DEBRECENI EGYETEM

AGRÁRTUDOMÁNYI KÖZLEMÉNYEK 34.

ACTA AGRARIA DEBRECENIENSIS

2009

AGRÁRTUDOMÁNYI KÖZLEMÉNYEK, 2009/34.

Ihrig Károly Gazdálkodás- és Szervezéstudományok Doktori Iskola

Károly Ihrig Doctoral School of Management and Business Administration

Elektronikus aláírás alkalmazása az elektronikus kereskedelemben

Péntek Ádám
Debreceni Egyetem Agrár- és Műszaki Tudományok Centruma,
Gazdálkodástudományi és Vidékfejlesztési Kar,
Gazdaságelemzés-módszertani és Alkalmazott Informatikai
Intézet, Debrecen
penteka@agr.unideb.hu

ÖSSZEFOGLALÁS

Az Internet felhasználásának folyamatos bővülése jellemző napjainkban. Mind a szervezeti, vállalati, mind pedig az egyéni felhasználói piacon az internetet használók arányának folyamatos növekedése, illetve a felhasználási területek bővülése figyelhető meg hazánkban és világszerte egyaránt. Ez új lehetőségeket kínál az érdeklődő vállalatok számára az üzleti siker elérésére. Ugyanakkor a bizalom, az azonosíthatóság minden üzlet alapja. Az új kommunikációs csatorna új azonosítási technikákat követel meg. A digitális aláírás egy szabványos és jól használható lehetőséget biztosít. Dolgozatomban bemutatom a digitális aláírással jelenleg Magyarországon elérhető szolgáltatásokat.

Kulcsszavak: *digitális aláírás, e-kereskedelem, biztonság, titkosítás*

SUMMARY

Expansions of the use of the Internet applications are increasing continuously. The distances have disappeared and decreased the necessary trade time. The bases of the businesses are the confidence and the other parties identification. The new communication channel demands new identify methods. The digital sign is a standard and easy to use possibility to identify one another and their documents, e-mails etc. In my paper I show the availability of e-commerce services which can be used to identify by digital sign in Hungary.

Keywords: *digital signature, e-commerce, safety, encryption*

BEVEZETÉS

Az elektronikus kereskedelem (e-commerce) kifejezést először az Interneten való web alapú vásárlások elnevezésére alkalmazták, a 90-es évek elejétől. Az új terminológia bevezetése azért volt indokolt, mert egy új általánosan használható kereskedelmi mód született, melynek segítségével mindenki sokkal gyorsabban bonyolítja le valamennyi üzleti tranzakcióját. A korai időkben kizárólag a kiskereskedelmi tevékenységekre, azon belül is a vásárlót érintő olyan szakaszokra vonatkoztatta a meghatározás az elektronikus kereskedelmet, mint az áru/szolgáltatás hirdetése és megrendelése. Később egyre több tevékenységet soroltak be az elektronikus kereskedelem körébe. Ez a folyamat a mai napig tart.

Az e-commerce és e-business szavakat gyakran egymás szinonimájaként is használjuk, különösen igaz ez Magyarországon, ahol mindkét szó fordítása elektronikus kereskedelem.

A két fogalom nem teljesen fedi egymást. Az e-business tágabb területet ölel fel, és magában foglalja az elektronikus kereskedelmet. Bármely olyan tevékenység e-business, amely összeköt üzleti rendszereket a vásárlókkal, dolgozókkal, viszonteladókkal és beszállítókkal intraneten (belső hálózat) és extraneteken, a világhálón keresztül.

A két meghatározás igen hasonló és egyre inkább összefonódik, mert az elektronikus üzletvitel a kereskedelmi profit növelésére irányzott tevékenység.

E-kereskedelem

Az elektronikus kereskedelem olyan, kifelé irányuló folyamatok megnevezése, amelyek az ügyfeleket, szállítókat és külső partnereket érintik, beleértve a kereskedelmet, a marketinget, a rendelések felvételét, a szállítást, az ügyfélszolgálatot, a nyersanyagok beszerzését, a gyártási utánpótlásról való gondoskodást. Ez a hagyományostól eltérő üzleti modelleket követel meg. Új bevételi források megszerzésével kecsegtet, a piacteret kitágítja, így az – általában földrajzi akadályok miatti – távolságokat csökkenti, vagy eltünteti. Új piacokat és konkurenseket ad a résztvevőknek.

- A vállalatok kiterjeszthetik tevékenységi körüket és szert tehetnek új ügyfelekre, illetve növelhetik meglévő ügyfeleik elégedettségi szintjét, emellett összefogottan és elektronikusan bonyolíthatják tranzakcióikat.
- Az ügyfelek, fogyasztók és partnerek, illetve a céges beszerzők azzal a tudattal vásárolhatnak, hogy a tranzakciók biztonságosan folynak, és a személyes adataik nem kerülnek illetéktelen kezekbe (Kondricz és Tímár, 2001).

