ELŐADÁSOK NYOMDAKÉSZ ANYAGA

ELEKTRONIKUS ARCHIVÁLÓRENDSZER FEJLESZTÉSE PKI ALAPOKON

Kollár Balázs, nypee@interware.hu
Krasznay Csaba, krasznay@ik.bme.hu
Budapesti Műszaki és Gazdaságtudományi Egyetem Informatikai Központ

1. Bevezető

A közelmúltban a Magyar Elektronikus Aláírási Szövetség (MELASZ) elkészítette a digitális aláírások formátumára vonatkozó közös ajánlását [1], mely nemzetközi szabványok [2], [3] alapján ad útmutatást a hazai fejlesztőknek. Ez az ajánlás mérföldkőnek tekinthető az elektronikus iratkezelés hazai elterjedésének szempontjából, amely számos előnye ellenére még várat magára, habár a jogi szabályozás már 2001 óta lehetővé teszi a váltást. Az ajánlás megteremti az alapját az elektronikus iratkezelésre épülő termékek és szolgáltatások hazai piacának. Ugyanis az intézmények iratkezelésük megszervezésekor szabványos felületen kapcsolódó alkalmazások közül válogathatnak, melyek egymást kiegészítve komplex iratkezelő rendszerek kialakítását teszik lehetővé.

Célul tűztük ki egy saját alkalmazás elkészítését, amely képes a MELASZ ajánlásának megfelelő dokumentumok kezelésére, és amelyre később összetett szolgáltatásokat lehet építeni, különös tekintettel az elektronikus archiválásra. Követtük a korszerű szoftver-technológiai irányvonalakat, így az alkalmazás Web-alapú, több-felhasználós, többrétegű, relációs adatbázisra és XML állományokra épül, hardware platform független és objektum-orientált.

A szoftvert kilenc hónapja fejlesztjük, mely idő alatt kiforrtak a rendszer alacsony szintű funkciói, valamint több magas szintű szolgáltatása is rendelkezésre áll. Ezek a tervek szerint folyamatokban fognak egyesülni.

2. A szabványok

2.1. XML Advanced Electronic Signature (ETSI TS 101903)

Az XML elektronikus aláírás „európai” kierjesztése a XAdES. A különböző követelmények teljesítésére különböző elektronikus aláírás formátumokat dolgoztak ki. A meghatározott aláírás-típusok az alábbiak.

1. BES, az alapszintű elektronikus aláírás. Ez a formátum megfelel az Eat. fokozott biztonságú aláírásának, hitelesítést és integritásvédelmet biztosít, de letagadható.
2. XAdES-T, az aláírás időpontjával kiegészített elektronikus aláírás. Az XAdES-T az előző formát egészíti ki egy (megbízható) időbélyegzés szolgáltatótól származó időpecséttel. A megbízható időbélyeg egy kezdeti lépést jelent az aláírás hosszú távra szóló érvényességének biztosítására.

3. XAdES-C, a teljes körű érvényesítő adatokkal kiegészített elektronikus aláírás. Az XAdES-T formához képest hivatkozásokat tartalmaz a teljes érvényességi láncra, és a szükséges tanúsítvány-visszavonási listákra. Előnye, hogy az aláírás későbbi érvényesítéséhez minden adat rendelkezésre áll. Erre a típusra akkor lehet szükség, ha az aláíró, és esetleg a hitelesítés-szolgáltató tanúsítványának lejárta után is szükség lesz az aláírás ellenőrzésére. A XAdES-C aláírást nem lehet „azonnal" létrehozni, mivel annak eldöntése, hogy egy tanúsítvány egy időpillanatban érvényes-e, csak egy bizonyos kivárási idő eltelte után lehetséges teljes bizonyossággal. Például a hitelesítés-szolgáltatónak is idő kell a visszavonási listák frissítéséhez. A kivárási idő az ITKTB [4] ajánlásban az elvárt biztonsági szinttől függően 1-3 nap.
4. XAdES-X, az XAdES-C elektronikus aláírás kibővített változata. Az XAdES-X Long nem csak hivatkozásokat tartalmaz az érvényesítő adatokra, hanem magukat az adatokat is magába foglalja.
5. XAdES-A, az archív érvényesítő adatokkal kiegészített elektronikus aláírás. Azokra az esetekre biztosítja az elektronikus aláírás hitelességét, integritását és letagadhatatlanságát, amikor az aláírás elkészítéséhez használt algoritmus, kulcs, tanúsítvány meggyengült. A XAdES-A egy időbélyeggel látja el a teljes aláírást, amelynek kriptográfiai erőssége mindig elég erős lehet a kor technológiai követelményeihez igazodva. Az Eat. az archiválási-szolgáltatók számára a következőt írja elő.

