható, a *codebase*-ben file:////c://FIRA érték megadásával (feltételezve, hogy a FIRA készlet telepítési helye*: c:/FIRA*).

indító HTML nyomógomb:

A *Hívás előtt statikusan beállított paraméterek* szekcióban és a *Hívásnál átadott input paraméterek* szekcióban beállított értékekkel elkészíti az applet indító HTML fájl tartalmát, amelyet egy szerkeszthető szövegdobozban jelenít meg.
A *mentés* nyomógombbal a HTML fájl tetszőleges helyre menthető.
Tipp: a HTML fájlt a lokális gépen célszerű a *c:/FIRA* könyvtárba menteni, vagy a szövegdobozban a HTML tartalom szabadon szerkeszthető.

FIRA fül:

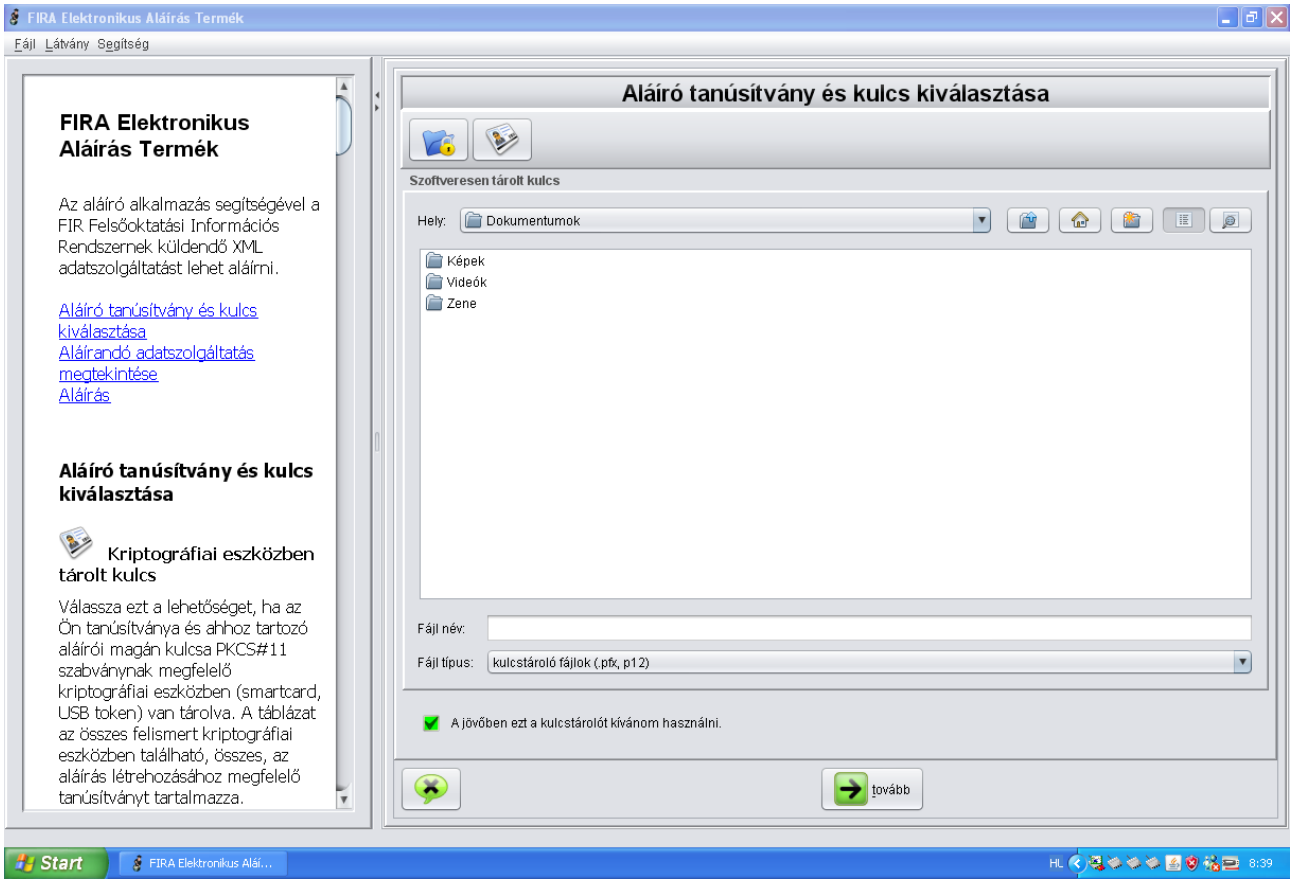
Erre a fülre kattintva a FIRA teljes értékűen használható, kipróbálható, részletesen lásd az 5. fejezetben.

5 FIRA kipróbálása

Egy számítógépen, egy adott felhasználói névvel bejelentkezve, a FIRA-nak egy példánya, egy aláíró részére használható. A FIRA az első futáskor létrehoz egy könyvtárat, amelyben a beállításokat, adatokat tárolja. Ez a könyvtár a következő: *{felhasználó alapkönyvtára}/.fira*, ahol a *{felhasználó alapkönyvtára}* a felhasználó alap könyvtárát jelenti az adott számítógépen. Ez Windows környezetben pl. c:/Documents and Settings/Rendszergazda, Linux környezetben pl. /home/username. Ebből következően, ha ugyanazon a számítógépen ugyanazon felhasználói névvel bejelentkezve, egy újabb aláíró kezdi meg a FIRA használatát, akkor az eredeti beállítások, adatok felülírásra kerülnek.