Az e-kereskedelmi módszerek használatának hajnalán mindössze a termékkatalógusok weben való publikálására, és az alapvető elektronikus kereskedelmi funkciók biztosítására használták az Internetet. A valódi elektronikus kereskedelem túlmutat az eladásokon és a vásárlásokon: valójában az üzleti folyamatok korszerűsítéséről, a hatékonyabb tranzakció-feldolgozásról, a gyorsabb termékbevezetésekről, a kisebb raktárkészletekről, az ügyfél- és partnerkapcsolatok megerősítéséről, az ügyfél igényeihez igazodó, személyre szabott ajánlatokról és marketingről szól. E technológiák segítségével tovább lehet növeli az ügyfelek kötődését.

E-Business

Az e-business magába foglalja az elektronikus kereskedelmet, s emellett belesorolhatók az olyan belső műveletek is, mint a gyártás- és leltárkezelés, a termékfejlesztés, a kockázatkezelés, a pénzügyek, a tudáskezelés, vagy a humánerőforrások. Az e-üzleti stratégia sokkal bonyolultabb, jobban figyel a belső folyamatokra, és mindenekelőtt a költségcsökkentést, illetve a hatékonyság, a termelékenység javítását tűzi ki célul. Végrehajtani is lényegesen nehezebb feladat, melyhez a következő integrációs feladatokat kell megoldani. Felhasználói szempontból vertikálisan a webes végfelhasználói felület és a háttérrendszerek között; horizontálisan pedig a cég és ügyfelei, üzleti partnerei, szállítói, illetve közvetítői között. Technológiai szempontból horizontálisan az e-kereskedelmi, tudáskezelési és beszállítói-lánc kezelési (SCM), ügyfélkapcsolat-kezelési (CRM) és vállalatirányítási (ERM) rendszerek között. Vertikálisan pedig a vállalaton belül, hogy a vadonatúj technikákat szerves egységbe építhessék a radikálisan újjátervezett üzleti folyamatokkal. Az e-business alkalmazás várhatóan jobban megtérül, mint az e-kereskedelmi, mivel hatékonyabbá teszi a különféle folyamatokat, csökkenti a költségeket, és potenciálisan nagyobb profittal kecsegtet. Azonban az elektronikus kereskedelem és az elektronikus üzletvitel is ezekre a folyamatokra, valamint az adatbázisokból, alkalmazás-kiszolgálókból, biztonsági és rendszerfelügyeleti eszközökből, s a meglevő öröklött megoldásokból összeálló technológiai infrastruktúrára irányul. Mindkettő megvalósítása azt feltételezi, hogy az adott cég új értéket képviselő láncolatokat építsen ki részint ügyfeleivel és szállítóival, részint magán a szervezeten belül.

Az e-kereskedelem népszerűsége

A magyarországi internetezőknek több mint a fele (51%) szeret on-line módon vásárolni, és a többségük (91%) tisztában is van e vásárlási mód lehetőségével. Ebből adódóan nem is csoda, hogy az internetezők 45%-a már vásárolt a világhálón. Azok, akik legalább havonta egyszer vásárolnak az Interneten, az összes „e-vásárló" közel negyedét (24%) teszik ki. Ezen felül, az internetes vásárlást már korábban kipróbáló válaszadók 23%-a az eddiginél is gyakrabban szeretne a jövőben on-line vásárolni. A felhasználók on-line vásárlásra való ösztönzése érdekében az eladóknak különleges figyelmet kellene szentelniük árpolitikájukra. A felmérések szerint, a válaszadók gyakrabban vásárolnának, ha különleges kedvezményekkel (16%), vagy alacsonyabb árakkal (18%) találkoznának. Mivel az Internet-használók több mint harmada (36%), aki hallott már valaha is az on-line vásárlás lehetőségéről, kockázatosnak ítéli meg azt, ezért a tranzakciók biztonságának növelése valószínűleg újabb ügyfeleket hozhatna (Gemius Hungary, 2007). Az agárgazdaságban, különösen az élelmiszeripari és kereskedelmi szektorban is egyre növekszik a szolgáltatók és az on-line vásárlók száma (Herdon et al., 2006).

On-line üzletek és aukciós oldalak

Az Internetezők többsége az online üzleteket részesíti előnyben az aukciókkal szemben. Az Internetezők 45%-a válaszolta, hogy már vásárolt e-boltban (Gemius Hungary, 2007). Az előbbi vásárlók mintegy 92%-a költött már pénzt korábban, 51%-uk kifejezetten szereti az on-line vásárlást. Legnagyobb előnyként az ott történő vásárlással nyert időmegtakarítást (50%) és a rendelés leadásának tetszőleges idejét (42%) jelölték meg. A felhasználók többségének fontos a termékinformáció megbízhatósága, valamint, hogy valóban azt a terméket kapják kézhez, amit megrendeltek. Minden negyedik válaszadó szerint ezek a főbb előnyei az on-line boltoknak az aukciós oldalakkal szemben. Ezen felül az Interneten vásárlók nagy hányada elégedett, az on-line üzletekben valaha is vásárolt Internetezők 70%-a nem találkozott semmilyen problémával a vásárlás folyamán.

