BME IK

Informatikai Központ

Elektronikus aláírás-létrehozó alkalmazások együttműködési képessége

Szabó Áron
BME Informatikai Központ

BME IK
Informatikai Központ

Az elmúlt néhány év…

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

Az elmúlt néhány év…

Műszaki szabályozás

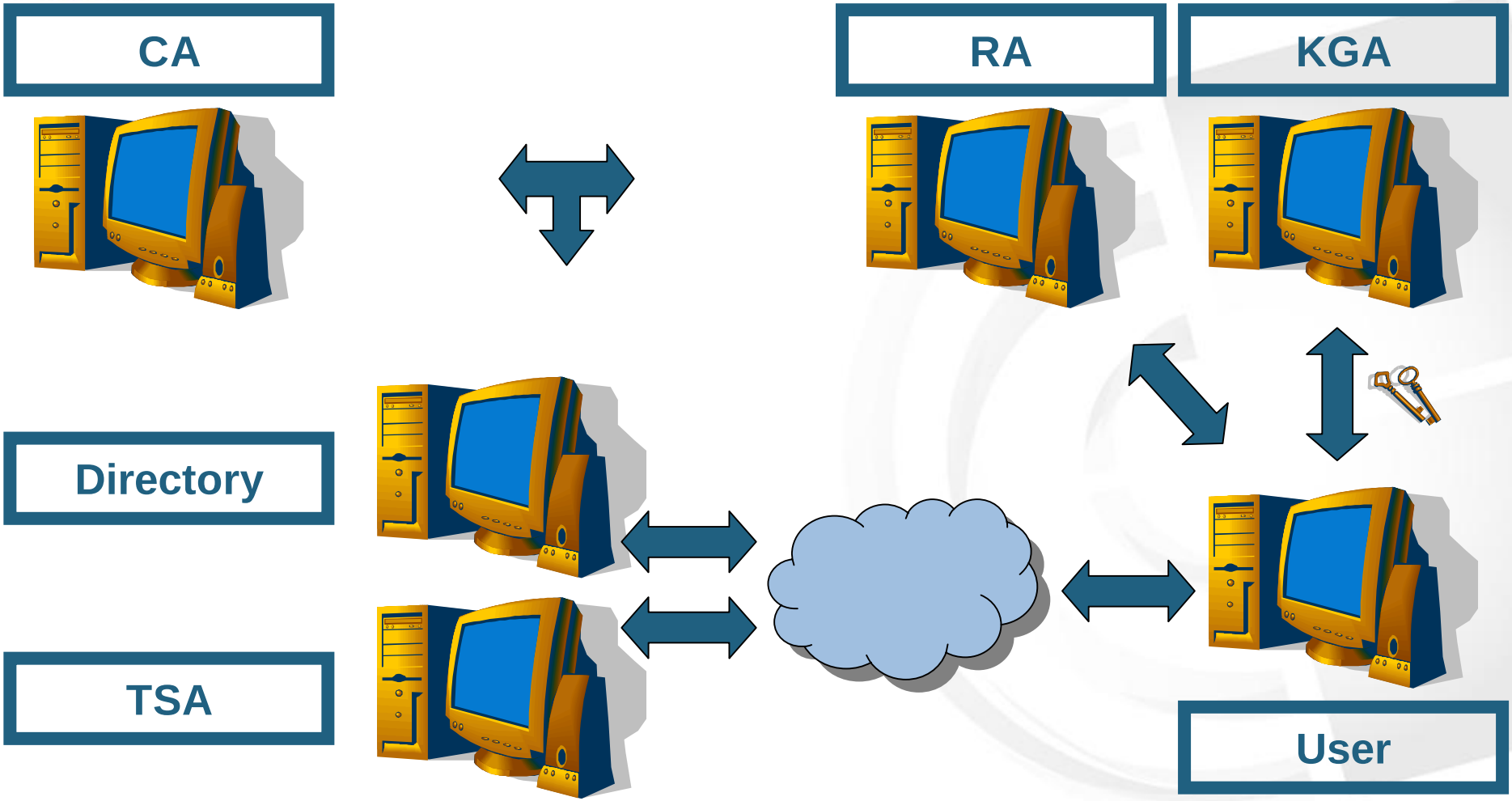
- IETF: S/MIME v3.0 (RFC 2633), S/MIME v3.1 (RFC 3851)
  W3C és IETF: XML elektronikus aláírás, XMLDSig (RFC 3275)
  ETSI és W3C: XAdES (TS 101 903 v1.2.2)
  CEN: követelmények (CWA 14170, CWA 14171)

