Fax vagy elektronikusan aláírt dokumentum? (Biztonság és hamisítási lehetőségek)

Dr. Bartók Sándor Péter - Dr. Beinschróth József
Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar

1084. Budapest, Tavaszmező u. 17.

beinschroth.jozsef@kvk.uni-obuda.hu
"BARTóK_Sándor_P" <BSP@BSP.hu>

***Összefoglalás* – Az üzleti világban a fax-ot több évtizede tipikusan hiteles dokumentumként fogadták el annak ellenére, hogy lényeges jogi szabályozás nem vonatkozott rá és hamisítása is egyszerű volt. Később megjelentek a különböző elektronikusan aláírt dokumentumok, amelyek jogi szabályozásokra támaszkodva különböző biztonsági szinteket garantálnak. A cikk bemutatja a technológiák és a szabályozási környezet fejlődését jelenleg is fennálló ellentmondásait továbbá ismertet a gyakorlatban is elfogadható megoldásokat.**

I. Bevezetés

A telefax története nagyon régi időkbe nyúlik vissza. Technikailag egészen a XIX. századra érdemes gondolnunk, mert akkor találta fel Alexander Bain a kémiai telegráfot. Persze a mai faxolás ténylegesen a Xerox 1966-os megoldásával kezdődött és utána a japánok intenzív belépésével terjedt el igazán. A lényeg, hogy egy oldalon 1145 sort és azon belül 1782 pontot tapogat le és küld át a telefonvonal másik végére.

Amerikában 1973 és 1983 között 30ezerről 300 ezerre nőtt a telefaxok száma és 1989-ben már 4millió felett volt. [1]

Magyarországon az 1980-as évek közepén (Matávnál 1985) kezdődött a telefax felhasználása. A telefonhálózaton már lehetett volna korábban is, de nem volt ismert és elterjedt a megoldás.

Az elektronikus aláírás kezdetét már nehezebb megtalálni a történelemben, mert ez - mint informatikai dolog - sok helyen indult és sokan játszottak vele. Ráadásul megnehezíti a meghatározást, hogy a definíciójától is függ a kezdet időpontja. (Szélső esetben ugyanis mondhatjuk, hogy már a távíró is tartalmazott elektronikus aláírást, hiszen odaírták a nevet!)

Mindezek miatt érdemes a fogalmakat meghatároznunk, definiálnunk. A tárgyalt témához a következő releváns fogalmak tartoznak:

Fax, Telefax:
Olyan adatátviteli eljárás, ahol a képi információt az adatkommunikációs vonal - gyakorlatban általában telefonvonal - egyik végén beszkenelik és az átvitt digitális információtartalom alapján a vonal másik végén kiprintelik az adott (általában) A/4-es oldalt.

Elektronikus aláírás:
Olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ.

Elektronikus bélyegző:
Olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét.

Elektronikus dokumentum:
Elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom.

II. A fax-ra vonatkozó jogi környezet

Ahogyan a szakmai kezdeteket is nehéz egyértelműen maghatározni, úgy a változások következtében a jogi környezet is nehezen vizsgálható, bár szakmai környezet meghatározásához nem is kell bírósági szintű bizonyosság.

A továbbiakban időrendben visszafelé haladva bemutatjuk a legjellemzőbb jogszabályhelyeket, amelyek a faxra vonatkoztak.

2004:

RPtké 1960.11.tvr 38.§ (2)

A faxhoz mindössze olyan jogszabályi kiindulópont került elő, mint a RPtké 1960.11.tvr 38.§(2), amely szerint „Ha jogszabály a szerződés érvényességéhez írásbeli alakot rendel, jogszabály eltérő rendelkezése hiányában írásbeli alakban létrejött szerződésnek kell tekinteni a levélváltás, a táviratváltás, valamint a távgépírón és telefax útján történt üzenetváltás, továbbá a külön törvényben meghatározott maradandó eszközzel tett nyilatkozatváltás - így különösen fokozott biztonságú elektronikus aláírással aláírt okirat - útján létrejött megegyezést." Ezt a §-t a 2004: CXIX. törvény 1. §-a állapította meg. Ez természetesen nem a meghatározását tartalmazza, hanem csak az elfogadottságát szabályozza és semmit nem mond a technikai megfelelőségéről.

