

BME IK



**Informatikai
Központ**

Elektronikus aláírás-létrehozó alkalmazások együttműködési képessége

Szabó Áron
BME Informatikai Központ

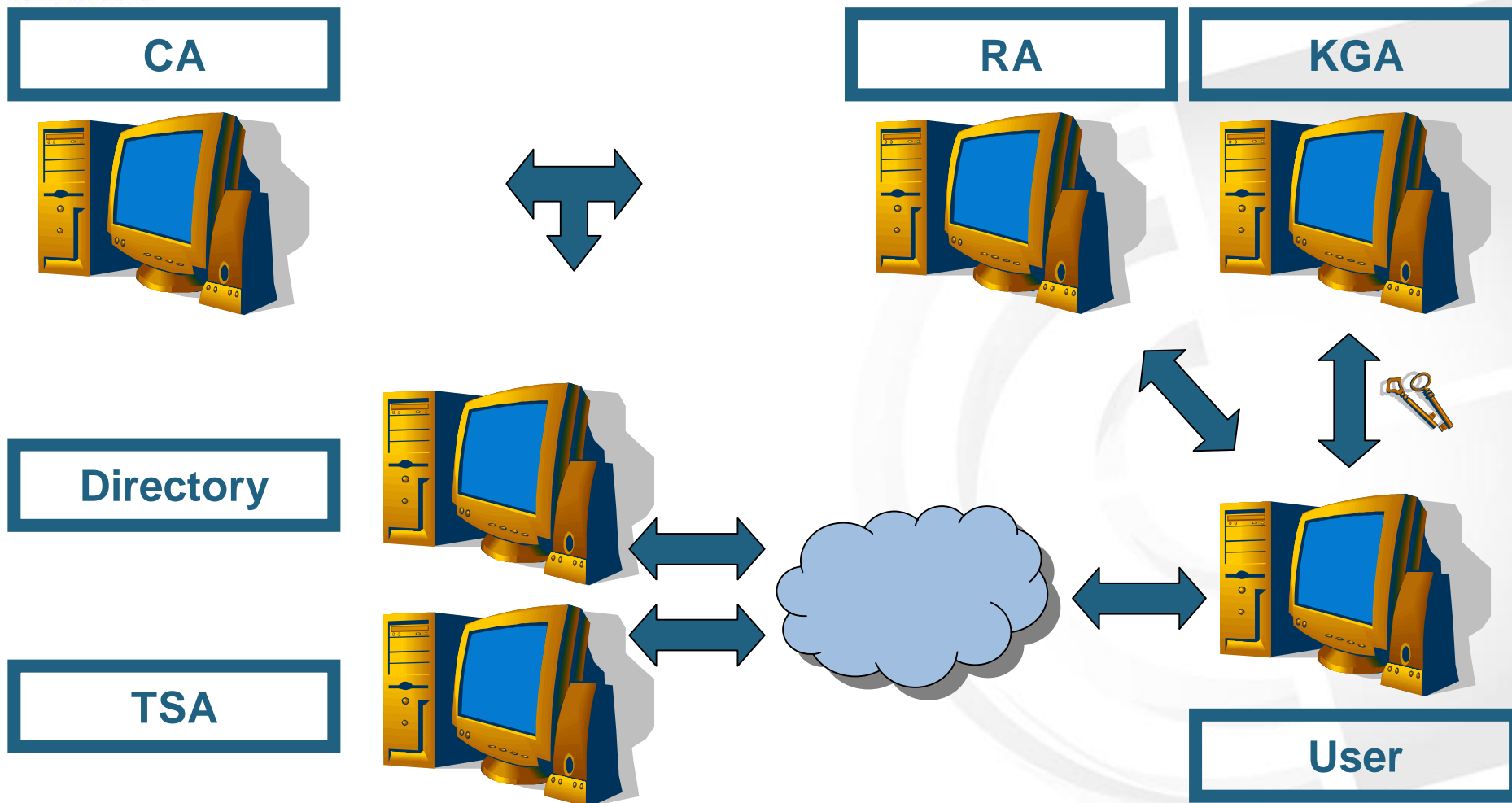
Jogi szabályozás

- a 2001. évi XXXV. törvény az elektronikus aláírásról (1999/93/EC)
- elektronikus adóbevallás (2004. február 1.)
elektronikus számla (2004. május 1.)
elektronikus közjegyző (2004. július 1.)
elektronikus közbeszerzés (2004. július 1.)
elektronikus archiválás (2004. július 14.)
elektronikus magánnyugdíjpénztári tagdíjbevallás (2005. január 1.)
elektronikus cégiratok (2005. január 1.)
- a 2004. évi LV. törvény az elektronikus aláírásról szóló 2001. évi XXXV. törvény módosításáról