Habár az aukciók kevésbé népszerűek, mint az on-line üzletek – az Interneten vásárlók csupán 24%-a vásárolt valamilyen terméket aukciós oldalon –, ez a vásárlási mód is számos előnnyel rendelkezik. Az aukción pénzt költő felhasználók szerint a pozitívumok közé tartozik a hagyományos üzletekkel szemben a nehezen fellelhető tárgyak beszerezhetősége (48%) és az olcsóbb árak (45%).

Az elektronikus kereskedelemi rendszerek kialakítására újabb és újabb technológiai eszközök állnak rendelkezésre (Péntek és Herdon, 2007). A kereskedelem egyik sarkalatos pontja a bizalom. Az elektronikus kereskedelemben – ahol az üzleti partnerek sokszor soha nem is találkoztak – ez hatványozottan jelentkezik. A bizalom létrehozására és fenntartására alkalmas eszközök kifejlesztésére igény van. Az egyik ilyen eszköz a digitális aláírás.

DIGITÁLIS ALÁÍRÁS

A kézzel írt dokumentum igazolja az aláíró személyét. Ha géppel írjuk, és kézzel aláírjuk, még két tanúra van szükség, hogy hiteles legyen. A szöveg eredetisége, sértetlensége látszik. Elektronikus dokumentumnál ezt kell kiváltani az elektronikus aláírással.

A hagyományos aláírás szerepe:

- a kézjegy igazolja az aláíró személyét,
- a szöveg és aláírás együttese (a papíron) igazolja, hogy az aláíró látta (megismerte) a szöveget,
- a dátum az aláírás időpontját igazolja,
- a papír utal a szöveg eredeti formájára.

Az e-business-nek és általában a távközlő hálózaton, az Interneten történő üzletvitel terjedésének legnagyobb akadálya a bizalom és a biztonság hiánya volt. A vállalatokat egyre nagyobb mértékben kényszerítik az elektronikus kereskedelem és ügyintézés, a pénzügyi tranzakciók munkahelyről/otthonról történő végzésére.

Ezen kényszerítő körülmények hatására Magyarországon is megszülettet a törvény az elektronikus aláírásról (2001. évi XXXV. törvény).

Digitális aláírás (*1. ábra*) alatt az elektronikus okirat védelmét szolgáló, titkos aláírási kulccsal készített digitális jelsorozatot értünk, amely a hozzá tartozó időbélyegzővel és hitelesítési tanúsítvánnyal azonosítja az aláírási kulcs tulajdonosát, és egyértelműen bizonyítja az okirat hitelességét és sértetlenségét. Maga a folyamat az aszimmetrikus titkosítási rendszerre épül: a titkos kulcsot használják a digitális aláírás létrehozásához, a nyilvános kulcs ennek ellenőrzésére szolgál. Ez a gyakorlatban azt jelenti, hogy az elektronikusan aláírt okirat „végén" lévő jelsorozat tulajdonosának személyéről hitelesen szerezhet tudomást a fogadó partner.

A digitális aláírás részei:

- MD (Üzenetpecsét) algoritmus (Ködmön, 1999)
- Az aláíró neve, azonosítója
- Az aláírás ideje
- MD algoritmus azonosítója (Pásztor, 2001)
- Az aláírás helye
- Egyéb fontos adatok

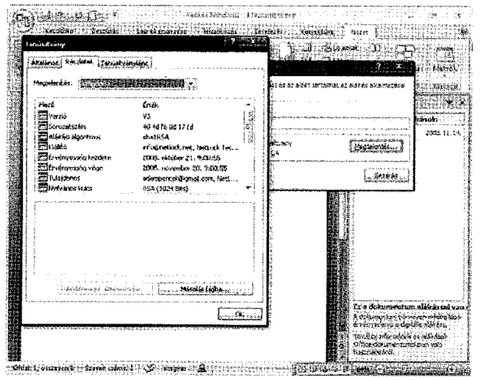
A törvényjavaslat háromféle elektronikus aláírást definiál. Egyszerű e-aláírásnak nevezi, ha egy számítógépes szöveg végére annak szerzője elhelyezi valamilyen azonosítóját. A bíróságok az ilyen dokumentumot is elfogadnák bizonyítéknak, komolyabb jogkövetkezménye azonban csak a második fajta, úgynevezett fokozott biztonságú elektronikus aláírásnak van, amely nem csupán az aláíró azonosítására alkalmas, hanem annak bizonyítására is, hogy a szignálás után senki más nem módosította a dokumentumot. A harmadik típusú, úgynevezett minősített elektronikus aláírás hitelességét az erre felhatalmazott szolgáltató által kibocsátott tanúsítvány igazolja. Az utóbbival ellátott dokumentumok teljes bizonyító erejű magánokiratnak számítanak, vagyis egyenértékűek azokkal a papíralapú iratokkal, amelyeket két tanú is aláírt. Ezeket a bíróságok mérlegelés nélkül fogadják el bizonyítéknak. Az aláíró személyazonosságát, az aláírás biztonsági szintjét üzleti alapon működő aláírás-hitelesítők (CA-k) igazolják, akik előzetesen ellenőrzik ügyfeleik személyazonosságát, amihez adatokat is kérhetnek a közigazgatási szervektől.

