Az elektronikus aláírás

KISS PÉTER
Budapesti Gazdasági Főiskola, Pénzügyi és Számviteli Főiskolai Kar
kiss_p@freemail.hu

Konzulens: Benkőné dr. Deák Ibolya

ABSTRACT

The most important challenge in our life is the move toward a knowledge based information society. This new era has brought new concepts such as E-business that makes the enterprises possible to transcend the barriers of time and distance and to take advantage of the computer networks, especially the Internet, and the global market. But the Internet has its own threats as well: a sent message can be intercepted, modified and therefore the identity of its sender is disputable. It is particularly critical when the sensible data, e.g. transfer orders are transmitted. Electronic signature based on PKI (Public Key Infrastructure) is one of the main solutions that make the Internet secure. The Hungarian Electronic Signature Law codified in 2001 is a legal solution for solving the document security problems

Az utóbbi évtizedben az Internet általános térhódításával az üzleti szférában és más területeken egyaránt komoly innovatív megoldások születtek, így kialakult az elektronikus üzletvitel (e-business) és az elektronikus kormányzat (e-government) koncepciója is, amelyek alapvető célja a valóságos folyamatok elektronikus (internetes) környezetre történő leképzése. Az Internet megszünteti a földrajzi korlátokat, ami például az üzleti életben a vevőkör kiszélesedését jelentheti, de ezzel együtt számos veszély forrása is: az üzenetek lehallgathatók, módosíthatók, eredetük letagadható, a szereplők pedig szimulálhatók. Ezek a veszélyek fokozottan érvényesülnek az elektronikus üzletvitelben és az elektronikus kormányzatban, hiszen kritikus információk továbbításáról és hozzáférhetőségének biztosításáról van szó (például banki tranzakciók indításáról). A dokumentumok elektronikus kezelésének biztonságos megoldását a PKI alapú elektronikus aláírás jelenti, amelynek jogi hátterét a 2001. évi XXXV. törvény alapozta meg.

A digitális aláírás

Mielőtt részletesen foglalkoznánk a digitális aláírással, meg kell különböztetnünk az elektronikus és a digitális aláírás fogalmakat. Míg az elektronikus aláírás – mint később látni fogjuk – egy átfogó, jogi kategória, magában foglalva például azt is, ha valaki begépeli a nevét egy e-mail végére, addig a digitális aláírás egy konkrét informatikai fogalom, és úgymond része az elektronikus aláírások halmazának.

A digitális aláírás mint folyamat, két algoritmus szekvenciája. Első lépésben az ún. hashfüggvény előállítja az alapul szolgáló elektronikus dokumentum ujjlenyomatát, majd ebből az ujjlenyomatból az ún. aszimmetrikus (nyilvános kulcsú) titkosítás alkalmazásával elkészül a digitális aláírás.

> A **hashfüggvény** (one-way hash function) olyan algoritmus, ami az input adatnak (itt az elektronikus dokumentumnak) előállítja az ujjlenyomatát (digest).

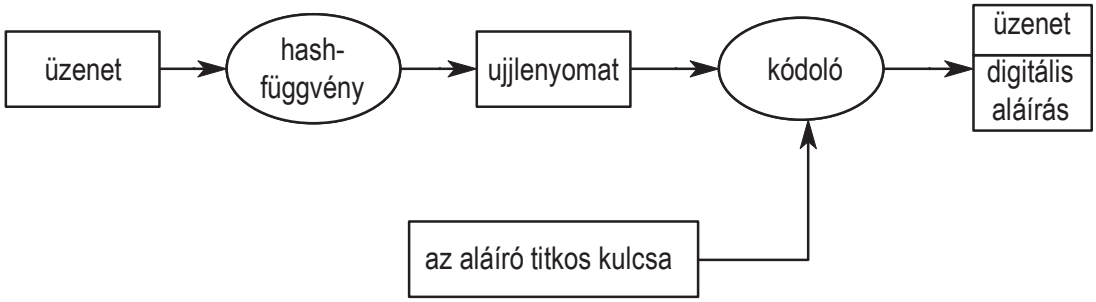
Az ujjlenyomat hossza algoritmusonként adott, azt nem befolyásolja az input adat mérete (az SHA-1 algoritmus outputja 160, az MD5-é pedig 128 bit hosszú). Az ujjlenyomat egyértelműen hozzárendelhető az input adathoz, azaz köztük 1:1 kapcsolat áll fenn. Ebből adódóan az input adat akár 1 bitjének megváltoztatása is jelentős változást okoz az ujjlenyomat értékében. A függvény egyirányú, azaz az ujjlenyomatból nem lehet visszaállítani az input adatot [7].

Az **asszimmetrikus titkosítás** (asymmetric cryptography) olyan titkosítási módszer, ami kulcspárra épül. Az egyik kulccsal kódolt adatot csak a másikkal lehet dekódolni. A legismertebb aszimmetrikus titkosítási algoritmus az RSA. A kulcspárgenerálásról külön algoritmus gondoskodik, amivel véletlenszerűen végtelen számú kulcspár készíthető.

A **nyilvános kulcsú titkosítás** (PKI: Public Key Cryptography) csak elnevezésében tér el az aszimmetrikus titkosítástól. Arról van szó, hogy a kulcspár két tagjához funkciót rendeltek: az egyiket titkos kulcsnak, a másikat nyilvános kulcsnak nevezték el. Egy véletlenszerűen generált kulcspár birtokbavételénél a titkos kulcsot senkinek sem szabad kiadni, a nyilvános kulcs viszont odaadható bárkinek.