[5] Eat. 16/G. § (2) A szolgáltató köteles a Hatóság határozata szerinti, elfogadott kriptográfiai algoritmuson alapuló minősített elektronikus aláírást elhelyezni és minősített szolgáltató által kibocsátott időbélyegzőt elhelyezni vagy elhelyeztetni az érvényességi láncon:

1. a szolgáltatási szabályzatban meghatározott időközönként;
2. a határozatban előírt időpontban.

2.2. MELASZ XAdES profil

A Magyar Elektronikus Aláírás Szövetség (MELASZ) 2005. szeptemberében fogadta el az ETSI XAdES szabványra alapuló aláírás profilját. A MELASZ a hazai elektronikus aláíró alkalmazást fejlesztő cégeket tömörítő civil szervezet.

A profil tartalmazza a XAdES szabvány minden kötelező elemét, a választható elemek jelentős részének használatát azonban nem engedi meg. A szűkítést a magyarországi felhasználói és szolgáltatói szempontok figyelembevételével tették meg. Szűkítették a használható XML elemek, valamint a hivatkozható algoritmusok körét. Ezzel egyszerűsödik a profilnak megfelelő alkalmazások megvalósítása, hiszen kevesebb elem és algoritmus kezelésére kell felkészülni, míg az alkalmazás funkcionalitása ezzel nem csökken.

Két aláírás formátumot határoztak meg, a „hosszú távú" és az „archív" MELASZ aláírást.

3. A lehetséges felhasználók

A technológia biztosítja, hogy elektronikusan keletkező iratokat hitelesen alá lehessen írni, és ez az aláírás évek múltán is megőrizze biztonságát. Szabványok biztosítják, hogy az egyes szoftverek képesek legyenek együttműködni.

Az archiválás feladata dokumentumok hosszú távú megőrzése. Ha megvalósul olyan alkalmazás, amely teljesen papírmentes, továbbá a keletkezett iratokat meg kell őrizni, akkor elektronikus iratokat kell archiválni. Ilyen alkalmazási terület lehet az elektronikus államigazgatás és az elektronikus számlázás, hiszen előbbinél a megőrzési idő lehet akár több tíz, utóbbinál legfeljebb tíz év.

Az archiválás egyfelől megbízható adattárolási probléma, amely az állományok fizikai elveszését hivatott elsősorban redundáns tárolással megelőzni. Másfelől a digitális aláírás logikai felépítésében rejlő gyengeségeket kell kezelni, amelyek hosszú távon jelentkezhetnek. Meggyengülhet valamely kriptográfiai módszer, amelyet az aláíráshoz használtak. Innen természetesen még hosszú út vezetne archivált iratok megváltoztatásához, vagy új hamis iratok készítéséhez, de az elvi lehetőség fennáll.

Ha feltételezzük, hogy mindig lesz aktuálisan erős lenyomatképző és aláíró eljárás, akkor az archivált iratokat időközönként meg lehet erősíteni egy-egy újabb, erősebb időbélyeggel, ami tanúsítja, hogy a bélyegzés időpontjában a dokumentumon szereplő aláírások még hitelesek voltak.

