INSPIRÁCIÓ HÍRLEVÉL

TARTALOM

AZ ELEKTRONIKUS ALÁÍRÁSRÓL

A jövő munkaerőpiacán bizonyosan nagyobb eséllyel próbálkozik az, aki az elektronikus kommunikációban hitelesen tud részt venni, aki képes használni az elektronikus hitelesség különböző formáit is.

Az informatikában a digitális világ fejlődésével és annak a mindennapokban való térnyerésével mára egyre fontosabb kérdéssé vált a hitelesség biztosítása a legtöbb elektronikus folyamatban. Egyre inkább tapasztalható, hogy kizárólag elektronikus folyamatok vesznek minket körül.

Az utóbbi évek eseményei megmutatták, hogy hitelesség nélkül csak egy bizonyos szintig lehetséges bármilyen elektronikus folyamatot (állami, piaci vagy magánszférában) hosszú távon fenntartani.

Az elektronikus folyamatok fejlődésének és továbbfejlesztésének irányai ismertek, de sok esetben ennek korlátjává vált a hitelesség hiánya, vagy alacsony szintje. Emiatt és a digitális fejlődési kényszerek miatt válik indokolttá az elektronikus hitelességnek a diákság számára való megismerése és ehhez kapcsolódóan a gyakorlatban való használati tudásának elsajátítása. A jövő munkaerőpiacán bizonyosan nagyobb eséllyel próbálkozik az, aki az elektronikus kommunikációban hitelesen tud részt venni, aki képes használni az elektronikus hitelesség különböző formáit is. 2009-re műszaki értelemben már széles körben lehetséges az elektronikus hitelességet megvalósító műszaki szolgáltatásokat (viszonylag olcsón) megvásárolni, hiszen több éve léteznek a piacon a hitelesítés szolgáltatások és ezek hatósági felügyelete: minősített és nem minősített hitelesítés-szolgáltatás, minősített időbélyeg-szolgáltatás, minősített archiválás szolgáltatás.

Az ISZE küldetése az, hogy az informatikával kapcsolatos oktatási vonatkozású újdonságokat, ismereteket, tapasztalatokat összegyűjtse és tagjai számára hozzáférhetővé tegye. Elérkezettnek láttuk az időt arra, hogy az elektronikus aláírással – mint a digitális hitelesség tudományával – részletesebben foglalkozzunk. Ebben partnerre találtunk a Magyar Elektronikus Aláírás Szövetségben (MELASZ[1]). Együttműködésünk 2007. májusában kezdődött.

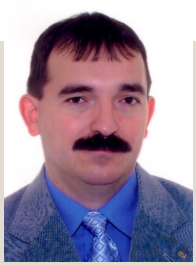
Sok olyan információt kaptunk tőlük, melyeket az e-Inspirációban külön-külön megjelentetve elaprózottnak találtunk volna, ezért felmerült az ötlet, hogy készítsünk együtt egy különszámot az elektronikus aláírásról, amiben részletesen és terjedelmi korlátoktól mentesen, csak erre a területre fókuszálva gyűjtjük össze az eddig megtett lépéseket, azok eredményeit és a jövőben várható további lehetőségeket is.

Sok szeretettel ajánlom minden tanár – nemcsak informatikusok – figyelmébe ezt a különszámot.

Bánhidi Sándorné

ISZE főtitkár

[1] http://www.melasz.hu



Erdősi Péter Máté

MIÉRT SZÜKSÉGES AZ ELEKTRONIKUS ALÁÍRÁS OKTATÁSA

Az Eurostat adatai azt mutatják, hogy az EU népességének 37%-a semmilyen számítógépes készséggel nem rendelkezik, az alapfokú oktatás második szintjénél/a középiskola alsó tagozatánál tovább nem tanulóknak pedig több mint 60%-a nem rendelkezik alapvető e-készségekkel.

Európa azt a célt tűzte ki, hogy 2010 -re megteremtse az elektronikus Európában a dokumentumok hiteles kezelésének, mozgatásának, tárolásának és archiválásának különböző lehetőségeit, ami nem nélkülözheti az elektronikus aláírás használatának bevezetését. Erre példaként felhozható számos olyan európai irányelv, ajánlás, bizottsági határozat, mely az elektronikus dokumentumok kezelésére vonatkozik többek között az adminisztrációban, a vámeljárásokban és az igazságszolgáltatásban is, és mindegyikben szerepel az elektronikus aláírás használata, annak előírása, illetve a használati lehetőség megteremtése.

Nem tagadható, hogy az elektronikus aláírás megvalósítása részben műszaki feladat, de ez a mai trendeket, az informatika előretörését és a társadalmi rendszerek ettől való függőségét tekintve már nem jelent, nem jelenthet akkora gátat azok számára, akik a mai és a holnapi társadalmi rendszerek működtetésében és előnyeinek kihasználásában részt kívánnak venni. Annál is inkább igaz ez, mert a bíróságok már több olyan határozatot hoztak, amivel kizárták az írásbeliség köréből a legalább fokozott biztonságú aláírásokat nélkülöző elektronikus leveleket, különösen a közbeszerzési eljárásokban, ott is a vitatott elektronikus kommunikációkban.

Idézzünk két bekezdést az Európai Bizottság COM(2007) 496 végleges anyagából[2]. „Az alapműveltség hagyományos fogalmába a tudás alapú gazdaságban és társadalomban nélkülözhetetlen e-készségek és médiakompetenciák teljes tárának bele kell tartoznia. Az Eurostat adatai azt mutatják, hogy az EU népességének 37%-a semmilyen számítógépes készséggel nem rendelkezik, az alapfokú oktatás második szintjénél/a középiskola alsó tagozatánál tovább nem tanulóknak pedig több mint 60%-a nem rendelkezik alapvető e-készségekkel. A hiányzó e-készségek következtében ezek az emberek **nem fogják tudni használni az e-kereskedelem és az e-kormányzat számítógépes alkalmazásait, és nem fognak tudni teljes mértékben bekapcsolódni az információs társadalomba**. Emellett az e-készségek hiánya növeli a társadalmi és oktatási hátrányokat, és gátolja az egész életen át tartó tanulást és a készségek fejlesztését.

A piac önerőből nem képes a digitális szakadék áthidalására. Éppen ezért mind az élethosszig tartó tanuláshoz szükséges kulcskompetenciákról szóló európai parlamenti és tanácsi ajánlás, mind az elektronikus társadalmi integrációval foglalkozó, 2006. júniusi miniszteri konferencián elfogadott rigai nyilatkozat innovatív közintézkedésekre és több érdekelt fél részvételével létrejövő partneri kapcsolatokra összpontosít. ”

Igaz, hogy az elektronikus aláírás elterjedése még nem következett be Magyarországon sem személyi szinten áttörő jelleggel. A Nemzeti Hírközlési Hatóság statisztikai adatai szerint tízezres a tanúsítványbirtokosok nagyságrendje, de például a cégeljárást elektronikus aláírás nélkül a több ezer ügyvéd ma már nem tudja működtetni, több ezer vállalkozás és közintézmény elektronikusan aláírva teljesíti adatszolgálta-

tási kötelezettségét a felügyeleti szervek számára és a közlekedési hatóság is több tízezer digitális tanúsítványt vásárolt a mérnökei és a járműparkja számára – azaz működő és hatékony részeredmények már léteznek és eredményesen működnek ma is.

Az tény, hogy az információs társadalomban az ember helyének megőrzéséhez egyetlen dolog szükséges: hiteles, aktuális és pontos információ. Ezek nélkül semelyik társadalmi folyamat nem töltheti be célját, semelyik vállalkozás nem érheti el küldetését és egyetlen magánszemély sem képes minőségi életet kialakítani a saját környezetében. A folyamatok java része azonban mára átalakult, többségében elektronikus vagy elektronikusan támogatott lett. Ebből adódik, hogy a mai kor tevékeny embere számára létfontosságúvá vált a hiteles és a nem hiteles információ közötti különbségek felismerése, a hitelességi technikák használata. Ezért tartjuk szükségesnek az elektronikus aláírás technikáinak tanítását, használatának elsajátítását már az iskolai tanulmányok során, összhangban a Nemzeti Alaptanterv előírásaival. Az iskolai oktatás részévé válásáig az elektronikus aláírási technikákat graduális és posztgraduális képzéseken is szükséges átfogó jelleggel oktatni, hogy a tudás elterjedése ne legyen gátja a technológia használatának. Hiába gyártott volna annak idején Henry Ford többmillió T-modellt, ha nem jönnek létre az autóvezetést tanító iskolák a technológia mellé, az autók használata talán még ma sem terjedt volna el, hiszen ismeretes az autónak számos ellenzője is abból a korból. És talán még ma is van olyan, aki nem szívleli az autókat és ma sem tud autót vezetni – de azért el tud jutni másképp is egyik helyről a másikra, legfeljebb az autóvezetés örömeiről lemond.

A Magyar Elektronikus Aláírás Szövetség és az Informatika-Számítástechnika Tanárok Egyesülete által a 2008/2009-es tanévben szervezett kísérleti oktatás során bebizonyosodott, hogy a technológia érthető, átadása nem ütközik akadályokba, a diákok könnyen és gyorsan képesek elsajátítani az elektronikus aláírás műszaki aspektusait. Számukra már lehetővé vált a társadalmi aspektusok tárgyalása és az ebben rejlő hatalmas előnyök kiaknázása is.

