Elektronikus aláírás-létrehozó alkalmazások együttműködési képessége

1. Bevezetés

Napjaink biztonságos – bizalmas, hiteles, sértetlen, letagadhatatlan – kommunikációjának alapfeltétele, a kriptográfia és a ráépülő megoldások története a ’70-es évekbe nyúlik vissza, amikor a matematikai értelemben vett nehéz problémákon (pl. prímfaktorizáción, azaz a prímtényezőkre való bontáson) alapuló első algoritmusok – mint az RSA (R. Rivest, A. Shamir, L. Adleman) aszimmetrikus kódoló algoritmus – megszülettek.

A TCP/IP protokollokon alapuló és más nem biztonságos hálózatokon szimmetrikus és aszimmetrikus kódoló algoritmusok révén lehet biztosítani a biztonságos kommunikáció feltételeit. Az informatikai háttér megteremtéséhez szükséges egy PKI (Public Key Infrastructure) megoldás, amelynek RA (Registration Authority) eleménél az ügyfél igényelhet tanúsítványt (az ügyfél megkülönböztetett nevének és nyilvános kulcsának összerendelés, amely alapján egyértelműen lehet azonosítani az elektronikus világban), a CA (Certification Authority) eleme kibocsátja és nyilvános adatbázisba (Directory) helyezi a tanúsítványt, amelyet bárki el tud érni. A szolgáltató által előállított kriptográfiai kulcsok nyilvános fele a tanúsítványban található, míg a titkos fele olyan adathordozó eszközre kerül, amelyből nem nyerhető ki. Az intelligens kártyák (akár a SIM-kártyák is) képesek bizalmasan tárolni az adatokat, egy kriptográfiai műveletnél a bemeneten megkapott adatok kódolása a chip belsejében – a titkos kulcs kiadása nélkül – megy végbe és a kimeneten a kódolt adat jelenik meg. Az ügyfél oldalán futó alkalmazás, az adathordozón (pl. intelligens kártya) tárolt titkos kulcs és a bárki által elérhető tanúsítvány segítségével digitális aláírást (azaz kriptográfiai algoritmuson alapuló elektronikus aláírást) és rejtjelezett üzeneteket lehet előállítani.

Zárt csoportoknál, cégek berkein belül működő PKI megoldásoknál a kiszolgáló és az ügyfél oldalának termékei egy gyártótól származtak, így napjaink legnagyobb problémája, az együttműködési képesség hiánya fel sem merült. Maga a kiszolgáló és az ügyfél oldala sem vált szét, hiszen a legtöbb esetben a böngészőbe vagy irodai alkalmazásokba beépülő elemek a PKI részét képezték, kevés olyan alkalmazás volt, amelyek jól elhatárolt, szabványos felületeken keresztül kizárólag létrehozták és ellenőrizték a kriptográfiai eljárások révén előállt adatokat, így a különböző gyártóktól származó termékek különböző módon állították elő és ellenőrizték a digitális aláírással ellátott, rejtjelezett üzeneteket.

Megszületett az Európai Unió 1999/93/EC jelölésű direktívája (amelyen a 2001. évi XXXV. és a 2004. évi LV. törvény alapul), amellyel kitárult a világ és az együttműködési képesség alapvető fontosságúvá vált azoknál, akik ki is akarták használni az előnyöket, azaz a külvilággal való kapcsolattartást biztonságos, gyors és költséghatékony alapokra akarták áthelyezni.

2. Együttműködési vizsgálatok a kiszolgáló oldalán

A kiszolgálói oldalon problémák merültek fel a tanúsítványkérelmekkel, kereszt-tanúsításokkal, intelligens kártyák kezelésével kapcsolatban. A CA elemek által alkotott fa-struktúrában, a CA-hierarchiában az egyes elemek alá-fölérendeltségi (root-CA és subordinate-CA) és mellérendeltségi viszonyban (cross-certification) helyezkedhetnek el. A hierarchiába való betagozódáshoz – amely szükséges ahhoz, hogy egy adott felhasználói

tanúsítvány tanúsítási láncolatát végig lehessen követni – egymás tanúsítványait kell a megfelelő protokollok révén felültanúsítani, azonban az ehhez szükséges kommunikáció is több szabványon alapulhat. A tanúsítványkérelem előállítása történhet az IETF RFC 2314 (IETF RFC 2986) szabvány szerint, amely PKCS#10 név alatt jobban ismert, illetve a CRMF (IETF RFC 2511) szabványban leírtak alapján is. Az üzenetek beágyazására is több megoldás létezik, hiszen a CMC (IETF RFC 2797) mellett lehet használni a CMP (IETF RFC 2510) szabványon alapulót is.