A FIRA telepítőkészlet tartalmaz egy, a kipróbáláshoz alkalmas teszt aláírói tanúsítványt és kulcstárolót, valamint a teszt aláíró tanúsítványhoz tartozó licenc fájlt, lásd részletesen a 3.1.1.4 fejezetben. A teszt aláíró tanúsítvány használatához, az alkalmazás indítása előtt, a telepítőkészlet a *trial* könyvtárban található *a2-licence.xml* licenc fájlt be kell másolni a FIRA konfigurációs könyvtárába.

5.1 Aláíró tanúsítvány és kulcs kiválasztása



Ezen a képernyőn lehet kiválasztani az aláírás létrehozásához használni kívánt tanúsítványt tartalmazó kulcstárolót.

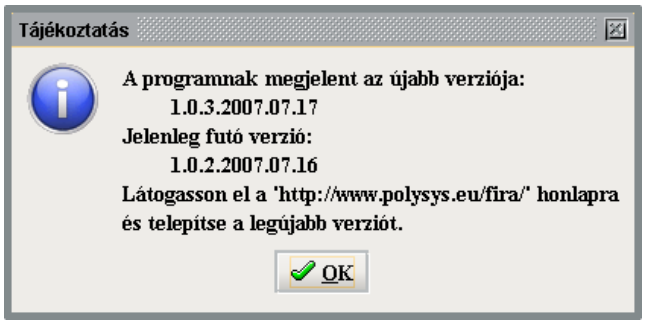
A kipróbáláshoz a *fájl* lehetőséget kell választani, majd a gombra kattintva megjelenő fájl választó ablakban a FIRA telepítési könyvtár *trial* alkönyvtárából a *test.pfx* fájlt kiválasztani.
A teszt aláíró tanúsítvány használatához szükséges teendőket az 5. fejezet írja le.

A végfelhasználó környezetben ezen a képernyőn a *kriptográfiai eszköz* lehetőséget kell választani, majd a megjelenő legördülő listából a megfelelő kriptográfiai eszközt (a *FIRA Elektronikus Aláírás Termék* alkalmazás környezetében általában: Axalto).

A kiválasztott kulcstárolót a FIRA megjegyzi, és a következő futásnál ki fogja ajánlani.

Amennyiben az „*A jövőben ezt a kulcstároló kívánom használni*” jelölőnégyzet megjelenése engedélyezett, és az be van kattintva, akkor a FIRA a következő futásnál megkísérli a most megadott adatokkal a kulcstároló automatikus kiválasztását, és ennek a képernyőnek az automatikus átlépését. A következő futások során, ha mégis szükség lenne eltérő kulcstároló kiválasztására, akkor a képernyő alján látható „*vissza*” nyomógomb többszöri megnyomásával vissza lehet lépni erre a képernyőre, és más kulcstárolót választani.

Amennyiben a FIRA-t futtató számítógép Internet eléréssel rendelkezik, ellenőrzi, hogy van-e futó verziónál újabb, elérhető verzió publikálva a www.polysys.eu/fira honpalon. Újabb verzió megléte esetén egy figyelmeztető ablak jelenik meg.