Az aláírás hitelesítők feladatai, jellemzői (Virrasztó, 2004):

- az aláíró személy azonosítása,
- kulcsok azonosítás utáni kiadása,
- aláírását mindenki elismeri,
- tevékenysége ellenőrizhető,
- mulasztása, vagy gondatlansága szankcionálható.

A fokozott, illetve a minősített e-aláírás az úgynevezett aszimmetrikus kulcsú titkosítással valósítható meg. Ennek lényege, hogy az aláíró titkos kulcsával – aminek hordozója például egy chipkártya vagy egy USB kulcs is lehet – „lepecsételi" a dokumentumot. Az aláírót azonosító és egyúttal a dokumentum sértetlenségét bizonyító, – esetleg az aláírás időpontját is tartalmazó – „pecsét" a titkos kulcs nélkül gyakorlatilag feltörhetetlen, a dokumentum módosíthatatlan. Ugyanakkor magát a pecsétet bárki elolvashatja, és azonosíthatja feladóját annak nyilvános kulcsa segítségével, amely az Internetre is feltölthető. A minősített, hitelesített dokumentummal okozott kárért a szolgáltató felel, kétség esetén neki kell bizonyítania, hogy betartotta a törvény előírásait.

1. ábra: **Digitálisan aláírt dokumentum**



Forrás: Péntek, 2009

Figure 1: Digital signed document

A digitális aláírással kapcsolatos kérdésekben a felügyeletet gyakorló hatóság a Hírközlési Főfelügyelet. 2001. szeptember 1-jén lépett hatályba az elektronikus aláírásról szóló törvény (*2. ábra*). Ezután sorban jelentek meg cégek, pl. NETLOCK Kft., MÁV Informatika Kft., melyek a nyilvános kulcsú (PKI – Public Key Infrastructure) infrastruktúrán alapuló szolgáltatásai, először üzleti, majd magánszemélyek részére is.

A megoldások közül leginkább az aszimmetrikus kriptográfiát, titkos és nyilvános kulcspárt alkalmazó, nyilvános kulcsú infrastruktúrán alapuló hitelesítés és elektronikus aláírás terjedt el.

Két üzleti partner mellett létezik az őket hitelesítő, úgynevezett megbízható harmadik fél, az ún. Trusted Third Party. Ez a szerep voltaképpen egy kereskedelmi szolgáltatás, amelyet a legkorszerűbb technikai megoldás, a nyilvános kulcsú infrastruktúra (PKI) támogat.

Digitális tanúsítvány

A digitális tanúsítvány, mint a biztonsági szolgáltatásokhoz tartozó „alaptermék", és az ezzel létrehozható elektronikus aláírás, mint biztonsági szolgáltatás lehetővé teszi a nyílt hálózatokon a biztonságos kommunikációt, az üzenetek biztonságos cseréjét, a „home banking"-et, az e-kereskedelmet, az elektronikus ügyintézést. A digitális tanúsítvány olyan elektronikus dokumentum, amely hitelesen igazolja a tanúsítvány alanyának és nyilvános kulcsának összetartozását. Felhasználható például elektronikus aláírás készítésére, üzenetek titkosítására, tartalmi sértetlenségük ellenőrzésére, továbbá egyfajta elektronikus személyi

igazolványként az azt alkalmazó azonosságának igazolására az elektronikus világban.

A hitelesítési szolgáltató (*3. ábra*) (Registration Authority, RA) főleg a tanúsítványt igénylő személyek és szervezetek hiteles azonosítását végzi. A hitelesítő-központ (Certification Authority, CA) fő feladata a különböző típusú tanúsítványok kiadása, a tanúsítványok lejárat utáni, vagy egyéb indokolt esetben történő visszavonása, illetve felfüggesztése, valamint az érvényes, illetve visszavont tanúsítványok (CRL, Ceritificate Revokation List) listáinak nyilvántartása és nyilvános közzététele a felhasználók számára. Bizalomra épülő alkalmazásnál nem lényegtelen, hogy a felhasználó regisztrálásáért és a tanúsítványok kiadásáért, kezeléséért a szolgáltató (Certification Service Provider, CSP) felelősséget vállal. A felhasználó cégek, intézmények így biztonságosan köthetnek egymással elektronikus úton szerződéseket, megnő a bizalom az elektronikus kereskedelem iránt, bevezethető az on-line ügyintézés (http://www.ediport.hu/szakmaioldalak.html).

A jogi, törvényi hátteret az elektronikusaláírás-törvény biztosítja illeszkedve a nemzetközi elektronikus biztonsági követelményekhez és normákhoz. A minősítetten hiteles elektronikus aláírással ellátott elektronikus ügyiratok, okiratok jogi értelemben teljes bizonyító erejű, értékű magánokiratnak minősülnek.