Érdekesség, hogy a RPtk/Rptké a 38.§(2)-ben 2004 óta tartalmazza, hogy „Ha jogszabály a szerződés érvényességéhez írásbeli alakot rendel, jogszabály eltérő rendelkezése hiányában írásbeli alakban létrejött szerződésnek kell tekinteni a levélváltás, a táviratváltás, valamint a távgépírón és telefax útján történt üzenetváltás, továbbá a külön törvényben meghatározott maradandó eszközzel tett nyilatkozatváltás – így különösen fokozott biztonságú elektronikus aláírással aláírt okirat – útján létrejött megegyezést."

Ket. (2004.CXL.) – a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

28/A.§(1) „A hatóság
a) írásban
aa) postai úton,
ab) írásbelinek minősülő elektronikus úton, ideértve a **telefax**ot,
. . . .
b) szóban
ba) személyesen
bb) hangkapcsolatot biztosító elektronikus úton, ideértve a telefont, vagy
c) írásbelinek nem minősíthető elektronikus úton
tart kapcsolatot az ügyféllel."
78.§(5): „**Telefax** útján nem közölhető a határozat és az önállóan fellebbezhető végzés, kivéve, ha a döntés közlésére jogosult személy vagy szerv ezt előzetesen kérte vagy ehhez hozzájárult."

1991-2000

158/2000. (IX. 13.) Korm. Rendelet - a reprográfiára szolgáló készülékek körének meghatározásáról
Mellékletben „A reprográfiára szolgáló készülékek: . . . 84433120 A nyomtatási, másolási vagy faxtovábbítási funkció"

17/1999. (II. 5.) Korm. Rendelet - a távollevők között kötött szerződésekről
(a Fogyasztóvédelemről szóló 1997. évi CLV. törvény 55. §-ának e) pontja alapján):
1.§(5) „E rendelet alkalmazásában távközlő eszköz: bármely eszköz, amely alkalmas a felek távollétében – szerződés megkötése érdekében – szerződési nyilatkozat megtételére. Ilyen eszköz különösen a címzett vagy a címzés nélküli nyomtatvány, a szabványlevél, a sajtótermékben közzétett hirdetés megrendelőlappal, a katalógus, a telefon, az automata hívókészülék, a rádió, a videotelefon, videotex (mikroszámítógép képernyővel) billentyűzettel vagy érintőképernyővel, az elektronikus levél (e-mail), a távmásoló (telefax) és a televízió."

30/1998. (VI. 24.) BM–HM–NM–PM együttes rendelet - a bajba jutott légijárművek megsegítését ellátó kutató-mentő szolgálatokról
„2.§ k) összeköttetést biztosító berendezések: a gyors és megbízható összeköttetést létesítő és fenntartó analóg, digitális adatcserét lebonyolító eszközök (pl. telefon, telefax, rádiótelefon)"

62/1997. (XI. 7.) BM rendelet - a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvénynek a belügyminiszter ágazati irányítása alá tartozó szerveknél történő végrehajtásáról
3. számú melléklet „Ügyviteli munkakörök: . . . .Telex-, telefaxkezelő"

14/1991. (XI. 26.) IM rendelet - a közjegyzői díjszabásról
20.§ „A közjegyző készkiadás címén igényt tarthat az ügy ellátásával kapcsolatban ténylegesen felmerült és igazolt postai (levél, csomag, telefon, távirat, telex, telefax) díjak és egyéb költségek megtérítésére."

1991. évi IL. törvény - a csődeljárásról és a felszámolási eljárásról
69.§(1): " A kérelemben meg kell jelölni az adós vezetőjének a Pp. 96. § (3) bekezdése szerinti rövid úton történő idézéséhez szükséges adatokat is (az adós vezetőjének elektronikus levélcíme, telefonszáma, telefax száma)"

1991 előtt

15/1990. (V. 14.) BM rendelet 2.§- a rendezvények rendjének biztosításával kapcsolatos rendőri feladatokról
2.§(5): „A távirati úton, illetve levélben, telefaxon, telexen érkezett bejelentést írásbeli bejelentésnek kell tekinteni."

Lényeges kiemelni, hogy 1985-ben már megindult a telefax („távmásoló") szolgáltatás a Matávnál, gyakorlatilag a telex kiváltására! [2]
Még korábbra is visszamenve megállapítható, hogy már a korábbi távíró is tartalmazott elektronikus aláírást, hiszen a távíró esetén is odaírták a nevet! (Ez viszont nem témánk jelenleg.)