Műszaki szabályozás

- **IETF:** S/MIME v3.0 (RFC 2633), S/MIME v3.1 (RFC 3851)
W3C és IETF: XML elektronikus aláírás, XMLDSig (RFC 3275)
ETSI és W3C: XAdES (TS 101 903 v1.2.2)
CEN: követelmények (CWA 14170, CWA 14171)
- pkiC, Bridge-CA, European Bridge-CA, eESC, MELASZ Ready
- együttműködési képesség vizsgálatai a szabványosító szerveknél
XMLDSig: IETF és W3C
XAdES: ETSI

Nyilvános kulcsú infrastruktúra



- alá-fölrendeltségi és mellérendeltségi viszony megteremtése
tanúsítványkérelem: több szabvány
- tanúsítvány kibocsátása
tanúsítvány felépítése: megkülönböztetett név, mezők, kiterjesztések
- intelligens kártyák megszemélyesítése, kulcsok előállítása
kommunikáció: gyártók saját megoldásai
- névtár felépítése, elérése, keresés folyamata
protokoll: IETF szabványok egyszerűbbek, mint az ITU ajánlásai

- PKI megoldások részei
szabvány: gyártók saját megoldásai
- tanúsítvány mezőinek, kiterjesztéseinek értelmezése
ellenőrzés: keyUsage, extKeyUsage, certificatePolicies, cRLDistributionPoints, subject, issuer, validity
- kriptográfiai megoldások kiválasztása
egységesség: legyen egységesen kiválasztott, támogatott (pl. algoritmusoknál SHA-1 és RSA, felépítésnél ETSI TS 101 903 v1.2.2 szabványon alapuló XML elektronikus aláírás)
- fejlesztés során keletkezett, megvalósításban rejlő hibák
szabványértelmezés: szabványban leírtak betartása, szükség esetén szabványok pontosítása

- **IETF és W3C: XML-Signature Interoperability**
<http://www.w3.org/Signature/2001/04/05-xmldsig-interop.html>

W3C XML-Signature Syntax and Processing
IETF RFC 3275

- **ETSI: XML Advanced Electronic Signature**
<http://www.etsi.org/plugtests/>

ETSI TS 101 903 v1.2.2

- **Magyar Elektronikus Aláírás Szövetség: MELASZ Ready**

- fejlesztői levelezőlisták:
kanonizálás, névterek megfelelő használata
- szabványosító szervek vizsgálatai
OCSP válasz beágyazása (**OCSPResponse** üzenet), **TimeStampType** módosítása (**referencedData** tulajdonság), **ArchiveTimeStamp** elemhez kapcsolódó kiegészítés (**Id** tulajdonság, sorrendiség), leírások pontosítása (IETF RFC 2119), **QualifyingProperties** elem kiegészítése, **AnyType** kiegészítése, **CertID** elem kiegészítése, **DataObjectFormat** elem módosítása, **X509SerialNumber** elem értékeinek pontosítása (nagy számok), **X509IssuerName** elem értékeinek pontosítása (megkülönböztetett név IETF RFC 2253 szabvány szerint)

- ingyenes, bárki által hozzáférhető termékek vizsgálata
- **Infomosaic Corporation**
(W3C és IETF XML-Signature Interoperability résztvevője)
SecureXML Digital Signature Toolkit version 2.3.140.40 (SecureXML Digital Signature & Encryption Toolkit) próbaváltozata
- **Sertifitseerimiskeskus**
(ETSI plugtest résztvevője)
OpenXAdES.org ActiveX vezérlője
- **Cladonia Ltd.**
Exchanger XML Editor v3.0 próbaváltozata

XML Signature: Verify Signature - Microsoft Internet Explorer
 [All Spérkesítés gőcöt kedvencelk Csőbőzök gőpő]

http://www.infomosaic.net/2PL/verify.asp

Infomosaic DoD PKI / HIPAA / XML DSIG Compliant
 The Easy to Use Digital Signature

About Us Products Services Solutions Technology Customers Partners Contact Buy Software Try Demo Support

[Infomosaic Announces Success of HITEducation PKI Pilot Phase 2](#) [Download Free SecurSign Reader](#)
[Try SecurWebSign](#)

Trial Home [View Instructions](#)
 Verify XML Signature

Developer Select the signature file to be verified

Downloads E:\SW\Dig_Sig_Viewer\test.xml

Tutorial Click on buttons to verify signature

Licencing

 **Signature Verification Output**

Software made in the U.S.A.