3.1. Ügyintézés

2005. november 1-jével lép hatályba a Közigazgatási eljárásról szóló törvény (KET), amely kimondja, hogy a hivatalok ügyfelei online kapcsolatba léphetnek az ügyeiket intéző szervekkel egy központi rendszeren keresztül. Így várhatóan egyre kevesebb ügy miatt kell okmányirodába és más hivatalokba bemenni. „Jelenleg már Interneten keresztül igényelhető vállalkozói igazolvány, jogosítvány, lakcímigazolvány, forgalmi, útlevél és egyéb hivatalos irat, 2005 végéig 27-re nő azoknak az okmánytípusoknak a száma, amelyeket Interneten keresztül igényelhet a lakosság.” [7].

3.2. Elektronikus számlázás

2006. január 1-től már az APEH is elfogadja az elektronikus számlákat hitelesnek, így nagy mennyiségű papíralapú számla kiváltása várható a közeljövőben. Elsősorban a nagy szállító cégek lehetnek érdekeltek, hiszen egymás között nagy számlaforgalmat bonyolítanak le. A nagy lakossági ügyfélkörrel rendelkező szolgáltatóknál inkább lassú váltás várható, melynek korlátja a lakossági internet használat aránya.

Ilyen számlakibocsátók a közüzemi szolgáltatók, valamint a nagy lakossági bankok, vagy az ilyen szempontból optimális helyzetben lévő internet szolgáltatók, hisz nekik minden ügyfelük rendelkezik elektronikus elérhetőséggel. Ezek a szervezetek számlák millióit állítják ki évente, amelyek költsége postázással együtt darabonként körülbelül 100Ft. Elektronikus számlázás esetén a szolgáltató fokozott biztonságú digitális aláírással és időpecséttel látja el a számlát a biztonság érdekében. Ennek a költsége a papír-alapú megoldás 10-30%-a. [6] A számlákat a fogadó csak akkor köteles archiválni, amennyiben azt az APEH felé el szeretné számolni. Ez a kötelezettség a vállalkozásokat érinti, így ők az archiválási szolgáltatások lehetséges felhasználói.

4. A kifejlesztett alkalmazás

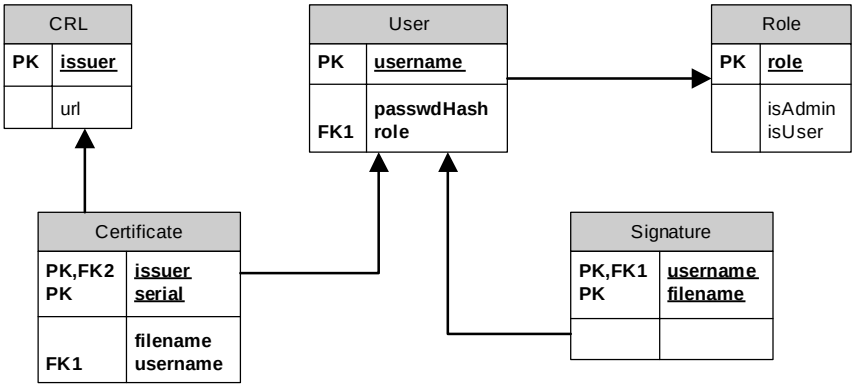
4.1. A fejlesztés célja

A fejlesztési munkánk célja egy olyan alkalmazás létrehozása volt, amely képes a MELASZ ajánlásnak megfelelő aláírás típusokkal kapcsolatos feladatok elvégzésére. A

rendszer lehetővé teszi több-felhasználó párhuzamos elérését, felhasználói felületét web böngésző jeleníti meg, külön üzemeltető felülettel is rendelkezik.