Problémák merültek fel az előállított tanúsítvány felépítésével kapcsolatban is. A valós világban létező objektumok (pl. természetes személyek) elektronikus világba történő egyértelmű leképezéséhez megfelelően kell előállítani a megkülönböztetett nevet (distinguished name), amely a tanúsítványba is bekerül, éppen ezért nem mindegy, hogy mely névelemeket tartalmazza, melyeket tudja értelmezni egy PKI megoldás. A tanúsítvány többi elemével (mezők, kiterjesztések) is voltak gondok, hiszen az eredeti ITU ajánlások és az IETF vonatkozó szabványai között is léteznek eltérések, illetve az Európai Unió jogi szabályozásának megfelelendő az ETSI szabványai is tartalmaznak kiegészítő elemeket.

Az intelligens kártyákkal, kártyaolvasókkal való kommunikáció is nehézkesnek bizonyult, így külön projekt keretén belül kellett megvizsgálni az együttműködési képesség hiányának okait. A PKCS szabványokkal kiegészített ISO/IEC 7816 szabványsorozat határozza meg többek közt a fizikai tulajdonságokat, a kommunikációhoz szükséges függvények, utasítások felépítését. Az intelligens kártyákon való bizalmas adatok elhelyezése a kiszolgáló oldalán történik, azonban az ügyfél használja, fér hozzá ezen adatokhoz, ezért az ügyfél oldalán is biztosítani kell az együttműködési képességet.

A névtár a PKI megoldások azon része, amely kívülről és a belső elemek számára is elérhető. Az eredeti elképzelések az ITU ajánlásai szerint világméretű működésről, elosztott rendszerekről, lekérdezésre optimalizált adatbázisokról szóltak. Az ITU-T X.500-as ajánlások követelményei mellett az egyszerűsített elérési protokollt és felépítést – LDAP – leíró szabványok (pl. IETF RFC 2251) is megjelentek és termékeket is fejlesztettek ezen alapulva. A csökkentett képességekkel bíró névtárak nem tudnak elosztott rendszerként működni, hiszen az ITU-T X.500-as névtárak DSP (Directory System Protocol) protokollja hiányzik az LDAP szabványból, így ezen probléma kiküszöbölésére külön megoldást kellett a szakembereknek keresni.

A kiszolgálói oldal együttműködési képességét vizsgáló munkák között a pkiC (PKI Challenge), Bridge-CA, European Bridge-CA, eESC (eEurope Smart Cards) projekteket érdemes megemlíteni.

3. Együttműködési vizsgálatok az ügyfél oldalán

Az ügyfél oldalán futó alkalmazások később kerültek terítékre, de a gondok is komolyabbak voltak az aláírás felépítésével, a tanúsítvány kezelésével kapcsolatban.

A kezdeti idők ügyfél oldalán futó alkalmazásai inkább a PKI megoldás szerves részeként működtek, gyártónként változott, hogy milyen módon épültek be az egyes alkalmazásokba (irodai alkalmazásokba, böngészőkbe), milyen módon hozták létre és ellenőrizték a digitális aláírást, az ellenőrzés során hogy kezelték a tanúsítvány visszavonási adatokat, éppen ezért az együttműködési képesség hiánya volt tapasztalható a különböző termékek között.

Az S/MIME version 2 és version 3 változatokról, illetve a CMS üzenetekről (Cryptographic Message Syntax) szóló IETF szabványok megjelenése után nem sokkal adta ki a W3C és IETF az XML elektronikus aláírás felépítését meghatározó szabványát, amelyet a webes technológiák térhódításának köszönhetően ma már alapkövetelményként határoznak meg a különböző elektronikus kormányzati, elektronikus közigazgatási dokumentumokban. Az XML alapokon nyugvó elektronikus aláírás mellett szól, hogy az S/MIME szabványnak vannak hiányosságai (pl. nincs lehetőség időbélyeg kezelésére a `signingTime` tulajdonságnál), illetve az, hogy a jövőben könnyebben tud együttműködni a webes megoldásokkal, a web service technológián alapuló szolgáltatások SOAP (Simple Object Access Protocol) révén történő elérésénél, amelyhez a WSDL (Web Services Description Language) leírás és az UDDI (Universal Description, Discovery and Integration) nyilvántartás is szükséges lehet.

