MELASZ

Az elektronikus hitelesség vizsgáztatási tapasztalatai

Erdősi Péter Máté, CISA

Magyar Elektronikus Aláírás Szövetség, alelnök
elektronikus aláírással kapcsolatos szolgáltatási szakértő
NJSZT Információrendszer-ellenőrzési szakértő
ISACA Education and Dissemination Committee volunteer
mailto: elnokseg@melasz.hu
web: http://www.melasz.hu

Tartalom

MELASZ

- MELASZ READY 2.0 program
- MELASZ-ISZE oktatási program tanároknak és diákoknak
- ECDL Elektronikus hitelesség, elektronikus aláírás magyar modul MELASZ támogatása
- Gondolatkísérlet

MELASZ READY 2.0

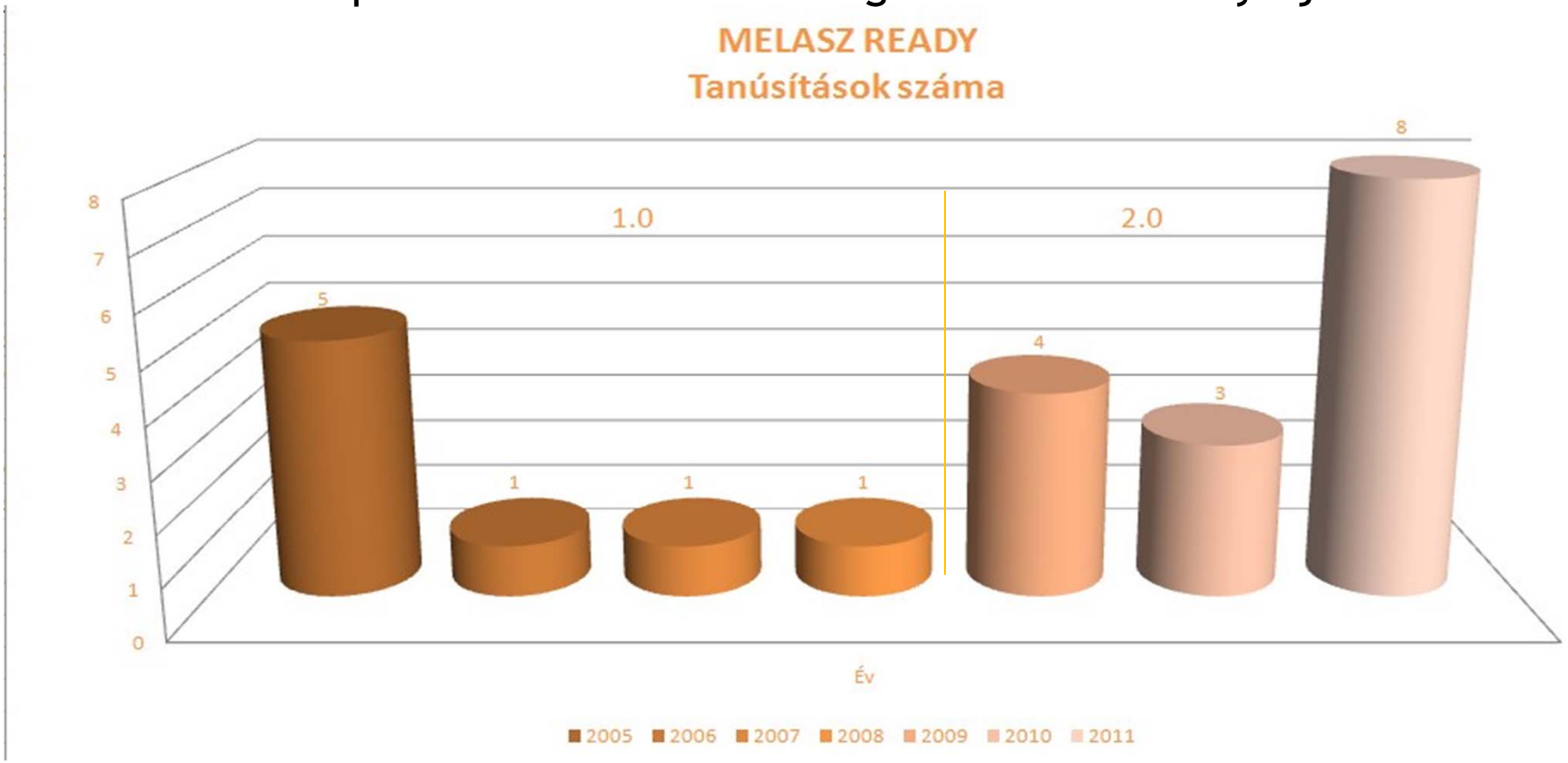
MELASZ

- Egységes formátum elektronikus aláírásokra (verzió 2.0)
- A meghatározott aláírási formátumok az alábbi nemzetközi szabványokon alapulnak:
  - RFC3852 Cryptographic Message Syntax (CMS)
  - ETSI TS 101 733 Electronic Signature Formats
  - RFC3275 XML-Signature Syntax and Processing (XMLDSIG)
  - ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)
- Az időbélyegzés formátuma az alábbi ajánlás szerinti:
  - Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható időbélyegzés formátum műszaki specifikációjára
- Megfelelnek az 1999/93/EU Irányelvben definiált „Advanced Electronic Signature” követelményeinek -> legalább fokozott biztonságú aláírások, melyek minősítettek is lehetnek

