

Az elektronikus hitelesség vizsgáztatási tapasztalatai
Erdösi Péter Máté, CISA
Magyar Elektronikus Aláírás Szövetség, alelnök
ISACA Education and Dissemination Committee volunteer member
elektronikus aláírással kapcsolatos szolgáltatási szakértő
NJSZT Információrendszer-ellenőrzési szakértő
mailto: elnokseg@melasz.hu
web: <http://www.melasz.hu>

Az előadás a Magyar Elektronikus Aláírás Szövetség (MELASZ) által támogatott különböző elektronikus aláírási oktatások vizsgáztatásainak tapasztalatait mutatja be, három szempontból:

1. vizsga iskolai érdemjegyekért
2. vizsga akkreditált tanár-továbbképzési program részeként
3. az új ECDL modul vizsgáztatás műszaki háttere

A MELASZ azzal a céllal jött létre 2003 decemberében, hogy az elektronikus aláírást és annak rokon, kapcsolódó és származékos technológiáit népszerűsítse, széleskörű hazai bevezetésüket támogassa, elterjedésüket elősegítse. Ebben a folyamatban a Szövetség katalizátor szerepet vállal és kommunikációs, koordinációs tevékenységet is folytat. Három tevékenysége kiemelt figyelmet érdemel:

- I. MELASZ READY 2.0 program, a magyar fejlesztésű aláíró alkalmazások szabvány szerinti együttműködési képességeinek tanúsítására,
- II. Graduális oktatás aktív támogatása az Informatika-Számítástechnika Tanárok Egyesületén (ISZE) keresztül,
- III. ECDL Elektronikus hitelesség, elektronikus aláírás új, magyar modul kialakításában szakmai támogatás nyújtása az NJSZT ECDL Iroda számára.

A MELASZ READY 2.0 program keretében 2011 áprilisában már nyolc olyan alkalmazás van Magyarországon, melyek szabványos keretek között együtt tudnak működni, azaz az egyik által készített szabványos aláírást a másik tudja fogadni, értelmezni és feldolgozni. Meg kell említeni azt is, hogy a nyolcból kettő alkalmazás az európai interoperabilitási teszteken is sikeresen szerepelt. Az alkalmazások tanúsítványai a MELASZ honlapjáról letölthetők.

A MELASZ támogatja az elektronikus aláírási iskolai oktatását is, ennek keretében 2009-ben létrejött egy Tanári Kézikönyv és 7-12. évfolyamok számára Tanmeneteket is kialakítottunk, melyek kipróbálására 2010-ben került sor. A tapasztalatok azt mutatják, hogy a diákok minden nehézség nélkül képesek elsajátítani az elektronikus aláírási technikai elemeket, de általános iskolában még vannak nehézségek az elméleti háttér megismerésével kapcsolatosan, hiszen a matematikai alapozást csak az elemi matematika segítségével lehetséges itt megtámogatni. A gyakorlatban az aláírási funkciókat és az aláíró programok használatát a diákok nagyon könnyen elsajátították, és ezt a tudást java részben a záró dolgozatig megőrizték, vagyis mondhatjuk, hogy beépült a saját tudástárukba a digitális aláírási technológiája. Az oktatás metodikája egyenlő részben tartalmazott elméleti és gyakorlati kérdéseket is, hiszen ez a korosztály (8. osztály) a számítógép előtt ülve inkább a gyakorlati tennivalókra volt fogékonyabb, mintsem a száraz elméleti magyarázatokra.

A záró dolgozat feladatai között voltak négyelemű feleletválasztásos tesztkérdések és gyakorlati feladatok is az aláírási készítésére és ellenőrzésére vonatkozóan. A tapasztalat szerint az órai munka akkor ment a legjobban, amikor a számítógépes környezet homogén volt, és előre fel volt készítve az elektronikus aláírási feladatokra – ideértve a tanúsítványok előzetes feltöltését és az aláíró programok előzetes installálását is.