4.2. A rendszer adatmodellje

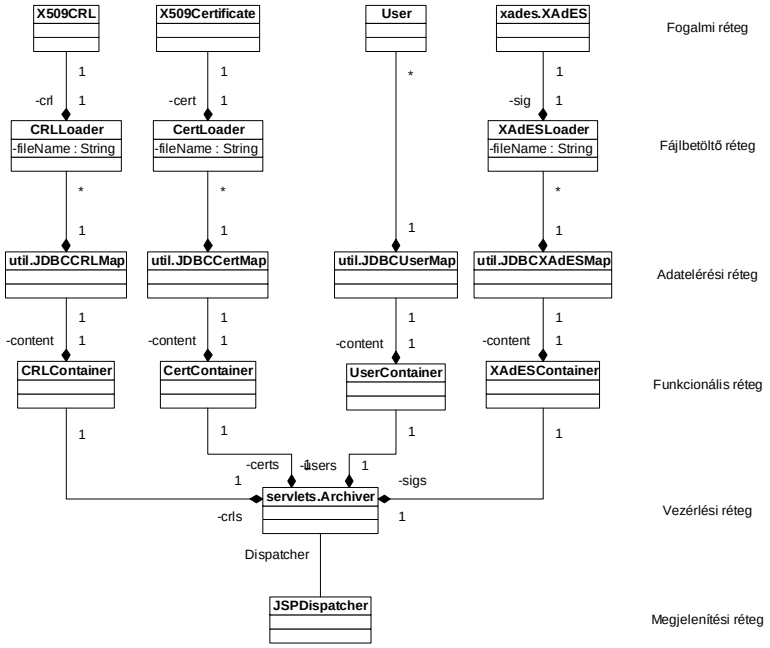
A rendszerben kezelt hosszú élettartamú adatok tárolása két módon történik. A fájlokban érkező adatokat a fájlrendszerben tárolja a rendszer, így azok a megszokott, kiforrott, kényelmes formában állnak a fejlesztők és a rendszer üzemeltetői részére. A rendszer egyéb adatait relációs adatbázisban tárolja, melynek adatmodellje a következő ábrán látható.



1. ábra A rendszer adatmodellje

4.3. A rendszer szerkezete

A rendszer szerkezete a következő ábrán látható. A struktúra elsősorban az adattárolás követelményei után szervezett.



2. ábra - A rendszer szerkezete

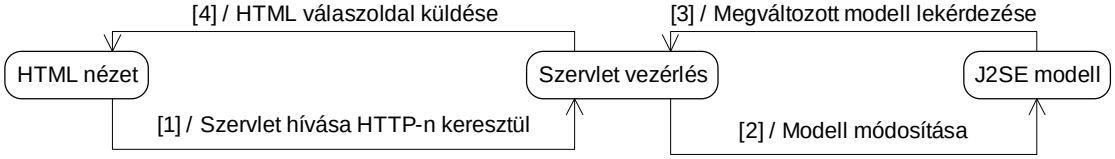
A legfelső szinten helyezkednek el a fogalmi modell elemei, a tanúsítvány visszavonási lista, a tanúsítvány, a felhasználó és az aláírás. Közöttük az előző fejezetben leírt kapcsolati viszonyok állnak fenn.

A harmadik adatelérési réteg vonja be a relációs adatbázist a tárolásba. Az adatbázis tartalmazza az előző fejezetben szereplő táblákat, amelyek leírják az egyes visszavonási listák, tanúsítványok, felhasználók és aláírások egymás közötti viszonyát. Az adatelérési réteg ezeket a táblákat és a fájlokat rejti el, amennyiben a funkcionális réteg felé csak a fogalmi réteg osztályait (CRL, Certificate, User, XAdES Signature) szolgáltatja.

A funkcionális réteg magas szintű műveleteket nyújt. Az egyes entitásokat, és a rajtuk értelmezett műveleteket a következő táblázat foglalja össze.

	Tanúsítvány-visszavonási lista	**Tanúsítvány**	**Felhasználó**	**Aláírás**
Felvétel	**X**	**X**	**X**	**X**
Kikérés	**X**	**X**	**X**	**X**
Összes kikérése	**X**	**X**	**X**	**X**
Eltávolítás	**X**	**X**	**X**	**X**
Frissítés	**X**			
Mentés	**X**		**X**	**X**

A vezérlési réteg az alkalmazás dinamikus viselkedésének központi eleme.