MELASZ READY 2.0

- MELASZ READY 1.0 érvényes 2005-től
- MELASZ READY 2.0 érvényes 2008 decemberétől

http://www.melasz.hu/lang-hu/melasz-ready-ajanlas



MELASZ-ISZE oktatási program

MELASZ

- Célkitűzés: mind a 20 régióban legyen hozzáértő informatika-tanár az Informatika-Számítástechnika Tanárok Egyesületében az akkreditált tanár-továbbképzési program keretében
- Eredmények 2010-2011-ben:
  - Budapest, Salgótarján, Eger, Szeged, Miskolc régiókban
  - Összesen 29 gyakorló tanár vett részt a képzésben
- Vizsgakövetelmények
  - Elméleti teszt: 10 kérdés, 4 feleletválasztós teszt, 1 helyes válasszal
  - Gyakorlati rész: 8 kérdés, aláírás készítése, ellenőrzése, biztonságos honlap adatainak ellenőrzése
  - Óravázlat készítése és prezentálása egy adott témakörben
- 75-100% közötti teljesítmények minden esetben

  http://www.melasz.hu/lang-hu/remository?func=select&id=20

MELASZ-ISZE oktatási program

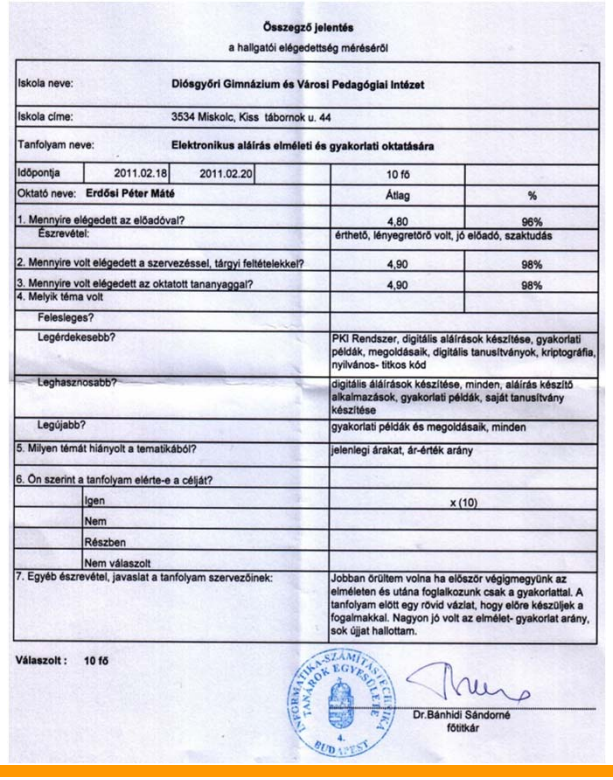
MELASZ

- A MELASZ és tagjainak támogatási formái
  - Szakértői támogatás
  - Mentor/tréneri támogatás
  - Eszköz támogatás (tesztkártyák, kártyaolvasók, aláíró programok)
  - Anyagi támogatás