Az XML elektronikus aláírási séma legszűkebb halmazát az IETF RFC 3275 szabvány tartalmazza, azonban ezt az ETSI TS 101 903 szabvány kiegészítette. Az elmúlt csaknem 5 évben a W3C, az IETF, illetve az ETSI több vizsgálata (a 2003. és 2004. évben tartottak) alapján ma már kiforrott szabványról lehet beszélni (IETF RFC 3275 és ETSI TS 101 903 v1.2.2), amelyek alapján együttműködésre képes alkalmazásokat lehet fejleszteni. A közeli jövőben a régebbi fejlesztések szabványhoz igazítása, illetve az újonnan fejlesztettek megfelelőségének vizsgálata kerül középpontba, így biztosítandó, hogy a piacon kapható termékek képesek legyenek együttműködésre. A szabványosító szervek által végzett vizsgálatok tapasztalatai alapján a MELASZ (Magyar Elektronikus Aláírás Szövetség) is hasonló vizsgálatot kezdeményez Magyarországon. A vizsgálathoz szükséges közös szempontokat, követelményeket, az Európai Unió jogi feltételeinek megfelelő XML elektronikus aláírást az ETSI TS 101 903 szabvány határozza meg.

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

/ETSI TS 101 903 v1.2.2/

Az együttműködési képesség hiányosságai a szolgáltatótól kapott tanúsítvány feldolgozásánál már jelentkeztek. A megkülönböztetett nevek nem megfelelő kezelése révén előfordulhatott, hogy egy alkalmazás e-mail cím alapján azonosította a felhasználót, azaz nem magát a felhasználót kezelte, hanem csak a postafiókját. Bár, az e-mail cím egyedi adat (kivéve, ha pl. nem használják fel újra egy webes, ingyenes levelezőrendszernél a megszűnt azonosítót) a felhasználó megkülönböztetett nevét egyszer meghatározott és egyedi adatok alapján érdemes előállítani (pl. felhasználó neve, születés helye és ideje, anyja neve), különben az értelmezésnél problémák merülhetnek fel. Az alkalmazásoknál súlyosabb problémát vetett fel a tanúsítványok `keyUsage` és `extKeyUsage` kiterjesztéseinek nem megfelelő kezelése, hiszen ezek révén lehet a kulcshasználatot meghatározni úgy, hogy az megfeleljen a jogi (pl. külön kulcsok rejtjelezésre és digitális aláírásra) és technológiai (pl. minősített tanúsítvány esetében letagadhatatlan digitális aláírás, amelynek ellenőrzését – szükség esetén – megbízható harmadik fél által kell tudni biztosítani) szabályozásnak is. A tanúsítványok felhasználási feltételeinek ellenőrzéséhez kapcsolódik a CP (Certificate Policy) dokumentum is, amelyben a szolgáltató meghatározza ezeket. A CP dokumentum – `certificatePolicies` kiterjesztésben megadott – elérhetőségét és azonosítóját az alkalmazásnak értelmezni kell tudnia. A tanúsítványok visszavonási adatainak beszerzése és értelmezése kritikus pontja az ellenőrzésnek mégis nagyon sok alkalmazásnál lehet hibás működést tapasztalni. A tanúsítványban szereplő megkülönböztetett név alapján az elosztott adatbázisban, névtárrendszerben indított keresés mellett lehetőség van a