3. ábra - Vezérlés

A vezérlés fogadja a beérkező kérést, majd annak tartalmától függően módosítja a modellt a funkcionális réteg metódusain keresztül. A módosított modellt lekérdezi, majd visszaküldi a kérőnek a megváltozott nézetet. Az implementációban a nézet egy böngészőprogramban megjelenő HTML oldal, a vezérlést Java Servlet kód végzi, a modell pedig az előzőekben bemutatott Java objektumokból áll. Utóbbi úgy készült el, hogy kizárólag J2SE technológiákat használjon. Ennek az előnye az, hogy a modell újrafelhasználható más szerkezetű rendszerekben, például könnyen építhető rá Webszolgáltatás (WebService), vagy átalakítható EJB modellé.

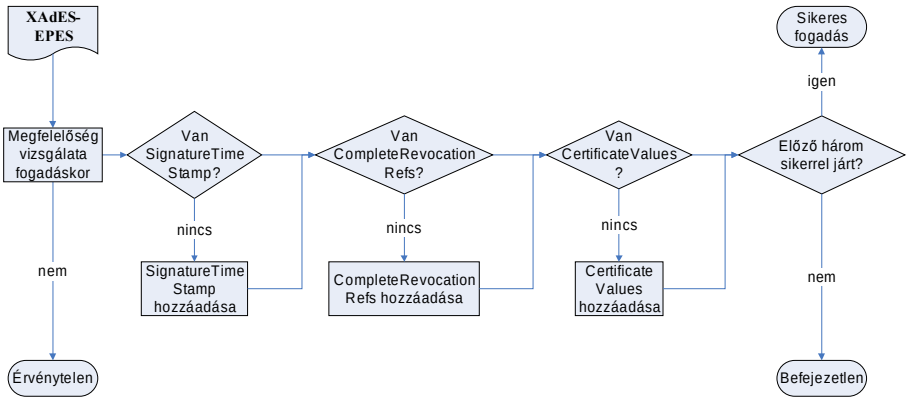
Fontos jellemzője a vezérlési rétegnek, hogy itt jelenik meg először a bejelentkezett felhasználó fogalma. Ilyenből több is lehet egyidejűleg, megkülönböztetett kiszolgálásuk az ún. munkameneteken keresztül történik.

A megjelenítési réteg formázza a felhasználónak küldött választ. Bemenetként kapja a modell megváltozott paramétereit, a kimenete pedig egy HTML oldal. Az implementációban a megjelenítést JSP technológiát használó oldalak végzik.

4.4. Folyamatok

A rendszer a kezelt aláírásokon az alábbi négy folyamatot képes végrehajtani, melyek összhangban vannak a [1] MELASZ szabvány hatodik fejezetével. Az egyes folyamatokat folyamatábrák szemléltetik, a bennük szereplő feldolgozások ún. magas szintű funkciók, melyeket a funkcionális réteg nyújt.

4.4.1. Az aláírás fogadása



4. ábra - Az aláírás fogadás utáni ellenőrzése

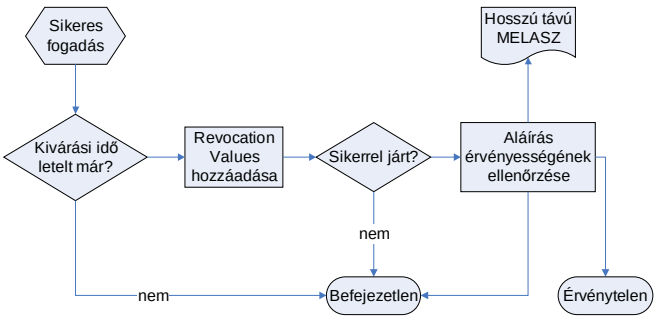
Amikor egy aláírás bekerül a rendszerbe, számos feltételnek kell meg felelnie, amelyeket a rendszer ellenőriz. A szabvány szerint ezeket a feltételeket az aláírást létrehozó alkalmazásnak kell biztosítania. Ha az elvárt minimális feltételek nem teljesülnek, a folyamat eredménye „érvénytelen”. Megfelelőség esetén három további elem meglétéről kell gondoskodni, amelyeket nem kötelezően az aláírást létrehozó alkalmazás is csatolhat. Ha mind a három elemet sikerül csatolni, akkor az aláírás fogadása sikerrel zárult.

