DIGITÁLIS ALÁÍRÁS: EGYÜTTMŰKÖDÉSRE KÉPES ÉS BIZTONSÁGOS ALKALMAZÁSOK

Szabó Áron, aron@ik.bme.hu
BME Informatikai Központ
Szigeti Szabolcs, szigi@ik.bme.hu
BME Informatikai Központ

1. Bevezetés

Az elektronikus aláírás elterjedésének technológiai nehézségei között az együttműködési képesség megteremtését szokták emlegetni. Az aláírás struktúráját meghatározó, a webes alapokhoz könnyebben illeszkedő XML elektronikus aláírás szabványai ([1], [2], [3]) önmagában nem elegendők ezen együttműködési képesség biztosításához, bár vitathatatlanul elengedhetetlen feltételei. Az alkalmazások működésének logikája, a szolgáltatói oldal és a fejlesztőkörnyezet adta lehetőségek komoly mértékben tudják befolyásolni a világméretű együttműködés sikerét.

A veszélyeket felismerve az IETF (Internet Engineering Task Force) és W3C (World Wide Web Consortium) nemzetközi szabványosító szervek bonyolították le az első, független vizsgálatokat több neves fejlesztő bevonásával. Az alkalmazások az XMLDSIG ([1], [2]) szabványon alapultak, vizsgálatuk több körben zajlott le 2000. márciusa és 2004. áprilisa között.

> http://www.w3.org/Signature/2001/04/05-xmldsig-interop.html

Az XMLDSIG szabvány hamar felkeltette az Európai Unió egyik szabványosító szerve, az ETSI (European Telecommunications Standards Institute) figyelmét. Az 1999-ben kiadott direktíva az elektronikus aláírásról a jogszabályi hátterét is megteremtette az amúgy 70-es évek második felében megszületett technológiának. Az ETSI szakemberei ehhez a jogi környezethez próbálták igazítani az XMLDSIG ([1], [2]) elektronikus aláírást, így – ennek kiegészítéseként – megszületett a XAdES ([3]) szabvány.

> *The XAdES-BES satisfies the legal requirements for electronic signatures as defined in the European Directive on electronic signatures.*
>
> /forrás: [3]/

A XAdES ([3]) szabványon alapuló fejlesztések az XMLDSIG ([1], [2]) szabványban leírtaknál összetettebb, a valós élethez, igényekhez jobban igazodó struktúrát kellett, hogy megvalósítsanak, ezért itt is felmerült az együttműködési képesség vizsgálatának igénye. Az ETSI szakemberei 2003. novembere és 2004. október között több vizsgálatot is tartottak. A tapasztalatok alapján módosították, pontosították a XAdES szabványt.

> http://www.etsi.org/plugtests/History/History.htm

Magyarországon is több fejlesztés indult el, hogy az információs társadalom számára elérhetővé váljanak olyan szolgáltatások, amelyek alapvető feltétele bizonyos biztonsági szempontok megvalósítása. Kiemelt szerepet kaptak ezek közül az *e*Europe 2005 Action Plan dokumentumban taglalt elektronikus kormányzati szolgáltatások (12 + 8 közszolgáltatás), ahol külön felhívják a figyelmet a szabványosság, együttműködő-képesség fontosságára.

> *Interoperability. [...] It will be based on open standards and encourage the use of open source software.*
>
> /forrás: [4]/

Magyarországon 2005. november 1-ével lépett hatályba a Ket. (2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól), amely értelmében már valóban szükségessé vált a szabványos, együttműködésre képes alkalmazások fejlesztése.