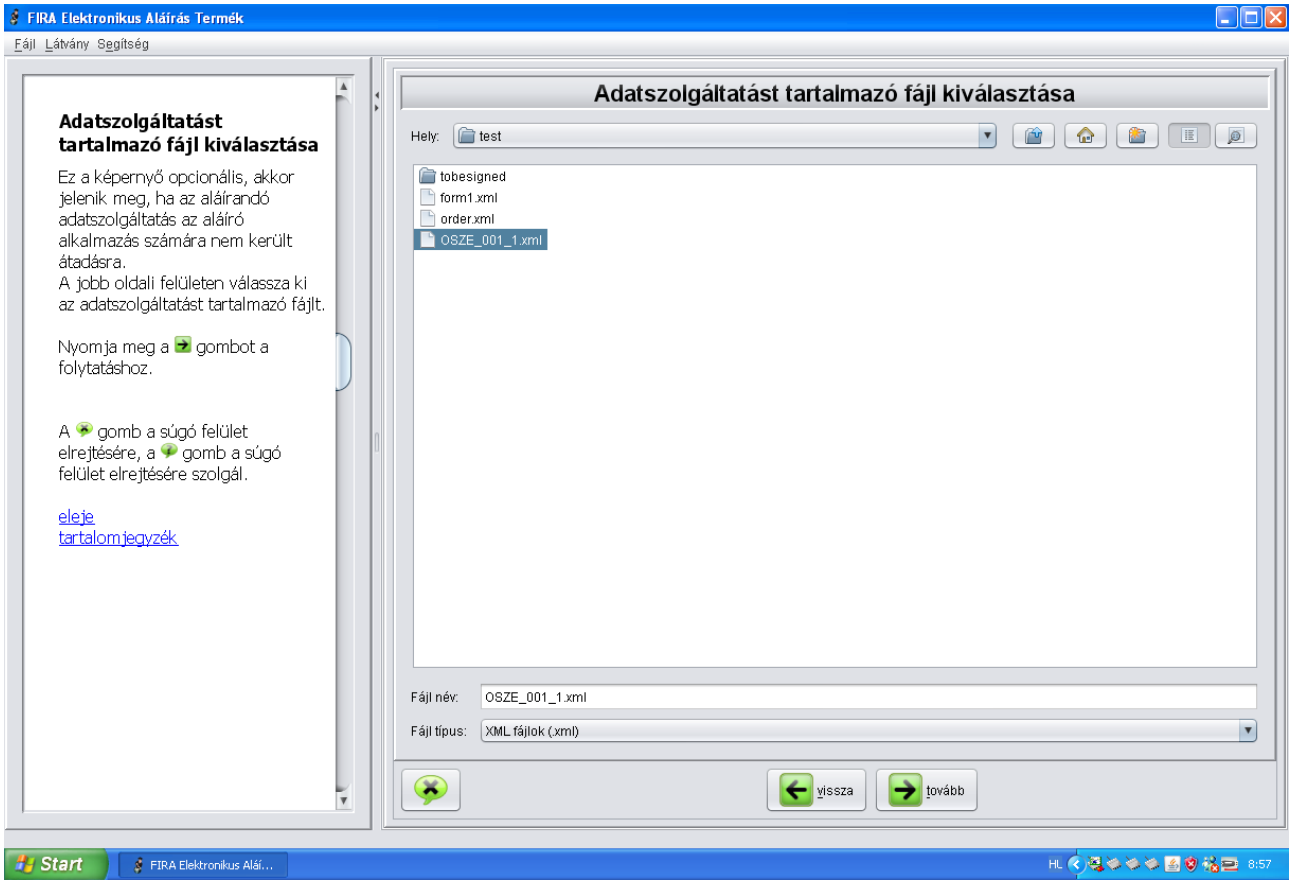


Ez akkor fordulhat elő, ha a FIRA nem közvetlenül az Internet-ről, hanem pl. egy Java alkalmazásba integrálva került felhasználásra.

Azoknak a felhasználóknak a számára, akik a FIRA-t Java WebStart technológiával, közvetlenül az Internetről használják, a verziófrissítés teljesen automatikus.

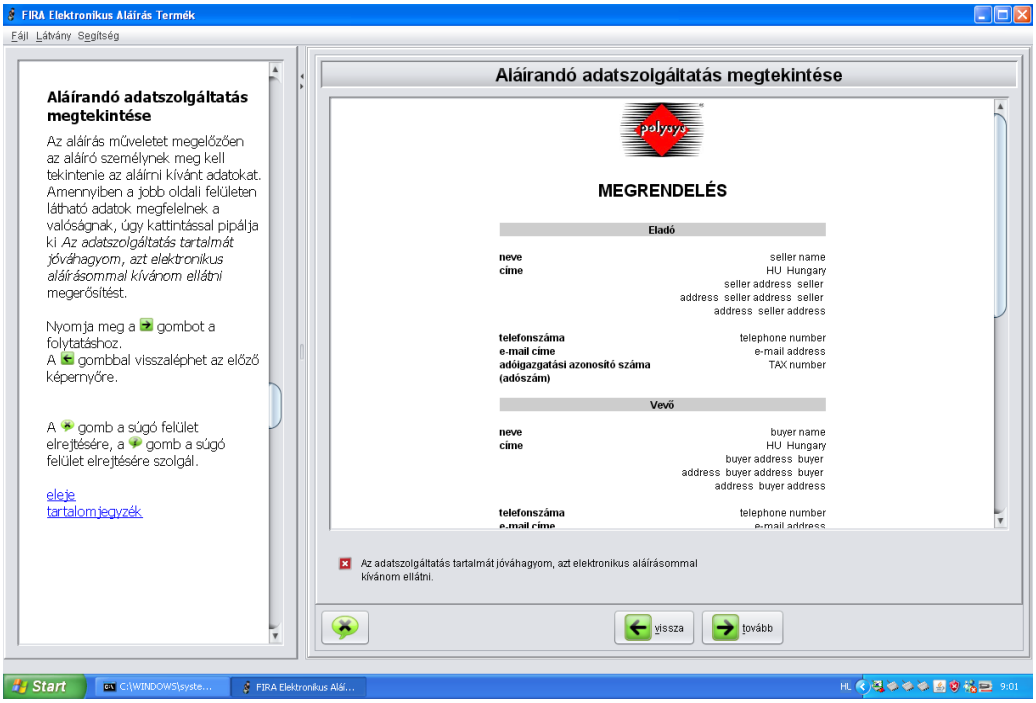
5.2 Adatszolgáltatást tartalmazó fájl kiválasztása

Ez a képernyő opcionálisan akkor jelenik meg, ha a FIRA számára nem került hívásnál átadásra az aláírandó XML adat:



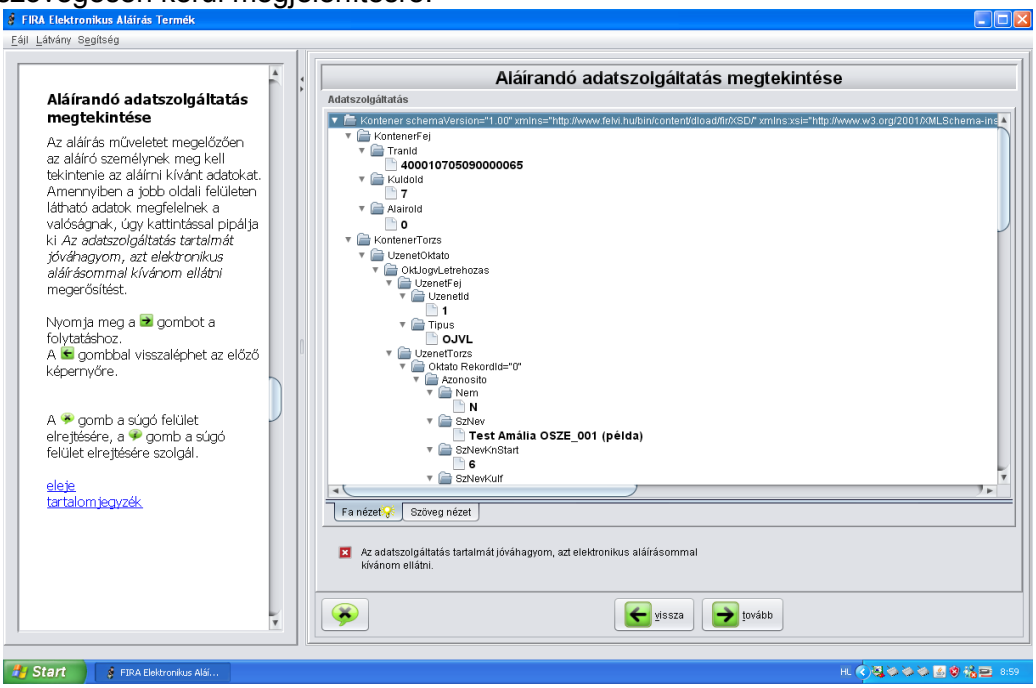
A képernyőn ki kell választani az adatszolgáltatást tartalmazó fájlt.