Az első az aláírás időbélyege (SignatureTimeStamp), amely hitelesen igazolja, hogy az aláírás létezett egy bizonyos időpillanat előtt. Ettől számítva a kivárási idő letelte után lehet az aláírás kezdeti ellenőrzését, azaz a következő folyamatot.

A második elem hivatkozásokat tartalmaz mindazon tanúsítványok visszavonási listájára, amelyek a hitelesítési láncban szerepelnek (CompleteRevocationRefs).

A harmadik elem tartalmazza a hitelességi láncban szereplő tanúsítványokat.

4.4.2. Az aláírás kezdeti ellenőrzése



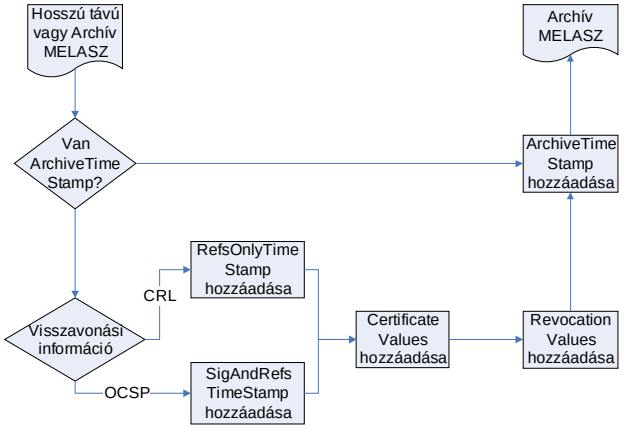
5. ábra - Aláírás kezdeti ellenőrzése

A sikeresen fogadott aláírások feldolgozásának következő lépése az ún. kezdeti ellenőrzés. Ez a folyamat a kivárási idő letelte után hajtható végre sikerrel. A kivárási időszak kezdete az aláírás első hiteles időbélyegzésétől számítandó, hossza CRL visszavonási listák használata esetében 24 óra, OCSP azonnali tanúsítvány állapotot szolgáltató szerver használata esetén 30 perc.

Amennyiben a kötelező kivárási idő már eltelt, be kell szerezni a hitelességi láncban szereplő tanúsítványok állapotát igazoló adatokat. Ezután ellenőrzést kell végrehajtani az aláíráson. Ha az ellenőrzés megerősíti az aláírás érvényességét, azaz a kriptográfiai aláírás

érvényes, és az aláíró tanúsítványt sem veszítette el az érvényességét a kivárási idő alatt, akkor az aláírás érvényes hosszú távú MELASZ aláírás.

4.4.3. Az aláírás archiválása



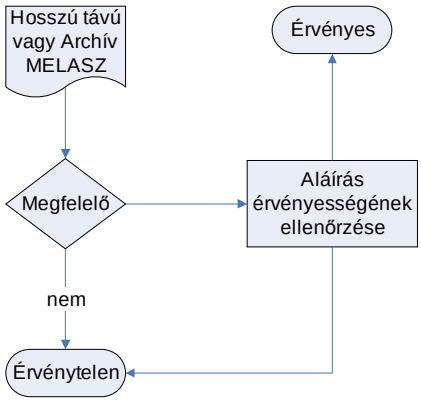
6. ábra - Aláírás archiválása

Archív MELASZ aláírás előállításához egy érvényes hosszú távú, vagy egy érvényes archív MELASZ aláírásra van szükség. Utóbbi esetben csak egy újabb archív időbélyeg kerül az aláírásra.