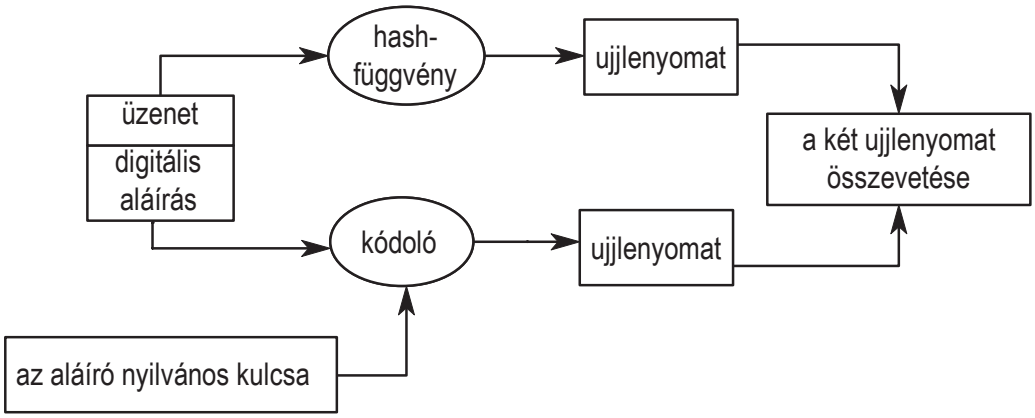
Ebből kiindulva, ha egy személy kódol egy elektronikus dokumentumot a saját titkos kulcsával, akkor az olyan, mintha „aláírta" volna azt, hiszen a saját titkos kulcsa kizárólag az ő birtokában van. Bárki, aki rendelkezik az „aláíró" nyilvános kulcsával, és sikerrel dekódolja a rejtjelezett dokumentumot, meggyőződhet arról, hogy csak a nyilvános kulcshoz tartozó titkos kulccsal történhetett a kódolás, amit pedig csak az aláíró" ismer.

Mindezek alapján tehát a digitális aláírás létrehozásának menete a következő (lásd 7-1. ábra): az aláíró elkészíti az elektronikus dokumentum ujjlenyomatát egy hashfüggvénnyel, majd kódolja azt a saját titkos kulcsával. Ez lesz a digitális aláírás, amit hozzácsatol a dokumentumhoz



7-1. ábra A digitális aláírás létrehozása

A digitális aláírás ellenőrzése az alábbi módon történik (lásd 7-2. ábra): az ellenőrző fél először dekódolja a digitális aláírást az aláíró nyilvános kulcsával, így hozzájut az eredeti ujjlenyomathoz. Ezután elkészíti a megkapott dokumentum ujjlenyomatát az adott hashfüggvénnyel. Ha e két ujjlenyomat értéke megegyezik, nem csupán az aláíró személyének azonossága garantált, hanem az is, hogy a dokumentumot az aláírás után nem módosították. A korábban leírtakkal összhangban ugyanis a dokumentum akár 1 bitjének a módosítása a két ujjlenyomat eltérését okozta volna [1].



7-2. ábra A digitális aláírás ellenőrzése

PKI

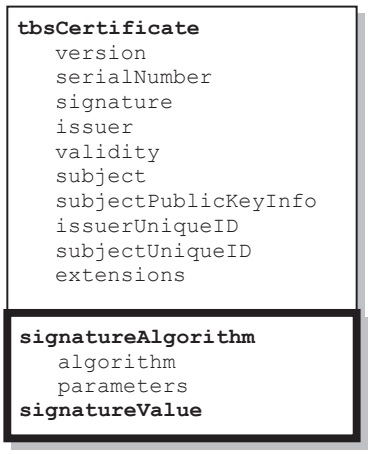
Eddig hallgatólagosan feltételeztük, hogy az aláíró és az ellenőrző fél között a nyilvános kulcs átadása személyesen történt. Interneten keresztül ugyanis bárki állíthatná, hogy ő egy adott nyilvános kulcs tulajdonosa. Erre a problémára nyújt megoldást a PKI, ami a nyilvános kulcsú titkosításra és a tanúsítvány használatára épülve feleslegessé teszi a személyes kulcsátadásokat [6].

> A **nyilvános kulcsú infrastruktúra** olyan, a nyílt hálózatok (Internet) felett álló bizalmi rendszer, amelynek alapja a nyilvános kulcsú titkosítás és a tanúsítványok használata.

A **tanúsítvány** (certificate) olyan elektronikus irat, amely igazolja egy adott nyilvános kulcsnak és annak birtokosának összetartozását; azaz mintegy személyi igazolványként szolgál az Interneten. Következésképpen elvárható, hogy egy ilyen fontos iratot csak egy megbízható, felügyelt, szigorú biztonsági követelményeknek megfelelő szervezet, a Hitelesítő Központ bocsáthasson ki.

A **Hitelesítő Központ** (CA: Certification Authority) olyan szervezet, amelynek legfőbb feladata a hitelesítés (azaz a tanúsítvány-kibocsátás), illetve a tanúsítványok menedzselése.