A téma hazai szakértőit tömörítő MELASZ (Magyar Elektronikus Aláírás Szövetség) idejében felismerte, hogy a későbbiekben felmerülhetnek problémák, ezért az elektronikus aláírás-létrehozó és –ellenőrző alkalmazások fejlesztőinek, illetve a hitelesítés-szolgáltatók képviselőivel együtt átfogó munkába kezdett. A megbeszélések során a vonatkozó szabványok egyes pontjait vették sorra: ahol nem volt teljesen egyértelmű a szöveg, ott pontosítottak rajta, ahol a jogi vagy más szabályozás miatt szükséges volt, ott szigorítottak az eredeti szabványon, ahol nem volt útmutatás a szabványban, ott kidolgoztak bizonyos követelményeket. A megbeszélések eredményeként született meg az „Egységes MELASZ formátum elektronikus aláírásokra” címet viselő dokumentum első változata, amely a jelen jegyzőkönyvben leírt együttműködőképesség-vizsgálat egyik bemenete volt.

Az együttműködési képesség, a szabványosság az informatikai biztonság egyik alapvető követelménye. Együttműködésre képtelen, nem szabványos megoldásoknál azt tapasztalhatnánk, hogy ugyanazon bemenetre különböző kimenetek születhetnek. Ezek az eredmények jelenthetik egy elektronikus aláírás elfogadását vagy visszautasítását, vagy más területen pl. egy bizalmas dokumentumhoz való hozzáférés engedélyezését vagy tiltását. Egy adott termék (pl. elektronikus aláírás létrehozó és –ellenőrző alkalmazás) informatikai biztonsági követelményeknek való megfelelését több szempontból lehet vizsgálni. Az együttműködőképesség-vizsgálat mellett a Common Criteria módszertanon alapuló hazai sémának (MIBÉTS) való megfelelés elvárt. A két vizsgálat egymást kiegészíti, a különbségre talán jó példával szolgál pl. az SHA-1 lenyomatképző algoritmus elemzése. Az együttműködés biztosított, ha a fejlesztőkörnyezet SHA-1 kriptográfiai függvénye pontosan betartja a szabványban leírtakat a működésnél, más szempontból megközelítve viszont azt kell vizsgálni, hogy ismerve a közelmúltban közzétett kisebb gyengeségét az SHA-1 algoritmusnak, elegendő védelmet biztosít-e, vagy át kell térni az SHA-256 vagy SHA-512 alkalmazására. A jelen vizsgálat kizárólag az együttműködő-képességre összpontosított.

2. A mérés adatai

A mérést Szabó Áron (BME Informatikai Központ) és Krasznay Csaba (BME Informatikai Központ) végezte a Budapesti Műszaki és Gazdaságtudományi Egyetemen (BME), az Informatikai Központban (IK). A vizsgálat másfél hónapig tartott (2005. október 1. – 2005. november 15.), amelyen öt alkalmazásfejlesztő cég (E-Group Magyarország Rt., MICROSEC Számítástechnikai Fejlesztő Kft., NetLock Kft., Polysys Kft., SDA Stúdió Kft.) terméke vett részt.

3. A mérés folyamata

3.1. Bevezetés

A mérés három nagy lépcsőből állt.

Az „első körös ellenőrzés” során az XML-elemzők (XML parser) és kanonikalizációs függvények szabványnak való megfelelőségét kellett vizsgálni. A mérést végzők által szerkesztett és szétküldött minta-állományokra, mint bemenetekre kapott választ, mint kimenetet kellett vizsgálni „bit-szinten”. A kanonikalizációs függvényeknél feltárt hibák, eltérések már más együttműködőképesség-vizsgálatnál is előtérbe kerültek. Az IETF és W3C szakemberei hasonló tapasztalatokat szereztek, ezért az elektronikus aláíráshoz kapcsolódó vizsgálataik előtt 2000. októberében a kanonikalizációs függvények működését is ellenőrizték a különböző alkalmazásoknál.

http://www.w3.org/Signature/2000/10/10-c14n-interop.html

A kanonikalizációs függvények az XML állományokat készítik elő a további feldolgozáshoz (pl. „white space” karakterek, névterek kezelése). Az XMLDSIG ([1], [2]) és XAdES ([3]) elektronikus aláírásoknál kanonikalizálandó XML állományba ágyazódnak az adatok, amelyeken le kell futtatni a lenyomatképző (hash) és aszimmetrikus kódoló függvényeket. Eltérő kanonikalizáció esetén változik „bit-szinten” is az adat, ami alapján teljesen más lenyomat áll elő. Az XMLDSIG ([1], [2]) szabvány kötelezően elvárja a C14N ([5]) kanonikalizációs algoritmus támogatását.