5.3 Aláírandó adatszolgáltatás megtekintése



Megjegyzés: a képernyő azt szemlélteti, hogy ha formázáshoz az *xsl-url* input paraméter megadása megtörtént, akkor az aláíró „ehető” formában látja az aláírandó adatokat.

Ha a formázott megjelenítéshez XSL nem áll rendelkezésre, az aláírandó adatszolgáltatás XML fában és szövegesen kerül megjelenítésre:



Az aláírás létrehozását meg kell erősíteni a folytatáshoz.

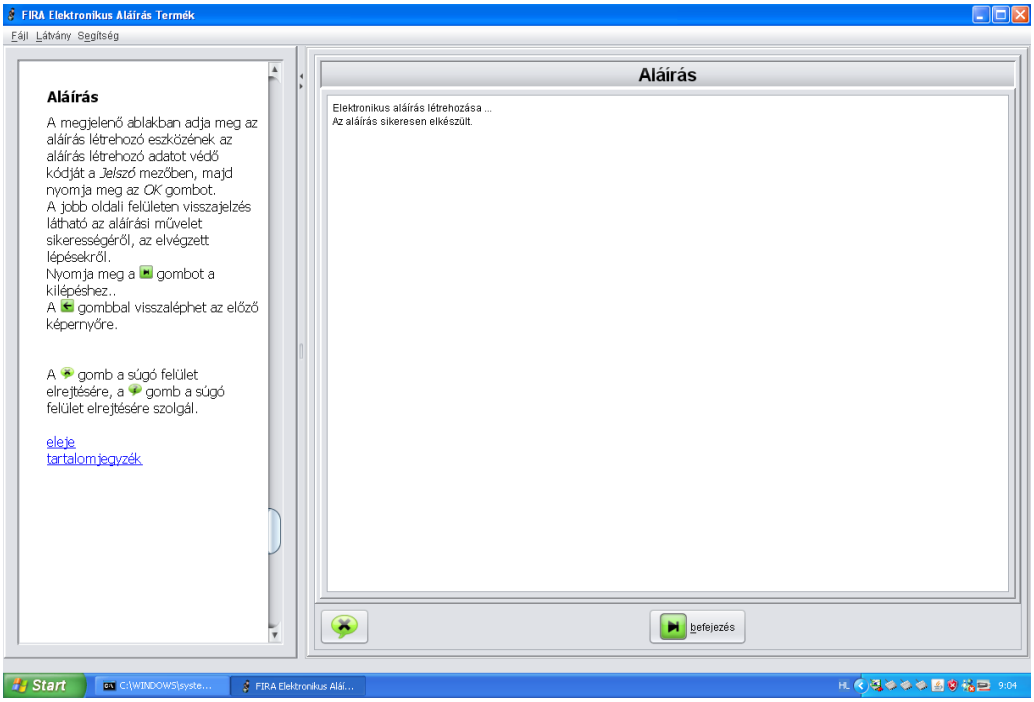
5.4 Aláírás

Erre a képernyőre továbblépve, a FIRA bejelentkezteti az aláírót a választott kulcstárolóhoz:

FIGYELEM: - a jelszó mezőben kriptográfiai eszköz (pl. Axalto) használata esetén annak PIN kódját, kulcstároló fájl esetén a PKCS#12 fájlnak a jelszavát kell megadni. Kriptográfiai eszköz használata esetén nagy figyelmet kell fordítani a PIN kód helyes megadására, hibás kód többszöri megadása után a kártya zárolt állapotba kerülhet!

Amennyiben licenc fájl nincs még jelen, a FIRA elektronikus aláírást nem hoz létre, hanem tájékoztató képernyőt jelenít meg. Ekkor az 1.3. fejezetben leírtak szerint kell eljárni.