`cRLDistributionPoints` kiterjesztésben megtalálható adatok alapján (pl. URL) megszerezni a legfrissebb tanúsítvány visszavonási listát (CRL). A tanúsítvány visszavonási állapot lekérdezése egy másik protokoll, az OCSP (IETF RFC 2560) révén történhet meg. A műveletet az ellenőrzés pillanatában kell végrehajtani, a legfrissebb visszavonási adatok alapján folytatni, azonban sok alkalmazás már korábban letöltött, ütemezett letöltés révén megszerzett adatokat használ, de a régebbi fejlesztéseknél nem is volt kidolgozva a távoli szolgáltatás elérésének lehetősége. A tanúsítvány visszavonási adatok ellenőrzésének fontossága kulcskérdés, hiszen mindennapi eset lehet, hogy a felhasználó elveszti intelligens kártyáját és azt be is jelenti a szolgáltatónál, amely visszavonási listára helyezi tanúsítványát. Az intelligens kártyát és a PIN kódot illetéktelen megszerzi, majd az átutaltat saját bankszámlájára pénzt. Az átutalási megbízás digitális aláírással van ellátva, azonban az alkalmazás nem tölti az ellenőrzés pillanatában létező legfrissebb tanúsítvány visszavonási adatot, így nem szerez tudomást arról, hogy az adott tanúsítvány vissza van vonva, és az átutalási kérelmet el kell utasítania. A nem megfelelő működés tehát felelős lehet a hamis biztonságérzet kialakulásáért, amely nagyobb károkat okozhat, mintha a felhasználó tudatában lenne a veszélyeknek. A tanúsítványok és a tanúsítványi láncolatok vizsgálata is összetettebb a kriptográfiai adatok visszafejtésénél. A tanúsítványon elhelyezett digitális aláírás ellenőrzése során fel kell térképezni az egész tanúsítványi láncolatot a végfelhasználótól egésze a megbízható pontig (root-CA), amelyek mindegyikét meg kell vizsgálni a kriptográfián túlmenően is (pl. a `subject` elem a kibocsátó – CA – tanúsítványában megegyezik az `issuer` elem tartalmával a kibocsátottében, a `validity` mezőben szereplő érvényességi határidőket is vizsgálni kell).

Az ügyfél oldalán futó alkalmazásokkal kapcsolatban általánosságban el lehet mondani, hogy nem a digitális aláírás létrehozása a bonyolult művelet, hanem annak ellenőrzése, ennek ellenére a legtöbb terméknél az ellenőrző összetevők ingyenesen elérhetők az interneten. A tanúsítványok kezelésén túlmenően az alkalmazások számára meg kellett határozni a kezelendő kriptográfiai algoritmusok körét is (pl. SHA-1 lenyomatképző algoritmus és RSA aszimmetrikus kódoló algoritmus), hiszen az MD5 algoritmus révén képzett lenyomatot nem tudna egy az SHA-1 algoritmust használó alkalmazás érdemben kezelni, ezért ez is egy újabb lépés volt az együttműködési képesség biztosítása felé vezető úton. Az előállítandó digitális aláírás formátuma is a bemenő adatok között kell, hogy szerepeljen, hiszen az XML elektronikus aláírás ellenőrzésére képes alkalmazás nem tudná értelmezni az S/MIME version 3 szabványnak megfelelő üzenetet.

A technológiai szabványok alapján fejlesztett alkalmazásoknál – hiába állítja a gyártó, hogy megfelel a követelményeknek – gyakran a termék megvásárlása és telepítése után derül ki a felhasználó számára, hogy az bár látszólag valóban teljesíti a szabvány által leírtakat, mégis hiba lép fel más termékekkel való együttműködés közben. A hibák okaira alkalmazásszintű vizsgálat során gyakran csak következtetni lehet, a tényleges feltáráshoz és javításhoz forráskód szinten kell elemezni a működést. Az együttműködési képesség vizsgálatainál gyakori hiba lehet – ehhez elég a nyílt szövegként megjeleníthető digitális aláírás felépítését elemezni – az adatok szabványtól eltérő sémája (pl. más névelem használata az XML esetében, aláírt állomány beágyazása nem megfelelő módon, a szabványban kötelezőként megjelölt elemek kihagyása).

4. Szabványosító szervek vizsgálatai

4.1. IETF, W3C, ETSI

Az IETF és W3C szabványosító szerv elsőként 2000. márciusában tartotta az első együttműködési képességet vizsgáló rendezvényét. A 2001. áprilisában tartott rendezvényen részt vett a Baltimore, Ubisecure, Wedgetail, Fujitsu, GapXse, HP, IAIK, Infomosaic, IBM, Microsoft, NEC, Phaos, RSA, Apache, XMLSec és DataPower, amelyek termékei alapos vizsgálaton estek át.

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

A vizsgálatok alapját az IETF RFC 3275 szabvány adta, amely a W3C „XML-Signature Syntax and Processing" ajánlásán alapul.

