Digitális aláírás: együttműködésre képes és biztonságos alkalmazások

Szabó Áron

BME Informatikai Központ

Szigeti Szabolcs

BME Informatikai Központ

Az elmúlt néhány év…

Jogi szabályozás

- a 2001. évi XXXV. törvény az elektronikus aláírásról (1999/93/EC)
- a 2004. évi LV. törvény az elektronikus aláírásról szóló 2001. évi XXXV. törvény módosításáról
- a 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (Ket. hatályos 2005. november 1.)

Az elmúlt néhány év…

Műszaki szabályozás

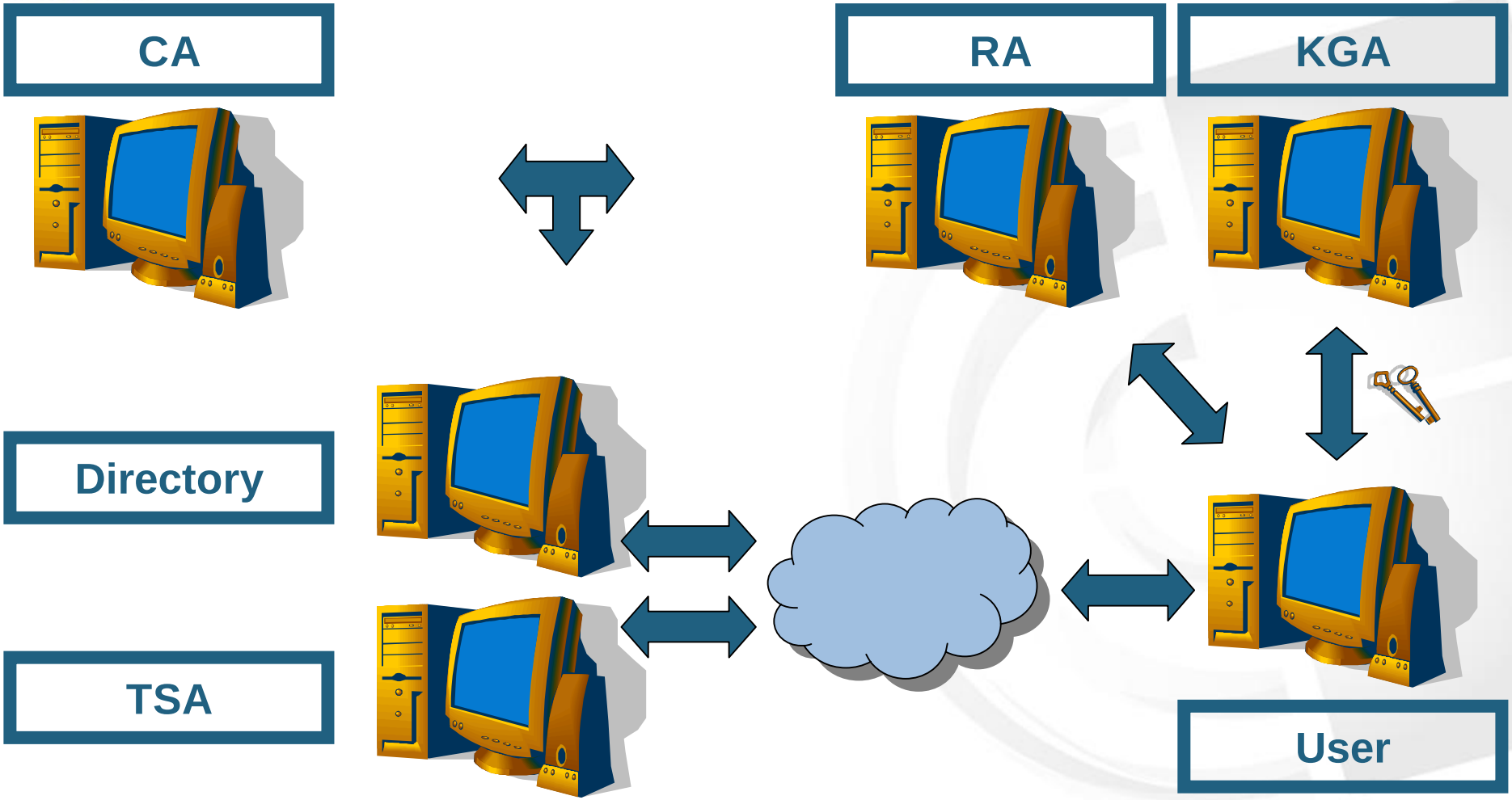
- IETF: S/MIME v3.0 (RFC 2633), S/MIME v3.1 (RFC 3851)
  W3C és IETF: XML elektronikus aláírás, XMLDSig (RFC 3275)
  ETSI és W3C: XAdES (TS 101 903 v1.2.2, v1.3.1)
  CEN: követelmények (CWA 14170, CWA 14171)