Fontos kiemelni, hogy a fenti jogszabályhelyek egyike sem a telefax működésére vonatkozik, hanem mindegyik annak felhasználására és hatására. A működésre eleinte volt valami (nem törvényi, hanem feltehetően az akkori Matávtól származó) előírás, hogy a telefonkönyvben fel kellett tüntetni, ha egy szám faxon csörgött ki (ugyanilyen előírás létezett üzenetrögzítőre is), de ez a szabály már régen feledésbe merült.

Szintén a kezdetekben volt egy másik kvázi kötelező előírás, miszerint a forgalomban eladott faxokba a "feladó" telefonszámát csak szervizes rögzíthette be, és nem lehetett a küldő telefonszámát tetszőlegesen átírogatni. Ennélfogva volt valamiféle hitelessége, legalábbis a küldő helyére/személyére. Ezzel valamivel több volt a hitelessége, mint ha csak egy írógéppel odaírta volna valaki a nevét. Szerintünk szinte nincs és épphogy csak valamivel volt több bizonyító ereje magára a dokumentumra nézve, mint egy "egyszerű" fénymásolat.

Mindezek ellenére a faxot az üzleti élet elfogadta és komoly szerződésteljesítéseket is elkezdtek egy-egy magkapott fax hatására.

III. Az eAláírásra vonatkozó jogi környezet

A faxnál tapasztaltakkal gyakorlatilag éppen ellentétesek az elektronikus aláírásnál tapasztalhatóak. Míg a fax tényleges használata után évekkel találhatunk jogszabályi hivatkozást a faxra, az eAláírásnál fordított a helyzet.

Ennek egyik alapvető oka, hogy a számítógépben zajló titokzatos dolgokkal kapcsolatban mindig nagy a bizalmatlanság, míg a fax esetén „csak" annyi történt, hogy a már megszokott fénymásolás két helyre osztódott szét, vagyis egyik helyen beolvasták, másik helyen kinyomtatták.

Másik alapvető oka, hogy az eAláírás felhasználásához - legalábbis a PKI rendszerű esetben - feltétlenül szükség van megbízható harmadik félre, és így csak jogilag is jól szabályozott környezetben tud a társadalom által elfogadhatóan működni.

Érdekesség, hogy előfordul, hogy egy szinten van említve a fax és eAláírás pl. a Kbt. (2015. évi CXLIII. törvény) 79.§(2)ben: „Az ajánlatkérő az ajánlatok és a részvételi jelentkezések elbírálásának befejezésekor az (1) bekezdés szerinti tájékoztatást az írásbeli összegezésnek minden ajánlattevő, a részvételi szakasz lezárása esetén részvételre jelentkező részére egyidejűleg, telefaxon vagy elektronikus úton történő megküldésével teljesíti."

A továbbiakban időrendben haladva bemutatjuk a legjellemzőbb jogszabályokat és szetenderdeket, amelyek az eAláírás szempontjából leginkább relevánsnak tekinthetők. Miután az eAláírás logikai kiindulópontja a 2001.XXXV. tv az elektronikus aláírásról törvény (Eat) volt, estében nem követjük az időrendiséget, ezt elsőként kiemeljük

<u>2001.XXXV. tv az elektronikus aláírásról</u>

Ez a törvény pontosan meghatározta az eAláírás feltételeit, jogi környezetét és felhasználhatóságát is. Szabályozva vannak benne többek között a következők:

- az aláírások jellemzői és megvalósításukra vonatkozó jellemzők és feltételek;
- a megbízható 3.személyre vonatkozó előírások
  (Ők igazolják a kulcspárok összetartozását és az aláíró személyét);
- az ellenőrzések.

Fontos kiemelendő a 3.§(1) bekezdés, miszerint „Elektronikus aláírás, illetve dokumentum elfogadását – beleértve a bizonyítási eszközként történő alkalmazást – megtagadni, jognyilatkozat tételére, illetve joghatás kiváltására való alkalmasságát kétségbe vonni – a (2) bekezdés szerinti korlátozással – nem lehet kizárólag amiatt, hogy az aláírás, illetve dokumentum elektronikus formában létezik."

<u>2001 eMail RFC</u>

A 2001.áprilisi az aktuális állapota az RFC 2822 –nek, ami az **e-mail** üzenetek formátumát definiálja. (Request for Comment)

<u>2/2002. (IV. 26.) MeHVM irányelv - a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről</u>

Hatályos: 2002.04.26 - 2012.01.01

Szolgáltatók rendszereitől kezdve, a kulcskezelési követelményein, leállásukon, hitelesítés, időbélyeg, illetve aláírás-létrehozó eszköz szolgáltatókra vonatkozó különleges követelményeken és a minősített tanúsítványokon át a kriptográfia algoritmusokig részletesen szabályoz már.