A nagy kereskedelmi vállalatoknak, pénzintézeteknek, kormányzati szerveknek és közhivataloknak, ahol a biztonságos internetes kommunikációt speciális alkalmazásokhoz kell adaptálni (például elektronikus ügyintézés, „home-banking", elektronikus kereskedelem, vállalati elektronikus levelezés). Az egyedi tanúsítványok a felhasználó vállalat ügyfelei, illetve munkatársai részére nyújtanak az adott alkalmazáshoz kapcsolódó biztonságos és hiteles hozzáférést, titkos üzenetküldési, tranzakció-kezelési lehetőséget.

Az üzleti tanúsítványok a kis- és közepes vállalkozásoknak nyújtnak eszközt a biztonságos vállalaton belüli intranetes felhasználói azonosításhoz, elektronikus aláíráshoz, illetve PKI-technológián alapuló felhasználói alkalmazásokhoz, például B2B (Business to Business: Vállalat-Vállalat) típusú üzletkötésekhez.

A lakossági felhasználóknál a személyes tanúsítványok lehetővé teszik a biztonságos e-mail küldést és annak elektronikus aláírását, illetve a nyilvános kulcsú infrastruktúrát alkalmazó megoldásokat, így a megbízható otthoni elektronikus vásárlást.

A Tanúsítvány-kibocsátók a következő szolgáltatásokat nyújtják:

- Tanúsítvány-kérelmek ellenőrzése
- Tanúsítvány-kérelmek feldolgozása
- Tanúsítványok kibocsátása és menedzselése

Nem-minősített szolgáltatók

A nem-minősített szolgáltatás végzését a belföldi lakhelyű vagy belföldön tartózkodási hellyel rendelkező természetes személy, illetve belföldi székhelyű (telephelyű) jogi személy vagy jogi személyiség nélküli szervezet 30 nappal a megkezdést megelőzően köteles bejelenteni a hatóságnak.

Minősített hitelesítés szolgáltatók

1. Netlock Kft.
2. MÁV Informatika Kft.
3. Matáv e-szignó
4. Microsec e-szignó
5. IHM Biztonsági hitelesítés szolgáltató

A minősített szolgáltatás végzését a belföldi lakhelyű vagy belföldön tartózkodási hellyel rendelkező természetes személy, illetve belföldi székhelyű (telephelyű) jogi személy vagy jogi személyiség nélküli szervezet 30 nappal a megkezdést megelőzően köteles bejelenteni a hatóságnak és nyilatkoznia kell arról, hogy tevékenységét minősített szolgáltatóként kívánja folytatni. A szolgáltatókra vonatkozó részletes követelményeket az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendelet tartalmazza.

Fokozott biztonságú hitelesítés szolgáltatók

1. Netlock Kft.
2. Matáv e-szignó
3. Microsec e-szignó
4. MÁV Informatika Kft.
5. Giro Elszámolásforgalmi zRT.

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény, valamint a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól szóló 45/2005. (III. 11.) számú kormányrendeletnek megfelelően az alábbi nyilvántartásokat vezeti és teszi közzé:

Tanúsított elektronikus aláírási termékek

Az aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza. Elektronikus aláírási termék: olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevő, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, valamint elektronikus aláírások, illetőleg időbélyegző készítéséhez vagy ellenőrzéséhez használható.

Kijelölt tanúsító szervezetek

Kijelölt tanúsító szervezet: olyan személy vagy szervezet, amely az elektronikus aláírási termék megfelelőségének tanúsítására a kijelölésben foglaltak szerint jogosult.

Felelősségvállalás külföldi hitelesítés szolgáltatók tanúsítványáért

A hatóság a külföldi székhelyű, illetve lakóhelyű hitelesítés-szolgáltató által kibocsátott tanúsítvánnyal kapcsolatos felelősségvállalást nyilvántartásba veszi, és arról bárki számára hozzáférhető és folyamatosan elérhető nyilvántartást tesz közzé.

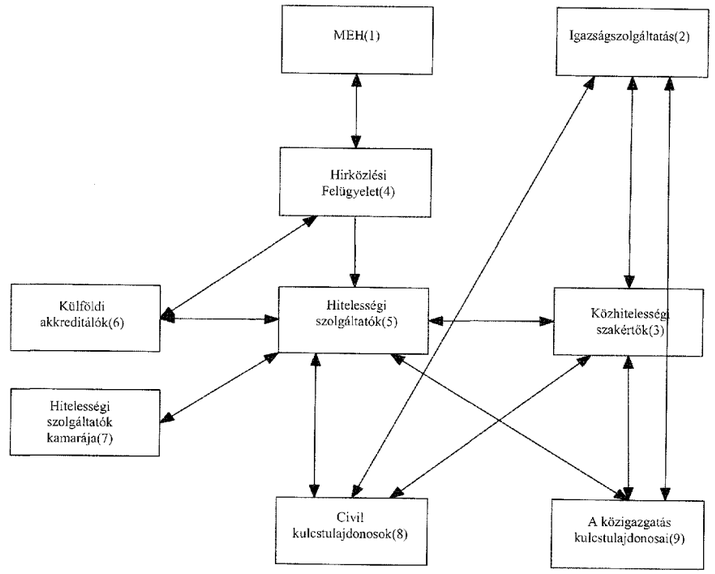
Szakértők

Az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről szóló 7/2002. (IV.26.) MeHVM rendelet szerint a szakértői engedélyeket a Nemzeti Hírközlési Hatóság Hivatala adja ki és vezeti a szakértői névjegyzéket, melyet elektronikus úton bárki számára hozzáférhető és folyamatosan elérhető módon közzétesz.