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

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

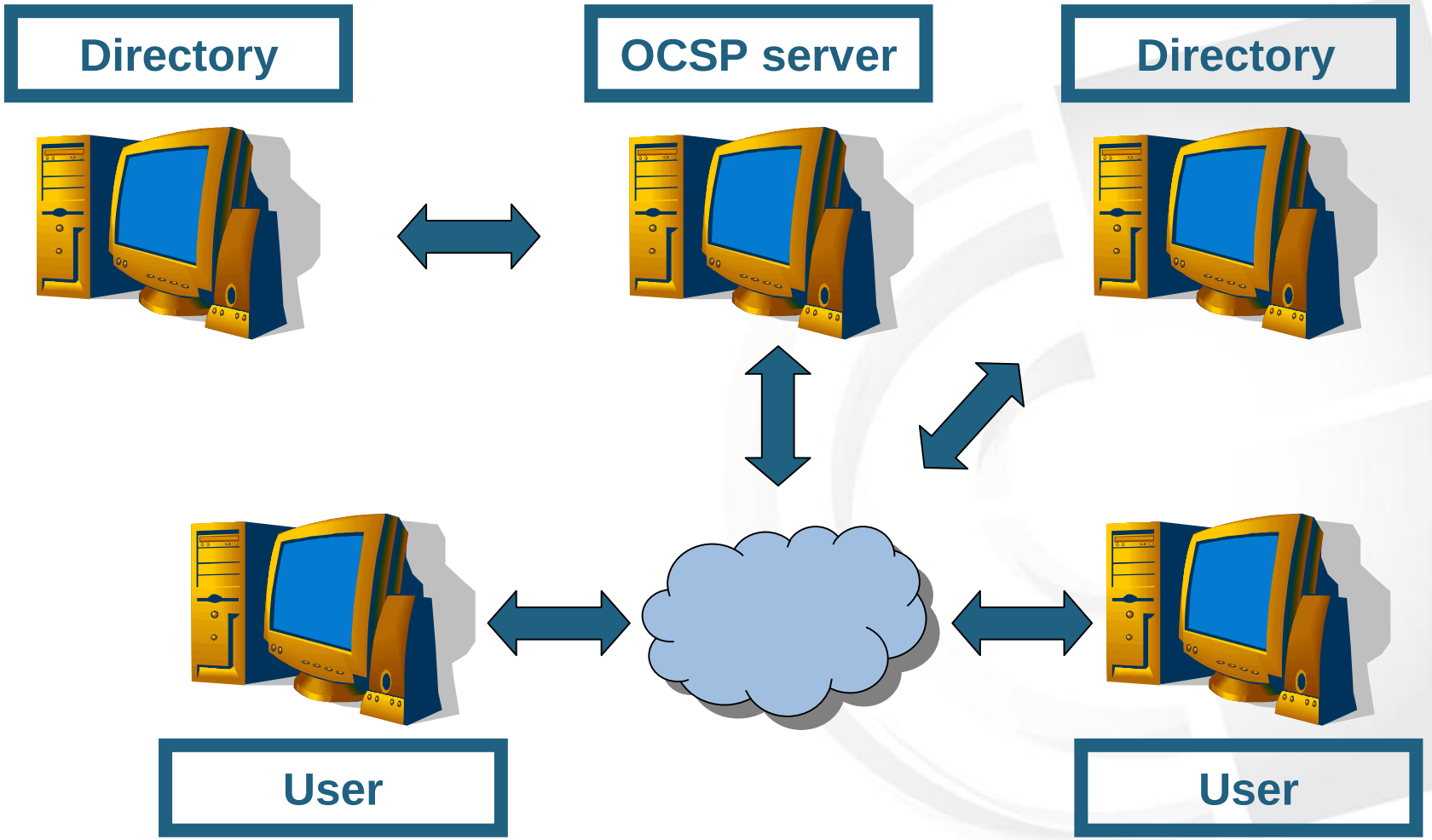
BME IK
Informatikai Központ

Nyilvános kulcsú infrastruktúra



BME IK
Informatikai Központ

Nyilvános kulcsú infrastruktúra



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 (ETSI TS 101 903 v1.3.1)

- **Magyar Elektronikus Aláírás Szövetség: MELASZ Ready**
  http://www.melasz.hu/

Együttműködési képesség vizsgálata

A mérés adatai

végezte:	Szabó Áron, Krasznay Csaba
helye:	BME Informatikai Központ
ideje:	2005. október 1. – 2005. november 15.
eszközök:	ASN1 Editor (Liping Dai)
	Asn1Viewer 1.3.4 (Objective Systems Inc.)
	XMLSpy 2006 Home Edition (Altova GmbH)
	OpenSSL 0.9.8
	saját fejlesztésű segédalkalmazás
résztvevők:	E-Group Magyarország Rt.
	MICROSEC Számítástechnikai Fejlesztő Kft.
	NetLock Kft.
	Polysys Kft.
	SDA Stúdió Kft.