Az ETSI szabványa kiegészítette az XML elektronikus aláírás alapsémáját, amely a vizsgálati szempontok listáját is bővítette. Az ETSI TS 101 903 szabványon (XAdES) alapuló elektronikus aláírás-létrehozó alkalmazások együttműködésének vizsgálata címszóval 2003. novemberében, 2004. májusában és 2004. októberében tartottak rendezvényt.

http://www.etsi.org/plugtests/

A vizsgálatok eredményein alapulva az ETSI TS 101 903 szabványt többször módosították, pontosították. A jelenlegi v1.2.2 változat 2004. áprilisa óta nem változott, azaz a legutóbbi együttműködési képességet vizsgáló rendezvényeken nem merültek fel olyan problémák, amelyek miatt nem élhetnénk azzal a feltételezéssel, hogy az ETSI TS 101 903 v.1.2.2 változata kiforrott szabványnak tekinthető. A kifejlesztésre kerülő alkalmazásoknak meg kell felelniük a szabvány ezen változatának, és az esetleges későbbi módosítások esetén is a v1.2.2 változatnak megfelelő XML elektronikus aláírást mindenképpen kezelnie kell tudni a különböző termékeknek.

Érdemes áttekinteni, hogy az elmúlt két évben milyen tapasztalatokkal lettek gazdagabbak a fejlesztők és a szabványosítók az ETSI TS 101 903 szabványon alapuló együttműködési vizsgálatok során. Az együttműködési problémák gyökereinek vizsgálatához hasznos lehet a fejlesztések során felmerülő kérdéseket, a fejlesztői levelezőlisták témáit is áttanulmányozni (pl. a kanonizáláshoz – canonicalization – és a névterek – namespace – megfelelő használatához is sok kérdés kapcsolódott).

4.2. ETSI XAdES plugtest – 2003. november 3-7.

Az OCSP válasz (IETF RFC 2560) beágyazása az XML elektronikus aláírásban nem volt egyértelmű a szabványban, így több megoldás is született és volt olyan megoldás, hogy az egész adathalmazt – `OCSPResponse` – vagy csak a lényegi információt – `BasicOCSPResponse` – tárolták.

Az XML elektronikus aláírás `TimeStampType` típusánál átdolgozták a leírást, így az új változatban az azonosítók és a kanonizáló algoritmusok szerepe tisztázódott, illetve új tulajdonság bevezetése révén – `referencedData` – lehetőség nyílt a teljes állományról készítendő lenyomat elkerülésére (helyette – kevésbé időigényes módon – csak a hivatkozásban szereplő adatok szolgálnak bemenetül).

Az archív időbélyeg – `ArchiveTimeStamp` – összeállításánál problémát jelentett, hogy a `SignedSignatureProperties` és a `SignedDataObjectProperties` elemeknél

hiányoztak az azonosítókat tartalmazó tulajdonságok – `Id` – megnehezítve így a meghivatkozhatóságukat.

A szabvány szövegét összhangba kellett hozni az IETF RFC 2119 szabvány által meghatározottakkal, így egységesítve a különböző követelményszintekre vonatkozó fogalmakat.

Pontosítás került a szabványba a `QualifyingProperties` elemre vonatkozó részbe (milyen `Id` értéket kell megadni a `Target` tulajdonságnál).

Az ASN.1 kódolás pontosítása végett került bele a szabvány szövegébe több helyen a DER (Distinguished Encoding Rules) kódolásra való utalás.

Az ETSI szakemberei a bizalmi szolgáltatást nyújtók (Trust Service Provider) állapotát jelző adat – az XML elektronikus aláírásba történő – beágyazását is javasolták a tanúsítványok és visszavonási adatok mellett.

A szabvány áttekinthetőbbé tétele miatt egyes bekezdéseket más részhez helyeztek át (pl. `SigningCertificate`).

A redundanciák elkerülése végett (tanúsítványok, visszavonási adatok esetében) az ETSI szakemberei javasolták, hogy az archív elektronikus aláírási sémában meg lehessen különböztetni a „csak hivatkozásokat tartalmazó”, a „csak adatokat tartalmazó” és a „vegyes” megoldásokat.

Az `ArchiveTimeStamp` létrehozásához szükséges elemek módosítása volt szükséges (a sorrendiségben adódtak problémák pl. a `SigningTime` elemnél).

Az `AnyType` típuson is változtatni kellett, hogy olyan adatstruktúrákat is megengedhessen, amelyekhez nem tartozik séma.

A `CertID` elem tartalmazza a tanúsítvány azonosításához szükséges adatokat (a tanúsítvány kibocsátójának nevét, a kibocsátott tanúsítvány sorszámát és a tanúsítvány lenyomatát). A szakemberek kiegészítették a sémát az `URI` tulajdonsággal, amely révén más módon is lehet azonosítani a tanúsítványt.