Közigazgatásban alkalmazható tanúsítványt kibocsátó hitelesítés-szolgáltatók és közigazgatással kapcsolatos hitelesítési rendek

A közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés szolgáltatókra vonatkozó követelményekről szóló 194/2005. (IX. 22.) Kormányrendelet határozza meg közigazgatásban alkalmazható elektronikus aláírásokat (http://www.nhh.hu/index.php).

2. ábra: **Hitelesítési szolgáltatás struktúrája**

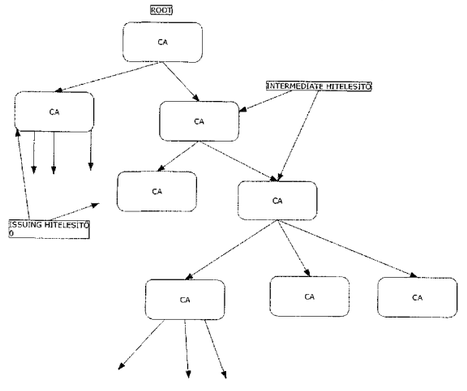


Forrás: Virrasztó, 2004

Figure 2: Structure of Authencity service provider

Prime Minister's office(1), Administration of Justice(2), Professionals of Authencity(3), National Communications Authority(4), Authenticity service(5), Abroad accreditor(6), Chamber of authencity service provider(7), Civilian key holder(8), Key holders of the public services(9)

3. ábra: **Hitelesítő szervezetek struktúrája**



Forrás: Virrasztó, 2004

Figure 3: Structure of the authencity organisations

MAGYARORSZÁGON ELÉRHETŐ ELEKTRONIKUS SZOLGÁLTATÁSOK

Az elektronikusan elérhető szolgáltatások köre napjainkban folyamatosan bővül. Igen örömteli, hogy Magyarország sem marad ki ebből a folyamatból. Jelenleg az alábbi szolgáltatásokat kínálják:

- **Elektronikus számlázás**
- **Megbízható információcsere**
- **Ügyvitel**
- **Dokumentum- és iratkezelés**
- **Elektronikus üzenetek**
- **Azonosítás**
- **Szerződéskötés**
- **Mobil munkatársak**
- **Logisztika – fuvarlevelek, egyéb okmányok**

Az elektronikus számlázás az érvényben levő jogi szabályozás, a számviteli törvénnyel összhangban megengedi az elektronikus számviteli bizonylatok

létrehozását és azok hosszú távú megőrzését. Ilyen módon mind kibocsátói, mind befogadói oldalon lehetőség van a számviteli bizonylatok elektronikus kezelésére, jelentős összegeket megtakarítva a papír alapú számlakezeléssel szemben. Jelenleg már több nagy és közepes vállalat alkalmazza ezt az eljárást.

A megbízható információcsere biztosítja a legmagasabb információbiztonsági szintet. Ez vonatkozik a dokumentumok eredetének bizonyíthatóságára, az aláírt dokumentumok megfelelő titkosítására, valamint a felek megbízható azonosítására bármilyen tranzakcióban (pl. levélváltás, megrendelés, jelentéstétel, stb.). A titkosító kulcs 1024 bites kulcsot használ, melynek feltörése a jelenleg rendelkezésre álló informatikai eszközökkel gyakorlatilag lehetetlen.

Bármilyen ügyviteli folyamat használhat elektronikus aláírást. Ilyen lehet pl. az adattovábbítás, az iratok és dokumentumok áramlása a szervezeten belül és kívül, a jóváhagyási és engedélyezési folyamatok és kérelmek, a hivatalos belső és külső közlemények, értesítések, az adatbázisok védelme, a folyamatvezérlés, a beszerzési és a logisztikai folyamatok, és a hosszú távú bizonyító erejű elektronikus dokumentumok archiválása.

Sokszor problémát jelent az elektronikus üzenetek esetében, hogy a továbbított dokumentum a továbbítás során megváltozik, azt valaki jó- vagy rosszhiszeműen megváltoztatja, felhasználja. Az elektronikus üzenetek tartalma erős védelmet kap az elektronikus aláírás felhasználásával. Egyrészt biztosítható, hogy az aláírt dokumentum a továbbítás során nem változik meg, így teljesen mindegy, hogy az elektronikus levelezés milyen csatornán történik (levelezőprogram, portál, stb.). Másrészt biztosított a továbbított tartalom védelme a titkosítás révén.