A tanúsítvány felépítésére nézve az X.509 szabvány az irányadó, ami a PKI adatszerkezeteit specifikálja. A tanúsítvány mindig tartalmazza tulajdonosának egyedi nevét a *subject* mezőben és nyilvános kulcsát a *subjectPublicKeyInfo* mezőben (lásd 7-3. ábra). Az egyedi név (Distinguished Name, DN) olyan hierarchikus címzési formátum, amellyel a DNS-hez (Domain Name System) hasonlóan egyedi azonosítás valósítható meg. Kötelező mező még a tanúsítvány sorszáma *(serialNumber),* ami a CA-n belüli azonosítást teszi lehetővé, illetve a kibocsátó egyedi neve *(issuer).* A tanúsítvány egy meghatározott periódusban érvényes *(validity),* így értelemszerűen ezen időtartamon kívül a személyazonosságot nem igazolja.



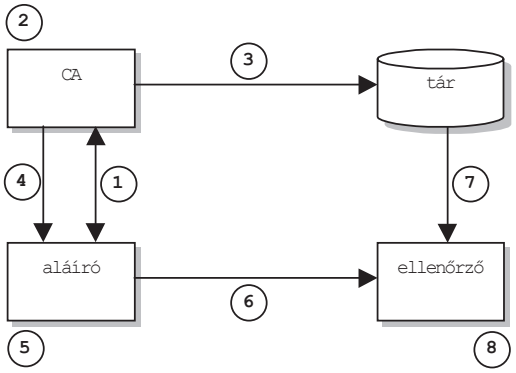
7-3. ábra A tanúsítvány felépítése

A tanúsítványt a CA digitálisan aláírja, hogy a benne foglalt adatok hitelesek legyenek, és így biztosítja annak származását és sértetlenségét. A tanúsítványon szereplő aláírást mindig ellenőrizni kell; erre a célra általában egy ún. „self-signed" CA tanúsítvány alkalmas.

A **„self-signed" CA-tanúsítvány** olyan tanúsítvány, amelyben a CA önmagát hitelesíti, és amellyel az általa kibocsátott ügyféltanúsítványokon szereplő aláírások ellenőrizhetők. A „self-signed" CA-tanúsítvány alanya és kibocsátója tehát maga is a CA.

A *hitelesítés menete* a következő: A CA fogadja a tanúsítvány iránti kérelmet, majd megvizsgálja a kérelmező személyének azonosságát (például elkéri az útlevelét vagy a személyi igazolványát; lásd 7-4. ábra 1. pont). Ki kell hangsúlyozni, hogy ez a lépés meghatározó fontosságú, ugyanis ha nem megfelelően történik a kérelmező azonosítása (például hamis igazolvánnyal másnak adja ki magát), akkor az visszaélésekhez vezethet az Interneten is! Ezután a CA egyedi kulcspárt generál (lásd 7-4. ábra 2. pont). Elkészíti a nyilvános kulcsot tartalmazó tanúsítványt, majd elhelyezi az ún. tanúsítványtárban. (lásd 7-4. ábra 3. pont).

A **tanúsítványtár** (repository) egy adattároló egység, ahová a CA elmenti a tanúsítványokat, illetve a Visszavonási Listákat (lásd később), és ahonnan azok később letölthetők (a CA szerveréhez való kapcsolódás révén). A tanúsítványtárral szemben elsődleges követelmény a folyamatos rendelkezésre állás, hogy az ellenőrző felek bármikor hozzáférhessenek a tanúsítványokhoz, illetve a visszavonási listákhoz.



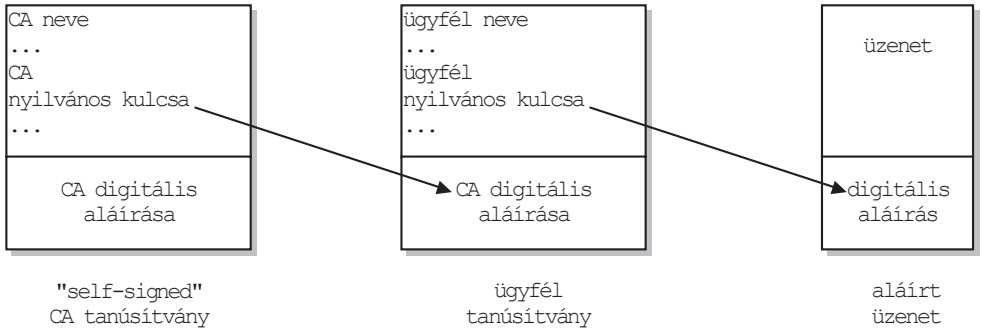
7-4. ábra A PKI működése

A kérelmező végül megkapja a titkos kulcsát, amelyet a tanúsítvány érvényességi periódusának kezdetén használatba vehet, valamint a CA „self-signed" tanúsítványát (lásd 7-4. ábra 4. pont).

A hitelesítés lépéseinek kötelezően személyes találkozásra kell épülniük. Ez a találkozás a PKI rendszer bizalmi alapja, hiszen például, ha a CA saját „self-signed" tanúsítványát nem személyesen adná át az ügyfélnek, hanem Interneten küldené el, akkor azzal a korábbi problémával állnánk szemben, amely szerint Interneten bárki bemutatkozhat bárkiként. A „self-signed" tanúsítványt tehát személyes találkozás nélkül nem tekinthetjük hitelesnek.

Összefoglalva megállapíthatjuk, hogy egy személyes találkozásra mindenképpen szükség van, de ez az egy kiváltja az összes (levelező) partnerhez kötődő potenciális kulcsátadást.