Célunk az, hogy ezen az úton még több társukat indítsuk el, és a hiteles kommunikációból adódó személyes előnyöket hozzájuk is közelebb hozzuk.

Kommunikálni – ahogyan hajózni is – márpedig minden társadalomban kell. Hitelesen kommunikálni az információs társadalomban szerintem már nem lehetőség, hanem követelmény. Véleményem szerint csak az képes szabadon választani a kommunikáció előírt és választható (szóbeli, papíralapú, elektronikus, elektronikusan aláírt) formái közül, aki megszerezte a jártasságot mindegyikben, és ezért képes a saját belátása szerint használni – az előírások korlátai között – azokat a lehetőségeket, amelyeket felkínáltak számára.

Erdősi Péter Máté

Certified Infomation Systems Auditor (CISA),
MELASZ-alelnök,
elektronikus aláírással kapcsolatos szolgáltatási szakértő,
NJSZT információrendszer-ellenőrzési szakértő

[2] http://eurolex.europa.eusmartapi/cgi/sga_doc?smartapi!celexplus!prod!

ELEKTRONIKUS ALÁÍRÁS VAGY DIGITÁLIS ALÁÍRÁS?

Ha egy bűnöző netán megszerzi az aláírás-létrehozó adatunkat és az azt védő kódot, onnantól kezdve pontosan olyan aláírásokat hozhat létre, mint mi.

Az ember aláírási formája – a kötelezettségvállalás hitelesítése – a történelem során sokat változott, ilyenek például a pecsétnyomók, pecsétgyűrűk, és egyéb aláírási jelek. Ennek jelentősége a polgári társadalmakban nőtt meg, ahol az emberek együttélését és együttműködését szerződések szabályozzák. Az elektronikus aláírás szükségességét az elektronikus dokumentumok terjedése, lehetőségét pedig a többkulcsos titkosítás felfedezése teremtette meg. Az elektronikus aláírás nem egyenlő a digitális aláírással, de igaz az, hogy minden digitális aláírás egyben elektronikus aláírás is (fordítva azonban nem).

Az elektronikus aláírás egy jogi gyűjtőfogalom, technológiasemleges szabályozási kezdeményezésekben bukkant fel akkor, amikor a digitális aláírások használata elérte azt a szintet, ami a szabályozási oldalról választ igényelt európai szinten is 1990 körül, azaz lassan húsz éve. Minden olyan eljárás elektronikus aláírásnak nevezhető, amely elektronikus hitelesítés céljára szolgál. A hitelesítés pedig az állított azonosság megerősítése, ami megtehető személyről, fizikai tárgyról vagy valamely tulajdonságról is. Nagyon fontos európai szabály ebben a témakörben, hogy az elektronikus aláírás elfogadási szabályainak kialakítására a 93/1999. irányelv kötelezi a tagállamokat. Ez azt jelenti, hogy ha például valamely tagállamban létrejött egy olyan műszaki aláírás, mely megfelel a minősített elektronikus aláírással szemben támasztott irányelvi követelményeknek, akkor azt minden olyan tagállamban kötelezően el kell fogadni kézírással egyenértékű aláírási formának, amelyik alkalmazza az elektronikus aláírási technológiát. Az irányelv minden tagállamra nézve kötelező előírásokat tartalmaz.

A digitális aláírás fogalma műszaki, az aszimmetrikus kriptográfiára épülő konkrét matematikai eljárás (ami annyit tesz, hogy olyan matematikai algoritmust használnak a bemenő adatok rejtjelezésére, ahol a titkosító és a megoldó kulcs különbözik). A két kulcs és az aláíró algoritmus segítségével készül el az aláírás egy előre legyártott fix hosszúságú adatból (hash, kivonat). Az aláírás készítő kulcsot nevezzük titkos kulcsnak – és védjük a továbbiakban az illetéktelen felhasználástól, a megoldó kulcsot nevezzük nyilvános kulcsnak, és széles körben terjesztjük, hiszen az aláírásunkat csak ennek segítségével tudja bárki is ellenőrizni.

Ha egy bűnöző netán megszerzi az aláírás-létrehozó adatunkat és az azt védő kódot, onnantól kezdve pontosan olyan aláírásokat hozhat létre, mint mi. (Ez olyan, mintha sok-sok általunk aláírt üres papírlapot adtunk volna neki, vagy a bankkártyánkat PIN-kóddal együtt megszerzi.) Azért, hogy ez ne fordulhasson elő, az aláírás létrehozó adatot nagyon gondosan szokás tárolni, kezelni, ugyanolyan módon, mint a bankkártyánkat. Gyakori megoldás, hogy az aláírás-létrehozó adatot intelligens kártyán, chipkártyán vagy más kriptográfiai védelmet nyújtó eszközön (kriptotokenen) tartják. Ekkor, amíg az eszköz a fennhatóságunk alatt van, joggal bízhatunk benne, hogy senki nem szerezte meg az aláírás-létrehozó adatunkat, ellenkező esetben jelezzük, és letiltják

annak elfogadását – ugyanúgy, mint a bankkártyák esetében. A digitális aláírás készítés elvi lépései az alábbiak:

1. az aláírandó dokumentumból elkészül annak kivonata
2. a kivonat az aláíró algoritmus és a titkos kulcs segítségével rejtjelezésre kerül, és digitális aláírásnak nevezzük
3. a digitális aláírást a dokumentummal együtt elküldjük a fogadónak. Az ellenőrzéskor az ellenőrzést végző szoftver is automatikusan végzi el a fenti ellenőrzési folyamatot:
4. a fogadó oldalon a dokumentumból újra elkészül az új kivonat
5. a digitális aláírásból a nyilvános kulcs segítségével visszanyerik az eredeti kivonatot
6. a fogadó oldalon az új kivonatot és az eredeti kivonatot a rendszer összehasonlítja, és ha egyezik, akkor az aláírás rendben van, ha pedig nem, akkor az aláírás nem tekinthető hitelesnek.

Az aláírás készítése a gyakorlatban szinte teljesen automatikus, a rendszer egyedül a titkos kulcs használata előtt kéri el annak titkos kódját. Ha ezt az aláíró nem vagy nem jól adja meg, az aláírás nem készül el, a kötelezettségvállalás hitelesítése nem történik meg. A történet biztonságát a felhasználói titkos jelszó, a használt kriptográfiai algoritmusok, a hardveres és szoftveres eszközök, a nyilvános szolgáltatások működtetése és ezek felügyelete együttesen adják. Vagyis – ismét csak a bankkártyákra utalunk – a biztonságról az aláíró, a gyártók és a szolgáltatók együttesen gondoskodnak, ez itt nem kizárólag az egyénre, az aláíróra bízott feladat. Nem is működhet ez másképp.

A feltett kérdésre tehát a pontos válasz az, hogy ha elektronikus hitelességet megvalósító módszerről beszélünk, akkor az elektronikus aláírás gyűjtőfogalmat használjuk, ha pedig a nyilvános kulcsú titkosításon alapuló aláírás a beszélgetés tárgya, akkor ezt a digitális aláírás műszaki fogalom használatával jelezzük. Persze csak akkor, ha a szabatos kifejezés igényével kell élnünk.

Erdősi Péter Máté

Felkészítő elektronikus aláírási oktatás az ISZE-ben, milyennek látta ezt egy résztvevő?

Egyike voltam annak a több mint 20 tanárnak, aki elfogadta Erdősi Péter meghívását és részt vett az egyik hétvégén, 2009. március 14-én az elektronikus aláírás kurzuson. Manapság szokás tanfolyam és tréning fogalmak egymást helyettesítőként való emlegetése. A mi képzésünk igazi trénig volt! Péter ötórányi időben úgy mutatta be a tudnivalókat, hogy első perctől velünk együtt csinálta. Így lépésről lépésre haladtunk, míg délutánra mindannyian aláírtuk levelünket, amelyet trénerünk címére küldtünk.

Mivel ez a képzés eszközöket is igényelt, amelyeket trénerünk szakavatott cégektől támogatásként kapott – nagy meglepetésünkre megkaptuk ezeket az aláírások elkészítéséhez szükséges hardver- és szoftvereszközöket: kártyaolvasót, kártya, alkalmazásokat és tanúsítványokat. A tréningen részt vett tanárok zömmel azok közül kerültek ki, akik az országos kutatás után kifejlesztett tananyag és tanári kézikönyv összeállítását és kipróbálást végezték.

Jó hangulatú munkalégkörben tanultuk meg a digitális biztonság ezen elemét, amely az informatikától megszokott módon újabb kihívást jelent számunkra.

Köszönöm trénerünk segítő támogatását, amelylyel megtanított a számomra eddig ismeretlen eszközök használatára.

Bánhidi Sándorné

HOL TARTUNK MA AZ ELEKTRONIKUS ALÁÍRÁS OKTATÁSÁBAN

Arra a kérdésre kerestük a választ, hogy a közoktatásban mennyire van jelen az informatikai biztonság, és benne az elektronikus aláírás, mint tananyag.