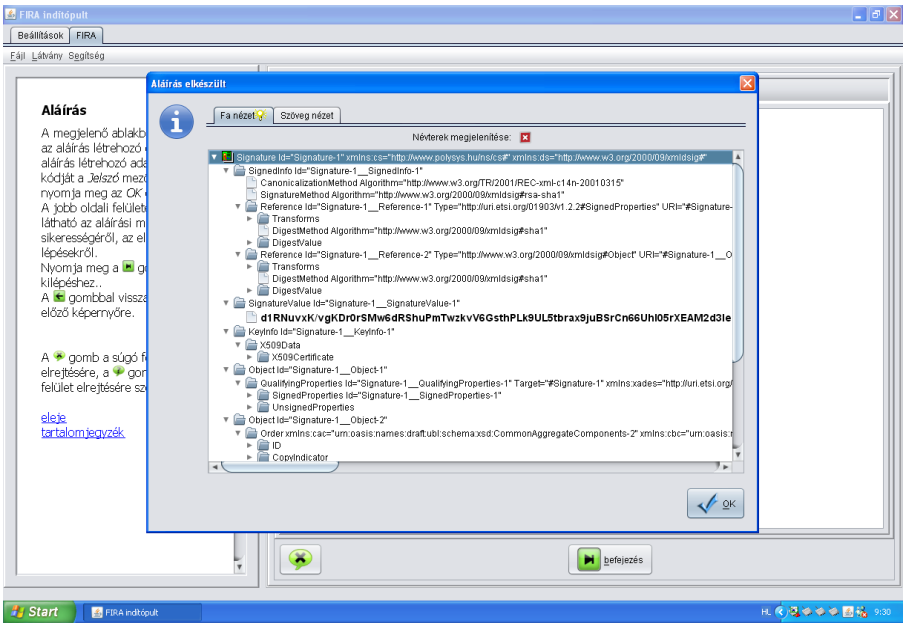
Amennyiben licenc fájl rendben van, akkor a jelszó, PIN kód megadását követően a FIRA létrehozza az elektronikus aláírást, valamint elvégzi az input paraméterezésből következő további lépéseket, fájlba mentés, feltöltés http címre, stb. A jobb oldali részen visszajelzés látható az elvégzett lépésekről.



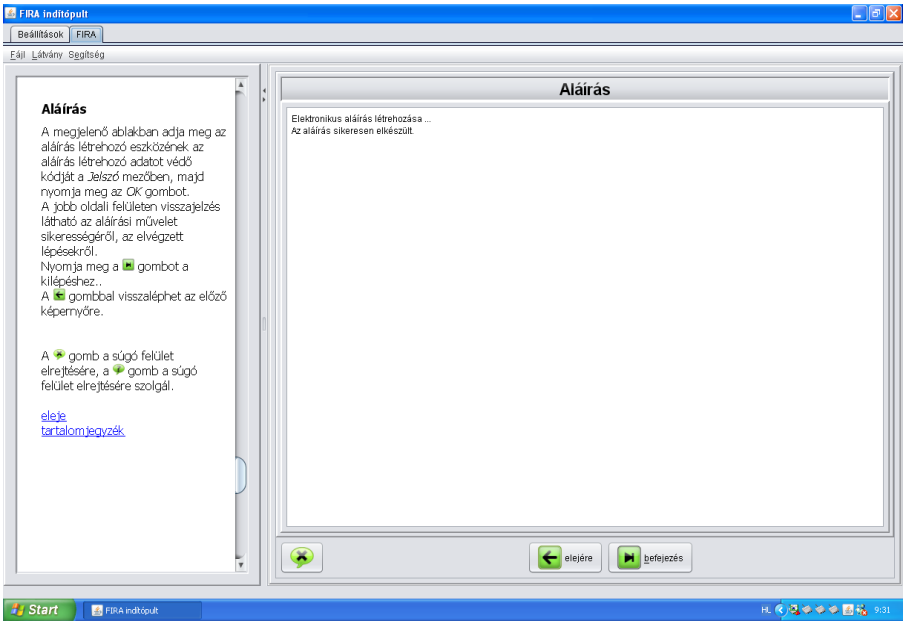
Az elkészített aláírást az input paraméterezéstől függően, de az esetek nagy részében a FIRA a saját könyvtárába elmenti, amely a következő *{felhasználó alapkönyvtára}/.fira/outbox/{időből képzett alkönyvtár név}, XMLSignature.xml* fájl néven.

A befejezés gombra kattintva, a *FIRA* fül eltűnik, ismét a *Beállítások* fül lesz aktív.

Az elektronikus aláírás létrejöttének pillanatában, a *FIRA indítópult* környezetben megjelenik a kész aláírást megjelenítő ablak, az *addXmlSignatureReadyListener* működését bemutatva:



Amennyiben a FIRA számára a hívásnál nem került átadásra az aláírandó adat (az *xml-url* paraméterrel), akkor az aláírás elkészülte után a „befejezés” gomb mellett megjelenik az „elejére” nyomógomb, amelyre kattintva lehetőség nyílik egy FIRA indítással több adatszolgáltatás egymás utáni aláírására:



6 FIRA, mint web alkalmazás üzembe helyezése

6.1.1 Előkészítés

A web címet, amelyen az alkalmazás látható lesz, a *build.xml* WEB_ROOT paraméterével kell beállítani.

6.1.2 Üzembe helyezés lépései

A web alkalmazás war elkészítése a build scripttel történik. Az alkalmazás üzemeltetési környezetével kapcsolatos beállítások a build scripttel és konfigurációs fájlokkal kerülnek elvégzésre. A *web* könyvtárban több sablon fájl található*: index_.html, web_.xml,*stb.. Ezekben a fájlokban a @ karakterrel határolt részek behelyettesítését a build script végzi el, a build scriptben beállított értékek szerint.

1. A *build.xml* scriptben a WEB_ROOT paraméter beállítása.
2. JAVA_HOME, ANT_HOME környezeti változók beállítása.
3. A A *web* könyvtárban található sablonok értelemszerű módosítása, szükség esetén.
4. A következő parancs kiadása:
   ant build
   Ez a target elkészíti a web alkalmazást tartalmazó war fájlt, amely a *dist* könyvtárban jön létre, neve: *fira.war*.
5. War deployment a használt konténer dokumentációjában leírtak szerint.

A deployment eljárást követően, a FIRA akár mint Java Web Start alkalmazás, akár mint Java applet, használható.