Az egyértelmű azonosítás lehetőséget ad egy adott tranzakcióban résztvevő szereplők megbízható azonosítására. Ilyen például a kormányzati portál, ahol csak azonosítás után kezdeményezhető tranzakció. Számos helyen használják az autentikációs tanúsítványokat a helyi számítógépes rendszerbe való belépéshez is. Az autentikációs technológia minden olyan esetben indokolt, ahol egy személy, szervezet, vagy egy szervezet nevében eljáró egyén megbízható azonosítása szükséges.

Szerződéskötés hitelesnek elfogadott, ha bármely fél elektronikus aláírásával ellátja a dokumentumot. Ebben az esetben a feleknek nem szükséges személyesen találkozniuk, illetve nem szükséges a papíralapú másolatok logisztikai kezelése. A szerződések e-mailen is továbbíthatóak. Lehetőség van úgynevezett ellenjegyző aláírás készítésére is. Az aláírt dokumentum minden másolata eredetinek tekintendő.

Az elektronikus aláírás használata igen hasznos olyan esetekben, amikor egymástól fizikailag elkülönült egységek, vagy munkatársak dolgoznak úgy, hogy adatokat, szerződéseket, megrendelőket továbbítanak egy központi számítógépes hálózat felé. Ilyen lehet egy kereskedelmi ügynök, vagy egy területi képviselő, aki jellemzően nem irodában tölti az idejét, de fontos számára a hiteles kommunikáció egy adott központtal.

Logisztika – fuvarlevelek, egyéb okmányok hitelesítése. Igen fontos felhasználási terület lehet a logisztikai terület, ahol áruk, termékek, esetleg szolgáltatások mozognak jelentős dokumentációt hordozva magukkal. Amennyiben ezek a dokumentációk elektronikusan aláírva közlekednek, úgy nem csak az ügyintézési idő rövidül le (nem kell várni egy adott dokumentum fizikai megérkezésére), hanem biztosítható a dokumentációk bizalmassága is.

EGYÉB, AZ E-KERESKEDELEMHEZ KÖZVETLENÜL NEM KAPCSOLÓDÓ SZOLGÁLTATÁSOK

- **Elektronikus cégeljárás**
- **Portál és egyéb web alapú alkalmazás**
- **Minősített archiválás**
- **PDF aláírás – dokumentumok egységesítése, nemzetközi szabvány**
- **Adatszolgáltatás és jelentéstételi kötelezettség teljesítése**

Az elektronikus cégeljárásban résztvevő felek elektronikus aláírást használva kommunikálnak egymással úgy, hogy a bizonyító erejű iratok, dokumentumok elektronikus formában léteznek. Az ügyvéd elektronikusan írja alá a kérelmeket, elektronikusan fizeti az eljárási illetéket, és e-mailen továbbítja az aktát a cégbíróság felé. Az elektronikusan aláírt akták beküldéséről az adott szervezet egy elektronikus tértivevényt küld, mely bizonyítja azt, hogy átvette az aktát (http://www.ediport.hu/szakmaioldalak.html).

A cégbíróság belső folyamataiban az APEH, a KSH, a MÁK és a kereskedelmi bankok elektronikus aláírással ellátott adatokat szolgáltatnak a cégbíró felé, aki végzését szintén elektronikusan aláírva hozza meg. Az elektronikus cégeljárás folyamatába bármely ügyvéd vagy vállalati jogász szabadon bekapcsolódhat. Napjainkban számos szervezet jogi képviselője elektronikus úton bonyolítja a cégügyeit, és a résztvevők köre folyamatosan bővül.

Portál és egyéb web alapú alkalmazás Az elektronikus aláírás használható web szerverek azonosítására is, így egy adott webhelyről megállapítható annak „személyazonossága", vagyis megbízhatósága. Portálokon az elektronikus aláírással megbízható bejelentkezés és azonosítás eszközölhető, az on-line tranzakciók biztonságos környezetben történnek, a letöltött dokumentumok forrása hiteles. Jellemzően önkormányzatok használják elektronikus ügyintézésre, de használják elektronikus számlakibocsátó cégek, valamint olyan társaságok is, amelyek web-alapú kereskedelmet, beszerzést bonyolítanak, illetve jelentéstételi kötelezettséget teljesítenek.

A minősített archiválás-szolgáltatást a Nemzeti Hírközlési Hatóság felügyeli. A minősített archívum elektronikusan aláírt dokumentumokat tárol hosszú távra, akár évtizedekre úgy, hogy azok megőrzzék joghatásukat, azaz bizonyító erejüket. Az

archívumban tárolt dokumentumok védelmét az adott kor technológiájának megfelelő aláírással és a megfelelő titkosítási eljárással biztosítják. A minősített archívum használata minden olyan esetben célszerű, ahol a 7/2005 IHM rendeletben meghatározott tárolási feltételeknek kell megfelelni. Így használható pl. számlák, orvosi akták, kutatási dokumentumok, titkos akták, bizalmas dokumentumok tárolására, vagy a törvény által előírt hosszú távú megőrzési kötelezettség teljesítésére.