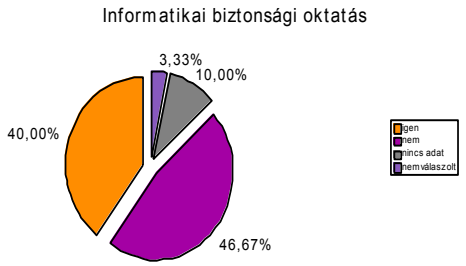
A digitális világban tehát központi szerepet játszik sok esetben az információnak a hitelessége vagy hiteltelensége. Az elektronikus szolgáltatásokba vetett bizalom sokszor azon múlhat, hogy mennyire tudjuk azokat biztonságos, és ezen belül hiteles módon használni. Ennek egyik fontos eszköze a digitális aláírás, az elektronikus kötelezettségek felvállalásának, és az 93/1999. EU irányelvben definiált elektronikus aláírás megvalósításának széles körben kevéssé ismert módja. A digitális aláírás szerepét az oktatáspolitika is olyan fontosnak ítélte meg, hogy részt kapott a Nemzeti Alaptantervben (17/2004. (V.20.) OM rendelet), ahol az információs társadalomról a 8. évfolyamosok számára megszerzendő ismeretanyagok között szerepel. Kiegészítésképpen megemlítjük, hogy a 130/1995. (X. 26.) Korm. rendelet a Nemzeti alaptanterv kiadásáról szó szerint nem említi a digitális aláírást, viszont több olyan területet is felsorol, amenynek része lehet ez (program- és adatvédelem, hálózatbiztonság, információ-szerzés...)

A MELASZ – küldetésének megfelelően – támogatja a digitális aláírás, elektronikus aláírás magyarországi elterjedését, fejlődését, és egy olyan felmérést indított útnak 2007. májusában az ISZE-vel közösen, mely során arra a kérdésre kerestük a választ, hogy a közoktatásban mennyire van jelen az informatikai biztonság, és benne az elektronikus aláírás, mint tananyag. Ennek a felmérésnek az eredményekét megjelent egy tanulmány, amely a MELASZ honlapján olvasható, és számos további publikációban ismertettük ennek a felmérésnek az eredményeit. Nem volt célunk, hogy minden egyes oktatási intézményt felkeressünk, de abban bíztunk, hogy mintavételezésünk reprezentatív lesz, és alkalmas arra, hogy helyes következtetéseket vonjunk le az elektronikus aláírás oktatásának helyzetéről.

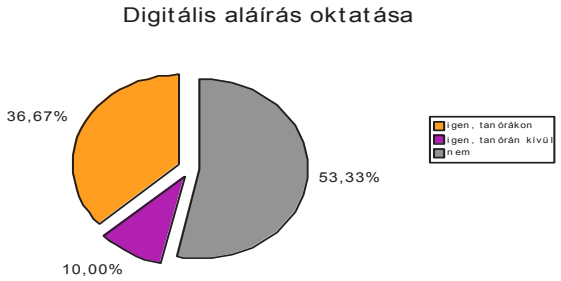
Kérdőívünk hét szakmai plusz egy tájékozódó kérdést fogalmazott meg a tárgyban, melyet 30 válaszadó töltött ki. A kérdőívek teszt-jellegűen, előre megfogalmazott esetek közüli választással gyűjtötték össze a válaszokat. Az eredményeket statisztikai úton dolgoztuk fel, ezáltal biztosítottuk a válaszadók és intézményeik adatainak bizalmasságát. A felmérés időszaka 2007 nyarára esett, azaz a 2006/2007 tanév végére. Külön kiemelve itt is szeretnénk megköszönni a felmérés során nyújtott nagyfokú együttműködést és segítséget Budaörs Város Polgármesteri Hivatal Közoktatási Irodavezetőjének Karsainé Kovács Juditnak, Salgótarján Város Polgármesterének Székyné dr. Sztrémi Melindának, az Informatika és Számítástechnika Tanárok Egyesülete Elnökének Dr. Kőrös Andrásné Dr. Mikis Mártának és az ISZE főtitkárának Dr. Bánhidi Sándornénak, akik segítettek eljuttatni a kérdőíveket a megfelelő helyekre, és végül de nem utolsósorban minden tanár kollégának, aki időt és energiát áldozott a kérdőív kitöltésére, ami az eredmények létrejöttéhez elengedhetetlenül szükséges volt.

A kérdések eredményein érdemes egy kicsit elgondolkodni, mi is ezt tettük – itt a részletek nélkül ismertetjük a válaszokat:

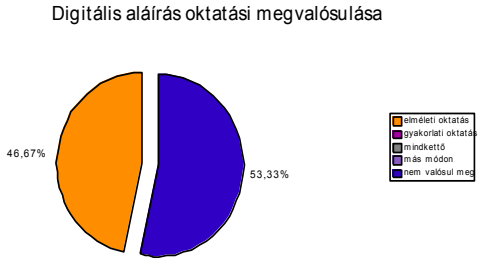
1.) Intézményében folyik-e különösen a 8. évfolyamon oktatás az informatikai biztonság kérdéseinek, illetve az elektronikus információ hitelességének tárgyában?



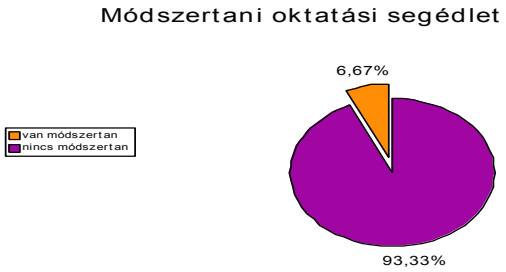
2.) Megvalósul-e iskolájában a digitális aláírás ismertetése?



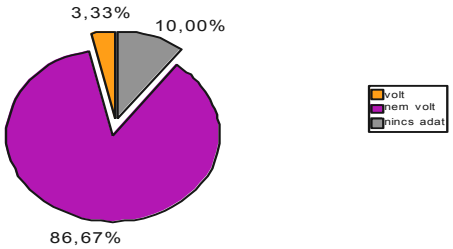
3.) Ha megvalósul a digitális aláírás ismertetése, hogyan történik? (amennyiben az előző kérdésre igennel válaszolt, akkor kellett ezt is kitölteni)



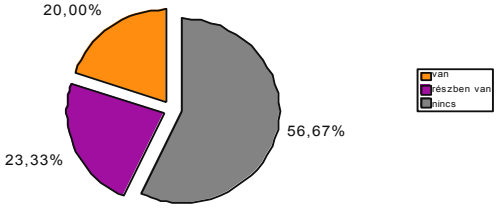
4.) Rendelkeznek-e a digitális aláírás oktatásához módszertani segédlettel / tananyaggal?



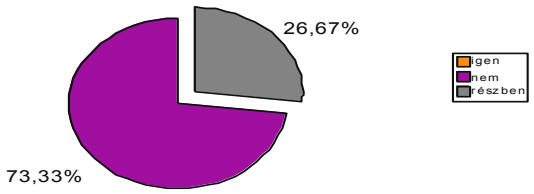
5.) Kaptak-e a szaktanárok továbbképzést az elmúlt két évben digitális aláírás témakörben?



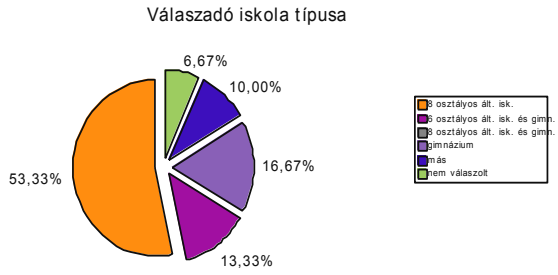
6.) Iskolája rendelkezik-e a digitális aláíráshoz szükséges tárgyi eszközökkel (pl. tanúsítvány, aláíró szoftverek, intelligens kártya, kártyaolvasó...)



7.) Megítélése szerint ismerik-e a 8. osztályos tanulók a digitális aláírás használatát?



8.) Milyen típusú iskola volt a válaszadó?



A felmérés során megismert adatok és helyzet megmutatta, hogy van még mit tennünk a digitális írástudás hitelességi elemeinek fejlesztésében, elterjesztésében, amihez a MELASZ is szándékozott és szándékozik további támogatást nyújtani.

A megismert helyzetet javítására az alábbi akciótervet foglalta írásba 2007 októberében a MELASZ:

Sz.	Feladat	Leírás
1.	Aláíráshoz szükséges hardver- és szoftver eszközök biztosítása oktatási intézményeknek	A MELASZ tagjai között számos olyan cég van, akik ilyen eszközök piaci értékesítését végzik, és támogathatják ezen eszközök használatának elterjedését is, különböző formákban (teszt-célú stb.)
2.	Módszertani oktatási anyag kidolgozása	A MELASZ szakértői birtokában vannak mindazon tudásnak, mely szükséges ezen terület magas színvonalú oktatásához, amit a tanár-kollégák didaktikai módszereivel ötvözve közösen elő lehet állítani minden szükséges oktatási anyagot
3.	Tanárok továbbképzése	A MELASZ szakértőinek tudását be lehet csatornázni a tanár-továbbképzés rendszerébe, ily módon biztosítani azt a tudástranszfert, mely révén egyrészről a szaktanárok tudásbázisa bővül, másrészről a nem informatikai beállítottságú tanár-kollégák is képet kaphatnak a digitális aláírásról, és annak működéséről.