<u>2/2003. (MK 111.) PSZÁF irányelv - a magánnyugdíjpénztári tagdíjbevallások, önellenőrzések és a tagdíj, pótlék és bírság befizetések feldolgozására és nyilvántartására, a tagdíjbefizetések bevallás alapján történő elszámolására vonatkozó magánnyugdíjpénztári eljárások kialakításáról</u>

3.2: „A számítógépes hálózaton, elektronikus dokumentum formájában előállított adatszolgáltatások teljesítésével kapcsolatban az elektronikus aláírásról szóló 2001. évi XXXV. törvény rendelkezései az irányadók [Tbj. 51. § (5) bekezdés]."
„2004. január 1-jétől a tagdíjbevallás – a vonatkozó jogszabályi és technikai feltételek megléte esetén – minősített (fokozott biztonságú) elektronikus aláírással és időbélyegzővel ellátott elektronikus dokumentumban, számítógépes hálózat útján is teljesíthető."

2004 Ket - 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

28/A.§(1) „A hatóság
a) írásban
aa) postai úton,
ab) **írásbelinek minősülő elektronikus úton**, ideértve a telefaxot,
. . . .
b) szóban
ba) személyesen
bb) hangkapcsolatot biztosító elektronikus úton, ideértve a telefont, vagy
c) írásbelinek nem minősíthető elektronikus úton
tart kapcsolatot az ügyféllel."
A törvényben szemmel látható cél a technológiasemlegesség biztosítása. Figyelemre méltó az írásbelinek nem minősíthető elektronikus út, miközben van írásbeli elektronikus út és hangkapcsolatot biztosító elektronikus út is.

1/2004. (MK 108.) MeHVM tájékoztató az országosan kiemelt termékekre vonatkozó állami normatívákról

„Elektronikus közigazgatáshoz kapcsolódó szolgáltatások, eszközök	K-00-00-000
- Elektronikus aláírás létrehozó hardver és szoftver eszközök	K-01-00-000
- Minősített elektronikus aláírást létrehozó hardver és szoftver eszközök	K-01-01-000
- Biztonságos aláírás létrehozó eszköz (BALE)	K-01-01-100
- Intelligenskártya-olvasó	K-01-01-200
- Minősített elektronikus aláírást létrehozó és ellenőrző alkalmazás	K-01-01-300
- Elektronikus aláírás használatához kapcsolódó szolgáltatások	K-02-00-000
- Hitelesítés-szolgáltatás	K-02-01-000
- Minősített tanúsítványokhoz kapcsolódó hitelesítés szolgáltatás	K-02-01-100
- Titkosító tanúsítványokhoz kapcsolódó hitelesítés szolgáltatás	K-02-01-200
- Hitelesítő (authentikációs) tanúsítványokhoz kapcsolódó hitelesítés-szolgáltatás	K-02-01-300
- Időbélyegzés-szolgáltatás	K-02-02-000"

1952. évi III. törvény - a polgári perrendtartásról 2004. CXXVII. tv 20.§(2) iktatta be a következőket:

195.§(3) „Az eredeti papír alapú vagy elektronikus közokiratéval azonos bizonyító ereje van annak a közokiratról készített elektronikus okiratnak, amelyet a közokirat kiállítására jogosult ügykörén belül, a megszabott alakban készített el, és amelyen minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást vagy bélyegzőt, valamint – ha jogszabály így rendelkezik – időbélyegzőt helyezett el."

2005. MK 51. szám IM tájékoztató- az új társasági törvény és cégtörvény téziseinek részletes indokairól
7.pont: „A minősített elektronikus aláírásával tett ellenjegyzéssel az ügyvéd azt bizonyítja, hogy a kiállító minősített elektronikus aláírásával aláírt elektronikus okirat tartalma az ügyvéd által készített elektronikus okiratéval megegyezik."

IV. Az eAláírásra vonatkozó első magyar szabályozás előzményei és mai szabályozása

Az elektronikus aláírás már az eMail-lel együtt kezdődött, hiszen az eMail aljára oda szokták írni a civilizáltabbak a saját nevet is. Ennek persze semmilyen komolysága, vagy bizonyító ereje sincs még. Mikor jelent meg a jogban és milyen irányból?

