PROHARDVER ELEKTONIKUS PIACTÉR ELEKTONIKUS ALÁÍRÁSSAL

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

1. Bevezetés

A PROHARDVER Informatikai Kft. elektronikus piactere műszaki követelményeinek meghatározásánál mind a technológiai, mind a jogi szabályozásokat figyelembe kellett venni. Ezek között elsődlegesek voltak a hazai szempontok, illetve ezen túlmenően az Európai Unió vonatkozó iránymutatását is figyelembe kellett venni. Az Európai Unió 2001/115/EC direktívájának értelmében 2004. január 1-től (Magyarországon a csatlakozás napjától, 2004. május 1-től) minden tagállamban az irányelveknek megfelelően létrehozott jogszabályi keretek között kell tudni kezelni az elektronikus számlákat. A jogszabályi alapokat még az 1999/93/EC direktíva fektette le, amely kimondta az elektronikus aláírás használhatóságát az élet különböző területein, így az elektronikus számlázásnál is. Ebből is látszik, hogy e két téma szorosan összefügg. A jogszabályi háttér megszületése révén a követelményeknek a tagállamok (Magyarország a „20/2004. (IV. 21.) PM rendelet az elektronikus számláról" című rendelet révén) eleget tettek, azonban néhány technológiai részletkérdés tisztázása tekintetében mind a hazai, mind a nemzetközi szinten van még elmaradás. A probléma megoldásának fontosságát jelzi az, hogy az elektronikus aláírásról szóló direktíva és törvény megszületése óta talán ez az első eset, ahol valóban komoly előnyök jelentkeznek a papírról elektronikusra történő áttérés révén, igény mutatkozik az elektronikus számlák használatára minden területen, így nagy valószínűséggel megindulhat az elektronikus aláírás használatának elterjedése, amelynek majd újabb lökést adhat a bankok részéről a kriptográfiát használó intelligens kártyák bevezetése.

2. Általános szempontok

Az elektronikus világban létező személyek valós világnak való megfeleltetésére a gyakorlatban több módszer is elterjedt (pl. felhasználói nevek és jelszavak hozzárendelése természetes személyekhez), azonban a legmagasabb biztonsági szinten (pl. kormányzati szféra) ez nem képzelhető el nyilvános kulcsú infrastruktúra (PKI) és elektronikus aláírás nélkül. A biztonsághoz és a megbízható működéshez azonban alapvető fontosságú az együttműködési képesség vizsgálata is a különböző technológiai megoldásokon alapuló alkalmazásoknál, ezért nagy hangsúllyal kell figyelembe venni az Európai Unió ebben az irányban tett komoly erőfeszítéseit. Célunk olyan megoldás kifejlesztése, amely jövőbe mutató és akár az Európai Unió elektronikus kormányzati szintjének biztonsági követelményeinek is megfelel a nyilvános kulcsú infrastruktúra és az elektronikus aláírás területén.

A nyilvános kulcsú infrastruktúra és az elektronikus aláírás alkalmazása az alábbiakban felvázoltak szerint valósulna meg:

1. Az ügyfél nyilvántartásba kerül az intelligens kártya és a szükséges kriptográfiai adatok kibocsátásakor.

2. Az ügyfél az interneten keresztül el tudja érni az elektronikus piacteret a megadott címen (URL) a böngésző segítségével. A kommunikációs csatorna a TLS v1.0 (RFC 2246) protokollt használja és megköveteli az ügyfél hitelesítését is.

3. A böngészőben megjeleníthető, webes felületen megjelenik az elektronikus piactér.

4. Az ügyfél (client) által kiválasztott termék megrendelésével az elküldésre kerülő űrlap (form) ellátódik elektronikus aláírással (ETSI TS 101 903 szabványnak megfelelő XAdES-A típusú XML elektronikus aláírás).

5. A kiszolgáló (server) oldalán a megrendeléshez tartozó elektronikus aláírás ellenőrzésre kerül.

6. A megrendelt termékkel kapcsolatos pénzügyek rendezése az ügyfél (client) feladata, amelynél (pl. a banki átutalás) szintén használni kell az elektronikus aláírást.