7 FIRA, mint helyi gépen futó Java alkalmazás üzembe helyezése

Azoknál az alkalmazási környezeknél, ahol web szerver nem áll rendelkezésre, vagy más okból kifolyólag a lokális telepítés és futtatás mellett döntenek, a FIRA a következő módon futtatható:

1. Egy tetszőleges könyvtárba fel kell másolni az alábbi fájlokat:
   fira.jar
   fira2.jar
   serializer.jar
   xalan.jar
   xercesImpl.jar
2. A következő parancs kiadása:
   java –jar fira.jar
3. Parancsikon asztalra, Start menübe, a fenti információk alapján szintén elkészíthető.

Figyelem: egy számítógépen egy adott felhasználói névvel bejelentkezve, a FIRA-nak egy példánya, egy aláíró részére használható. A FIRA az első futáskor létrehoz egy könyvtárat, amelyben a beállításokat, adatokat tárolja. Ez a könyvtár a következő: *{felhasználó alapkönyvtára}/.fira*, ahol a *{felhasználó alapkönyvtára}* a felhasználó alap könyvtárát jelenti az adott számítógépen. Ez Windows környezetben pl. c:/Documents and Settings/Rendszergazda, Linux környezetben pl. /home/username. Ebből következően, ha ugyanazon a számítógépen ugyanazon felhasználói névvel bejelentkezve, egy újabb aláíró kezdi meg a FIRA használatát, akkor az eredeti beállítások, adatok felülírásra kerülnek.

8 Tanúsítványok, kriptográfiai eszközök kezelése, hibaelhárítása

8.1 Aláírói tanúsítvány

Végfelhasználói környezetben „éles” tanúsítvány szükséges az adatszolgáltatás aláírásához, amely az Educatio-tól beszerzett tanúsítvány, vagy bármely piaci hitelesítés szolgáltatótól beszerzett, úgynevezett közigazgatási tanúsítvány lehet. A http://www.kgyhsz.gov.hu honlapon található azoknak a hitelesítés szolgáltatóknak és tanúsítvány osztályoknak a felsorolása, melyek közigazgatási tanúsítványt adnak ki.

Figyelmeztetés:- A FIRA kipróbálását és üzembe helyezését követően ne használja a telepítőkészletben található teszt tanúsítványt adatszolgáltatás aláírására!

A hitelesítés szolgáltató a fokozott biztonságú, vagy minősített aláírói tanúsítványt és az ahhoz tartozó aláíró kulcsot általában kriptográfiai eszközre telepítve adja át az aláíró részére.

8.2 Kriptográfiai eszközök és aláíró kulcsok kezelése

Ahhoz, hogy a FIRA a kriptográfiai eszközre telepített aláíró kulcsot és tanúsítványt használni tudja, szükséges, hogy az eszköz meghajtó programjai megfelelően telepítve legyenek és működjenek (kártyaolvasó driver, smartcard driver, stb), valamint az, hogy a kriptográfiai eszköz PKCS#11 interfésze telepített, engedélyezett és megfelelően működőképes legyen.

A kriptográfiai eszközzel kapcsolatos információkat (megnevezés, PKCS#11 interfész, stb) a hitelesítés szolgáltatótól – akitől a tanúsítványt beszerezte – kérdezheti meg.

A FIRA a telepített kriptográfiai eszközök PKCS#11 könyvtárait (DLL) keresi és felismeri, ez alapján tölti ki az *Aláírói tanúsítvány és kulcs választása* képernyőn látható kriptográfiai eszköz lista tartalmát, következőekben részletezett módon.

Az első futásnál a FIRA az alapkönyvtárában elhelyezi a *SmartcardOrTokenTypes.dat* fájlt, amely tartalmazza az egyes kriptográfiai eszközök megnevezését, és a PKCS#11 könyvtárt tartalmazó fájl megnevezését. A PKCS#11 könyvtár DLL fájl általában a c:/WINDOWS/system32 könyvtárban található meg az eszköz telepítését követően. Ennek a listának a tartalmát használja a FIRA ahhoz, hogy megállapítsa, hogy az adott számítógépen milyen kriptográfiai eszközök vannak telepítve.

Tehát, az *Aláírói tanúsítvány és kulcs választása* képernyőn látható listában csak azok a kriptográfiai eszközök jelennek meg, amelyek PKCS#11 könyvtára az adott számítógépen jelen van. Ez még nem jelenti feltétlenül azt, hogy az eszköz megfelelően működik és az aláírás létrehozása sikeres lesz.

A FIRA megvizsgálja az összes felismert, telepített kriptográfiai eszközön jelen levő tanúsítványt, és megállapítja, hogy van-e megfelelő, aláírás célú tanúsítvány. Ha egy sincs, akkor az aláíráshoz választható tanúsítványok táblázata üres. A táblázat megfelelő sorára kattintással kell kijelölni az aláíráshoz használni kívánt tanúsítványt. A táblázat alatti panel jelzi vissza a kiválasztott tanúsítvány főbb adatait.