1994 Vbtv -LXXI törvény a választottbíráskodásról

Volt már jogi szabályozás a Eat. Előtt is, amelyben az írásbeliséget már általánosabban fogalmazzák meg és nincs leírva se a telefax, se az eAláírásos eDokumentum. Ilyen pl. a Vbtv.(1994.LXXI) – a választottbíráskodásról: 5.§(3) „A választottbírósági szerződést írásba kell foglalni. Írásban létrejött szerződésnek kell tekinteni azt a megállapodást is, amely a felek közötti levélváltás, táviratváltás, géptávírón vagy más, a felek üzenetét tartósan rögzítő eszközön történt üzenetváltás útján jött létre."

1999 EU irányelv

Az európai közösség is már az Eat előtt megpróbálta azonos irányba terelni a tagállamokat az eAláírás területén, és ennek következménye az EU-irányelv 1999/93/EK - az elektronikus azonosításról és bizalmi szolgáltatásról
„Ennek az irányelvnek a célja az elektronikus aláírások alkalmazásának megkönnyítése, továbbá az elektronikus

aláírások jogi elismeréséhez való hozzájárulás. Ez az irányelv a belső piac megfelelő működése érdekében létrehozza az elektronikus aláírásra és egyes hitelesítésszolgáltatásokra vonatkozó jogi keretet.
2.cikk(1): „'elektronikus aláírás': olyan elektronikus adat, amely más elektronikus adathoz van csatolva, illetve logikailag hozzárendelve, és amely hitelesítésre szolgál; "Ennek az irányelvnek betartásával hozták meg a tagállamok a saját szabályozásukat az eAláírásra vonatkozóan. Ezen szabályok betartásával azonos logikával építették ki a rendszereiket, de mivel nem voltak elegendően azonosak a tagállamokban használt eAláírások, nem lehetett az egyik országban létrehozott aláírást a másikban felhasználni, úgy hogy annak jogi hatása is legyen.

Az új Ptk (2013.V.tv)

2014.03.15-től már teljesen technológia semleges és se a telefax, se az elektronikus aláírás szavak nem szerepelnek benne.

„6:7. § [Írásbeli alakhoz kötött jognyilatkozat]

(2) Ha e törvény eltérően nem rendelkezik, a jognyilatkozat akkor minősül írásba foglaltnak, ha jognyilatkozatát a nyilatkozó fél aláírta.

(3) Írásba foglaltnak kell tekinteni a jognyilatkozatot akkor is, ha annak közlésére a jognyilatkozatban foglalt tartalom változatlan visszaidézésére, a nyilatkozattevő személyének és a nyilatkozat megtétele időpontjának azonosítására alkalmas formában kerül sor."

„6:565. § [Az értékpapír fogalma]

(1) Ha valaki írásban, nem elektronikus formában vagy elektronikus formában rögzített és értékpapírszámlán nyilvántartott (dematerializált) módon egyoldalúan kötelezettséget vállal . . . . az okirat, illetve a nyilatkozatot rögzítő elektronikus jelsorozat értékpapírnak minősül."

eIDAS – Az Europai Parlament és a Tanácsa 910/2014/EU Rendelete - az elektronikus azonosításról és bizalmi szolgáltatásról

Earlier there were different laws in European countries. There was a law "Eat" in Hungary too, which was very strict and serious. (Act XXXV of 2001 - on the electronic signature) It was very useful inside Hungary, but nobody can use it abroad. The problem was the personal appearance in front of the eSzigno provider which was checked strictly by the authority. Of course, there were similar laws in other countries, too. The technical specification and the regulation are different and as a consequence of it, they couldn't work together. 'Work together' means that one of them can create a signature, and other one can check it. It was true in spite of the fact that there was a directive (1999/93/EK), which tried to move in the same direction the legislation of countries. This could set up only some main idea and the realizations were different. (For example, because of the past history in the countries.) There was a contra fact that the EU is a common economical area and the firms and people have to work together! To help this common work the European Parliament and the Commission created a new regulation, the eIDAS.

3.cikk(10): „'elektronikus aláírás': olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ; "

V. Technológia

A különböző technikákkal megvalósított távmásolás idestova 200 éve létezik, de a gyakorlatban széleskörűen csak az 1980-as években terjedt el. Széles körű használatának elsősorban gyorsasága és hivatalos dokumentumként történő elfogadottsága volt az oka.