7. A pénzügyek rendezése után a szükséges adatok felhasználásával előáll a kiszolgáló (server) oldalán az elektronikus számla. A számlázó alkalmazás nyílt szövegű kimenete az UBL v2.0 (OASIS) megfelelő sémájába ágyazott – a tartalmi szempontból az Európai Unió és a hazai szabályozásnak is megfelelő – elektronikus számla, mint XML állomány kerül elektronikus aláírásra.

3. Elektronikus aláírás és elektronikus számlázás

Az elektronikus aláírás elsősorban a megrendelő űrlapnál, illetve az elektronikus számla dokumentum hiteelsségének és sértetlenségének biztosításánál jelenik meg.

A több évtizede létező kriptográfiai, matematikai alapokat használó alkalmazások a világméretű igény növekedése miatt komoly megmérettetésen estek át az elmúlt néhány évben. Az egységes akarat kialakulását a jogi szabályozás megszületése követte az elektronikus aláírás használatáról, majd szigeteket alkotott csoportok kezdték el használni tanúsítványukat, intelligens kártyájukat különböző területen. A szakemberek korán felismerték, hogy a viszonylag kevés felületet, interfészt lefedő szabványok miatt a különböző alkalmazások együttműködésénél komoly problémák lehetnek. Több nagyobb projekt indult el, amelyek mind az együttműködési képességet vizsgálták a különböző (akár végfelhasználói, akár hitelesítés-szolgáltatói) alkalmazásoknál. A biztonságnak és megbízható működésnek alapvető feltétele az együttműködési képesség, hiszen annak hiányában (pl. a tanúsítvány visszavonási adatainak nem kielégítő ellenőrzése gyakori hiba) kialakulhat „hamis biztonságérzet” a felhasználóban, ami ugyanolyan rossz tanácsadó, mint a „túlzott veszélyérzet”.

A szabványok az Európai Unió 1999/93EC direktívája, és annak hazai megvalósítása, a 2001. évi XXXV. törvény az elektronikus aláírásról kiadása óta megszaporodtak. A háttérben folyó munkákból a nyilvánosság keveset ismert meg (pl. a KEAR projekt, nemzetközi bejegyzések a névfába), de 2004. tavasza óta Magyarországon 3000 adóalanynak (2004. február 1.), illetve a magánnyugdíjpénztári tagdíjbevallásnál a befizetőknek elektronikus aláírással ellátott adatot kell (vagy lehet) benyújtania. Az első szélesebb körben elterjedő használat feltehetőleg az

elektronikus számlázás terén fog megvalósulni, amely jelentős anyagi terheket vesz le a számlát kibocsátók válláról. Az elektronikus aláírás terjedését fokozhatja a bankok mágneskártyáról intelligens kártyára való átállása is, de a mobil telefonok SIM-kártyái is jó alapul szolgálhatnak a különböző megvalósítások használatánál, hiszen az ország 81%-os lefedettséggel büszkélkedhet. Részben az elektronikus számlázáshoz kapcsolódóan módosult az elektronikus aláírásról szóló törvény (ld. 2004. évi LV. törvény), amely kiegészült az elektronikus aláírással ellátott adatok archiválásának feltételeivel.

Az elektronikus aláírás átlátható felépítése, könnyű – és emiatt együttműködésre képes – kezelése miatt alkották meg az XML elektronikus aláírás alapjait, mint XML sémát a W3C és az IETF gondozásában (RFC 3275), amelyet az Európai Unió szabványosító szerve, az ETSI kiegészített (XAdES), hogy megfeleljen a törvényi értelemben vett fokozott biztonságú elektronikus aláírásnak.

> *The XAdES-BES satisfies the legal requirements for electronic signatures as defined in the European Directive on electronic signatures.*
> (forrás: ETSI TS 101 903 v1.2.2)

Az ETSI különböző, XAdES elektronikus aláírást létrehozó alkalmazások együttműködési vizsgálatát végezte el („plugtest”), s a zárójelentések azt mutatják, hogy a kisebb eltérések egységesítése, a szabványban tett módosítások elvégzése után a szabványnak teljes mértékben megfelelő alkalmazások együttműködési képessége biztosítottá vált.

A XAdES elektronikus aláírási formátummal összhangban a CEN szabványosító szerv ISSS munkacsoportja meghatározta az elektronikus aláírás-létrehozó és -ellenőrző alkalmazásokkal szemben támasztott biztonsági követelményeket.