A .NET környezet XML elemzője a korábbi szabványban meghatározott sémát nem tudta értelmezni, ezért a hibákat javítani kellett.

A szabványban meghatározott séma ki lett egészítve a névterek (`namespace`) beillesztésével az `import` elem révén.

A XAdES és az XMLDSig sémában meghatározott `Transforms` elemet egységesítették az együttműködési képesség javítása érdekében.

Az ETSI TS 101 903 korábbi változatában szereplő példa (Annex D) nem volt összhangban a szabványban meghatározott sémával, ezért a hibákat javítani kellett.

A `DataObjectFormat` elemmel kapcsolatban merültek fel problémák (pl. hány objektumra vonatkozhat), amelyeket a szakemberek további vizsgálódásnak vetettek alá.

Aggályok merültek fel a tanúsítványok beágyazásával kapcsolatban is, ugyanis a szabvány korábbi változatánál az `ArchiveTimeStamp` elem nem fedte le a `KeyInfo` elemet, amelybe szintén el lehetett helyezni az aláírói tanúsítványt (a `CertificateValues` elem helyett), így az nem szolgált bemenetként a hosszú távú hitelességet biztosító archív időbélyeghez.

A `Cert` elemnek kötelező jelleggel kell tartalmaznia a tanúsítvány kibocsátójának nevét és a kibocsátott tanúsítvány sorszámát (a szabvány korábbi változatában szereplő ellentmondásos állításokat javítani kellett).

4.3. ETSI XAdES plugtest – 2004. május 24-28.

Az `integer` típus (XML típusa) bizonyos esetekben nem bizonyult megfelelőnek a sorozatszámok tárolására (az `X509SerialNumber` elemben), a túl hosszú sorozatszámokat nem tudta kezelni, értelmezni.

A tanúsítvány kibocsátójának nevét `X509IssuerName` elemben kell tárolni, azonban problémák merültek fel a névelemek értelmezésével. A fejlesztőknek ügyelniük kell arra, hogy az együttműködési képesség megőrzése érdekében a névelemek megadásakor az IETF RFC 2253 szabványban leírtak szerint járjanak el.

5. Együttműködési képesség vizsgálata Magyarországon

Az elmúlt években végzett vizsgálatok alapján született szabványok, szabályozások mára már letisztultak, a fejlesztők számára pontos és részletes leírások állnak rendelkezésre, hogy különböző alkalmazásokat tudjanak létrehozni. A különböző fejlesztések, alkalmazások együttműködési vizsgálata bizonyítja és biztosítja a szabványoknak való megfelelőséget, így az egyszerű felhasználó olyan terméket kaphat kézhez, amely minden tekintetben megfelel a hazai és az Európai Unió jogi és technológiai szabályozásainak, és amely révén tetszőleges másik felhasználóval tud – hibás működést kiküszöbölve – biztonságosan kommunikálni.

Az elektronikus aláíráshoz kapcsolódó témakörök szakértőit – hitelesítés-szolgáltatók, tanúsítók, fejlesztők, tanácsadók részéről – tömörítő MELASZ (Magyar Elektronikus Aláírás Szövetség) a MELASZ Ready program keretében kívánja útnak indítani a különböző elektronikus aláíráshoz kapcsolódó alkalmazások együttműködési képességének vizsgálatát. A cél – többek közt – a XAdES sémán (ETSI TS 101 903 v1.2.2) alapuló XML elektronikus aláírás létrehozására és ellenőrzésére képes alkalmazások együttműködési képességének megteremtése.

http://www.melasz.hu/

6. Együttműködési képesség vizsgálatainak eredményei

6.1. Tapasztalatok

Az együttműködési vizsgálatok zárójelentéseiben a szakemberek részletesen leírták, hogy az egyes alkalmazások mely sémákat tudták előállítani, és ellenőrizni, ezen sémák mennyire

voltak teljesek (bizonyos elemeket nem kezeltek), milyen tisztázandó kérdések merültek fel, az egyes vizsgálati eseteket milyen eredménnyel teljesítették.

Az első vizsgálaton résztvevő alkalmazások részben a szabványban szereplő pontatlanságok miatt kisebb-nagyobb módosításra szorultak, hogy az együttműködés képességet biztosítani tudják. Ezen rendezvényen a szakemberek a Baltimore termékét emelték ki, mint a szabványoknak leginkább megfelelőt, de még ennél is akadtak hiányosságok. A második rendezvényen a már letisztult szabvány alapján vizsgálták az alkalmazásokat, ahol a legteljesebb és a szabványokat legpontosabban megvalósító alkalmazás a UPC (Universitat Politècnica de Catalunya) terméke lett, amely minden más termékkel képes volt együttműködésre.