Együttműködési képesség vizsgálata

Első körös ellenőrzés

- XML-elemzők (XML parser) és kanonikalizációs függvények

Második körös ellenőrzés

- XML elektronikus aláírás (XML állomány) jólformázottsága (well-formedness) és XML sémának (XMLDSIG, XAdES) való megfelelése (schema valid)

Harmadik körös ellenőrzés

- különböző alkalmazások keresztpróbája (teszt-mátrix)

Együttműködési képesség vizsgálata

Első körös ellenőrzés

- Már a W3C/IETF és ETSI vizsgálatoknál az derült ki, hogy nagy bajok vannak az XML állományok kanonikalizálásával (pl. „white space” karakterek, „xmlns” elemek nem megfelelő kezelése, szülő- és gyerekelemek kezelése), ezért nem jók a lenyomatolásra (hash) előkészített adatok.

- Három minta-állomány készült, amelyeket a különböző alkalmazások fejlesztői a megadott feltételeknek megfelelően kanonikalizáltak. A kimeneteket a laborban „bitszinten” kellet vizsgálni.

Együttműködési képesség vizsgálata

Második körös ellenőrzés

- Az ETSI szabvány (XAdES) szerint kötelező elemek szerepeljenek, a nem kötelezők közül csak azok legyenek benne az aláírásban, amelyeket még külön a „MELASZ Ready” dokumentum is megkövetel (az együttműködési képesség biztosítása érdekében).

- Egy módosított XML séma (XAdES) állomány készült, amelyet hozzárendelve a különböző alkalmazások által előállított aláíráshoz, könnyedén lehetett ellenőrizni a megfelelőségüket („well-formedness” és „schema valid”).

Együttműködési képesség vizsgálata

Harmadik körös ellenőrzés

- A különböző alkalmazások a laborban egymás kimeneteit (elkészített aláírásokat) kapták meg bemenetül (ellenőrizendő aláírásként).
- Időbélyeget (SignatureTimeStamp) és tanúsítványokat (CompleteCertificateRefs, CertificateValues) tartalmazó, „soft token”-nel (PKCS#12 szabványnak megfelelő .pfx állományok) létrehozott aláírásokat („enveloping signature”) kellett előállítania kimenetként minden alkalmazásnak.
- A „kezdeti ellenőrzésnél” minden másik (az előállítótól különböző) alkalmazás ellenőrizte az aláírást (kriptográfia, elemek szintjén) és kiegészítette a kivárási idő („grace period”) után letöltött tanúsítvány visszavonási listákkal (CRL), elemekkel (CompleteRevocationRefs, RevocationValues) azt.

Együttműködési képesség vizsgálata

A szolgáltatói oldal

- Az alkalmazások megfelelő működésének kulcsfontosságú feltételei az általuk használt – szolgáltatóktól származó – dokumentumok megfelelősége is (tanúsítványok, tanúsítvány visszavonási adatok, időbélyegek).

- Az adatoknál tartalmi (keyUsage, extKeyUsage, critical bit beállításai, cRLDistributionPoints) és formai hibák (ASN.1 megfelelőség) is előjöttek.

Biztonsági vizsgálatok

Common Criteria

- A Common Criteria módszertan alapján egy adott terméket (működését) vizsgálják, hogy a folyamatok megfelelően biztonságosak-e (pl. elég erős-e az SHA-1 lenyomatkészítő algoritmus, vagy szükséges átváltani az SHA-256 vagy SHA-512 algoritmusra?).

Interoperability testing

- Az együttműködési vizsgálatok során nem a termék belső működését, hanem annak kimeneteit (amit egy másik termék láthat) kell vizsgálni (pl. az SHA-1 algoritmus a szabványnak megfelelően fut-e le, ugyanazt az eredményt kapja-e egy másik SHA-1 lenyomatot készítő függvény?).

Köszönöm a figyelmet!

Elérhetőségek

Szabó Áron, M. Sc.
tudományos munkatárs

Szigeti Szabolcs, M. Sc., CISA
tudományos munkatárs

Budapesti Műszaki és Gazdaságtudományi Egyetem
Informatikai Központ

1117, Budapest
Magyar tudósok körútja 2.