Annak érdekében, hogy az informatika-tanárok is képesek legyenek ezt a technológiát oktatni, 2010-ben és 2011-ben több helyszínen (Budapest, Eger, Miskolc) elindult az ISZE vezető oktatóinak, informatika tanárainak a továbbképzése. Ennek során egyrészt kialakult a továbbképzés módszertani háttere (tematika), másrészt a képzés lebonyolítási struktúrája (akkreditált pedagógusképzés). A képzések a MELASZ aktív támogatásával működtek. A tanárok a továbbképzés során mind az elméleti, mind a gyakorlati ismeretekkel megismerkedtek, számos

dobozos és nyílt forráskódú aláíró programot használtak és változatos aláírás-fajtákat hoztak létre és hasonlítottak össze. A lebonyolított tanfolyamok végére a résztvevő tanárok képesek voltak egy önálló óravázlat összeállítására és egy olyan vizsgafeladatsor megoldására is, mely 10 elméleti és 8 gyakorlati kérdésből állt. Az eddigi tanfolyamok tapasztalatai szerint a tanárok számára ezek az ismeretek az újdonság erejével hatottak, de rövid idő alatt képessé váltak az új ismeretek oktatására, amihez éles, személyes aláíró tanúsítványt is kaptak az oktatást segítő eszközökön túlmenően. A továbbképzés létrehozásakor a célkitűzés az volt, hogy minden régióban legyenek felkészítve olyan tanárok ennek a témakörnek az oktatására, akik tovább tudják adni ezt a tudást mások (diákok, tanárok) számára.

A továbbképzés tematikája az alábbi főbb pontokból áll:

1. Az információ és a mai társadalom
2. Az elektronikus aláírás az információs társadalomban
3. Nyilvános kulcsú infrastruktúra rendszerek (public key infrastructure, PKI)
4. A tanúsítvány és tulajdonságai
5. Az elektronikus aláírások osztályozása
6. A digitális aláírások készítése
7. Az elektronikus ügyintézés és megvalósulási formái
8. Didaktikai követelmények megvalósítása

Ezeket a témaköröket keresztül készítjük fel az iskolákban tanító tanárokat az elektronikus hitelesség oktatására. A programban 2011 első negyedévéig 29 gyakorló pedagógus vett részt 5 régióból (Budapest, Szeged, Salgótarján, Eger, Miskolc).

Az ECDL Elektronikus Hitelesség, Elektronikus Aláírás modul vizsgáztatásának háttere 2011 első negyedévében alakult ki, tekintettel arra, hogy a modul újdonság az eddig megszokott modulok között. Alapvető igényként fogalmazódott meg, hogy a vizsgáztatás legyen platformfüggetlen, egyszerű és könnyen adaptálható minden vizsgaközpont számára. A szakmai támogatást itt is a MELASZ nyújtotta. A vizsgakérdésekből milliárdon felüli vizsgasor állítható össze, a vizsgáztatás egyedisége tehát biztosított. A vizsgázóknak számot kell adniuk elméleti és gyakorlati tudásukról is, a súlypontot a gyakorlati ismeretekre helyezve. Csupán elméleti válaszokkal nem lehetséges sikeres vizsgát tenni – ez el is várható egy gyakorlat-orientált vizsgától. A 9 millió európai ECDL-vizsgával rendelkező felhasználó bizonyítja az európai népességben az informatikai írástudás meglétének szükségességét és létjogosultságát, ezért ez a vizsga várhatóan kiemelkedik majd a többi közül az e-világban általános jellege miatt. Az elektronikus hitelességet minden elektronikus területen lehet – és néhol ma már kötelező is – alkalmazni. Ahhoz, hogy a szoftverkönyezet ne legyen az akadálya az elektronikus hitelesítési tudás elterjesztésének, számos szoftverkombinációban meg kellett oldani a vizsgáztatási környezet kialakítását, mely magában foglalta a kérdések, válaszok és vizsgán szükséges előre elkészített munkafájlok szoftverkönyezetenkénti kialakítását is.