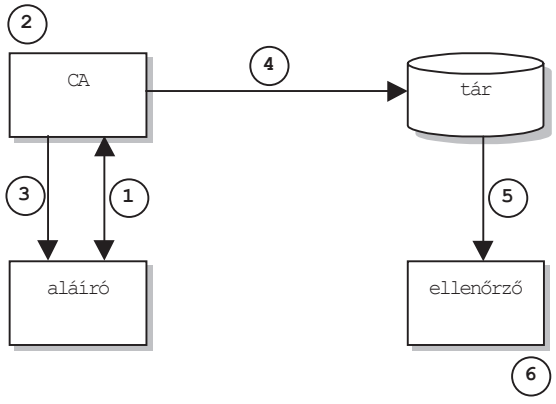
A CA ügyfele tehát rendelkezik a titkos kulccsal, amivel próbaképpen alá is ír egy dokumentumot (lásd 7-4. ábra 5. pont), majd átküldi az Interneten (lásd 7-4. ábra 6. pont). Tegyük fel, hogy a fogadó felet korábban ugyanaz a CA hitelesítette, mint a küldő felet, így a fogadó fél is megkapta a CA „self-signed" tanúsítványát. Ha ugyanis a fogadó fél egy másik CA ügyfele lenne, akkor nem bízhatna meg a küldő felet hitelesítő CA-ban, hiszen azzal nem találkozott személyesen. E probléma megoldását később ismertetem. A fogadó fél a dokumentum megérkeztével letölti a küldő tanúsítványát a tanúsítványtárból (lásd 7-4. ábra 7. pont), majd ellenőrzi az azon szereplő aláírást a CA „self-signed" tanúsítványával. Sikeres ellenőrzés esetén a tanúsítvány adatai hitelesek. Ha a tanúsítvány érvényes, azaz nem járt le, akkor a nyilvános kulccsal elvégezhető a dokumentumon szereplő aláírás ellenőrzése (lásd 7-4. ábra 8. pont). Ha ez is sikerül, a fogadó fél biztos lehet a küldő fél személyének azonosságában, valamint abban is, hogy a dokumentumot az aláírás után nem módosították (lásd 7-5. ábra).



7-5. ábra Az ellenőrzés menete

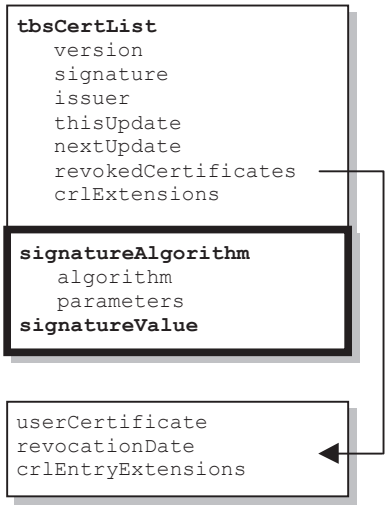
Előfordulhat, hogy az ügyfél titkos kulcsa a tanúsítvány lejárata előtt illetéktelenek kezébe kerül. Ilyenkor a tanúsítvány visszavonását kell kezdeményezni (lásd 7-6. ábra 1. pont). A kérelmező azonosítása után a CA rögzíti az illető tanúsítvány sorszámát az ún. tanúsítvány visszavonási listára (lásd 7-6. ábra 2. pont), majd visszaigazolást küld a visszavonás tényéről (lásd 7-6. ábra 3. pont). A tanúsítvány addig van feltüntetve ezen a listán, amíg a tanúsítványon szereplő lejárati idő el nem érkezik. A visszavonási lista is a tanúsítványtárban kerül elhelyezésre (lásd 7-6. ábra 4. pont) és adatait a CA meghatározott időközönként frissíti.

A t**anúsítvány visszavonási lista** (CRL: Certificate Revocation List) olyan elektronikus irat, ami tartalmazza az adott CA által visszavont tanúsítványok adatait.



7-6. ábra A visszavonás menete

A CRL mindig tartalmazza kibocsátójának egyedi nevét (*issuer*), a legutóbbi (*thisUpdate*) és a következő aktualizálás *(nextUpdate)* időpontját (lásd 7-7. ábra). Minél kisebb a két időpont közötti eltérés, annál sűrűbben aktualizálják az adatokat, így a lista annál jobban mutatja a valós helyzetet (viszont így annál gyakrabban kell letölteni azokat; lásd 7-6. ábra 5. pont). A listában a visszavont tanúsítványok azonosítóira *(userCertificate)* hivatkoznak, valamint a visszavonás dátumát *(revocationDate)* is feltüntetik. A CRL adatait szintén védi a kibocsátó CA digitális aláírása, ami a CA „selfsigned" tanúsítványával ellenőrizhető. Az ellenőrző félnek minden aláírás-ellenőrzés során meg kell győződnie arról, hogy az illető tanúsítvány nincs-e ezen a listán (lásd 7-6. ábra 6. pont). Ha rajta van, a tanúsítvány nem érvényes, azzal az aláírás ellenőrzése nem végezhető el.



7-7. ábra A CRL felépítése

A CA ügyfélszolgálati feladatainak ellátására általában külön szervezeteket, ún. Regisztrációs Központokat hoznak létre. A fenti modellben a könnyebb érthetőség kedvéért ezt figyelmen kívül hagytam.