A „második körös ellenőrzés” során egy tetszőleges, de legalább XAdES-C ([3]) XML elektronikus aláírást kell előállítania a különböző alkalmazásoknak, amelynél az XML állomány formázottságát (well-formedness) és az – XMLDSIG ([1], [2]) és XAdES ([3]) sémán alapuló MELASZ – sémának való megfelelőségét (schema valid) kellett vizsgálni. A mérést végzők által szerkesztett, módosított sémát hozzárendelve a fejlesztőktől kapott XML állományokhoz bizonyosságot lehetett szerezni azok megfelelőségéről. A MELASZ séma az eredeti sémában szereplő kötelező elemeket változtatás nélkül átemelte, illetve ezek mellett néhány elemnél, attribútumnál szigorított a követelményeken (pl. az „Id” attribútum sok helyen „optional” helyett „required”).

A „harmadik körös ellenőrzés” során egységes szempontoknak megfelelő, az alkalmazások által előállított aláírásokat kellett a létrehozó és minden másik alkalmazással ellenőriztetni. A mérést végzők által szerkesztett követelményeknek megfelelő aláírások készültek a különböző alkalmazásokkal. Ennél a lépésnél már biztosított volt, hogy az esetleges eltérések nem a kanonikalizációs függvények hibáiból fakadnak, illetve az aláírások megfelelnek a MELASZ sémának. Eltérések így is szép számmal jelentkeztek, amelyek mögött a különböző alkalmazások működési logikája (pl. elektronikus aláírás ellenőrzésénél a különböző tanúsítványok megtalálása, tanúsítványlánc felépítése) mellett a szolgáltatói oldalon felfedezett hiányosságok, pontatlanságok húzódtak meg.

3.2. Első körös ellenőrzés

Az első minta-állomány a C14N szabványból ([5]) lett kiemelve. Előnye, hogy a szabvány megadja a bemenetet és az elvárt kimenetet, hátránya, hogy ezek csak „karakter-szinten” adottak, holott a hibák a legtöbb esetben „bit-szinten” jelentkeztek. Az első minta-állomány

célja a „white space” karakterek, a nyitó- és záróelemek kezelésének, a névterek és attribútumok sorrendezésének, a névterek többszörös megadásának, illetve „kimozgatásának” és a fejrészben megadott adatok kezelésének vizsgálata volt.

A második minta-állomány egy „lecsupaszított” XML elektronikus aláírás, amelynél a gyökérelemben meg van adva az összes névtér („xmlns”). A C14N szabványban ([5]) leírtaknak megfelelően, ha az XML struktúrából ki kell emelni egy részhalmazt („subset of the nodes”), akkor a szülőelemek névtereinek a megfelelő helyekre kell kerülniük. Ennél a mintánál az egész készletből a „ds:SignedInfo” elemet kell kivenni kanonikalizálva.

A harmadik minta-állomány is a névterek kezelését vizsgálja, de kiemel egy fontos szempontot. A C14N szabvány ([5]) szerinti kanonikalizálás a névterek kezelése szempontjából lényegesen eltér az „exclusive” C14N szabványtól ([6]). A különbség abban mutatkozik meg, hogy a kanonikalizálás során a szülőelemekben megadott névtereket is figyelni kell-e, vagy elég a részhalmazban megadottakat jól elhelyezni.