A MELASZ az alábbi környezetekben tartja lehetségesnek az ECDL Elektronikus hitelesség, elektronikus aláírás vizsga lebonyolítását:

Sorszám	Operációs rendszer	Office program	Aláírás-létrehozó program	Aláírás-ellenőrző program	Internet Böngésző	JPG	BMP	TIFF	ODT	ODS	ES3	DOC	DOCX	XLS	XLSX	PDF	ASC	TSQ
I.	MS Windows XP	MS OFFICE 2003	MOKKA	Acrobat Reader	Internet Explorer	+	+	+	-	-	+	+	-	+	-	+	-	-
II.	MS Windows XP	MS OFFICE 2003	MOKKA	Acrobat Reader	Firefox	+	+	+	-	-	+	+	-	+	-	+	-	-
III.	MS Windows XP	MS OFFICE 2003	e-Szignó	Acrobat Reader	Internet Explorer	+	+	+	-	-	+	+	-	+	-	+	-	-
IV.	MS Windows XP	MS OFFICE 2003	e-Szignó	Acrobat Reader	Firefox	+	+	+	-	-	+	+	-	+	-	+	-	-
V.	MS Windows XP	MS OFFICE 2007	MOKKA	Acrobat Reader	Internet Explorer	+	+	+	-	-	+	-	+	-	+	+	-	-
VI.	MS Windows XP	MS OFFICE 2007	MOKKA	Acrobat Reader	Firefox	+	+	+	-	-	+	-	+	-	+	+	-	-
VII.	MS Windows XP	MS OFFICE 2007	e-Szignó	Acrobat Reader	Internet Explorer	+	+	+	-	-	+	-	+	-	+	+	-	-

Sorszám	Operációs rendszer	Office program	Alíráslétrehozó program	Alíráellenőrző program	Internet Böngésző	JPG	BMP	TIFF	ODT	ODS	ES3	DOC	DOCX	XLS	XLSX	PDF	ASC	TSQ
VIII.	MS Windows XP	MS OFFICE 2007	e-Szignó	Acrobat Reader	Firefox	+	+	+	-	-	+	-	+	-	+	+	-	-
IX.	MS Windows XP	OpenOffice	MOKKA	Acrobat Reader	Internet Explorer	+	+	+	+	+	+	-	-	-	-	+	-	-
X.	MS Windows XP	OpenOffice	MOKKA	Acrobat Reader	Firefox	+	+	+	+	+	+	-	-	-	-	+	-	-
XI.	MS Windows XP	OpenOffice	e-Szignó	Acrobat Reader	Internet Explorer	+	+	+	+	+	+	-	-	-	-	+	-	-
XII.	MS Windows XP	OpenOffice	e-Szignó	Acrobat Reader	Firefox	+	+	+	+	+	+	-	-	-	-	+	-	-
XIII.	MS Windows 7	MS OFFICE 2003	MOKKA	Acrobat Reader	Internet Explorer	+	+	+	-	-	+	+	-	+	-	+	-	-
XIV.	MS Windows 7	MS OFFICE 2003	MOKKA	Acrobat Reader	Firefox	+	+	+	-	-	+	+	-	+	-	+	-	-
XV.	MS Windows 7	MS OFFICE 2003	e-Szignó	Acrobat Reader	Internet Explorer	+	+	+	-	-	+	+	-	+	-	+	-	-
XVI.	MS Windows 7	MS OFFICE 2003	e-Szignó	Acrobat Reader	Firefox	+	+	+	-	-	+	+	-	+	-	+	-	-
XVII.	MS Windows 7	MS OFFICE 2007	MOKKA	Acrobat Reader	Internet Explorer	+	+	+	-	-	+	-	+	-	+	+	-	-
XVIII.	MS Windows 7	MS OFFICE 2007	MOKKA	Acrobat Reader	Firefox	+	+	+	-	-	+	-	+	-	+	+	-	-
XIX.	MS Windows 7	MS OFFICE 2007	e-Szignó	Acrobat Reader	Internet Explorer	+	+	+	-	-	+	-	+	-	+	+	-	-
XX.	MS Windows 7	MS OFFICE 2007	e-Szignó	Acrobat Reader	Firefox	+	+	+	-	-	+	-	+	-	+	+	-	-
XXI.	MS Windows 7	OpenOffice	MOKKA	Acrobat Reader	Internet Explorer	+	+	+	+	+	+	-	-	-	-	+	-	-
XXII.	MS Windows 7	OpenOffice	MOKKA	Acrobat Reader	Firefox	+	+	+	+	+	+	-	-	-	-	+	-	-
XXIII.	MS Windows 7	OpenOffice	e-Szignó	Acrobat Reader	Internet Explorer	+	+	+	+	+	+	-	-	-	-	+	-	-
XXIV.	MS Windows 7	OpenOffice	e-Szignó	Acrobat Reader	Firefox	+	+	+	+	+	+	-	-	-	-	+	-	-
XXV.	Ubuntu Linux	OpenOffice	PGP, OpenSSL	Acrobat Reader és WebSznó	Firefox	+	+	+	+	+	+	-	-	-	-	+	+	+