Az akciótervben megfogalmazott célokat sikerült elérni 2009 júniusára – nem egészen két év alatt, az alábbi módon:

1. MELASZ-oktatás az ISZE-ben: több, mint 20 jelentkező tanár vett részt két hétvégi alkalmon 2009. március 7-én és 14-én, amikor is egy ötórás tréning keretében megismerkedtek az elektronikus aláírás elméleti és gyakorlati hátterével, aláírásokat készítettek több alkalmazás segítségével és megkapták az aláírások elkészítéséhez szükséges hardver- és szoftvereszközöket (20 kártyaolvasó, 30 kártya, alkalmazások és tanúsítványok). Ezúton is köszönjük a felajánlott eszközöket a MÁV INFORMATIKA Zrt.-nek, a Microsec Kft.-nek és a Netlock Kft.-nek. A tréningen részt vett tanároktól cserébe kutatási lapokat várunk vissza, hogy a további elképzelések finomhangolását el tudjuk végezni.
2. Módszertani oktatási anyag: a MELASZ finanszírozásában elkészült az első Tanári Kézikönyv az elektronikus aláírás oktatásához, és kidolgoztunk ehhez tanmeneteket is a 7-12 évfolyamok számára, figyelembe véve a meglévő informatika tanmeneteket, iskolatípusokat és órakorlátokat is. Külön köszönetet mondunk ezért itt is Engelbrecht Károlynak és Dér Imrének, a közreműködésükért. A Tanári Kézikönyv és a tanmenetek ingyenesen letölthetők a MELASZ honlapjáról:

   (http://www.melasz.hu/lang-hu/remository?func=select&id=20).)
3. Tanárok továbbképzése: miután kiderült az, hogy a tanárok nem kaptak továbbképzést az elektronikus aláírás témakörében, nekiláttunk a tanártovábbképzés hátterének a kialakításához is. 2009. június 17-én az Oktatási és Kulturális Minisztérium Közoktatási Szakállamtitkára az OKM – 4/-101/2009. számú határozatában az elektronikus aláírás elméleti és gyakorlati oktatására felkészítő alapszintű tanfolyam címmel továbbképzési program indítását és alapítását engedélyezte.

A tanfolyam 30 órás, a tematika és a vizsgakérdések előálltak, a jelentkezések elindultak – ezúton is köszönjük az eddigi jelentkezéseket és bátorítunk minden érdeklődőt a jelentkezésre, hiszen itt a gyakorlati

készségek elsajátítását is célul tűztük ki, ami kiemeli ezt a képzési formát az átlagból.

A megvalósítás során elért eredmények publikálása többször, több helyen is megtörtént, kiemeljük ezek közül az alábbiakat:

1) Networkshop 2008 Konferencia, Dunaújváros

előadás: http://vod.niif.hu/nws2008/160/160_1M.wmv

Előadás cikk: https://nws.niif.hu/ncd2008/docs/ehu/055.pdf

2) Information Technology 2008 Conference, Kaunas, Lithuania (az Információs Társadalomért Alapítvány szponzorálásával)

előadások: http://isd.ktu.lt/it2008/Programme.pdf

3) Informatika a Felsőoktatásban 2008, Debrecen,

előadás: http://www.agr.unideb.hu/if2008/kiadvany/papers/A64.pdf

4) Networkshop 2009 Konferencia, Szeged

előadás: http://vod.niif.hu/player/index.php?q=1076/1M

előadás cikk: https://nws.niif.hu/ncd2009/docs/ehu/057.pdf

A MELASZ és az ISZE 2009-ben aláírtak egy olyan együttműködési megállapodást, melyben a MELASZ vállalja, hogy elektronikus aláírási kérdésekben mindig lehet hozzájuk fordulni, a MELASZ-tagok szakértelmét szakmailag képzett trénerek segítenek átadni az ISZE-nek és tagjainak, az ISZE pedig vállalja, hogy aktívan közreműködik ennek a területnek az oktatásában.

Összefoglalóan tehát az elektronikus aláírás oktatási helyzetét tekintve örömmel mondhatjuk, hogy kialakultak az ehhez szükséges háttérrendszerek (tanári kézikönyv, tanmenetek, pedagógus-továbbképzési program, trénerek), amelyek lehetővé teszik az elektronikus aláírás oktatását a közoktatási intézményekben.

Meg kell a végén említeni, hogy mi még a különlegessége ennek a továbbképzési programnak.

A program tematikája úgy lett összeállítva, hogy a továbbképzésen résztvevő tanár és az általa oktatott diák előkészülhessen a szintén 2009 júniusában elfogadott és 2010-ben induló ECDL Elektronikus Hitelesség, Elektronikus Aláírás modulvizsgára, és sikeres vizsgát tehessen, amennyiben az ECDL vizsgához szükséges – a továbbképzéstől egy kicsit bővebb – elméleti hátteret is elsajátította, és a gyakorlati feladatokat jól begyakorolta.

Erdősi Péter Máté – Bánhidi Sándorné

Szabó Áron

Az elektronikus aláírási technológia adott, azonban a jogi szabályozás teljes folyamatokra történő alkalmazása még gyerekcipőben jár.

INTERJÚ AZ E-GROUP ELEKTRONIKUS ALÁÍRÁSI SZAKEMBERÉVEL, MIT GONDOL Ő AZ ELEKTRONIKUS ALÁÍRÁSRÓL?

A MELASZ Elnöksége felhívta a MELASZ-tagság figyelmét a készülő elektronikus aláírással foglalkozó e-Inspiráció különszámára, és Szabó Áron elektronikus aláírással kapcsolatos szolgáltatási szakértő, az E-Group Kft. munkatársa vállalta, hogy pár kérdésre választ ad a piaci szakértő szemével.

Kérdés: Mit kell tenni, hogy használhasson valaki elektronikus aláírást?

Az elektronikus aláírás létrehozásához és ellenőrzéséhez (tetszőleges dokumentumon, állományon) szükség van egy kriptográfiai kulcspárra és egy alkalmazásra, amely használja ezeket. A kriptográfiai kulcspárt különböző paraméterek megadása (véletlen adatok, algoritmus) alapján létre tud hozni egy hitelesítésszolgáltató vagy akár az otthoni gépen néhány ingyenes alkalmazás is (pl. OpenSSL). A fontos különbség azonban a jogi szabályozásban van, hiszen csak ellenőrzött és felügyelt nyilvános hitelesítésszolgáltatótól származó kulcsokat lehet hivatalos ügyeknél használni. Ezeket a kulcsokat a megfelelő biztonság érdekében általában chipkártyán adják át az ügyfélnek – különösen a saját kezű aláírással egyenértékű elektronikus aláírásokhoz használható titkos kulcsok esetében. SHA-256), amelyeket elküld a chipkártyára, hogy a PIN kód beütése után kódolhassa azokat (pl. RSA algoritmussal), és a visszaadott adatot a megfelelő formátumba (pl. XAdES) beágyazva létrehozza az elektronikus aláírást.

Az elektronikus aláírás struktúra, mint fájl lehet különálló az aláírt dokumentumtól (csatolt aláírás), de be is ágyazhatja azt (ez az alapértelmezett eset).

Kérdés: Hol használják ezt ma Magyarországon?

Az elektronikus aláírási technológia adott, azonban a jogi szabályozás teljes folyamatokra történő alkalmazása még gyerekcipőben jár. Jelenleg létezik több sziget-megoldás is (pl. e-számla kibocsátás, papíralapú dokumentumok elektronizálása, Ügyfélkapu felhasználói regisztráció), de olyan, ahol egy teljes folyamatot végig lehetne vinni elektronikusan, elektronikus aláírással, még kevés van (pl. e-Cégeljárás). Ezen a területen is jóval előttünk járnak a skandináv államok (pl. Dánia, Észtország), ahol már régen megtörtént például a közigazgatásban az adatbázisokban az adattisztítás, adatbázis-sémák egységesítése, a szervek közötti kommunikációhoz szükséges üzenetek (XML) sémáinak egységesítése, kidolgozása, és ezeknél az elektronikus aláírás használata.

Jelenleg nálunk az elektronikus közigazgatásban már ott kezdődnek az együttműködési problémák, hogy a különböző adatbázisokban különböző módon tárolják az állampolgárok adatait (pl. lakcímnél "Budapest" és "1185" vagy "Budapest, XVIII").

folytatás a 14. oldalon

MENNYIRE BIZTONSÁGOSAK AZ ELEKTRONIKUS ALÁÍRÁSSAL KAPCSOLATOS SZOLGÁLTATÁSOK?

A biztonság – definíció szerint – olyan kedvező állapot, melynek megváltozása nem valószínű, de nem is lehet kizárni.