- pkiC, Bridge-CA, European Bridge-CA, eESC, MELASZ Ready

- együttműködési képesség vizsgálatai a szabványosító szerveknél
  XMLDSig: IETF és W3C
  XAdES: ETSI

BME IK
Informatikai Központ

Nyilvános kulcsú infrastruktúra



Kiszolgáló oldala

- alá-fölérendeltségi 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

Ügyfél oldala

- PKI megoldások részei

  szabvány: gyártók saját megoldásai

- tanúsítvány mezőinek, kiterjesztéseinek értelmezése

  ellenőrzés: keyUsage, extKeyUsage, ceritificatePolicies, 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

Együttműködési képesség vizsgálata

- **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**

BME IK
Informatikai Központ

Tapasztalatok

- 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)

BME IK vizsgálata

- 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

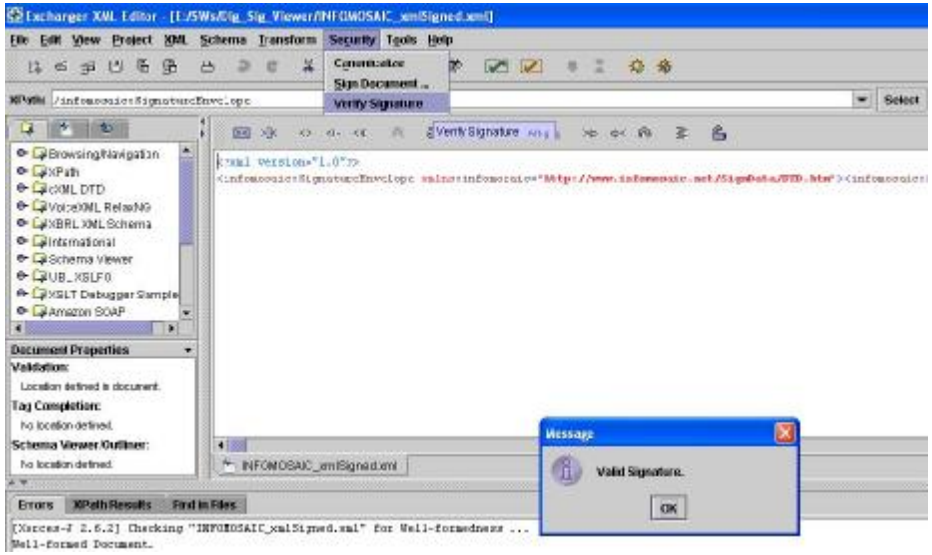
- **Cladonia Ltd.**
  Exchanger XML Editor v3.0 próbaváltozata

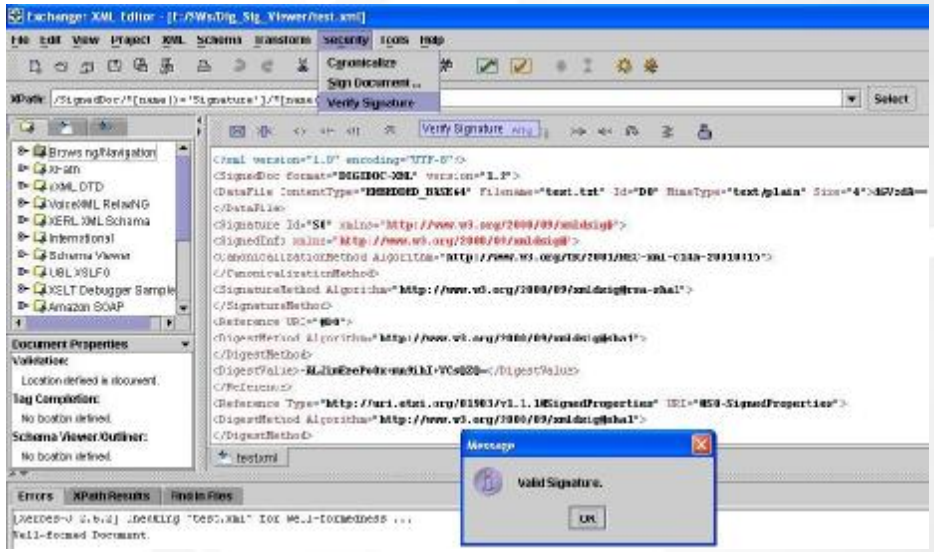
BME IK
Informatikai Központ

BME IK vizsgálata

BME IK
Informatikai Központ

BME IK vizsgálata





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