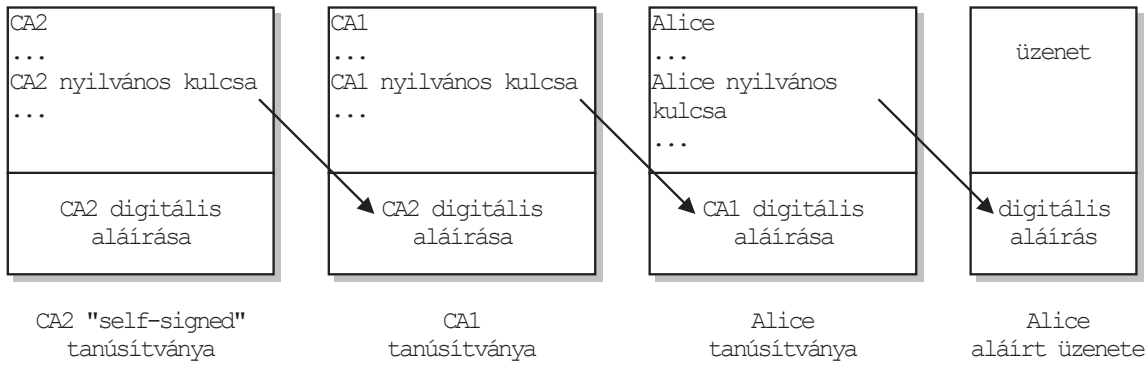
A **Regisztrációs Központ** (RA: Registration Authority) a CA-hoz kapcsolódó szervezet, amely regionális ügyfélszolgálatként funkcionál. A CA által delegált feladatok között szerepel a tanúsítvány és visszavonási kérelmek fogadása, az ehhez kapcsolódó ügyintézés, a CA-val való kapcsolattartás, így a CA-nál kizárólag az informatikai jellegű feladatok maradnak.

PKI-architektúrák

Arra az előbb felvetett problémára, miszerint a küldő és a fogadó felet eltérő CA-k hitelesítik, az jelenti a megoldást, hogy a CA-k egymást is hitelesítik. Ez lehet *egyirányú,* amikor egy CA hitelesít egy másikat, illetve *kölcsönös,* amikor egymást hitelesíti. Előbbi anya-leány, utóbbi egyenrangú kapcsolatot hoz létre. Ebből adódik, hogy előbbi hierarchikus, utóbbi pedig hálós architektúrát alakít ki. Természetesen egy bonyolult modellben e két elrendezés tetszőleges módon keveredhet. Ezekben az architektúrákban számos ún. hitelesítési lánc található.

A **hitelesítési lánc** (Certification Path) egymásra épülő hitelesítések sorozata, kézzelfogható tanúsítványok láncolata, ami útvonalat ír le a fogadó és a küldő fél között, lehetővé téve a fogadó számára a küldő személyazonosságának vizsgálatát.

Lássunk egy példát! A küldő fél (Alice) CA1, a fogadó fél (Bob) pedig CA2 ügyfele. Bob úgy tudja az Alice által aláírt dokumentumot ellenőrizni, ha CA2 hitelesíti CA1-et, amivel létrejön a következő hitelesítési lánc: CA2 -> CA1 → Alice. Bob CA2 „selfsigned” tanúsítványával indít, és lépésről lépésre ellenőrzi a tanúsítványokon szereplő aláírásokat párhuzamosan vizsgálva azok érvényességét. Így jut el az Alice által küldött dokumentumhoz (lásd 7-8. ábra). Ha akár egy helyen is probléma merül fel, a hitelesítési lánc megszakad, és Alice aláírása nem fogadható el.



7-8. ábra A hitelesítési lánc

A törvényi háttér

A PKI előnyeit akkor lehet igazán kihasználni, ha megfelelő jogi háttér áll mögötte. Az Országgyűlés ennek a kihívásnak eleget téve alkotta meg az elektronikus aláírásról szóló 2001. évi XXXV. törvényt [10]. A törvény lényegét tulajdonképpen a 3.§ 1. bekezdése foglalja magában:

„Elektronikus aláírás, illetve elektronikus irat vagy dokumentum elfogadását, beleértve a bizonyítási eszközként történő alkalmazását, megtagadni, jognyilatkozat tételére, illetve joghatás kiváltására való alkalmasságát kétségbe vonni nem lehet kizárólag amiatt, hogy az aláírás, illetve az irat vagy dokumentum elektronikus formában létezik."

Az elektronikus aláírás tehát alkalmazható bizonyítási eszközként, azonban öröklési jogi, illetve családjogi jogviszonyokban nem lehet érvényesen használni. A törvény alapelve, hogy jogszabály nem teheti kötelezővé az elektronikus aláírás használatát. A törvény az írásbeliség fogalmát kiterjeszti az elektronikus környezetre is, ehhez a következő fogalmak definiálása szükséges:

Az **elektronikus dokumentum** „*elektronikus eszköz útján értelmezhető adat, amely elektronikus aláírással van ellátva."*

Az **elektronikus irat** „*olyan elektronikus dokumentum, amelynek funkciója szövegek betűkkel történő közlése, amely a szövegen kívül az olvasó számára érzékelhetően kizárólag a szöveggel szorosan összefüggő, annak azonosítását (például fejléc), illetve könnyebb megértését (például ábra) szolgáló egyéb adatokat foglal magában."*

Az **elektronikus okirat** „*olyan elektronikus irat, amely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy nyilatkozat kötelezőnek elismerését foglalja magában".* A törvény ez alapján kimondja, hogy az írásbeliségnek azok az elektronikus iratok felelnek meg, amelyeket legalább fokozott biztonságú elektronikus aláírással láttak el. A törvény nevesíti az elektronikus aláírás fajtáit:

Az **elektronikus aláírás** „*elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum".* Ez a legtágabb definíció, ilyen aláírásról van szó abban az esetben is, ha egy személy begépeli a nevét egy e-mail végére. A törvény azonban, a már említett 3.§ 1. bekezdés kivételével, nem alkalmazható erre az aláírási típusra, hiszen ennek a hátterében nem áll ott a PKI.