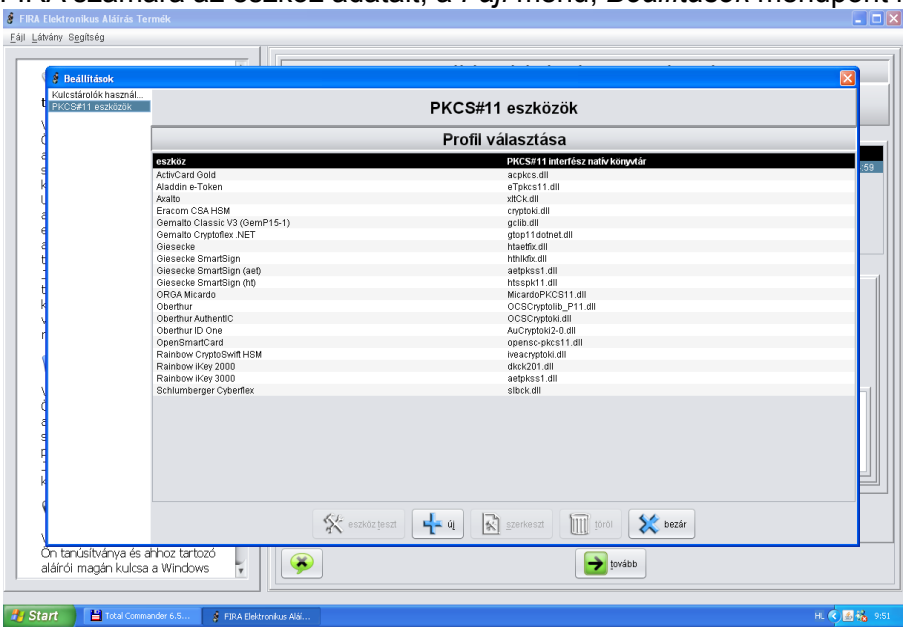
8.2.1 Teendők, ha a kriptográfiai eszközökben talált aláírói tanúsítványok listája üres

1. Érdeklődje meg hitelesítés szolgáltatójától az eszköz és a PKCS#11 interfészt tartalmazó könyvtár pontos megnevezését.

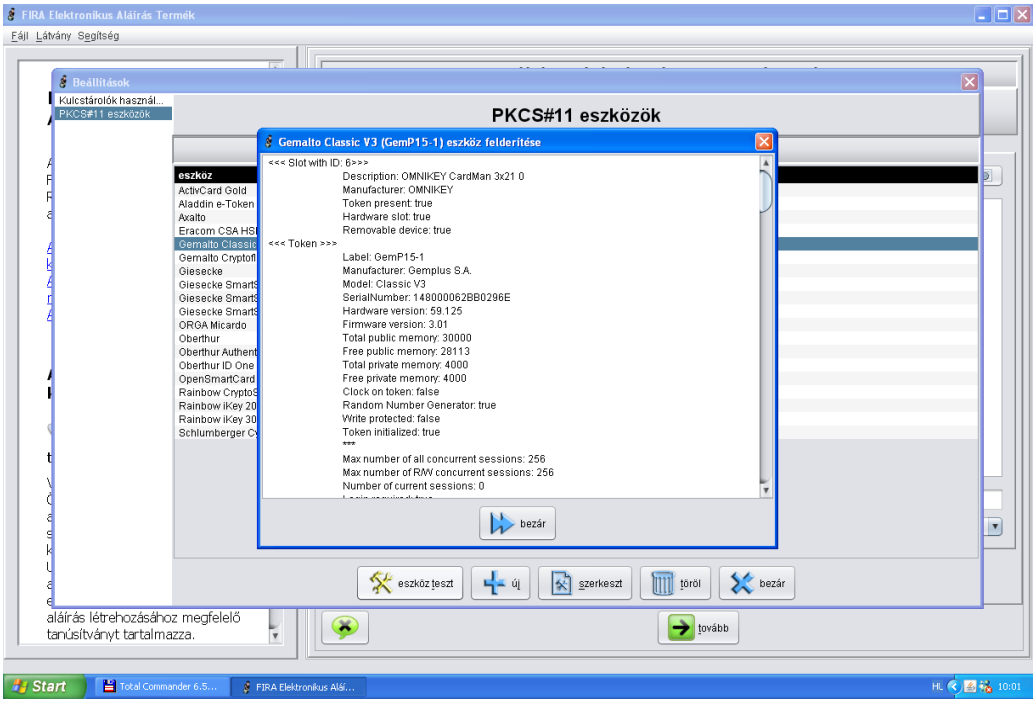
2. Szükség esetén telepítse az eszköz PKCS#11 interfészét.

3. Ha lehetséges, az eszköz valamely segédprogramjával állapítsa meg, hogy az eszköz és annak PKCS#11 interfésze megfelelően működik-e.

4. Adja meg a FIRA számára az eszköz adatait, a *Fájl* menü, *Beállítások* menüpont használatával:



Ha az eszköz szerepel a listán, jelölje ki a táblázatban, majd nyomja meg az *eszköz teszt* gombot.



Ha a szövegdobozban megtalálható a tanúsítvány visszajelzése, akkor az eszköz megfelelően működik.

Ha a táblázatban nem szerepel a kriptográfiai eszköz, akkor vegye azt fel azt az *új* nyomógombbal. Az eszköz nevét, és a PKCS#11 interfészt tartalmazó könyvtár (dll fájl) nevét kell megadni. Általában csak a fájl név megadása elégséges. Az új eszköz megadását követően próbálja ki annak működését, az *eszköz teszt* gombbal. Ha a teszt hibaüzenettel zárul, megpróbálkozhat a PKCS#11 interfészt tartalmazó könyvtár (dll fájl) teljes elérési útvonalának megadásával.

8.2.2 Teendők „nincs jelen közigazgatási, ügyfélhez kapcsolódó aláíró tanúsítvány” hibajelzés esetén

Ez akkor fordulhat elő, ha az eszközön nincs jelen megfelelő tanúsítvány, vagy akkor, ha az eszköz PKCS#11 interfésze nem teljesen működőképes.