Eredmény	Támogatás összege
Tanári Kézikönyv és tanmenetek	1 000 000 Ft
Teszt-eszközök a tanároknak	500 000 Ft
ISZE tanár-továbbképzés	350 000 Ft
2010-2011 összesen:	**1 850 000 Ft**

MELASZ-ISZE oktatási program

- Értékelések a tanár kollégák által
  - Új, korszerű ismereteket közöl
  - Gyakorlati arány megfelelő
  - Mind a szoftveres, mind a kártyás tanúsítványok használatára felkészít



Összegző jelentés

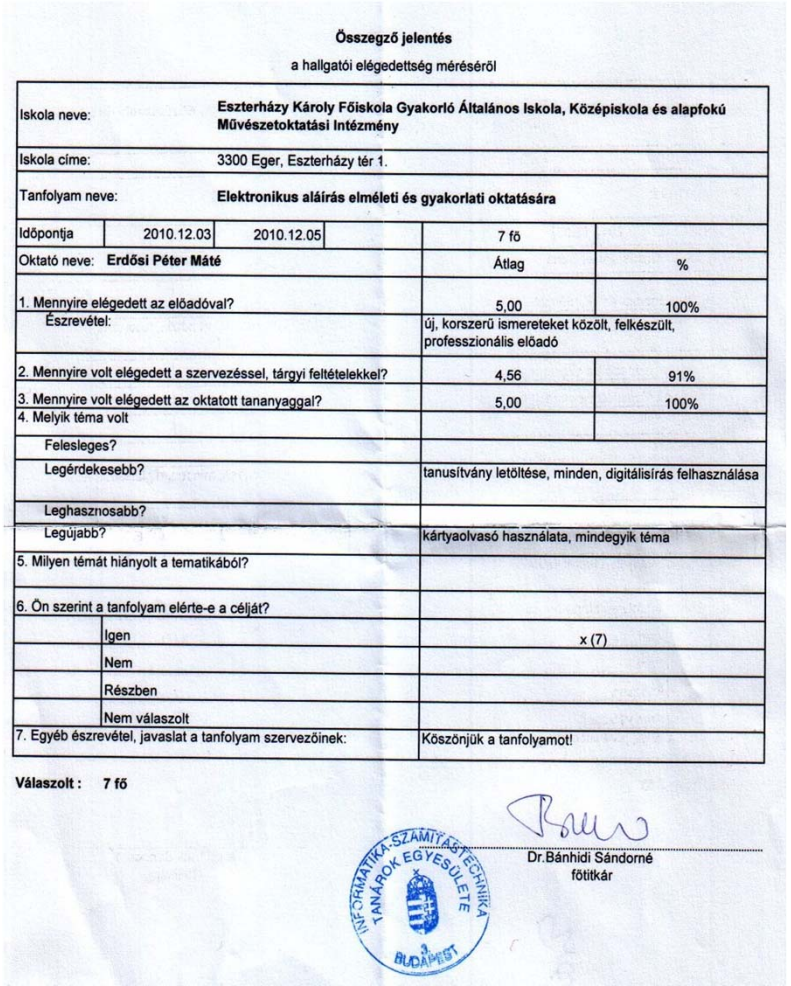
a hallgatói elégedettség méréséről

Iskola neve:	Diósgyőri Gimnázium és Városi Pedagógiai Intézet			
Iskola címe:	3534 Miskolc, Kiss tábornok u. 44			
Tanfolyam neve:	Elektronikus aláírás elméleti és gyakorlati oktatására			
Időpontja	2011.02.18	2011.02.20	10 fő	
Oktató neve: Erdősi Péter Máté			Átlag	%
1. Mennyire elégedett az előadóval?			4,80	96%
Észrevétel:			érthető, lényegretörő volt, jó előadó, szaktudás	
2. Mennyire volt elégedett a szervezéssel, tárgyi feltételekkel?			4,90	98%
3. Mennyire volt elégedett az oktatott tananyaggal?			4,90	98%
4. Melyik téma volt				
Felesleges?				
Legérdekesebb?			PKI Rendszer, digitális aláírások készítése, gyakorlati példák, megoldásaik, digitális tanusítványok, kriptográfia, nyilvános- titkos kód	
Leghasznosabb?			digitális aláírások készítése, minden, aláírás készítő alkalmazások, gyakorlati példák, saját tanusítvány készítése	
Legújabb?			gyakorlati példák és megoldásaik, minden	
5. Milyen témát hiányolt a tematikából?			jelenlegi árakat, ár-érték arány	
6. Ön szerint a tanfolyam elérte-e a célját?				
	Igen		x (10)	
	Nem			
	Részben			
	Nem válaszolt			
7. Egyéb észrevétel, javaslat a tanfolyam szervezőinek:			Jobban örültem volna ha először végigmegyünk az elméleten és utána foglalkozunk csak a gyakorlattal. A tanfolyam előtt egy rövid vázlat, hogy előre készüljek a fogalmakkal. Nagyon jó volt az elmélet- gyakorlat arány, sok újat hallottam.	