Verification Result	Digital Signature verified successfully 0		
Signature Count	1		
Signature File	E:\SW\Dig_Sig_Viewer\test.xml		
Document Signed	#D0		
Other Objects Signed	Reference	Object	Object Digest Status
	#D0	Signed Reference 0	1
	#S0-SignedProperties	Signed Reference 1	1
Signed By	HU, Budapest, Szabo Aron, Napfogy utca 25, 1016, aron@ik.bme.hu		
Signature Image	No Signature Image Recorded During Signature Creation		
Signed Window Image	No Window Image Recorded During Signature Creation		
Certificate Issuer	Trust&Sign_QCA v1.0		
Certificate Expiration Date	05/05/2005 22:00		
Signature Properties	No Properties Found		

All contents are Copyright © 2000--2004 Infomosaic Corporation. All rights reserved.

XML Signature: Verify Signature - Microsoft Internet Explorer
 [All Spérkesítés gőcöt kedvencelk Csőbőzök gőpő]

http://www.infomosaic.net/2PL/verify.asp

Infomosaic DoD PKI / HIPAA / XML DSIG Compliant
 The Easy to Use Digital Signature

About Us Products Services Solutions Technology Customers Partners Contact Buy Software Try Demo Support

[Infomosaic Announces Success of HITEducation PKI Pilot Phase 2](#) [Download Free SecurSign Reader](#)
[Try SecurWebSign](#)

Trial Home [View Instructions](#)
 Verify XML Signature

Developer Select the signature file to be verified

Downloads E:\SW\Dig_Sig_Viewer\xml.xch

Tutorial Click on buttons to verify signature

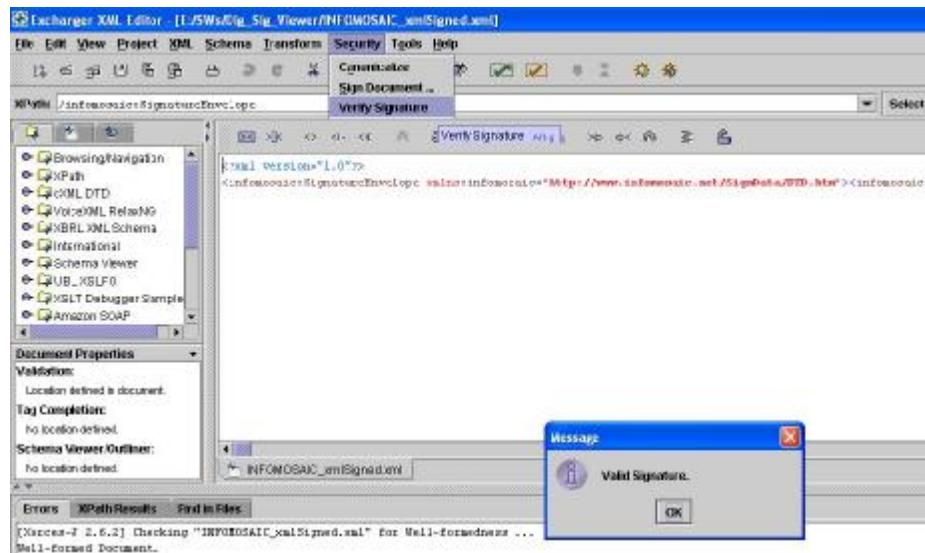
Licencing

 **Signature Verification Output**

Software made in the U.S.A.