A **fokozott biztonságú elektronikus aláírás** olyan „*elektronikus aláírás, amely megfelel a következő követelményeknek:*

- *alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,*
- *olyan eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll,*
- *a dokumentum tartalmához olyan módon kapcsolódik, hogy minden, az aláírás elhelyezését követően az iraton, illetve dokumentumon tett módosítás érzékelhető".*

Gyakorlatilag erről az aláírási típusról szólt a cikk eddigi része. Az aláíráslétrehozó eszközöket (például szoftver vagy chipkártya) tanúsítani kell, ami azt jelenti, hogy egy erre szakosodott szervezet az eszköz használatát, annak bevizsgálása után engedélyezi.

A **minősített elektronikus aláírás** *„olyan fokozott biztonságú elektronikus aláírás, amely biztonságos aláíráslétrehozó eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki".* Ez az aláírástípus a PKI tekintetében nem különbözik a fokozott biztonságú elektronikus aláírástól, de szigorúbb biztonsági követelmények kapcsolódnak hozzá. A szigorúbb biztonsági követelmények az aláíráslétrehozó eszközre, a tanúsítványra, valamint annak kibocsátójára vonatkoznak.

Összefoglalva: az elektronikus aláírás a legtágabb kategória, ezen aláírásfajta mögött nem áll infrastrukturális háttér (PKI). A fokozott biztonságú elektronikus aláírás viszont már feltételezi a PKI-t, így szükség van egy CA-ra, aki tanúsítványt bocsát ki, és aláíráslétrehozó eszközt biztosít az ügyfélnek. Minősített aláírás azonban csak biztonságos aláíráslétrehozó eszköz által jöhet létre és kizárólag minősített tanúsítvány kapcsolódhat

hozzá. Ez utóbbit pedig csak minősített CA bocsáthat ki.

A törvény szerint a minősített aláírással ellátott elektronikus okirat teljes bizonyító erejű magánokiratnak számít, ha azt az illetékes szerv eljárása során minősített elektronikus aláírással látta el [8]. A piaci alapon működő CA-k állami felügyeletét Magyarországon a *Hírközlési Főfelügyelet* (HIF) gyakorolja. A CA-k az elektronikus aláírás infrastrukturális hátterének a „tartóoszlopai", ezek stabilitásáért, azaz biztonságos, törvényes működéséért felel a HIF. A CA-nak már a működés megkezdése előtt fel kell vennie a kapcsolatot a HIF-fel. Ha fokozott biztonságú szolgáltatást kíván nyújtani, a működés megkezdését megelőzően köteles bejelentenie magát a HIF-nél. Minősített szolgáltatás nyújtásához azonban ez nem elég: meg kell szerezni a HIF által kiadott minősítést is. Ez tanúsítja a törvényben szereplő, a minősített szolgáltatás végzéséhez szükséges szigorú feltételek meglétét (személyi, pénzügyi, fizikai és informatikai biztonsági követelmények), amelyek vizsgálatát maga a HIF végzi el.

A HIF nyilvántartásba veszi a CA-kat; folyamatosan ellenőrzéseket végez arra vonatkozóan, hogy azok megfelelnek-e az előírásoknak, a követelményeknek, intézkedéseket és szankciókat foganatosít; nyilvántartást vezet a CA-król, az aláíráslétrehozó eszközökről, az aláírást létrehozó eszközöket tanúsító szervezetekről, és közzéteszi azokat.

Az elektronikus aláírásról szóló törvény szükségessé tette más jogszabályok módosítását, így újradeklarálják a pénzügyeket szabályozó egyes jogszabályok módosításáról szóló 2001. évi LXXIV. törvény releváns paragrafusait, mint például az elektronikus adóbevallás, valamint az elektronikus számviteli bizonylatok használatának feltételeit [11].

Az adózás rendjéről szóló törvény a módosítás következtében kötelezővé tette az elektronikus bevallást és adatszolgáltatást azon adózói kör számára, amelynek adóztatási feladatait az APEH Kiemelt Adózók Igazgatósága látja el. Látható, hogy ezen rendelkezés nem áll összhangban az elektronikus aláírásról szóló törvény azon elvével, miszerint egy jogszabály nem teheti az elektronikus aláírás használatát az ügyfél részére kötelezővé. Az ellentmondás úgy került feloldásra, hogy az előbb említett kivételt belefoglalták az elektronikus aláírásról szóló törvénybe. A törvény szerint a kiemelt adózóknak az első minősített CA nyilvántartásba vételét követő 180. nap utáni hónap adókötelezettségeit kellett volna először ily módon bevallaniuk. A bevallást ebből adódóan kizárólag minősített elektronikus aláírással és ún. időbélyegzővel ellátva lehetett volna elfogadni. 2002. március 1. volt a határidő, ameddig vártak az első minősített CA nyilvántartásba vételére; ennek hiányában az APEH végzett hitelesítő tevékenységet, vagyis a Kiemelt Adózók Igazgatóságához tartozókat ő látta el tanúsítvánnyal (ingyen). Az APEH által kibocsátott (nem minősített) tanúsítvány azonban csak ebben a zárt körben, kizárólag adóügyek intézésére használható.