A XAdES elektronikus aláírás formátum különböző felhasználási esetekre különböző, egymásra épülő típusokat határoz meg, amelyen belül az archiváláshoz szükséges adatokat – amelyekre az elektronikus számlák esetében is szükség van – a XAdES-A típus tartalmazza. A technológiai szabályozásban leírtakat össze kell vetni a jogi szabályozással, hogy minden tekintetben megfeleljen az elektronikus számlák archiválása az Európai Unió és Magyarország követelményeinek.

Az archiválás kapcsán történt elektronikus aláírás törvény módosítása (2004. évi LV. törvény) értelmében az érvényességi lánc áll magából a dokumentumból (vagy annak lenyomatából), a tanúsítványokból (nyilvános kulcsok), tanúsítvány visszavonási listákból (CRL) vagy tanúsítvány visszavonási állapotokból (OCSP válasza) és az időbélyegből (amely megfelel az RFC 3161 szabványnak).

Tételesen fel vannak sorolva az archiválási szolgáltató által – a benyújtott elektronikus dokumentumon – elvégzendő műveletek. Az érvényességi láncon (pl. a különböző adatokkal kiegészített elektronikus számlán vagy a megrendelői űrlapon) időbélyeget kell elhelyezni.

A szükséges elemeket a XAdES formátumok közül a XAdES-A, vagyis az archiválásra megfelelő struktúra tartalmazza. A hosszú távon megőrzendő adatok sértetlenségét védő időbélyeget (a technológiai követelményektől függően) időnként megújítva biztosítható az aláírt adatok védelme.

Advances in computing increase the probability of being able to break algorithms and compromise keys. [...] Over a period of time weaknesses may occur in the cryptographic algorithms used to create an electronic signature [...]. Before such weaknesses become likely, a verifier should take extra measures to maintain the validity of the electronic signature. [...] In such a case, a sequence of time-stamps will protect against forgery. [...] Archive validation data MAY thus bear multiple embedded time-stamps.
(forrás: ETSI TS 101 903 v1.2.2)

Az archivált adatok biztonsága az eltelt idő függvényében csökkenhet, ezért fontos hogy időnként kriptográfiai értelemben vett, az eredetinél erősebb algoritmussal vagy az eredeti algoritmussal, de erősebb kulccsal legyen megújítva az elektronikus aláírás. Nyilvánvalóan nehezebb lenne a dokumentumon, a felhasználói tanúsítványon, a szolgáltatói tanúsítványokon, tanúsítvány visszavonási listán (CRL) vagy tanúsítvány visszavonási állapoton (OCSP response) újból, külön-külön elvégezni a műveletet, ezért elég egy, az egész adathalmaz hitelességét és sértetlenségét biztosító elektronikus aláírást létrehozni – ami a XAdES esetében egy olyan időbélyeg, amelynek bemenetét a védendő adatok lenyomata (hash, messageImprint) adja –, amit az <ArchiveTimeStamp> XAdES sémában szereplő XML elem tartalmaz.

Az elektronikus számla kapcsán a fogalmak, jogszabályi feltételek megismerése után érdemes megvizsgálni a technológiai megvalósítás lehetőségeit.

A PM rendelet meghatározza az elektronikus számla fogalmát, amely szerint az elektronikus számla (ha nem EDI-rendszerekről van szó) legalább fokozott biztonságú elektronikus aláírással és időbélyegzővel ellátott elektronikus adat formájában bocsátható ki

A PM rendelet megemlít egy IHM közleményt a megőrzési, archiválási követelményekhez kapcsolódóan. Ez az *IHM közlemény az elektronikus aláírással ellátott számlák kiállításához és azokra vonatkozó megőrzési kötelezettség teljesítéséhez alkalmazott elektronikus aláírás és időbélyegző biztonságos kriptográfiai algoritmusairól* címet viseli, amely mindenki számára hozzáférhető.

1. §
(2) Az elektronikus számla az áfa-törvény 43. §-ának (7) bekezdésében meghatározott feltételek szerint adóigazgatási azonosításra akkor felel meg, ha az adóalany az elektronikus számla
a) eredetének hitelességét,
b) tartalmának teljességét, megváltoztathatatlanságát, sértetlenségét,
c) értelmezhetőségét (olvashatóságát),
d) a jogosultak általi hozzáférhetőségét, valamint
e) a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés elleni védelmét
a kibocsátáskor és a számla megőrzésére külön jogszabály által előírt időtartam alatt is biztosítja.