Válaszolt : 10 fő

INFORMATIKA-SZÁMÍTÁSTECHNIKA TANÁROK EGYESÜLETE 4. BUDAPEST

Dr.Bánhidi Sándorné
főtitkár



Összegző jelentés

a hallgatói elégedettség méréséről

Iskola neve:	Eszterházy Károly Főiskola Gyakorló Általános Iskola, Középiskola és alapfokú Művészetoktatási Intézmény			
Iskola címe:	3300 Eger, Eszterházy tér 1.			
Tanfolyam neve:	Elektronikus aláírás elméleti és gyakorlati oktatására			
Időpontja	2010.12.03	2010.12.05	7 fő	
Oktató neve: Erdősi Péter Máté			Átlag	%
1. Mennyire elégedett az előadóval?			5,00	100%
Észrevétel:			új, korszerű ismereteket közölt, felkészült, professzionális előadó	
2. Mennyire volt elégedett a szervezéssel, tárgyi feltételekkel?			4,56	91%
3. Mennyire volt elégedett az oktatott tananyaggal?			5,00	100%
4. Melyik téma volt				
Felesleges?				
Legérdekesebb?			tanusítvány letöltése, minden, digitálisírás felhasználása	
Leghasznosabb?				
Legújabb?			kártyaolvasó használata, mindegyik téma	
5. Milyen témát hiányolt a tematikából?				
6. Ön szerint a tanfolyam elérte-e a célját?				
	Igen		x (7)	
	Nem			
	Részben			
	Nem válaszolt			
7. Egyéb észrevétel, javaslat a tanfolyam szervezőinek:			Köszönjük a tanfolyamot!	

Válaszolt : 7 fő

INFORMATIKA-SZÁMÍTÁSTECHNIKA TANÁROK EGYESÜLETE 3. BUDAPEST

Dr.Bánhidi Sándorné
főtitkár

MELASZ-ISZE oktatási program

MELASZ

- Általános iskolában 8. osztályosok között
  - 5-10 órás tanfolyami jellegű oktatás
  - Záró dolgozattal számonkérve
    - Tesztkérdések
    - Aláírás készítése
  - Aláírások készítése általában nem probléma
  - Elméleti háttér néha probléma, elemi matematikával kell aszimmetrikus kriptográfiát megismertetni
  - Záró dolgozat értékei a Gauss-görbét követték
- Egyetemi kurzusokba beépülve (Fujitsu Akadémia)
  - 4-8 órás speciális szeminárium jellegű oktatás
  - Számonkérés elméleti jellegű
  - Önálló tanulásra erősebben lehet építeni (e-Learning)