Vizsgálja meg az eszköz segédprogramjával, hogy van-e rajta megfelelő tanúsítvány. Csak Educatio által kiadott nem közigazgatási, vagy más hitelesítés szolgáltató által kiadott közigazgatási, aláírás célú tanúsítvány tekinthető megfelelően. Aláírás célú tanúsítványt megtekintve a kulcshasználatban digitális aláírás és/vagy letagadhatatlanság kell, hogy szerepeljen.

Ha nincs jelen megfelelő tanúsítvány, forduljon hitelesítés szolgáltatójához!

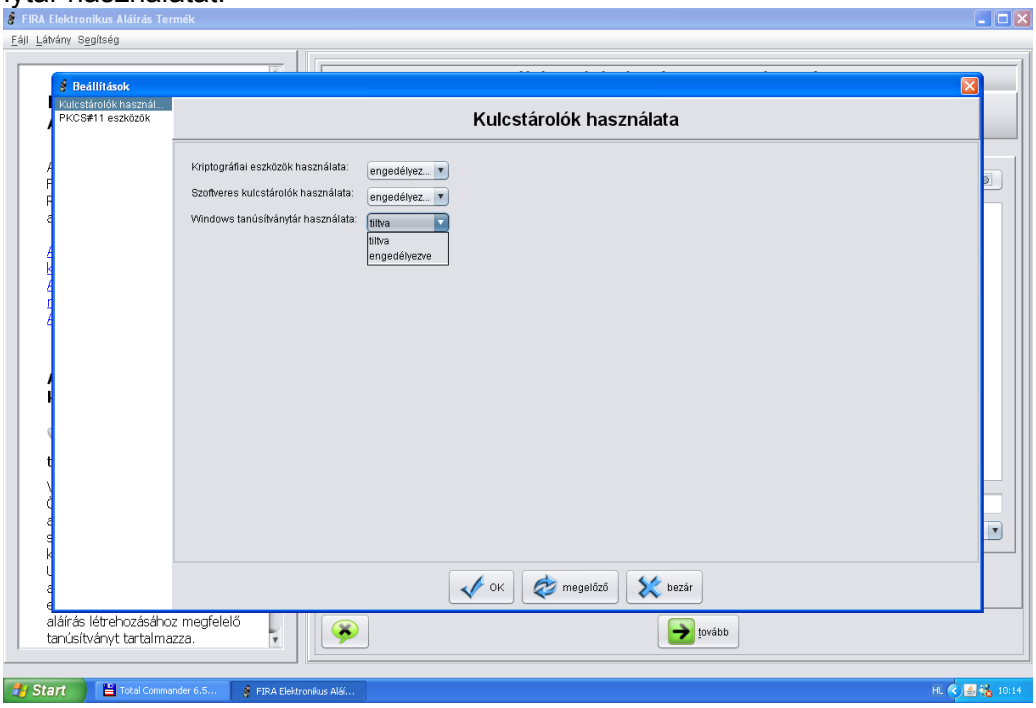
Ha jelen van megfelelő tanúsítvány, akkor:

Érdeklődje meg hitelesítés szolgáltatójától az eszköz és a PKCS#11 interfészt tartalmazó könyvtár pontos megnevezését.

Végezze el az előző fejezetben leírt lépéseket.

Ha ez eddig leírt lépések egyike sem vezetett eredményre, és Windows operációs rendszert használ, akkor megpróbálhatja a kriptográfiai eszközt a Windows tanúsítványtáron keresztül használni. Ehhez végezze el az alábbi lépéseket:

A *Fájl* menü, *Beállítások* menüpont, *Kulcstárolók használata* képernyőn engedélyezze a Windows tanúsítványtár használatát:



Majd nyomja meg az OK gombot. Lépjen ki, és indítja újra a FIRA alkalmazást.

Figyelmeztetések:

- Csak végső esetben engedélyezze a Windows tanúsítványtár használatát! Ha csak lehet, próbálja inkább az eszközt a PKCS#11 interfészen használni, amely sokkal gyorsabb és biztonságosabb működést jelent.
- Ha a Windows tanúsítványtár használata engedélyezett, akkor a FIRA indulása sokkal lassabb, mint akkor, amikor az tiltott volt, akár több percet is igénybe vehet. Ez a Windows operációs rendszer működéséből következő jellegzetesség.
- Ha a Windows tanúsítványtár használata engedélyezett, akkor az eszközben tárolt tanúsítványok csak a Windows tanúsítványtár választással jelennek meg, a kriptográfiai eszközökben tárolt tanúsítványok táblázatban a továbbiakban nem szerepelnek.
- A Windows tanúsítványtár működése vagy nem működése függ az operációs rendszer verziójától, a telepített javító csomagoktól. Előfordulhat, hogy egy újabb Windows frissítés után az addig működő tanúsítvány (aláíró eszköz) a továbbiakban már nem működik.

Táblázatok jegyzéke

1. táblázat: Témák..... 13
2. táblázat: A test könyvtár tartalma..... 20
3. táblázat: A trial könyvtár tartalma..... 20

Hivatkozott dokumentumok

Educatio Kht. EDUAP aláíráspolitika:
http://www.educatio.hu/download/ címen található aktuális aláíráspolitika

Uniform Resource Locators, URL
http://www.ietf.org/rfc/rfc1738.txt

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, PKIX
http://www.ietf.org/rfc/rfc3280.txt
http://www.ietf.org/rfc/rfc2459.txt

Personal Information Exchange Information Standard, PKCS#12
ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12-tc1.pdf

Java Language Specification 2.0
ftp://ftp.javasoft.com/docs/specs/langspec-2.0.pdf

Java Virtual Machine Specification, Second Edition
http://java.sun.com/docs/books/vmspec/2nd-edition/html/VMSpecTOC.doc.html