A telefax (fax, faximile) szolgáltatás arra épül, hogy beszédcélú távközlő hálózaton felépített kapcsolaton nem beszédet, hanem kódolt adatot továbbítanak két terminál (fax készülék) között. Az adatátvitel egyirányú, a szolgáltatáshoz szükséges kiegészítő funkciókat a magában a fax készülékben valósítják meg. A működés során az adó készülék a továbbításra kerülő dokumentumot letapogatja, fotografikus eljárással kódolja, és a felépített kapcsolaton keresztül a megfelelő protokoll szerint továbbítja azokat a vevő készülékhez. A vevő készülék a kapott jeleket dekódolja és előállítja az eredeti dokumentum hasonmását (faximile). A letapogatás soronként történik, így tetszőleges ábra, akár szabadkézi rajz és természetesen aláírás is továbbítható. [3]

A telefaxot először a kapcsolt telefonhálózaton alkalmazták, ahol oly mértékben sikeressé vált, hogy az újabb generációs hálózatokban is szükségesnek látszott valósítani, így került be ez az az ISDN és GSM telefax szolgáltatásokba. A rendszer széleskörű elterjedtségének fontos feltétele volt, hogy használatba vételekor nem volt szükség semmiféle hálózatfejlesztésre, csak a fax készüléket kellett a telefonvonalra csatlakoztatni. A fax készülékek együttműködését a szabványosított eljárások működés teszik lehetővé. A kapcsolt telefonhálózatban alkalmazott 3-as csoport˙, G3 (Group 3) analóg berendezések a kódokat hangfrekvenciás analóg jelekké alakítják. Az ISDN-ben szabványosított 4-es csoport˙, G4 (Group 4) digitális telefax berendezések a jelet digitális formában, jóval nagyobb adatátviteli sebességgel viszik át, ha a kapcsolat két G4-es telefax között épül fel. A G4-es

berendezések tipikusan rendelkeznek G3-as üzemmóddal is, így a működés akkor is biztosított, ha a vonal másik végén G3-as berendezés van. A GSM-ben szabványosított telefax távszolgáltatás a G3 üzemmódot teszi lehetővé. A mobil hálózatban a telefax külön távszolgáltatásként jelenik meg, mivel a telefon távszolgáltatás nem alkalmas fax átvitelre az alkalmazott beszédkódolás miatt. A telefax továbbítás az alábbi szakaszokból áll:

- Hívásfelépítés: a telefonhívás felépítésével azonos módon, a hívott berendezés hívószámának beadásával kezdeményezhető.
- Modem átviteli mód egyeztetés: a hívott jelentkezése után a két berendezés a szabványos protokollal megállapodik az alkalmazott üzemmódról, valamint a berendezések és a hálózat átviteli képességeinek megfelelő átviteli sebességről.
- Adatátvitel: A letapogatott és digitalizált adatok átvitele a megállapodás szerint. Ha az átvitel minősége a hívás során változik, a berendezések az átviteli sebességet változtatni tudják.
- Nyugta: Az átvitel sikerességéről, vagy a sikertelenségről a hívott berendezés visszajelzést küld, amit a hívó oldali készülék kijelez vagy kinyomtat.
- A fax üzenet hitelessége elvileg azzal biztosított, hogy a küldés során továbbításra kerül a hívó telefonszáma. Ez azonban meglehetősen primitív megoldás: a küldött telefonszám a fax végberendezésben beállított azonosító, ami könnyen átírható. [4]

Az üzleti-hivatali szférában a fax-nak több alternatívája is létezik. A hagyományos postai levelezésen túl alternatíva lehet az email, és az elektronikusan aláírt dokumentum. Előbbi hitelesített dokumentumként nem elfogadott, utóbbinak egy változata az ún e-signó.

Az e-Szignó (elektronikus aláírás) egy tanúsított , professzionális elektronikus aláírás-létrehozó és - ellenőrző alkalmazás, amely Magyarországon de facto szabvánnyá vált. A megoldás lényege, hogy az elektronikus dokumentumot az ügyfél pl. egy kézírás rögzítésre alkalmas hordozható eszközön (tablet-PC-n, mobilon, PDA-n) írja alá és az aláírás elvileg elválaszthatatlanul összekapcsolódik az elektronikus dokumentummal. Így elérhető, hogy közvetlenül elektronikus dokumentum (szerződés, munkalap, jegyzőkönyv stb.) készüljön úgy, hogy papír alapú, ténylegesen kézzel aláírt anyag nem is keletkezik. Az aláírt dokumentum késedelem nélkül, hitelesített és titkosított módon továbbítódik a meghatározott informatikai rendszerbe ill. az érintettekhez.