ECDL Elektronikus aláírás modul

MELASZ

- Modultankönyv széles szakmai támogatást élvez
  - Neumann János Számítógép-tudományi Társaság
  - Informatika-Számítástechnika Tanárok Egyesülete
  - Hírközlési és Informatikai Tudományos Egyesület
  - Miniszterelnöki Hivatal Elektronikuskormányzat Központ
  - Nemzeti Média- és Hírközlési Hatóság (NHH jogutód)
  - Magyar Elektronikus Aláírás Szövetség

http://www.elektronikusalairaskonyv.hu

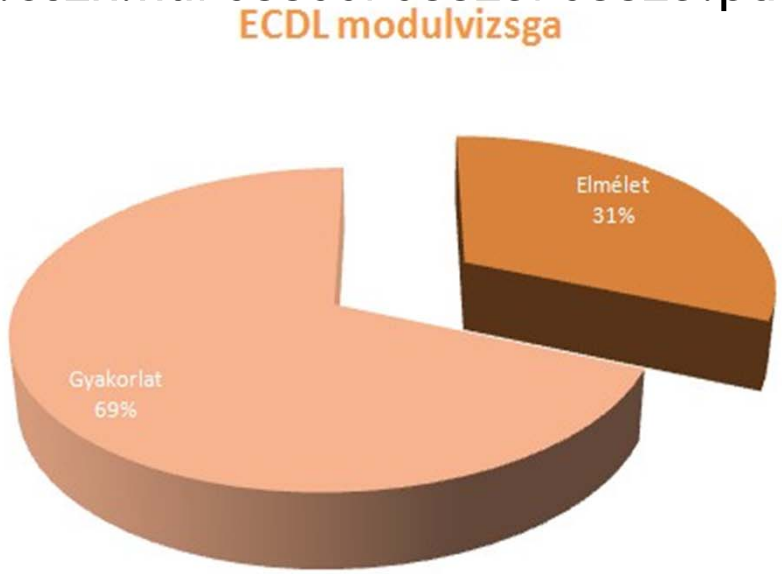
- A modul vizsgáztatásának előkészítése befejeződött 2011. március végén
  - Vizsgaközpontok számára a vizsgacsomagok (25 db) elkészültek
  - Vizsgáztatók felkészítése elindult
  - A modul minőségbiztosítása sikeresen megtörtént
  - Próbavizsga sikeresen lezárult

http://www.ecdl.hu/index.php?cim=opennews&f=20100507_elokeszuletben.htm

ECDL Elektronikus aláírás modul

MELASZ

- ECDL modulvizsga
  - 10 elméleti tesztkérdés 1-1 pont értékben
  - 11 gyakorlati feladat 2-2 pont értékben
  - Összesen 32 pont
- Hogyan oldjam meg a modulvizsga feladatait?
  - http://mek.oszk.hu/08800/08823/08823.pdf



ECDL Elektronikus aláírás modul

MELASZ

- A MELASZ támogatja 25 kombinációban az alábbi szoftverekből előállítható vizsgaplatformokat:
  - MS WINDOWS XP, Win7
  - Linux
  - MS OFFICE 2003, 2007
  - OpenOffice 3.x
  - MOKKA aláíró program
  - E-Szignó aláíró program
  - GNU PG aláíró program
  - OpenSSL TS időbélyegző program
  - MS Internet Explorer , Firefox
- A kimaradó kombinációkra egyedileg rövid idő alatt elkészíthetők a vizsgafájlok és tesztek (ezek természetesen minden csomagban különböznek egymástól)

ECDL Elektronikus aláírás modul

MELASZ

- Példa a tesztekre
  - Elméleti kérdések

18. FELADATSOR

A – Elméleti kérdések

Instrukciók:

Nyissa meg a ***VIZSGA*** fájlt és írja be válaszainak a betűjeleit a fájlban lévő táblázat E1)-E10) soraiba. Mentse el a kitöltött táblázatot ugyanezen a néven!