Lehetőség van arra, hogy a szabványként elfogadott PDF formátumú elektronikus aláírások készüljenek. Ez olyan esetben használatos, ahol a dokumentumok egységesítése egy formátum-platformra történik. Így az elektronikusan aláírt és időpecsételt dokumentum PDF formátumú marad. Nagy előnye, hogy a PDF aláírás ellenőrzéséhez nem szükséges egyéb alkalmazás, elég az Adobe Acrobat Reader. Miután a PDF nemzetközileg is elfogadott formátum, ezért ez a típusú aláírás igen jól használható nemzetközi viszonylatban is. Egyes területeken, mint pl. az elektronikus számlázás, szintén elterjedt a PDF formátum használata.

Adatszolgáltatás és jelentéstételi kötelezettség teljesítése során egyre elterjedtebb gyakorlat, hogy államigazgatási, illetve magán cégek bizonyos jelentéstételi vagy adatszolgáltatási kötelezettségeiket elektronikus úton teljesítik úgy, hogy azok tartalmát elektronikusan aláírva továbbítják. Néhány példa lehet a cégbíróságok felé az éves beszámoló letéti kötelezettség teljesítése, bankok számára az MNB és PSZÁF felé történő jelentéstételi kötelezettsége, stb.

ÖSSZEFOGLALÁS ÉS KÖVETKEZTETÉSEK

Az elektronikus kereskedelemi technológiák alkalmazása dinamikusan és megállíthatatlanul fejlődik. Ezen technológiák használatának a velejárója a személyes ismeretségek hiánya és az ebből fakadó bizalmatlanság. Ezt korán felismerték, és olyan eljárásokat próbáltak létrehozni, amellyel biztosítható az üzleti élet alappillérei, az azonosíthatóság, letagadhatatlanság, időbélyegek. A digitális aláírás képes megfelelni ennek a kihívásnak, és megteremteni a hagyományos üzleti életben létező környezetet. A kérdés az, hogy a digitális aláírás elterjedésének mi áll az útjában, hiszen kicsit több mint 8.000 személy használta a nyilvános és ellenőrzésre kötelezett magyarországi szolgáltatótól vásárolt tanúsítványához tartozó aláíró-kulcsát Magyarországon, ami kisebb, mint 1 ezreléke a népességnek (Erdősi, 2008). Amennyiben általánossá válik a használata, az alábbi előnyöket várhatjuk:

- ügyintézési folyamatok gyorsulása,
- megtévesztések csökkenése,
- rosszindulatú módosítások hatásainak kivédése,
- költséghatékonyság,
- energia-megtakarítás,
- számonkérhetőség, auditálhatóság magasabb szintre emelése.

Remélhetőleg egyfajta kormányzati ráhatással (Commission for the EU council, 2008) sikerül Magyarországon is általánossá tenni a digitális aláírást, így egy újabb szállal tudnánk kapcsolódni az Európa üzleti vérkeringésébe.

IRODALOM

Erdősi P. M. (2008): Az elektronikus aláírás kötelezettségvállalási szintjei és következményei. Információs társadalomért alapítvány biztonságmenedzsment kutatócsoport ajánlása. http://infota.org/biztmen/

Herdon, M.-Zimányi, K.-Rózsa, T. (2006): Factors of E-commerce in the Agri-food Sector, 3rd HAICTA International Conference in Information Systems in Sustainable Agriculture, Agroenvironment and Food Technology. 20-23 September 2006, Volos-Greece. CD-ROM Proceedings, 1-8.

Kondricz P.-Tímár A. (2001): Az elektronikus kereskedelem jogi kérdései. KJK-KERSZÖV Kft.

Ködmön J. (1999): Kriptográfia: az informatikai biztonság alapjai. ComputerBooks, 1999/2000

Pásztor M. (2001): Kulcs-kérdések a digitális aláírásban. Networkshop

Péntek Á. (2009): Vpn/Ipsec tananyag. TCO, 2008

Péntek, Á.-Herdon, M. (2007): New technologies for e-commerce, Agrarian prospects XV. Conference. 20th and 21st Sept 2006, Prague. CD-ROM Proceeding ISBN 80-213-1531-8.

Tóth M.-Randall K. N. (2000): A digitális aláírás. Budapesti Műszaki Főiskola tananyag

Virrasztó T. (2004): Titkosítás és adatrejtés. ISBN 963 214 253 5

Commission for the EU council (2008): Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market

Gemius Hungary (2007): E-kereskedelem Magyarországon http:files.gemius.pl/News/Hungary/2008_02_26_e-commerce_Hungary_HU.doc

http://www.ediport.hu/szakmaioldalak.html

http://www.nhh.hu/index.php

www.hszk.bme.hu/~ca307/security.PDF

3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

7/2002. (IV. 26.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

7/2005. (VII. 18.) IHM rendelet a digitális archiválás szabályairól, valamint az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos elektronikus archiválás szabályairól

45/2005. (III. 11.) Korm. Rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

194/2005. (IX. 22.) Korm. Rendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről

2001. évi XXXV. Törvény az elektronikus aláírásról