Az **időbélyegző** (time stamp) olyan elektronikus irat, ami hitelesen igazolja, hogy egy ügyfél által aláírt dokumentum egy bizonyos időpontban (az időbélyegzés időpontjában) már létezett. Használata hozzájárul az aláírás tényének letagadhatatlanságához. Időbélyegzést csak megbízható szervezetek, az ún. Időbélyegző Szolgáltatók nyújthatnak.

Az **Időbélyegző Szolgáltató** (TSA: Time Stamp Authority) olyan szervezet, amelynek feladata, hogy hiteles időforrás alapján az ügyfél által aláírt dokumentumhoz időbélyeget rendeljen hozzá. Az újrakodifikált számviteli törvény módosításával 2002. január 1-jétől számviteli bizonylatnak számít az olyan elektronikus dokumentum, irat is, amely megfelel a törvény előírásainak, és amelyet minősített elektronikus aláírással és időbélyegzővel láttak el.

Üzleti oldal

A törvény életbe lépése óta a HIF 5 fokozott biztonságú szolgáltatást nyújtó CA-t regisztrált, amelyek közül kettő már megszerezte a minősítést is.

A NetLock Kft. és a Matáv Rt. már korábban is foglalkozott tanúsítványok kibocsátásával, így a törvény hatályba lépésekor elsőként regisztráltatták magukat, mint fokozott biztonságú szolgáltatók. Míg a Matáv Rt. kimondottan nagyvállalati ügyfélkörre rendezkedett be, a Giro Rt., funkciójából adódóan, a banki szférát célozta meg. A Microsec Kft. az elektronikus iratkezelést támogató „E-szignó" elnevezésű szoftverével egyedülálló megoldást kínál. A MÁV Informatika Kft. pedig legifjabbként csatlakozott a hitelesítésszolgáltatók csapatához.

A CA-k alacsony száma azzal indokolható, hogy kiépítésükhöz jelentős pénzügyi forrásra van szükség. Az ICON Számítástechnikai Kft. becslései szerint egy fokozott biztonságú CA létesítése 10-15 millió forintos beruházást igényel [9], egy minősített CA kiépítésének költsége pedig több száz millió forint is lehet [4]. Az ilyen invesztíció csak hosszú távon térülhet meg. A jelenlegi szereplők (a látható tőkeerősség ellenére) kezdetben még nem nyújtottak minősített szolgáltatást. Ez különben sem volt lehetséges a törvény hatályba lépésekor, mert a HIF még nem volt felkészülve a CA-k minősítésére. A piaci szereplők nem zárták ki a későbbi minősítés lehetőségét, de azon az álláspontón voltak, hogy a piac tesztelése nélkül „nem érdemes egy ilyen hatalmas fába vágni a fejszét". Mára azonban közülük kettő (a NetLock Kft. és a MÁV Informatika Kft.) minősítéssel büszkélkedhet.

Az elektronikus aláírás ügyfeleknél jelentkező költségvonzatát egyrészt a tanúsítványhasználat díja, másrészt az aláírás kezelő szoftver/hardver elemek ára képezi. Profitorientált cégek lévén, a CA-k beruházási költségeiket áthárítják az ügyfelekre, ami a tanúsítványhasználat díjában mutatkozik meg. Ennek nagysága igen széles skálán mozoghat. Az aláíráskezelő szoftverek az ingyenes levelezőprogramoktól a komplett PKI-megoldásokig terjednek. Ha a titkos kulcsot chipkártyán rögzítik, szükség van egy kártyaolvasó berendezésre is.

A vállalkozásoknál az elektronikus aláírás alkalmazásával csökkenteni lehetne a papír alapú dokumentumok (számviteli bizonylatok) mennyiségét, amivel időt és pénzt lehetne megtakarítani. A bevezetés kérdését azonban nem szabad leszűkíteni egy vállalkozásra, hiszen annak környezete is van: szállítók, vevők, államháztartás stb. Ha a környezet nem rendelkezik az elektronikus aláírás létrehozásához/ellenőrzéséhez szükséges informatikai háttérrel, akkor az adott vállalkozás sem tudja kihasználni az előbb említett előnyöket. Meg kell vizsgálni, hogy a meglévő rendszereket miként érintené az elektronikus aláírás esetleges alkalmazása. A vállalkozásnak tehát alapos költség-haszon elemzést kell végeznie, mielőtt dönt a bevezetésről.

A közigazgatásban szintén csökkenteni lehetne a papírmennyiséget az elektronikus dokumentumok használatával. Ezen a területen kiemelt szerepet kaphat az elektronikus aláírás. Példaként megemlítem az adózást, ahol az elektronikus bevallás révén az adóhatóságnál egyes munkafázisok feleslegessé válnak, így jelentős költségmegtakarítás érhető el. A kiemelt adózók 2002. szeptember 1-jétől csak elektronikus formában tehetnek eleget bevallási kötelezettségeiknek. A többi adózó ugyan még nem élhet szeptembertől az elektronikus bevallás lehetőségével, de az APEH célja, hogy egy-két éven belül már a tízezer legnagyobb cég intézhesse ily módon az adózással kapcsolatos ügyeit. A kisebb vállalkozások és a magánszemélyek lennének az „utolsók", akik számára lehetővé tennék az elektronikus bevallást [3]. A kiemelt adózók esete jó példa arra, hogy törvény által kötelezővé lehet tenni az elektronikus aláírás használatát.