E1) Mi a gyökér-tanúsítványkibocsátó feladata általában?

a) a végfelhasználói aláírói és titkosító tanúsítványok kiadása

b) a végfelhasználói tanúsítványok visszavonása — 1 pont

c) az alsóbb szintű tanúsítványkibocsátók hitelesítése

d) weboldalak hitelesítése

E2) Mi a tanúsítványelőállítás első lépése az alábbiak közül?

a) tanúsítvány megújítása

b) tanúsítvány aláírása — 1 pont

c) kulcspár generálása

d) tanúsítvány közzététele

E3) Mi az a tanúsítási lánc?

a) a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítése

b) a szoftvereken szereplő aláírások — 1 pont

c) a tanúsítványtárban szereplő gyökértanúsítványok

d) a tanúsítványkibocsátók felülről lefelé építkező aláírásai

ECDL Elektronikus aláírás modul

MELASZ

- Példa a tesztekre
  - Gyakorlati kérdések

GY1)	Nyissa meg ***a BIRSALMA*** fájlt! Írja le az aláíráshoz használt tanúsítványnak a kiállítóját (CN)!	2 pont
GY2)	Nyissa meg ***az ALMA*** fájlt! Mi az aláírás készítőjének a városa (L)?	2 pont
GY3)	Nyissa meg ***a MEGGY*** fájlt! Van-e hiteles időbélyeg a fájlon?	2 pont
GY4)	Nyissa meg ***a MALNA*** dossziét! Mennyi időbélyeg van a dossziéban?	2 pont
GY5)	Nyissa meg ***a DINNYE*** dossziét! Hány aláírás van a teljes dosszién?	2 pont
GY6)	Nyissa meg a **https://www.otpbank.hu** honlapot! Mi az oldal SSL-tanúsítványában szereplő sorozatszám?	2 pont
GY7)	Nyissa meg a **https://www.magyarorszag.hu** honlapot! Mi az SSL-tanúsítvány aláíró algoritmusa?	2 pont
GY8)	Írja alá ***a VIZSGA*** dokumentumot a szövegszerkesztővel!	2 pont
GY9)	Készítsen egy új dossziét ***VIZSGAD*** néven, ***a VIZSGA*** és ***a KORTE*** fájlból az aláíró program segítségével! Írja alá ezt a dossziét egy normál (XADES-EPES), nem időbélyegzett aláírással!	2 pont
GY10)	Lássa el ***a VIZSGAD*** dossziét egy időbélyeggel!	2 pont
GY11)	Írja alá ***a VIZSGAD*** dossziét egy időbélyegzett (XADES-T) aláírással!	2 pont

Filozofálgatás

MELASZ

- Mi lenne, ha
  - teljesen elektronikusan tudnánk ügyeket intézni?
  - nem kellene több sorban állás és nagyobb papírraktár, irattár?
  - mindenkinek lenne saját személyes aláírói tanúsítványa?
  - mindenki ismerné a digitális hitelességi technikákat?
  - Európában vagy akár a világban tudnánk elektronikusan szerződni, teljesíteni, számlázni és fizetni?
  - bárhonnan bármikor bármilyen ügyet el tudnánk intézni teljesen elektronikusan? (B^3)
  - a vállalkozások egymás között áttérnének az elektronikus szerződési és számlázási formákra?
  - a köztisztviselők mindegyike rendelkezne ECDL Start vagy Select és elektronikus aláírás modulvizsgával Európában?
  - nem kellene feleslegesen nyomtatni és ügyintézéssel benzint pazarolni és időt tölteni?

Köszönöm a figyelmet!

MELASZ

Elérhetőségek:

Erdősi Péter Máté, CISA

MELASZ alelnök

E-mail: elnokseg@melasz.hu

Honlap: http(s)://www.melasz.hu

Mobil: +36 20 491 8143

Kérdések?