A vállalati célkitűzések elérése és a folyamatok megfelelő végrehajtása érdekében az információknak ki kell elégíteniük bizonyos követelményeket, amelyeket a COBIT[3] információkra vonatkozó üzleti követelményeknek nevez. A szélesebb körű minőségi, pénzügyi-megbízhatósági, és biztonsági követelmények alapján az alábbi hét megkülönböztethető, egymást néhol minden bizonnyal átfedő információkritériumot határoztak meg a szakirodalomban:

1. **hatékonyság**: arra vonatkozik, hogy az információkat az erőforrások optimális (legtermékenyebb és leggazdaságosabb) kihasználásával biztosítsák,
2. **hatásosság/eredményesség:** azzal foglalkozik, hogy az információk a folyamat szempontjából jelentőséggel bírnak, és hogy az információkat időben, helyes, ellentmondásmentes és használható módon biztosítják,
3. **megfelelőség:** a folyamatokat érintő előírások, törvények, jogszabályok, szabályozások és szerződéses megállapodások – azaz kívülről előírt jogi, üzleti és egyéb követelmények, illetve belső irányelvek – betartását jelenti, amelyeknek a folyamat a tárgyát képezi,
4. **megbízhatóság:** a vezetés számára olyan időszerű és pontos információk biztosítása, amelyek a folyamat működtetéséhez, pénzügyi megbízhatóságához és irányításához szükségesek,
5. **bizalmasság:** arra vonatkozik, hogy megakadályozza a bizalmas információk engedély nélküli megismerését, vagyis fontos információkhoz illetéktelenek ne férjenek hozzá,
6. **sértetlenség:** az információknak a mikrokörnyezeti (szervezeti) értékek és elvárások szerinti pontosságára, általános értelemben vett változatlanságára és teljességére, valamint az információk érvényességére és hitelességére vonatkozik,
7. **rendelkezésre állás:** azzal foglalkozik, hogy az információk akkor álljanak rendelkezésre, amikor azokra a folyamatnak szüksége van most és a jövőben is, továbbá a szükséges erőforrások és az erőforrások szolgáltatási képességeinek védelmére is vonatkozik. Nem terjed ki a szolgáltatások megbízhatóságára, azaz amikor a szolgáltatást nyújtó eszközök működnek, de a végeredmény nem az elvárt.

A biztonság – definíció szerint – olyan kedvező állapot, melynek megváltozása nem valószínű, de nem is lehet kizárni. Ebből következik, hogy ennek a kedvező állapotnak a megléte nem automatikus, annak fennmaradási valószínűségét csak tudatos intézkedésekkel lehet biztosítani, és mindig megjelenhetnek olyan fenyegetések, melyek ellen a védelem még nincs kialakítva.

[3] COBIT: Control Objectives for Information and Related Technology, Kontroll célkitűzések az információ- és kapcsolódó technológiák számára, kiadta az IT Governance Institute (ITGI)

http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=31519

Biztonság a gyűjtőneve minden olyan intézkedésnek, amely megteremti az adatok, számítógépek, alkalmazói programok bizalmasságát az adatok korlátozott megismerhetőségén és az eszközök korlátozott elérhetőségén keresztül, majd sértetlenségét – a jogosulatlan változtatásokat kizárva, illetve észlelve, és végül a rendelkezésre állását, vagyis működjön az eszköz akkor és ott, amikor szükség van rá.

A fentiek a vállalati biztonságra – így egy általános szintű piaci szolgáltatást nyújtó vállalati rendszerre – vonatkoznak. Könnyen belátható, hogy a biztonságnak különböző szintjei léteznek aszerint, hogy milyen fenyegetések ellen védett a vállalati rendszer, és melyek ellen nem tud védelmet felmutatni, védtelen. Például a biztonság különböző szintjén van az a vállalati rendszer, mely egy diszk meghibásodása esetén tovább tud szolgáltatni, de a gépterem megsemmisülése esetén már nem, ahhoz képest, amelyik vállalati rendszer a gépterme működésének fennakadása után is tud szolgáltatni egy alternatív helyszínen gyorsan működőképessé tett háttérrendszer segítségével.

Vagy biztonságosabbnak ítélünk meg egy olyan épületet, melyet földrengésbiztosnak terveztek és építettek ahhoz képest, amelyik tervezésénél ez a szempont fel sem merült.

Az elektronikus aláírással kapcsolatos szolgáltatásokat nyilvánosan, bárki számára nyújtó vállalatok biztonságára jogszabályi előírás vonatkozik (részletesen a 3/2005. IHM Rendelet vonatkozó paragrafusai írják le ezeket), melyek nagyon komoly előírásokat fogalmaznak meg a minősített szolgáltatásokkal szemben. Néhány elemet emeljünk ki az előírások közül:

- pénzügyi biztosítás (25 millió forint bankgarancia, óvadék vagy felelősségvállalás), a szolgáltatás befejezésekor fellépő költségekre,
- legyen megfelelően képzett személyzet, a megfelelő létszámban, több kritikus munkakört ne tölthessen be ugyanazon személy,
- rendszeresen külső független auditor által ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerek működtetése,
- 99,9%-os rendelkezésre állást biztosító hardver- és szoftverrendszerek üzemeltetése (ez azt jelenti, hogy egy évben a szolgáltatás maximum 8,76 órát állhat) és az egyes leállások ideje nem haladhatja meg a 3 órát(!).

Mi annak a garanciája, hogy ez felügyelet (EU, NHH, megszűnés) valóban így is működik?

A többszörös ellenőrzés! Egyrészről a szolgáltatók saját belső ellenőrzésük segítségével szűrik ki a hibákat, a biztonságot fenyegető tényezőket. Ezen kívül rendszeresen évente legalább egyszer ellenőrzik őket külső független auditorok is ISO 9001 és ISO 27001 szabvány betartása miatt.

A Nemzeti Hírközlési Hatóság is évente megvizsgálja szakmai szemmel a minősített szolgáltatások működését helyszíni szemlén, melyet megelőz egy szolgáltatással kapcsolatos független szolgáltatási szakértő részletes szakvéleménye az elmúlt időszak működésének megfelelőségéről.

Ezen kívül a szolgáltatóknak lehetőségük van önkéntes akkreditációs rendszerben is tanúsíttatniuk működésüket. Látható tehát, hogy az elektronikus aláírással kapcsolatos minősített szolgáltatások felügyelete jóval magasabb szintű, mint bármely más szolgáltatásé.

További egyedülálló biztonságot nyújt a minősített szolgáltatásokra építő ügyfelek számára az a jogszabályi kikötés, hogy a szolgáltató csak úgy fejezheti be a működését, ha gondoskodik arról, hogy az ügyfeleit átvegye egy másik minősített szolgáltató. Amennyiben ezt elmulasztaná, akkor ezt a feladatot a Nemzeti Hírközlési Hatóság veszi át és látja el – többek között ennek a fedezetét biztosítja a szolgáltatások megkezdésekor előírt bankgarancia vagy óvadék.

Összefoglalva a fentieket: 2009-re műszaki értelemben már széles körben lehetséges az elektronikus hitelességet megvalósító szolgáltatások igénybevétele, hiszen több éve léteznek az alábbiak és mindezek hatósági felügyelete, nyilvántartása:

- minősített és nem minősített hitelesítésszolgáltatás,
- minősített időbélyeg-szolgáltatás,
- minősített archiválás szolgáltatás.

Ezek a kialakult intézményrendszerek a mindennapokban teszik használhatóvá az elektronikus hitelességet, és garanciát jelentenek a folyamatosan ellenőrzött működésre. Nincs még egy olyan szolgáltatás, melynek ügyfelei ennyire erős garanciát kapnának a szolgáltatás folyamatos működésére, akármi is történik a szolgáltatást nyújtó céggel vagy annak eszközeivel. Ez példa nélküli a piaci szolgáltatások körében, és erre nyugodtan lehet akár e-számla szolgáltatásokat is építeni (melyek biztonsága az üzletvitelt erősen befolyásolhatja). Biztonsági problémákkal – a fentiek tanúsága szerint – a minősített szolgáltatásoknál találkozhatunk a piacon legutoljára, az összes igénybe vett szolgáltatásainkat tekintve, ezt a többszörös ellenőrzés garantálja.

Erdősi Péter Máté

Folytatás a 9. oldalról

Ebből a példából is látszik, hogy nem az elektronikus aláírás szintjén van gond, nem attól kell tartani. Szerencsére a háttérben azért zajlanak a munkálatok, amelyek orvosolják az egyéb problémákat (pl. adatbázisok, jogi háttér), ezért remélhetőleg 1-2 éven belül már nemcsak a cégeljárási ügyeket bonyolító ügyvédek számára lesz teljesen természetes az elektronikus aláírás használata (merthogy nekik az!), hanem bárkinek!

