PROHARDVER ELEKTRONIKUS PIACTÉR ELEKTRONIKUS ALÁÍRÁSSAL

Szabó Áron (aron@ik.bme.hu)

BME Informatikai Központ

Háttér

Jogi szabályozás

- a 2001. évi XXXV. törvény az elektronikus aláírásról (1999/93/EC alapján)
- a 2001. évi CVIII. törvény az elektronikus kereskedelemről (2000/31/EC alapján)
- az Európai Unió direktívája az elektronikus számlákról (2001/115/EC), amelyet minden tagállamnak 2004. január 1-ig kellett beillesztenie a saját jogrendjébe
- a 20/2004. (IV. 21.) PM rendelet az elektronikus számláról (Magyarország 2004. május 1-én csatlakozott az Európai Unióhoz)
- a 2004. évi LV. törvény az elektronikus aláírásról szóló 2001. évi XXXV. törvény módosításáról
- ...

Háttér

Műszaki szabályozás

- PKI Challenge (EU) vs. Bridge-CA (USA) és a KEAR projekt
- a W3C szabvány az XML elektronikus aláírásról (W3C DSIG, XML-Signature Syntax and Processing)
- az IETF szabványa az XML elektronikus aláírásról (RFC 3275), ami a W3C átvétele
- az ETSI szabványa az XML elektronikus aláírásról (ETSI TS 101 903), aláírási szabályzatról (ETSI TR 102 038)
- a CEN szabványai az elektronikus aláírás-létrehozó alkalmazásokkal szemben támasztott követelményekről (CWA 14170, CWA 14171)
- XAdES formátumú XML elektronikus aláírás „plugtests” magyar résztvevőkkel (ETSI szervezésében)
- ...

Használat, elterjedtség

- az XML elektronikus aláírás használata elektronikus kormányzati, elektronikus közigazgatási megoldásoknál az Európai Unió tagállamainál (pl. Észtország kísérleti elektronikus kormányzati portálján XAdES formátumú minősített elektronikus aláírás)
- az XML-alapú UBL elektronikus számlák használata Dániában a közigazgatásban
- ...

XML elektronikus aláírás

Az XML elektronikus aláírás előnyei:

- webes alapok (széleskörű használat)
- nyílt szöveg (plain text), ami könnyebb hordozhatóságot biztosít különböző adatbázisok között
- egységes séma használata (XSD)
- bármilyen állományhoz lehet rendelni XML aláírást (az aláírt adat base64 kódolva tárolódik az XML sémában)

XML elektronikus aláírás


```
<Signature ID?>
      <SignedInfo>
            <CanonicalizationMethod/>
            <SignatureMethod/>
            (<Reference URI? >
                  (<Transforms>)?
                  <DigestMethod>
                  <DigestValue>
            </Reference>)+
      </SignedInfo>
      <SignatureValue>
      (<KeyInfo>)?
      (<Object ID?>)*
</Signature>
```

XML elektronikus aláírás

- **Az ETSI TS 101 903 (XAdES) szabvány kiegészíti ezt a sémát néhány elemmel, így ez már megfelel az Európai Unió vonatkozó direktívájában szereplő fokozott biztonságú elektronikus aláírásnak.**

  „The XAdES-BES satisfies the legal requirements for electronic signatures as defined in the European Directive on electronic signatures.”

- **időbélyeg, aláírási szabályzat, tanúsítvány, tanúsítvány visszavonási lista (CRL), tanúsítvány visszavonási állapot (OCSP response)**

Elektronikus archiválás

Az elektronikus aláírással ellátott dokumentumokat (pl. számlákat, szerződéseket) archiválni kell a hazai jogszabályoknak megfelelően.

Az archiválásra vonatkozó feltételeket (ld. 5. § (1)) az elektronikus aláírás törvényről szóló törvénymódosítás határozza meg.

Az archivált elektronikus számlának tartalmaznia kell az **érvényességi láncot** (ld. Eat./2004. 6. § (4)):

- elektronikus dokumentum vagy annak lenyomata, tanúsítványok (nyilvános kulcs), tanúsítvány visszavonási listák (CRL), tanúsítvány visszavonási állapotok (OCSP response), időbélyeg

Elektronikus számla

20/2004. (IV. 21.) PM rendelet az elektronikus számláról:

- **elektronikus számla: fokozott biztonságú elektronikus aláírás és időbélyeg (ld. 2. § (1))**
- **minősített időbélyeg (ld. 5. § (2)), ha az archiválást nem archiválási szolgáltató végzi**
- **kriptográfiai követelményeket (ld. 5. § (3)) az IHM közlemény határozza meg (már kiadták)**

Elektronikus számla

Az elektronikus számlánál legyen biztosított (ld. 1. § (2)):

- **eredetének hitelessége**
- **tartalmának teljessége, megváltoztathatatlansága, sértetlensége**
  (=> elektronikus aláírás használata)

- **értelmezhetősége, olvashatósága**
  (=> technológiától lehető legfüggetlenebb megoldás a megjelenítésnél)

- **jogosultak általi hozzáférhetősége**
- **a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés elleni védelme**
  (=> nagy rendelkezésre állású adatbázisnál hozzáférési szabályok megfelelő beállítása)

Szabványok

RFC 3161 – Time-Stamp Protocol (TSP)
(időbélyeg)

RFC 3280 – Certificate and Certificate Revocation List (CRL) Profile
(ITU-T X.509 => tanúsítvány, tanúsítvány visszavonási lista)

RFC 2560 – Online Certificate Status Protocol (OCSP)
(tanúsítvány visszavonási állapot)

OASIS – Universal Business Language (UBL) v2.0
(elektronikus számla felépítése)

ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES)
(elektronikus aláírás felépítése)

Köszönöm a figyelmet!

Elérhetőségek

Szabó Áron, M. Sc.
tudományos munkatárs
Informatikai Központ

Budapesti Műszaki és Gazdaságtudományi Egyetem

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