Az „eredet hitelessége” és a „tartalom teljességének, megváltoztathatatlanságának, sértetlenségének” biztosítása jellemzően a kriptográfiai lenyomatok (hash), illetve a digitális aláírás használata révén valósulhat meg, amelyről a XAdES (XML) elektronikus aláírás kapcsán már esett szó.

Az elektronikus számla „értelmezhetőségét (olvashatóságát)” az elektronikus dokumentum formátumának megfelelő meghatározása biztosítja. Hosszú távon a technológiától lehető legfüggetlenebb megoldást kell keresni, ezért – bár alkalmas lenne a PDF (Portable Document Format) formátum is – célszerűbb egyszerű, nyílt szövegként kezelhető állományokként tárolni az elektronikus számlákat (pl. egy XSD sémának megfelelő, UTF-8 szerinti kódolású Unicode karakterkészletet használó XML formátumú állomány). Az XML segítségével a különböző adatbázisok, számlázó alkalmazások közötti hordozhatóság nem jelent problémát. Az informatika világában egyre több területen jelentkezik igény az együttműködési képesség biztosítására, és sok esetben nyújt megoldást az adatok leírásánál az XML.

Az állomány formátuma mellett figyelembe kell venni a tartalmi, az üzenetek formátumára vonatkozó követelményeket is. Az értelmezhető (olvasható), strukturált tartalom révén megoldhatóvá válik az elektronikus számlák automatizált feldolgozása. Nyilvánvalóan széles körben együttműködésre képes rendszerekkel lehet csak a problémától mentes működést elérni, ezért nemzetközileg elfogadott (elsősorban az Európai Unió tagállamaira vonatkozó) szabványokat kell követni az üzenetek formátumának meghatározásakor is.

Az APEH (Adó- és Pénzügyi Ellenőrzési Hivatal) a 2004/9. „Adó és ellenőrzési értesítő” című kiadványban tette közzé az elektronikus számla sémáját. A DTD (Document Type Definition) sémák alapján elő lehet állítani az XML sémákat (XSD állományokat), amelyek révén lehet bocsátani az elektronikus számlákat, mint XML állományokat. A megjelenítéshez (pl. böngészőben) mindössze egy stíluslap dokumentumra (XSL állomány) van szükség.

Az APEH elektronikus számlájának adattartalma megfelel a – 2004. május 1. után megváltoztatott – áfa-törvényben meghatározottaknak, azonban a gyakorlatban más jogszabályokat is figyelembe kell venni a számlák kitöltésénél (pl. számviteli törvény, jövedéki törvény).

Az APEH elektronikus számlájának felépítése igazodik az adattartalomhoz, azonban az együttműködési képesség megőrzése érdekében a technológiát is meg kell vizsgálni, ugyanis Magyarországnak ezen a téren is az Európai Unió elvárásainak megfelelő megoldást kell alkalmaznia.

Az egységes, szabványos számlaformátum kidolgozásához az APEH által meghatározott séma jó kiindulási alapul szolgál, azonban azt adószakértők segítségével ki kell egészíteni, illetve műszaki szakemberek révén megfelelő formátumba kell ágyazni.

Jelenleg három nemzetközi számlaformátum pályázik arra, hogy általánosan elfogadható, a jogi és technológiai szabályozásnak is megfelelő szabvánnyá váljon:

- OASIS UBL (Universal Business Language),
- UN/CEFACT Cross Industry Invoicing Process,
- IDA (Interchange of Data between Administrations) e-Ordering and e-Invoicing phases.

A jogi háttér azonos volta (pl. 77/388/EEC) miatt a különböző formátumok tartalmi elemei között könnyedén lehetne leképezéseket készíteni, a különbség inkább a szemléletmódban van. Az IDA (aminek utódja az IDABC – Interoperable Delivery of pan-European eGovernment Services to public Administrations, Businesses and Citizens) alapvetően

közigazgatási (az e-Procurement, azaz az elektronikus közbeszerzési) szemszögből, az OASIS és az UN/CEFACT kereskedelmi szemszögből közelíti meg a kérdést.