6.2. ETSI XAdES plugtest – 2003. november 3-7.

Baltimore

- minden sémát elő tudott állítani a `QualifyingPropertiesReference` elem kivételével
- kisebb problémák voltak az IAIK által előállított XAdES-A séma értelmezésével

IAIK

- minden sémát elő tudott állítani a `QualifyingPropertiesReference`, `CommitmentTypeIndication`, `DataObjectFormat`, `CounterSignature` elem kivételével
- kisebb problémák voltak a Baltimore által előállított XAdES-A séma értelmezésével

Kopint-Datorg Rt.

- a XAdES és az XMLDSig sémában is voltak kisebb problémák, amelyek miatt a többi alkalmazás nem tudta értelmezni az XML elektronikus aláírást
- nem tudta értelmezni a többi alkalmazás által előállított XML elektronikus aláírást

Microsoft

- a XAdES és az XMLDSig sémában is voltak kisebb problémák, amelyek miatt a többi alkalmazás nem tudta értelmezni az XML elektronikus aláírást (a fejlesztés korai szakaszában tartottak)
- nem tudta értelmezni a többi alkalmazás által előállított XML elektronikus aláírást

UPC

- minden sémát elő tudott állítani a `QualifyingPropertiesReference` elem kivételével
- kisebb problémák voltak a UPC által előállított időbélyegek értelmezésével

Sertifitseerimiskeskus

- nem tudott minden sémát előállítani
- kisebb problémák voltak a Sertifitseerimiskeskus által előállított OCSP válaszok értelmezésével

6.3. ETSI XAdES plugtest – 2004. május 24-28.

UPC

- minden sémát elő tudott állítani
- tudta ellenőrizni mindegyiket

Microsoft

- minden sémát elő tudott állítani a XAdES-A kivételével
- tudta ellenőrizni mindegyiket

Sertifitseerimiskeskus

- nem tudott minden sémát előállítani
- kisebb problémák voltak a `dateTime` típus és `KeyInfo` elem értelmezésével

6.4. BME IK

A BME Informatikai Központban néhány ingyenes és elérhető XML elektronikus aláírás-létrehozó alkalmazást vetettünk alá vizsgálatoknak. Az együttműködési képesség vizsgálata során eltekintettünk a teljességre való törekvéstől, azaz nem volt elsődleges cél, hogy az ETSI TS 101 903 v1.2.2 szabványban meghatározott XAdES sémáit mind elő tudják állítani, sokkal inkább arra helyeztük a hangsúlyt, hogy az előállított XML elektronikus aláírások pontosan igazodnak-e a szabványhoz (akár az IETF RFC 3275 szabványhoz), azaz tudják-e egymás XML elektronikus aláírását értelmezni.

Az együttműködési vizsgálatokat az Infomosaic Corporation (W3C és IETF XML-Signature Interoperability résztvevője) honlapján elérhető szolgáltatásnak igénybe vételéhez szükséges SecureXML Digital Signature Toolkit version 2.3.140.40 (SecureXML Digital Signature & Encryption Toolkit) próbaváltozata, a Sertifitseerimiskeskus OpenXAdES.org honlapján elérhető szolgáltatásnak igénybe vételéhez ingyenesen elérhető ActiveX (ETSI plugtest résztvevője) és a Cladonia Ltd. terméke, az Exchanger XML Editor v3.0 bevonásával végeztük el.

létrehozó ellenőrző	SecureXML	OpenXAdES	Exchanger XML Editor
SecureXML	megfelelt	megfelelt	megfelelt
OpenXAdES	–	–	–
Exchanger XML Editor	megfelelt	megfelelt	megfelelt

- Az összes termék képes volt kezelni az általa létrehozott XML elektronikus aláírást.
- A Sertifitseerimiskeskus OpenXAdES.org által nyújtott szolgáltatás kizárólag XML elektronikus aláírás létrehozására volt képes (ellenőrzésre nem).