Verification Result	Digital Signature verified successfully 0		
Signature Count	1		
Signature File	E:\SW\Dig_Sig_Viewer\xml.xch		
Document Signed	The Signed XML Element		
Other Objects Signed	Reference	Object	Object Digest Status
	The Whole XML	Signed Reference 0	1
Signed By	IE, Cladonia, Development, Exchanger		
Signature Image	No Signature Image Recorded During Signature Creation		
Signed Window Image	No Window Image Recorded During Signature Creation		
Certificate Issuer	Exchanger		
Certificate Expiration Date	05/25/2012 15:51		
Signature Properties	No Properties Found		

All contents are Copyright © 2000--2004 Infomosaic Corporation. All rights reserved.
 Page last updated on Monday, March 15, 2004



Exchange XML Editor - [I:\SWs\Dig_Sig_Viewer\INFO05AIC_xmlSigned.xml]

File Edit View Project XML Schema Transform Security Tools Help

Communication
 Sign Document...
 Verify Signature

XPath: /info:envelope:SignatureEnvelop...
 Verify Signature

```

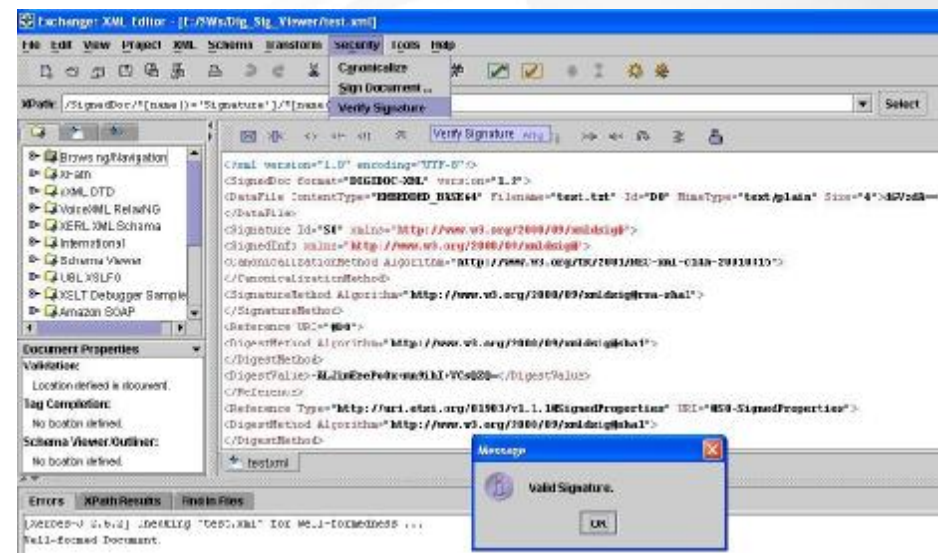
  <?xml version="1.0"?>
  <info:envelope:SignatureEnvelop... value="info:envelope:Sig.../info:envelope:envelope:
  
```

Document Properties
 Validation: Location defined in document.
 Tag Completion: No location defined.
 Schema Viewer Outline: No location defined.

Errors XPath Results Find in Files

[Access-7 2.6.2] Checking "INFO05AIC_xmlSigned.xml" for Well-formedness ...
 Well-formed Document.

Message
 Valid Signature.
 OK



Exchange XML Editor - [I:\SWs\Dig_Sig_Viewer\test.xml]

File Edit View Project XML Schema Transform Security Tools Help

Communication
 Sign Document...
 Verify Signature

XPath: /SignedDoc:/*[name()='Signature']/*[name()='Signature']
 Verify Signature

```

  <?xml version="1.0" encoding="UTF-8"?>
  <SignedDoc format="SIGNDOC-XML" version="1.0">
  <DataFile contentType="BINARY" filename="test.txt" id="DF" mimeType="text/plain" size="4">427cd8...
  </DataFile>
  <Signature id="S1" value="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo value="http://www.w3.org/2000/09/xmldsig#">
  <CanonicalizationMethod algorithm="http://www.w3.org/2001/08/xml-c14n-20010816">
  </CanonicalizationMethod>
  <SignatureMethod algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
  </SignatureMethod>
  <SignatureValue value="http://www.w3.org/2000/09/xmldsig#sha1">
  </SignatureValue>
  </SignedInfo>
  </Signature>
  </SignedDoc>
  
```

Document Properties
 Validation: Location defined in document.
 Tag Completion: No location defined.
 Schema Viewer Outline: No location defined.

Errors XPath Results Find in Files

[Access-7 2.6.2] Checking "test.xml" for Well-formedness ...
 Well-formed Document.

Message
 Valid Signature.
 OK

Köszönöm a figyelmet!



Elérhetőségek

Szabó Áron, M. Sc.
tudományos munkatárs

**Budapesti Műszaki és
Gazdaságtudományi Egyetem
Informatikai Központ**

**1117, Budapest
Magyar tudósok körútja 2.
mobil: (70) 505-4060
e-mail: aron@ik.bme.hu**