3.3. Második körös ellenőrzés

A vizsgálathoz el kellett készíteni az XMLDSIG ([1], [2]) és XAdES ([3]) szabványokon alapuló séma „MELASZ Ready” szerint módosított változatát. A „MELASZ Ready” séma a legtöbb helyen szigorítást tartalmaz az eredetihez képest (pl. az „Id” attribútum sok helyen „optional” helyett „required”), lényegi elemekben nem tér el az XMLDSIG ([1], [2]) és XAdES ([3]) szabványban leírtaktól. A vizsgálat során a fejlesztőktől kapott aláírásokhoz kellett hozzárendelni a módosított sémákat, és egy XML elemzővel az ellenőrzést elvégezni. A módosított sémák létrehozásakor problémát okozott, hogy az ETSI honlapjáról letölthető séma több helyen is eltért a XAdES szabványtól ([3]). Bizonyos attribútumok (pl. „Id”, „Encoding”) és elemek (pl. „AttributeCertificateRefs”, „AttributeRevocationRefs”) hiányoztak az eredeti sémából.

3.4. Harmadik körös ellenőrzés

Az együttműködőképesség-vizsgálat legfontosabb lépése a különböző alkalmazások összeeresztése. Minden alkalmazással az egységes peremfeltételeknek megfelelő aláírást hoztak létre a mérést végzők. Az „aláírás létrehozása”, a „kezdeti ellenőrzés” és az „utólagos ellenőrzés” elkülönültek egymástól a vizsgálat során.

A peremfeltételek:

- módosított XAdES-C formátum, amely tartalmazza a „SignatureTimeStamp”, „CompleteCertificateRefs”, „SignaturePolicyIdentifier” elemet, tartalmazhatja a „CertificateValues” elemet;
- „enveloping signature” aláírást kellett létrehozni;
- az aláírandó adatot base64 kódolva kellett beágyazni, és meg kellett adni a base64 dekódoló átalakítást a „ds:Transform” elemben (nyitó- és záróelem elhagyása, az aláírandó adat base64 dekódolása a lenyomatképzés előtt);
- a „DataObjectFormat” elemben a „MimeType” elem megadása minden aláírandó adat esetében;
- időbélyeg válaszokba beágyazott tanúsítvány kellett;
- az aláírói, szolgáltatói, időbélyegző tanúsítványok beágyazása, hivatkozásaik létrehozása („ds:KeyInfo”, „SigningCertificate”, „CompleteCertificateRefs” elem az aláírás létrehozásakor);

- a visszavonási adatok közül CRL-eket (Certificate Revocation List) kellett használni, az OCSP (Online Certificate Status Protocol) válaszok nem képezték a vizsgálat tárgyát;
- az adott alkalmazás által készített aláírást („aláírás létrehozása") kellett a többi alkalmazással ellenőriztetni a kivárási idő („grace period") után;
- az aláírás létrehozásához használt titkos kulcs „soft token" volt .pfx vagy .p12 kiterjesztésű állományban (az intelligens kártyák tehát nem képezték részét a vizsgálatnak);
- UTF-8 ékezetes karaktereket mellőzni kellett a vizsgált aláírásoknál (pl. tanúsítványban szereplő neveknél, aláírási szabályzatnál);
- egy aláírást kellett létrehozni (tehát nem volt „CounterSignature" elem és más aláírás).

A rendelkezésre álló idő rövidsége miatt a vizsgálat során szélsőséges esetekkel nem foglalkoztak a mérést végzők, azonban a peremfeltételeknek megfelelő, az esetek – vélhetőleg – 90%-át képező aláírások ellenőrzése során is sok együttműködési probléma oldódott meg.

3.5. Tapasztalatok, tanácsok az átfogóbb ellenőrzéshez kapcsolódóan

Az együttműködőképesség-vizsgálat kis lefedettsége miatt érdemes felsorolni néhány olyan helyzetet, esetet – a teljesség igénye nélkül –, ami a valós életben is előfordulhat, viszont jelen vizsgálatnál nem volt lehetőség kitérni rájuk. A „MELASZ Ready" tanúsításon átesett alkalmazásoknál komolyabb probléma (pl. kriptográfiai, kanonikalizációs) nagy valószínűséggel nem merül fel, legfeljebb a működési logikában lehet szükséges minimális változtatás (pl. ne csak a CRL-ek között keresgéljen visszavonási adatokat, hanem az OCSP válaszok között is). Egy esetleges nemzetközi együttműködőképesség-vizsgálatnál a még nagyobb rugalmasság lehet szükséges, hiszen bizonyos elemek, attribútumok a „MELASZ Ready" esetében kötelező jelleggel elvártak voltak, viszont amúgy nem feltétlenül kell szerepelniük a struktúrában (pl. a különböző elemek „Id" attribútumai).