Szabó Áron,

E-Group tanácsadó,

elektronikus aláírással kapcsolatos

szolgáltatási szakértő

AZ ALÁÍRÓ PROGRAMOK EGYÜTTMŰKÖDÉSI KÉPESSÉGEIRŐL

Mi a helyzet az elektronikus aláírást készítő alkalmazásokkal? Mennyire képesek együttműködni egymással? Mi a garancia arra, hogy amit az egyik aláíró programmal elkészítettünk, azt a másik aláíró program el is tudja olvasni? Ez a kérdés – nem tagadható – a múltban komoly akadálya volt az elektronikus aláírás terjedésének, de ma már ez sem lehet komoly gát. Az együttműködésre Európa is odafigyel (pl. PKI Challenge, ETSI együttműködési tesztek), amelyek eredményei Magyarországon is jelentkeznek, több olyan magyar cég van, akik Európában is sikeresen szerepelnek ezekben a programokban. De Magyarországon sem tétlenkedünk ennek kapcsán. Az elektronikus aláírási termékeket fejlesztő magyar cégek összefogásával, két hónap alatt többszázezer teszt végrehajtása után bebizonyosodott, hogy hat cég hat alkalmazása minden elképzelhető körülmény között szabványosan együtt tud működni.

A Magyar Elektronikus Aláírás Szövetség (MELASZ) 2009 májusában és júniusában szervezete meg interoperabilitási tesztelését, mely a Budapesti Műszaki és Gazdaságtudományi Egyetem Informatikai Központjában (BME IK) került végrehajtásra. Az elektronikus aláírási technológiával kapcsolatos leggyakrabban hallott kifogások egyike, hogy az egyik gyártó terméke nem képes felismerni a másik gyártó által kiadott aláírt dokumentumot. A MELASZ már 2006-ban végzett olyan tesztelést a BME IK-val közösen, melynek célja az volt, hogy ezt a mítoszt megcáfolja. Az akkori kézi tesztelést most alaposabb, gépesített eljárás követte, melynek során több mint 300 000 tesztesetet hajtott végre a laborban felállított tesztkörnyezet, miközben kb. 120 000 időbélyegzőt használt fel. Ez a nagyszabású projekt és minőségbiztosított eredménye újfent bizonyította, hogy hat cég, az Argeon Kft., az E-Group Kft., a Microsec Kft., a NetLock Kft., a Noreg Kft., valamint a Polysys Kft. termékei akár a legextrémebb aláírási szituációkban is képesek felismerni és kiegészíteni egymás dokumentumait. A tesztelés eredményeként a MELASZ kiadott MELASZ-Ready 2.0 tanúsítványokat, aminek valódi jelentősége azoknál az elektronikus kormányzati és elektronikus kereskedelmi alkalmazásoknál van, amikor az ügyfél egy tetszőleges alkalmazással létrehozott e-aláírt dokumentumot küld a szolgáltató felé, akinek ezt fel kell dolgozni, be kell illesztenie a dokumentumkezelési folyamatába, majd esetleg a hosszú távú megőrzés érdekében archiválnia is kell. Ez a folyamat akár 3 különböző alkalmazást is megkívánhat, ami miatt ezek együttműködése elengedhetetlenül fontos.

Fontos tudni, hogy a MELASZ-Ready 2.0[4] teljesen megfelel az európai szabványosító szervek által kidolgozott XAdES szabványnak, így ezek a magyar termékek az egész kontinensen egyszerűen felhasználhatók.

A MELASZ szabványt honosító és együttműködési képességet vizsgáló tevékenységének elismerése, hogy a piacon és az államigazgatásban is sokszor nevesített követelményként szerepel ma már a MELASZ-Ready tanúsítvány[5] elvárása. A különböző aláírási termékek közötti teljes együttműködés egyébként Európában is példa nélküli, célja pedig az, hogy mind a kormányzat, mind a piaci szolgáltatók számára a lehető leginkább problémamentessé váljon a technológia bevezetése.

Rózsahegyi Zsolt,

MELASZ Elnök, Netlock Kft. ügyvezető igazgató

Krasznay Csaba,

HP szakértő, CISA, CISM, CISSP, CEH, elektronikus aláírással kapcsolatos szolgáltatási szakértő, Common Criteria szakértő

[4] http://www.melasz.hu/lang-hu/melasz-ready-ajanlas

[5] http://www.melasz.hu/lang-hu/tanusitott-termekek

MIT TARTALMAZ AZ ECDL ELEKTRONIKUS ALÁÍRÁS, ELEKTRONIKUS HITELESSÉG MODULTANKÖNYV?

A tankönyv célja az, hogy tartalmazza mindazon elméleti és gyakorlati tudnivalókat az ECDL Elektronikus Hitelesség, Elektronikus Aláírás támogatott modulból vizsgázni kívánók számára, melyekkel a sikeres vizsgára felkészülhetnek.

A tankönyv az ECDL Foundation (Európai ECDL Alapítvány) által támogatott Elektronikus Hitelesség, Elektronikus Aláírás modulhoz készült. Az informatika, a digitális világ fejlődésével és annak a mindennapokban való térnyerésével egyre fontosabb kérdéssé vált a hitelesség biztosítása a legtöbb elektronikus folyamatban, és egyre inkább kizárólag elektronikus folyamatok vesznek minket körül. Az Európai Unió már 1999-ben szabályozta az elektronikus hitelesség európai közösségi alkalmazásának kérdéseit, de ennek széles körű elterjedése az európai társadalmakban – számos sikeres és eredménytelen kezdeményezést követően – a közelmúltig váratott magára. Az utóbbi évek eseményei azonban megmutatták, hogy hitelesség nélkül csak egy bizonyos szintig lehetséges bármilyen elektronikus folyamatot hosszú távon fenntartani, előbb-utóbb szükségessé válik az elektronikus hitelesség biztosítása, azaz meg kell tanulni, el kell sajátítani valahol ezt a tudást. Ehhez azonban olyan háttérrendszert kellett létrehozni, mely a társadalom minden tagja számára egyforma eséllyel biztosítja a tudás megszerzésének lehetőségét, legyen életpályájának bármelyik szakaszán, és rendelkezzen bármilyen ismeretháttérrel. Ezt a hátteret biztosította az ECDL Foundation az elektronikus aláírásról szóló támogatott modul akkreditálásával, mely a Neumann János Számítógép-tudományi Társaság (NJSZT) mint modulgazda és a Magyar Elektronikus Aláírás Szövetség szakmai támogatásával jöhetett létre.

A tankönyv célja az, hogy tartalmazza mindazon elméleti és gyakorlati tudnivalókat az ECDL Elektronikus Hitelesség, Elektronikus Aláírás támogatott modulból vizsgázni kívánók számára, melyekkel a sikeres vizsgára felkészülhetnek. A modul ismeretanyagának elsajátítása során – az elektronikus hitelesség jellegéből adódóan – előny az alapfokú számítógépes ismeret megléte (internethasználat, levelezés, szövegszerkesztés, táblázatkezelés stb.), mivel a tananyag ezek ismeretét feltételezi, és ezeket egészíti ki az elektronikus hitelesség elemeivel.

A vizsgán az elméleti kérdéseket és a gyakorlati megoldásokat is számítógép segítségével kell majd előállítani, ezért az ebbéli rutin megszerzése érdekében a tanár segítségével történő felkészülés mindenképpen előnyös lehet a sikeres vizsgához. A könyv felépítése azonban úgy lett kialakítva, hogy gyakorlottabb felhasználók otthon is el tudják sajátítani az elektronikus aláírást elmélettel és gyakorlattal együtt. Az egyes fejezetek azt az ismeretanyagot tartalmazzák, melyek az elektronikus aláírás mindennapi használatához feltétlenül szükségesek – ideértve annak eldöntési képességét is, hogy egy adott szituációban a kommunikáció melyik formája mellett lehet és kell dönteni, azaz lehetséges-e választani a papír, az elektronikus és az elektronikusan aláírt kommunikáció között. Váltakoznak a száraz, tudományos igényű fejezetek a könnyedebb, gyakorlatiasabb fejezetekkel.

Minden fejezet végén gyakorló kérdések segítenek a lényeg kiemelésében és a tudás elsajátításának ellenőrzésében.

Az alábbi rövid felsorolás a teljesség igénye nélkül tartalmazza azokat az előnyöket, amelyeket egyéni és társadalmi szinten lehet biztosítani a hiteles elektronikus kommunikációval – a mai európai közszolgáltatásokat is igénybe véve:

1. gyors és hiteles (azonnali) kommunikáció,
2. sorban állás nélküli (akadálymentesített) ügyintézés,
3. papír alapú ügyintézéshez felhasznált erőforrások és energia csökkentése,
4. távmunka, otthoni munkavégzés Európában és eredménye hitelességének biztosítása,
5. ügyintézés, munkavégzés helyszínére való utazáshoz szükséges üzemanyag elégetésének melléktermékeinek csökkentése (szmoghelyzetek csökkentése).

Ezeket az előnyöket realizáló tudáshoz és a mindennapokban is használható gyakorlathoz kívánja hozzásegíteni ez a könyv az olvasóit.

A könyvben szereplő fogalmak alkalmasak a tárgyban kialakult miszticizmus és zavarosság megszüntetésére, mivel minden fejezet pontos, jól megfogalmazott definíciókat tartalmaz és használ. Ennek oka – a tiszta tudás leírásának célkitűzésén kívül – az, hogy a könyv szerzőinek szándékában állt ezt a területet tudományos igénnyel integrálni napjaink tudásbázisába. Ebben – többek között – Georg Cantor példamutatását követik, akinek a „végtelen halmaz” pontos definíciója megnyerte az egzakt logika számára a végtelen számok területét, ami addig igen spekulatív és tisztázatlan volt – a végtelen szokatlan és nehezen felfogható tulajdonságai miatt.