7. Összefoglalás

Az elmúlt néhány év a technológiai szabályozás, az együttműködési képesség, a biztonságos működés feltételeinek megteremtése és vizsgálata jegyében telt el, és most már talán el lehet mondani, hogy letisztult, kiforrott szabványok állnak a fejlesztők rendelkezésére. A

szabványosító szervek által megtartott vizsgálatok – amelyek az együttműködési képességet helyezték a középpontba – a közeli múlt eseményei, azaz Magyarország nincs lemaradva a világ mögött, sőt, bízva a hazai szakemberekben és a MELASZ terveinek megvalósulásában felzárkózhat akár az élvonalhoz is. A közeli jövőben megvalósuló – a kriptográfiát használó – rendszereknél – legyen szó a 12+8 elektronikus közszolgáltatásról, a banki szférában megjelenő intelligens kártyákról, a BKV jegyrendszeréről, egy esetleges új diákigazolványról – már ezen véglegesített szabványokat kell alapul venni, hogy világméretű, szabványos együttműködésre képesek legyenek.

Mellékletek

1. számú melléklet

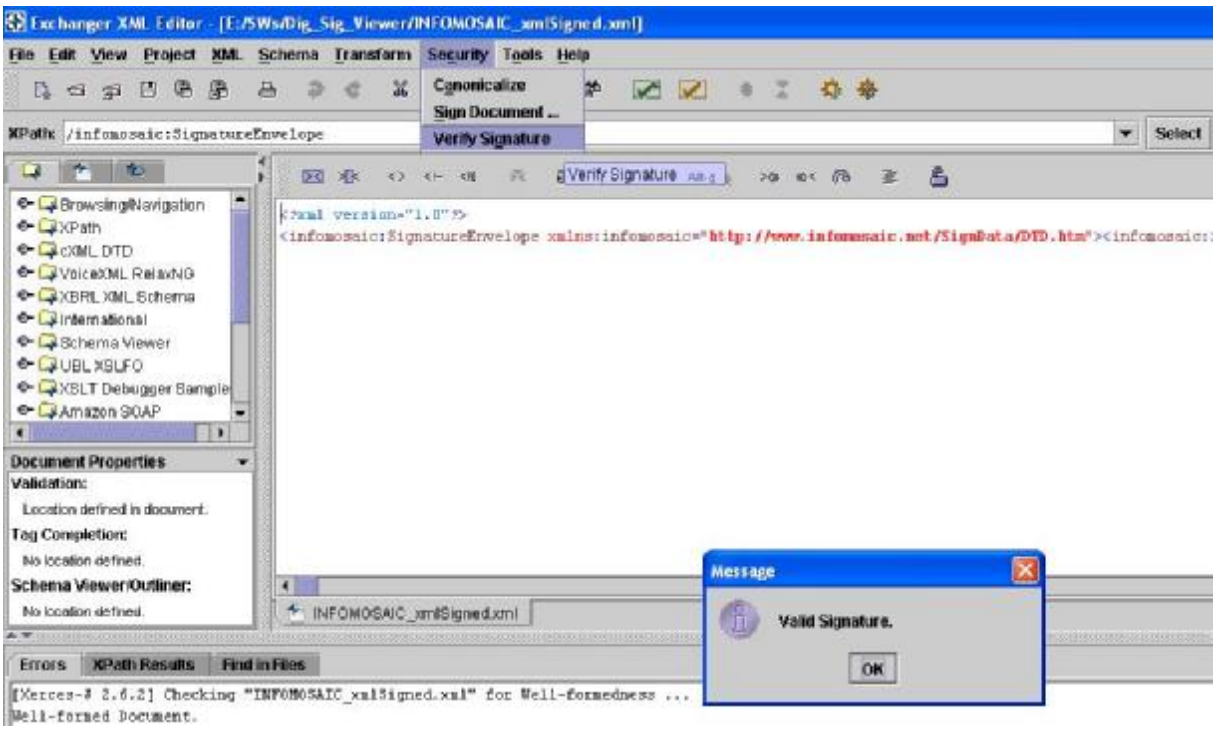
Az OpenXAdES által létrehozott XML elektronikus aláírást a SecureXML ellenőrizte.

2. számú melléklet

Az Exchanger XML Editor által létrehozott XML elektronikus aláírást a SecureXML ellenőrizte.

3. számú melléklet

A SecureXML által létrehozott XML elektronikus aláírást az Exchanger XML Editor ellenőrizte.



4. számú melléklet

Az OpenXAdES által létrehozott XML elektronikus aláírást az Exchanger XML Editor ellenőrizte.