Az alkalmazásoknak fel kell készülniük:

- kezdeti ellenőrzésnél esetleg „SignatureTimeStamp" beillesztésére, a korábban csatolt CRL-ek felülvizsgálatára, szükség esetén a megfelelő CRL-ek letöltésére, OCSP válaszok kezelésére, hiányzó tanúsítványok kezelésére (pl. külső forrásból származó „root" tanúsítvány URL segítségével megadva), más protokollok kezelésére (pl. HTTPS, LDAP);
- a „MELASZ Ready" keretein belül nem megengedett, de amúgy esetleg előforduló elemekre (pl. a „ds:KeyInfo" elemen belül a „ds:X509Data" elem mellett más is szerepelhet);
- „enveloped signature" és „detached signature" aláírások kezelésére;
- az „Id" attribútumok hiányára (pl. a tanúsítványok, tanúsítványlánc felépítésénél okozhat gondot);
- többszörös aláírásra (pl. „CounterSignature" elem használata vagy párhuzamos aláírás);
- archív időbélyegek (XAdES-A) létrehozására, ellenőrzésére, ahol az egyenként kanonikalizált bemeneteket össze kell fűzni (pl. a nem feltétlenül szereplő „Id" attribútumokat létre tudja-e hozni az alkalmazás az archív időbélyeg „Include" elemeihez kapcsolódóan);
- UTF-8 ékezetes karakterek kezelésére (pl. lenyomatképzésnél okozhat gondot).

3.6. Tapasztalatok, tanácsok a szolgáltatói oldalhoz kapcsolódóan

Az együttműködőképesség-vizsgálat során számos olyan problémával szembesültek a mérést végzők, amelyek nem az alkalmazások, hanem a szolgáltatói oldal esetleges hibáiból fakadtak. Az alkalmazások „MELASZ Ready" tanúsításai éppen ezért csak abban az esetben állják meg a helyüket, ha olyan tanúsítványokkal, visszavonási adatokkal, időbélyegekkel dolgoznak, amelyek szintén megfelelnek a vonatkozó szabványoknak. A szolgáltatói oldalnál felfedezett hiányosságok, pontatlanságok bizonyos esetekben a jogi szabályozásra vezethetők vissza, ezért szükséges a követelmények egységesítése.

4. Összefoglalás

Az elektronikus kormányzati, üzletviteli, kereskedelmi megoldások sikerének egyik feltétele a szükséges kriptográfiai hátteret megteremtő alkalmazások könnyű kezelhetősége, szabványossága, együttműködő-képessége, hiszen csak így lehet minden gond, hibaüzenet nélkül ügyeket intézni pl. az Ügyfélkapun. A „MELASZ Ready" vizsgálat nagyban hozzájárul ahhoz, hogy ezt a célt elérjük, bár a kriptográfiai alkalmazások csak kis részét képezik egy nagy pl. elektronikus kormányzati rendszernek, ahol gyakran a jogszabályi követelmények miatt túlbonyolítják a folyamatokat, és ez lesz az akadálya az egyszerű, felhasználóbarát megjelenésnek, működésnek.

A munka a Nemzeti Kutatási és Technológiai Hivatal (NKTH) támogatásával valósult meg.

5. Irodalomjegyzék

[1] W3C Recommendation: XML-Signature Syntax and Processing
[2] IETF RFC 3275: (Extensible Markup Language) XML-Signature Syntax and Processing
[3] ETSI TS 101 903 v1.2.2: XML Advanced Electronic Signatures (XAdES)
[4] eEurope 2005: An information society for all
[5] W3C Recommendation: Canonical XML - Version 1.0
[6] W3C Recommendation: Exclusive XML Canonicalization - Version 1.0