Az MS Windows és az MS Office szoftverek a Microsoft Corporation termékei, az e-Szignó szoftver a Microsec Kft. saját terméke, míg a MOKKA program a Netlock Kft. saját fejlesztése. Hozzá tartozik az informatikai háttérhez, hogy mind az e-Szignó, mind a MOKKA aláíró szoftverek rendelkeznek MELASZ-READY 2.0 tanúsítással, valamint a Microsec Kft., és a Netlock Kft. is hozzájárult szoftvereinek és szolgáltatói infrastruktúrájának az ECDL Elektronikus hitelesség, elektronikus aláírás modulvizsgán való felhasználásához (aláíró programok, minősített időbélyegek, tesztanúsítványok, teszt-időbélyegek, valamint webszolgáltatások tekintetében). A próbatanfolyam eredménye szerint a vizsgázatási környezet illeszkedik a tanfolyam elvárásaihoz, a felkészítő tanfolyam résztvevői kivétel nélkül elsajátították az elektronikus aláíráshoz kapcsolódó ismereteket és a próbavizsga során a tesztkérdésekre is 85%-on felüli arányban adtak helyes válaszokat.

Ha elfilozofálunk arról, hogy milyen változások jöhetnek létre az elektronikus hitelességi tudás széleskörű elterjedésének megvalósulásakor a magyar és az európai információs társadalomban, akkor sok esetben közelítenünk kell az Európai Unió célkitűzései felé. Az Európai Unió régóta bátorítja a tagállamokat a hiteles elektronikus kommunikáció alkalmazására, szeretné, ha az Európai Unión belül megvalósulhatna az egyablakos elektronikus ügyintézési rendszer, vagyis a polgárok elektronikusan bárhol is igénybe vehessék az alapvető közzolgáltatásokat, ami nyilvánvaló módon a belső, tagállami határokon átívelő megoldás, azaz nem lehetséges ezeket tagállami határokkal megakasztani. Erre vannak már működő példák ma is, egyrésztől Észtországban lehet vállalkozást alapítani elektronikusan portugál, finn, dán digitális tanúsítvány segítségével, másrésztől Dániában az államigazgatás kizárólag elektronikus számlát ad ki az ügyfeleknek,

továbbá az Európai Bizottság előtt sem ismeretlenek már a digitálisan hitelesített dokumentumok. Filozofálásunk végeztével elmerenghetünk azon, hogy milyen lehet az ügyintézés egy olyan világban, ahol bármelyik internet-csomóponttól feladható az ügyfél elektronikus dokumentuma – természetesen digitális aláírással hitelesítve, nem kéri meg arra, hogy töltsse le, nyomtassa ki, írja alá, majd postázza/faxolja vissza, vagy esetleg menjen be aláírni az ügyintézőhöz az ott létrehozott papír alapú iratot, hanem minden ügyfél teljesen elektronikusan ír egy dokumentumot, írja alá azt a dokumentumot, elektronikus úton lerója illetékfizetési kötelezettségét, és elektronikus számlát is kap minderről, amit tárolhat a saját elektronikus terrabájtos otthoni vagy mobil háttértárolóján, földön, vízen és levegőben egyaránt.

A globális információs társadalom nem képzelhető el elektronikus és egyben hiteles folyamatok, információk, adatok nélkül, a papír alapú folyamatok ma már sok esetben a hatékonyság és a hatásosság gátjaként lépnek fel. Az elektronikus aláírás széles körben elterjedt ismerete egy új világot tárhat fel a társadalmi folyamatok területén a jövőben, amelyben kevesebb időt töltünk irataink előállításával, továbbításával és hitelességének biztosításával – így talán több idő jut más, produktív tevékenységekre. De ez a jövő még mindig egy kicsit messzinek tűnik. Abban lehet ma bízni, hogy a jövő nemzedéke elektronikus hitelesítési tudással felvértezve sokkal közelebb fog kerülni ehhez a jövőhöz, mint ahol most mi vagyunk – ennek a jeleit sorolta fel ez a cikk.