Jelenleg a magyar háztartások csupán 7%-a rendelkezik Internet-hozzáféréssel [2], ami a magánszemélyek körében jelentősen korlátozza az elektronikus aláírások használatát. A legnagyobb probléma azonban, hogy még kevés olyan helyzet van (például elektronikus kereskedelem vagy elektronikus banki szolgáltatások), amelyben a magánszemélyek használhatnák az elektronikus aláírást. Ezekben a helyzetekben a többség megelégszik az adott biztonsági szinttel, mivel nem hajlandók többet fizetni az elektronikus aláírás nyújtotta biztonságért (külföldi tapaszta-

latok is ezt bizonyítják) [5]. Ezért (vagy önkényesen) a kereskedő/bank nem változtat a működő rendszerén. Aki esetleg fizetne a nagyobb biztonságért, az sem használhatja az elektronikus aláírást.

A bankok számára elkerülhetetlen az elektronikus aláírás használata 2002 szeptemberétől, mivel a kiemelt adózók közé tartoznak. Költség-haszon elemzésre támaszkodva eldönthetik, hogy beillesztik-e az elektronikus bizonylatokat a számviteli rendszereikbe. Felmerül az a kérdés is, hogy az elektronikus banki szolgáltatásaikat kiegészítsék-e a törvény nyújtotta lehetőséggel (azt azonban nem szabad figyelmen kívül hagyni, hogy e szolgáltatások tekintetében hiányzik a határozott fogyasztói igény, amely egyfelől a lakosság bizalmatlanságából, másrészt az Internet alacsony otthoni elterjedtségéből fakad). Ha valaki CA-ként szeretne működni, akkor nagy beruházást kell eszközölnie, ha viszont egy CA-hoz csatlakozna, mint RA, akkor alacsonyabb kiépítési költséggel számolhat. A Giro Rt. is ez utóbbi megoldást támogatja: rendszerének létesítési költségeit megosztja a csatlakozó bankok között. Az alternatívák közötti választásban ismét segít a költség-haszon elemzés. De ha egy bank a már meglévő, működő rendszerével is megfelelő biztonsági szintet tud garantálni (az azonosítást és a titkosítást tekintve), amellyel ráadásul az ügyfelek is meg vannak elégedve, akkor nem fogja az elektronikus aláírást alkalmazni. Amennyiben a jövőben valamilyen jogszabály kötelezővé tenné az elektronikus aláírás banki szolgáltatásokban való alkalmazását, akkor természetesen már nem lenne választási lehetőség.

Következtetések

Véleményem szerint az elektronikus aláírás alkalmazása a korábban említetteket figyelembe véve a jövőben azon vállalkozásoknál lenne célszerű, ahol jelentős papírmunkát lehetne kiváltani az elektronikus dokumentumok használatával. Ugyanezen ok miatt tartom nagyon valószínűnek a közigazgatásban való megjelenését, hiszen ezen a területen rengeteg az adminisztratív teendő. Úgy gondolom, hogy a magánszemélyek körében a közeljövőben nem fog széles körben elterjedni az elektronikus aláírás használata. Ezt a feltételezést a korábban kifejtett indokokra alapozom (alacsony Internet penetráció, bizalmatlanság, tanúsítványhasználati díj stb.). Az elektronikus banki szolgáltatások kiegészítését a megfelelő kereslet hiánya miatt szintén nem tartom valószínűnek.

Hivatkozások

[1] David K.: *Understanding Electronic Commerce* – Microsoft Press, 1997.

[2] Fűrész G. – Virágh M.: *Elektronikus Gazdaság* – KÓD Gazdaság- és Médiakutató Intézet, 1. sz., 2002.

[3] *Hiteles bizonylatok - Elektronikus aláírás* – Figyelő 2001. szeptember 27. - október 3.

[4] *Ne itt írja alá! - Hatályos e-szignó* – Heti Világgazdaság: 2001. október 27.

[5] *Fedőneve: XXXV - Avagy semmi sem egyszerű, még az elektronikus aláírás sem* – Business Online 2001. október

[6] Burr W.E.: *Public Key Infrastructure (PKI) Technical Specifications: Part A* – Technical Concept of Operations; NIST, 1998; http://-csrc.nist.gov/pki/twg/baseline/pkicon20b.pdf

[7] Olaf H. - *Frederik R.: Signaturen, Hashfunktionen und einfache eCash-Verfahren* – http://www.remote.org/frederik/projekts/cash

[8] Szilágyi K. B.: *Az elektronikus aláírásról szóló törvénytervezet egyes alapvető kérdéseinek elméleti vizsgálata* – http://www.jogiforum.hu/-e-alairas/publikaciok/szk_meh_ea_tv.pdf

[9] Buruzs T.: *Tanúsítványkiadó Központok létesítési kérdései* – ICON interjú; http://e-ker.-hu/news.php?id=348&type=printer

[10] *2001. évi XXXV. törvény az elektronikus aláírásról*

[11] *2001. évi LXXIV. törvény a pénzügyeket szabályozó egyes jogszabályok módosításáról*