A vizsga lebonyolítható platformfüggetlen módon is, mivel minden platformra léteznek már olyan szoftverek, amelyekkel a vizsgafeladatok – egyszerűbben vagy bonyolultabb módon – megoldhatóak.

Az alábbi táblázatban összefoglaltuk azokat a platformokat és alkalmazásokat, amelyeken a gyakorlás lehetséges és ajánlható.

Alkalmazások Operációs rendszer	Irodai csomagok	Böngészők	Aláíró programok, csomagok
Windows XP, 2000, Vista	MS Office XP, 2003, 2007 OpenOffice, Outlook	Internet Explorer Firefox, Opera	e-Szignó, PDFSigno, InfoProve, SDX, e-sign, CryptoSygno PGP, OpenSSL
Linux	OpenOffice, Evolution	Firefox, Ephiphany, Opera	CryptoSygno, GnuPG, OpenSSL, e-Szignó
Mac OS X	Mac Office Office 2008 OpenOffice	Internet Explorer Firefox, Opera	CryptoSygno GnuPG OpenSSL

Az elektronikus levelezéssel kapcsolatos ismeretek alulreprezentáltsága a könyvben szándékos, ezeknek az ismereteknek a használatát az Internet, kommunikáció ECDL-modul segít elsajátítani.

A mai könyvpiacon számos elektronikus aláírással kapcsolatos elméleti és gyakorlati könyvvel lehet találkozni. Egyesek komoly matematikai fejtegetéseket is tartalmaznak – ez egyetemi szinten és tudományos publikációknál figyelhető meg, mások részletesen ismertetik a rövid elméleti bevezető után egy-egy adott szoftver működését, használatát. Az ECDL-vizsga jellegét tekintve alapvetően gyakorlatias, számítógép-használati jogosítványt ad a birtokosának, ezért ennek a könyvnek az a kimondott célkitűzése, hogy olyan elméleti és gyakorlati ismereteket adjon át, amelyekkel bármelyik platformon tetszőleges alkalmazás használata elsajátítható a vizsgára felkészülni kívánó olvasó számára. Elméleti háttér nélkül csak megértés nélküli mechanikus folyamatvégzést („gombok nyomogatását”) lehet elsajátítani, hiszen a „Miért van ez így?” kérdésre a válasz nem adható meg az ehhez szükséges háttérismeretek nélkül. Emiatt a könyv elméleti részeket is tartalmaz, de csak annyit és olyan részletességgel, melyek a gyakorlati összefüggések megértéséhez szükségesek.

A könyv – szándéka szerint – olyan és annyi gyakorlati ismeretet ad át, amely nemcsak egyetlen alkalmazás használatát tanítja meg a vizsgára készülőnek, hanem minden aláírás-készítő programnál alkalmazható. De a könyvnek nem célja az összes aláírás-készítő szoftver működésének részletes ismertetése – célkitűzési, terjedelmi és szoftverváltozási okokból –, hanem csak olyan részletességű gyakorlati ismeretanyagot tartalmaz, melyekkel a szoftverek értő működtetése – a sikeres vizsgára való felkészülés – megvalósítható. A könyvben megnevezett szoftverek felhasználói útmutatói – a további részletes ismeretek begyűjthetősége érdekében – az internetes hivatkozások között szerepelnek.

A könyv tehát elsősorban az ECDL-vizsgára való felkészítés szándékával készült, de élményeket adhat a csupán érdeklődő olvasóknak is. Annál is inkább, mert a több mint 200 oldalban néhol olyan kérdések, fejtegetések is felmerülnek az apró betűs részekben, melyek nem feltétlenül szükségesek az ECDL-vizsga letételéhez, viszont a könyv anyagán túlmenően érdekes eszmefuttatások végiggondolására adnak lehetőséget. A könyv első kiadása várhatóan 2009. év végén készül el.

A könyv részeként kialakított példatár elméleti és gyakorlati feladatainak elvégzésével sikeres felkészülést kívánunk minden ECDL-vizsgát tenni szándékozónak. Sok pozitív élményt kívánnak a szerzők az elektronikus aláírás alkalmazásában most és a jövőben is! Elektronikus aláírásra fel, bátran!

Balázs László - Erdősi Péter Máté

A PEDAGÓGUS TOVÁBBKÉPZÉSI PROGRAM TEMATIKÁJA

1. AZ INFORMÁCIÓ ÉS A MAI TÁRSADALOM
1.1. Az információ jelentőségének bemutatása
1.1.1. Az információ fogalma, értelmezései
1.1.2. Az információk megjelenési formái a mindennapjainkban
1.1.3. Információ-források a digitális univerzumban
1.2. Hiteles és nem hiteles információ
1.2.1. A biztonsági követelmények és a hitelesség
1.2.2. A hitelesség fogalma
1.2.3. Hiteles információk kritériumai

2. AZ ELEKTRONIKUS ALÁÍRÁS AZ INFORMÁCIÓS TÁRSADALOMBAN
2.1 Az elektronikus aláírás fogalomrendszere
2.1.1. Az elektronikus aláírás fogalma
2.1.2. Az elektronikus aláírás magyarországi törvényi háttere
2.2. Az Európai Unió célkitűzései és a magyarországi joghatások
2.2.1. Az európai elektronizálási programok és magyarországi következményeik
2.2.2. Az elektronikus aláírás fontosabb EU szabályozásai
2.3. Az elektronikus aláírás működése
2.3.1. Digitális aláírás, üzenethitelesítő kódok
2.3.2. A digitális aláírás elvi működése

3. NYILVÁNOS KULCSÚ INFRASTRUKTÚRA RENDSZEREK (PUBLIC KEY INFRASTRUCTURE, PKI)
3.1. A PKI rendszer elemei
3.1.1. A PKI rendszerek felépítése
3.1.2. A PKI rendszerek elemei és tulajdonságai
3.2. A PKI elemeinek gyakorlati felismertetése
3.2.1. PKI rendszerek Magyarországon
3.2.2. PKI rendszerek külföldön

4. A TANÚSÍTVÁNY ÉS TULAJDONSÁGAI
4.1. A tanúsítvány fogalomrendszere
4.1.1. A tanúsítvány fogalma
4.1.2. A tanúsítványok típusai és felépítései
4.2. Tanúsítványok használata
4.2.1 Tanúsítványok igénylése, az igénylés lépései
4.2.2. Tanúsítvány telepítése és a kezelő segédprogram működése
4.3. Létező tanúsítványok a jelenlegi rendszereinkben
4.3.1. Tanúsítvány-tárolók felépítése, rekeszei az operációs rendszerekben
4.3.2. Személyes tanúsítványok kiválasztása, és adatainak ellenőrzése
4.4. Visszavonási listák, felfüggesztések ellenőrzése
4.4.1. A visszavonási listák helye
4.4.2. A visszavonási listák működése

5. AZ ELEKTRONIKUS ALÁÍRÁSOK OSZTÁLYOZÁSA
5.1. A digitális aláírás és lehetséges megvalósításai
5.1.1. Egyszeres aláírások és fajtáik
5.1.1. Többszörös aláírások és fajtáik
5.2. Szabványos aláírás-típusok
5.2.1. Alap szabványos aláírások: normál aláírások
5.2.2. Alap szabványos aláírások: időbélyegzett, aláírások
5.3. Joghatást kiváltó aláírás-fajták
5.3.1. Normál és fokozott biztonságú aláírások joghatása
5.3.2. Minősített aláírások joghatása

6. A DIGITÁLIS ALÁÍRÁSOK KÉSZÍTÉSE
6.1. A digitális aláírás támogatása dobozos termékekkel
6.1.1. Aláírás-készítő alkalmazás-programok típusai
6.1.1. Aláírás-készítő alkalmazás-programok aláírási funkciói
6.2. Aláírási politika és felépítése, feladatai
6.2.1. Az Aláírási politika szükségessége
6.2.2. Az Aláírási politika megvalósítási példái
6.3. Aláírások készítése különböző alkalmazásokkal
6.3.1. Aláírások gyakorlati elkészítése a nem nyílt irodai alkalmazások (pl. Microsoft Word, Excel) segítségével
6.3.2. Aláírások gyakorlati elkészítése a nyílt irodai alkalmazások (pl. OpenOffice) segítségével

7. AZ ELEKTRONIKUS ÜGYINTÉZÉS ÉS MEGVALÓSULÁSI FORMÁI
7.1. Az elektronikus ügyintézés meghatározása, elemei, és kapcsolódásuk az elektronikus aláírással
7.1.1. Az EU e-ügyintézési funkcióinak általános topológiája
7.1.2. Az e-ügyintézés ismertett funkcióinak kapcsolata az elektronikus aláírással
7.2. Az elektronikus aláírás helye és szerepe az elektronikus üzleti alkalmazásokban (pl. vásárlás, jegyrendelés)
7.2.1. Internetes vásárlás folyamata
7.2.2. Elektronikus menetjegy-rendelési funkciók

MELASZ
Magyar Elektronikus Aláírás Szövetség

Megbízólevél

A Magyar Elektronikus Aláírási Szövetség (továbbiakban MELASZ) Elnöksége megbízza Erdősi Péter Mátét (szig. MC-I 623388, továbbiakban: Szakértő), hogy készítsen összefoglaló jelentést a magyarországi elektronikus aláírás, elektronikus hitelesítés oktatásának helyzetéről, valamint állítson össze egy javaslatot a képzés fejlesztésére vonatkozóan.