Az IDA elektronikus közbeszerzéshez kapcsolódó programjának keretein belül elvégzett kutatások, a többi sémában a hiányosságok feltárása és a kidolgozott XML sémák mindössze útmutatóul szolgáltak. Az XML séma felépítése, tartalmi elemei a brit OGC (Office of Government Commerce), norvég eHandel és az UBL v0.7 sémáin alapultak. Az OASIS és UN/CEFACT szakembereivel folytatott megbeszélések szerint az Európai Bizottság nem fogja frissíteni a sémát, nem fogja az esetleges változásokat követni az IDA számlaformátumában. A hiányosságok feltárása nagyban hozzájárult az UBL v0.7 javításához, így az UBL későbbi változatai már megfelelnek majd az IDA által megfogalmazott követelményeknek.

Az ebXML technológián alapuló rendszerek meghatározása az OASIS és az UN/CEFACT feladata volt, amelyen belül az UN/CEFACT szakembereire hárult az üzenetek kidolgozása. A helyzetet bonyolítja, hogy az OASIS szabványosító szerven belül is létezik egy üzenetformátummal foglalkozó munkacsoport, az UBL, amely szintén alkalmas arra, hogy ebXML rendszereknél használják.

A CEN/ISSS e-IFG (e-Invoicing Focus Group) elektronikus számlázással foglalkozó munkacsoportja által támogatott UN/CEFACT jelenleg a számlaformátum elvi felépítését tartalmazó dokumentumot (Business Requirements Specification, Cross Industry – Supply Chain, Invoice Process) tudja felmutatni. Az Európai Unió az UN/CEFACT eredményeire fog támaszkodni, amelyeket Magyarországnak is figyelembe kell venni, de valószínűsíthető, hogy az egyes munkacsoportok között megegyezés fog születni.

Az UBL v1.0 formátumait az IDA szakemberei is megvizsgálták, sőt, az UBL v1.0 üzenettípusai révén a teljes üzleti folyamatot (a megrendeléstől a számlázásig) meg lehet valósítani elektronikusan, automatizáltan. Ezt bővítette az UBL v2.0, amely a beszerzéssel kezdi és a fizetéssel zárja a folyamatot. Nem kevésbé hangsúlyos előny, hogy az UBL számlaformátumának használata esetén a majdan bevezetésre kerülő ebXML rendszereknél problémáktól mentesen lehet átültetni az elektronikus számlákat (és egyéb UBL szabványnak megfelelő üzeneteket) az új környezetbe. Magyarország az Európai Unió tagállama, ezért csak akkor tudná elfogadni az UBL számlaformátumot szabványosnak, ha azt nemzetközileg is jóváhagyják.

Az UBL v1.0, illetve v2.0 üzenetei közvetett módon ugyan, de az EDIFACT üzenetein alapulnak, ezért az együttműködési képesség visszafelé is biztosított. Az UBL fejlesztésénél az EDIFACT szabványhoz szorosan kötődő xCBL v3.0 (XML Common Business Library) XML sémáit emelték át, és kezdték kiegészíteni.

A „jogosultak általi hozzáférhetősége” és a „jogosulatlan hozzáférés” szabályozására is vonatkoznak előírások az elektronikus aláírási törvény módosításában és a PM rendeletben akár archiválási szolgáltató tárolja az elektronikus számlákat, akár a kibocsátó.

Az elektronikus aláírási törvény módosítása szerint az előfizető által benyújtott elektronikus dokumentum hozzáférhetőségét biztosítania kell az archiválási szolgáltatónak (pl. az előfizető rendelkezik a megfelelő jogosultságokkal a nyilvántartáshoz, a nyilvántartás elérhető valamilyen hálózaton keresztül, a kiszolgáló üzemel nagy rendelkezésre állással). A PM

rendelet értelmében a jogosultak teljes körének kell hozzáférést biztosítania az archiválási szolgáltatónak.

4. Összefoglalás

A PROHARDVER Informatikai Kft. elektronikus piacterének hátterében meghúzódó folyamatok közül a kriptográfiát igénylő, újításokat jelentő megoldások lettek bemutatva. Ezek révén megvalósulhat a jogi követelményeknek teljes mértékben megfelelő elektronikus piactér, amelynél az elektronikus aláírással ellátott megrendeléstől kezdve az elektronikus számláig minden a legkorszerűbb technológia alapján működik.