Az első eset akkor fordul elő, ha az aláírást először kerül archiválása. Ekkor ki kell egészíteni a visszavonási listájának megfelelő időbélyeggel, amely CRL lista használata esetén egy RefsOnlyTimeStamp elembe kerül, vagy azonnali tanúsítvány állapot információ (OCSP) használata esetén egy SigAndRefsTimeStamp. Ezután hozzá kell adni az aláíráshoz a tanúsítványokat a CertificateValues elemben, majd a visszavonási információkat a RevocationValues elemben. Végül egy archív időbélyeget (ArchiveTimeStamp elemet) kell készíteni a teljes aláírásra. Ez az időbélyeg abban különbözik az előzőektől, hogy az aláírás minden elemét védi ellentétben a többi időbélyeggel, amelyek nem védik az összes csatolt információt.

A második esetben az aláírás már volt archiválva, és a mostani archiválás archív felülbélyegzést jelent. Erre akkor lehet szükség, ha az előző archiváláskor használt algoritmus vagy kulcs hitelét veszíti. Ebben az esetben csak az archív időbélyeget (ArchiveTimeStamp elemet) kell az aláírásra elhelyezni.

4.4.4. Aláírás utólagos ellenőrzése



7. ábra - Aláírás utólagos ellenőrzése

Aláírás utólagos ellenőrzésekor a már az aláíráshoz csatolt hitelesítő adatok alapján kell annak érvényességét eldönteni. Első lépésben a formátum helyességét kell megvizsgálni. Lényeges a kötelező mezők megléte és helyes tartalma. Második lépésben az aláírás kriptográfiai ellenőrzését kell elvégezni. Ha az aláírás mindkét ellenőrzésen átmegy, akkor érvényes, ellenkező esetben érvénytelen.

5. Továbbfejlesztési lehetőségek

Az alkalmazás továbbfejlesztése számos irányba folytatódhat. A folyamatok működését alapos tesztelésnek kell alávetni, valamint kiterjedt együttműködési tesztelést is kell végezni a jelenleg is fejlesztés alatt álló egyéb hazai MELASZ szabványt támogató alkalmazásokkal. Fontos feladat felmérni a rendszer potenciális felhasználóinak körét, valamint az ő részükről felmerülő igényeket.

A fejlesztéseket technológiai oldalról a futtató platform lecserélésével lehet a legjobban támogatni. A mostani webkonténer (Apache Tomcat) környezet EJB-alapú alkalmazásszerverre cserélése sok kisebb problémát megoldana.

Egy komoly alkalmazásszerver használata esetén a rendszer további felületeit is könnyen meg lehetne valósítani. A webes kezelőfelület mellé ki lehetne fejleszteni egy XML WebService felületet is, így a rendszer bármilyen platformon futó másik alkalmazásból elérhetővé válna, például Microsoft .NET alapú programokból.

6. Köszönetnyilvánítás

A mű a Nemzeti Kutatási és Technológiai Hivatal Támogatásával valósult meg. Köszönet illeti Dr. Frigó József tanár urat, aki előadásai során ismertette a korszerű szoftverfejlesztés filozófiáját és módszereit.

7. Irodalom

[1] Egységes MELASZ formátum elektronikus aláírásokra; verzió: 1.0

[2] RFC 3275 XML-Signature Syntax and Processing

[3] ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)

[4] Aláírási szabályzatra vonatkozó elvárások a magyar elektronikus közigazgatásban. *forrás:* Információs Társadalom Koordinációs Tárcaközi Bizottság, Elektronikus Közigazgatás Albizottság, http://www.itktb.hu/engine.aspx?page=ias

[5] 2004. évi LV. törvény az elektronikus aláírásról szóló 2001. évi XXXV. törvény módosításáról

[6] Lehetőség az e-számlázás http://www.montana.hu/MonWeb/Doc.asp?DocID=9&CikkID=390

[7] Jövőre indul az elektronikus számlázás – Index.hu; 2005 október 13. http://index.hu/tech/ihirek/?main:2005.10.13&239764