A jelentés az alábbiakra terjedjen ki:

- az elektronikus aláírás helye a digitális írástudásban,
- az elektronikus aláírás oktatása a közoktatásban,
- az elektronikus aláírás oktatása a felsőoktatásban,
- az elektronikus aláírás helyzete a szakképzésben,
- az elektronikus aláírással kapcsolatos oktatási anyagok módszertani háttere.

Ennek érdekében felhatalmazzuk arra, hogy a MELASZ nevében kérdéseket tegyen fel a fenti témákkal kapcsolatosan, átvegyen a fenti témával kapcsolatos anyagokat, és használhassa a MELASZ-logót a fenti témával kapcsolatban készített emlékeztetőiben, dokumentumaiban.

A feladat elkészítésének határideje: 2007. szeptember 30.

Kérjük az oktatásban közreműködő megkérdezett partnereket, hogy támogassák Szakértőink munkáját a lehető legjobb tudásuk szerint, ilyen módon járuljanak hozzá a digitális írástudás további hazai fejlesztéséhez.

Tisztelettel:

Budapest, 2007. május 2.

Almási János
MELASZ elnök

MELASZ Magyar Elektronikus Aláírás Szövetség

Csapodi Márton
MELASZ alelnök

090624

Oktatási és Kulturális Minisztérium

Közoktatási Szakállamtitkár

Előadó: Horváth Gréta
Tárgy: Alapítási és indítási engedély
Szám: OKM - 4 / 101 /2009.
Melléklet: 1 pld. hitelesített program

HATÁROZAT

Az Informatika-Számítástechnika Tanárok Egyesülete (1133 Budapest, Vág u. 2/c.) által benyújtott, A/5460/2009. számon nyilvántartásba vett pedagógus-továbbképzési program alapítási és indítási engedély kiadása iránti kérelmének - a miniszter által átruházott döntési jogkörömben eljárva -

helyt adok.

Ennek megfelelően az „Elektronikus aláírás elméleti és gyakorlati oktatására felkészítő alapszintű tanfolyam" című továbbképzési program alapítását és indítását jóváhagyom, továbbá a program alkalmazásához szükséges alapítási és indítási engedélyt megadom a következő feltételekkel:

Az alapítási és indítási engedély öt évre szól, ennek megfelelően a program a határozat aláírása napját követő hónap első napjától számított ötödik év eltelte után nem alkalmazható, és az engedélyt a nyilvántartásból hivatalból törölni kell.

A továbbképzés helyszínét a továbbképzés megkezdése előtt legalább harminc nappal be kell jelenteni az Oktatási Hivatal Közoktatási Akkreditációs Osztálynak (1054 Budapest, Báthori u. 10.).

A továbbképzés során a jóváhagyott program címe, a program teljesítésére meghatározott összes óraszám, a program célja és teljesítésének tartalmi követelményei nem változtathatók meg.

Tájékoztatom a továbbképzés szervezőjét, hogy

a) csak olyan továbbképzés szervezhető meg, amely szerepel a továbbképzési jegyzékben;

b) az engedély jogerőre emelkedése után megjelenő első továbbképzési jegyzékbe – külön kérelem nélkül – felkerül a továbbképzés, a jegyzék a kiadástól számított egy évig érvényes, ezt követően a továbbképzés csak külön kérelem alapján kerülhet fel a következő évi jegyzékre;

c) az engedély jogerőre emelkedését követően már a továbbképzési jegyzék megjelenése előtt is megkezdheti a továbbképzés szervezését;

d) az Oktatási Hivatal Közoktatási Akkreditációs Osztálya jogosult a helyszínen ellenőrizni a továbbképzés - program szerinti - megszervezését, illetőleg megtekinteni a már megtartott továbbképzések iratait. A továbbképzés szervezője köteles - a megbízólevéllel rendelkező részére - a továbbképzések okmányait rendelkezésre bocsátani, illetve a szükséges felvilágosítást megadni;

INFORMATIKA-SZÁMÍTÁSTECHNIKA TANÁROK EGYESÜLETE

e) vissza kell vonni az engedélyt, ha
- a továbbképzést nem a továbbképzési programban foglaltak szerint szervezték meg,
- a továbbképzés szervezője az engedély kiadását követő évtől kezdődően nem kérte felvételét a továbbképzési jegyzékbe, és továbbképzést szervezett,
- a továbbképzés szervezője nem vezette a továbbképzéssel kapcsolatos okmányokat,
- a továbbképzés szervezője nem tette lehetővé a továbbképzéssel kapcsolatos ellenőrzés lefolytatását;

f) vissza lehet vonni az engedélyt abban az esetben, ha
- a továbbképzést nem azokkal a feltételekkel szervezték meg, amelyek az engedélyben, valamint a továbbképzési jegyzékben szerepelnek,
- a továbbképzés szervezője nem jelentette be a továbbképzés helyét és idejét.

Az alapítási és indítási engedély nyilvántartási száma: OKM - 4 / 101 / 2009.

A határozat ellen államigazgatási úton további jogorvoslatnak helye nincs. A határozat felülvizsgálatát – jogszabálysértésre hivatkozással – a közléstől számított harminc napon belül a Fővárosi Bíróságnál lehet kezdeményezni.

Indokolás

A pedagógus-továbbképzésről, a pedagógus-szakvizsgáról, valamint a továbbképzésben résztvevők juttatásairól és kedvezményeiről szóló – többször módosított – 277/1997. (XII. 22.) Korm. rendelet (a továbbiakban: rendelet) 7. §-ának és 8. §-ának (1) bekezdése alapján a továbbképzés keretében olyan továbbképzés indítható, amelynek a programját az oktatási és kulturális miniszter jóváhagyta, alapítási és indítási engedélyét a miniszter kiadta. Az alapítási és indítási engedély kiadásának feltétele, hogy a továbbképzési program megfeleljen a rendeletben meghatározott célkitűzéseknek. Az alapítási engedély, illetve az indítási engedély iránti kérelem egy eljárásban is elbírálható, és az engedélyek egy határozatban is kiadhatók, ha a kérelmeket együtt, ugyanaz az ügyfél nyújtotta be.

A továbbképzési program elfogadására, az engedély kiadására a Pedagógus-továbbképzési Akkreditációs Testület javaslata alapján került sor. Az akkreditációs testület – szakértők bevonásával – megállapította, hogy az „Elektronikus aláírás elméleti és gyakorlati oktatására felkészítő alapszintű tanfolyam" című továbbképzési program a fenti célkitűzéseknek megfelel, javasolta annak jóváhagyását és az engedély kiadását.

E határozatom a rendeleten és a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL törvény (a továbbiakban: Ket.) 71. § (1) bekezdésén és 72. §-án, a jogorvoslathoz való jog – tekintettel a Ket. 100. § (1) bekezdés a) pontjában foglaltakra – a Ket. 109. § (1) bekezdésén alapul.

Budapest, 2009. jún. 17.

Az Oktatási és Kulturális Minisztérium Szervezeti és Működési Szabályzatának kiadásáról szóló 7/2006. (MK.94.) OKM utasítás alapján a miniszter nevében eljárva:

Dr. Szüdi János

OKTATÁSI ÉS KULTURÁLIS MINISZTÉRIUM Szakállamtitkár 1.

Határozatot kapja:

1. Címzett
2. Oktatási Hivatal Közoktatási Akkreditációs Osztály
3. Nemzeti Felnőttképzési Intézet Felnőttképzési Akkreditáló Testület
4. Irattár

INFORMATIKA-SZÁMÍTÁSTECHNIKA TANÁROK EGYESÜLETE

I) MELASZ megbízólevél a felmérés elvégzésére

II) A továbbképzésről szóló OKM határozat

INFORMATIKA -SZÁMÍTÁSTECHNIKA TANÁROK EGYESÜLETE
1133 Budapest, Vág u 2/C. Fsz/2.
ISZE 1393 Budapest, Pf.: 319.

- fax: 1/462-0415
- e-mail: isze@isze.hu
- web: www.isze.hu, www.isze.eu

Az egyesület alapítási éve: 1991.
FMK Azonosító: 01 – 0769 04
ISSN szám: 1217-0178
Felelős kiadó: Kőrösné Dr. Mikis Márta
Szerkesztő: Lakosné Makár Erika
erika@lakosvar.hu

Kik szerkesztik ezt a lapot?

Te és én, vagyis mi. Mindenki, akinek jó ötlete, okos gondolata van, s azt szívesen megosztja velünk. Természetesen van szerkesztőbizottság, hiszen másképen nem születne meg egy-egy szám, de a ti írásaitokból áll össze a tartalom.

Ha van kinek írnod, ha van miről írnod és van hozzá kedved is, akkor csatlakozz hozzánk.

Minden segítséget megköszönünk.
Az INSPIRÁCIÓ szerkesztősége

http://www.isze.hu/inspiracio