Kézi aláírás helyett más, aláírás-létrehozó adatok is szerepelhetnek, utóbbiak lényegesen nagyobb biztonságot nyújtanak. Ez esetben az elektronikus dokumentumokat elektronikus aláírással látjuk el. Ez azt jelenti, hogy a dokumentumokat úgy kódoljuk, hogy azok hitelességét annak szerkezete ill. kódolása biztosítja. A kódolás során tipikusan egy kulcsot is felhasználnak, amely a gyakorlatban egy nagy számot jelent.

A gyakorlatban az aláírás tipikusan az ún. nyilvános kulcsú kriptográfiára épül. Ez esetben minden szereplő egy kulcspárral rendelkezik, amelynek tagjai között meglehetősen bonyolult matematikai összefüggés van. A kulcspár tagjai közül az egyik az ún. privát kulcs, amelyet az illető szereplő titokban kell, hogy tartson, a másik kulcs pedig az ún. publikus kulcs, amely tetszőleges körben terjeszthető. A kulcspár tagjai közötti matematikai összefüggés olyan, hogy egy publikus kulcsból annak privát párja gyakorlatilag nem számítható. Az alkalmazott kódoló/dekódoló algoritmusnak olyannak kell lennie, hogy a publikus kulccsal kódolt üzenet a privát kulccsal dekódolható legyen és ennek fordítva is igaznak kell lennie. [5]

Az aláírás elvégzésének folyamata és ellenőrzése a következő:

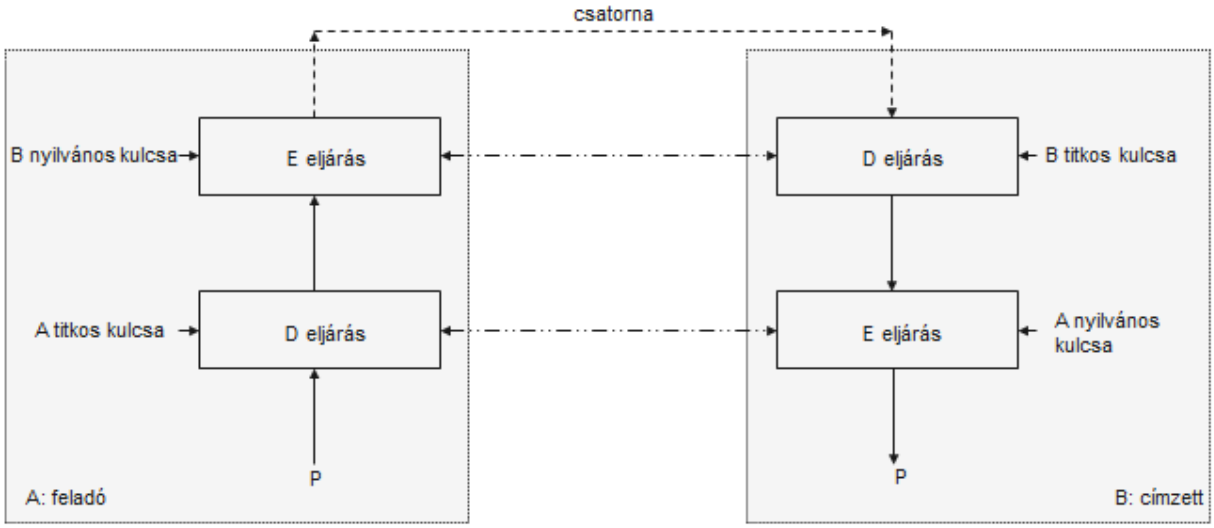
A küldő oldalon:

1. Az üzenet kódolása a címzett nyilvános kulcsával.
2. A kódolt üzenet kódolása a külső privát kulcsával

A címzett oldalon

1. A kapott üzenet dekódolása a küldő publikus kulcsával
2. A dekódolt üzenet újabb dekódolása a küldő publikus kulcsával

A folyamat a következő ábrán tekinthető át:

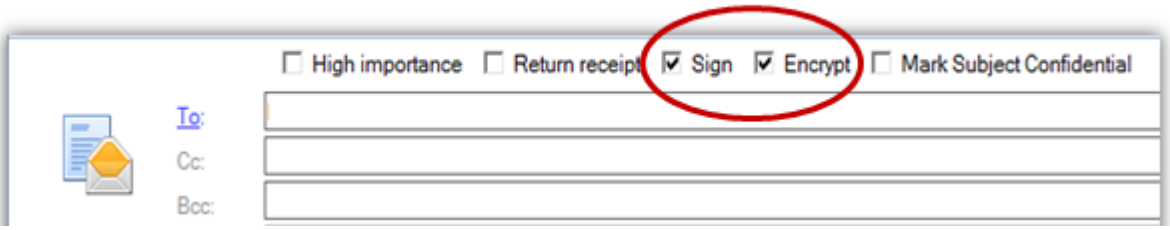


1. ábra: a digitális aláírás folyamata

A gyakorlatban nem feltétlenül szükséges a teljes üzenetet aláírni, az aláírást elegendő a belőle képzett ún. hash-re megtenni. Ezt a megoldást elsősorban a korlátozott erőforrások indokolják és akkor alkalmazható, ha valóban csak a hitelesség biztosítása az elvárás és nincs szükség titkosításra. [6]

A digitális aláírás művelete az alkalmazásokba beépül, a felhasználó számára teljesen transzparens. A felhasználónak maximum annyi tennivalója van, hogy meghatározza a, hogy az adott dokumentumot alá kívánja-e írni vagy nem. Erre mutat példát következő ábra, amely egy levelező alkalmazásból származik.

A gyakorlatban az aláírás három szereplőt követel meg. A küldőn és a címzetten kívül szökség van egy olyan szereplőre is, aki tanúsítja a szeplők hitelességét. A PKI (Public Key Infrastructure), olyan alkalmazás környezetet(infrastruktúrát) kínál, ami lehetővé teszi a törvények által elfogadott kétkulcsú harmadik személyes hitelesítési és adatbiztosítási eljárások használatát a számítógépes alkalmazások számára.



VI. Biztonsági szintek és hamisíthatóság

Faxok hamisíthatósága

A kezdetekben, amikor még csak olyan telefax készülékeket lehetett kapni, amelyekbe a küldő adatait csak a gyártó - esetleg szakszervize - volt képes beírni, a küldés helye nagy valószínűséggel volt beazonosítható. Ez nyilvánvaló, mert a készülékek egy-egy vonalas telefonvonalra voltak rákötve, amelyek helyhez kötöttek voltak.

Ezt ma már nehéz elképzelni, amikor a telefonok többsége már teljesen független a földrajzi helytől, ráadásul mindenkinek annyi példánya lehet, ahányat csak meg tud fizetni. Abban az időben viszont még a vonalas telefonok lehetőségére is éveket, évtizedeket kellett várni, és ezzel összefüggésben nagyon kis számú telefonvonal volt és még kevesebb telefaxos telefonszám

Mindezek következtében akár ellenőrizni is lehetett időnként a fax készülékeket.

Természetesen, a készülékek is mozgathatóak voltak, így a helymeghatározás sem volt teljes biztonságú, de a gyakorlati élethez szükséges biztonságot megadta.

Más kérdés az átvitt tartalom hitelessége, és hamisíthatósága.

Azt már abban az időben is tudtuk jól, hogy egy fénymásolóval össze lehet másolni össze-nem-tartozó dokumentumrészeket. Igaz, figyelni kellett rá, hogy az összeragasztott, vagy csak egyszerűen egymásra rakott lapok széle ne látszódjon a másolatokon, ha nagyon jó minőségű volt a másológép. Az, hogy a fénymásolás helyileg ketté lett bontva és egyik helyen történt a beolvasás, míg a nyomtatás a másikon, ezen a hamisíthatóságon semmit nem változtatott.

Elméletileg lehetett volna - a ma már jól ismert - man-in-the-middle módszerrel is megváltoztatni az átviendő tartalmat, de akkor még ez a mód nem is volt benne a tudatokban és sokkal egyszerűbb volt a hamisítás egyéb formája, pl. a fent említett hamis összemásolás.

A mai körülmények annyiban térnek el a kezdetektől, amikor legalább a hely volt viszonylag megbízhatóan meghatározható, hogy ma már minden fax-készülékben a tulajdonos állítja be a saját adatai, így a küldő fax számát is.

Ennek következtében a fax-nak ma már már semmilyen jellemzője, vagy tartalma nincs megvédve a hamisíthatóság ellen.

Egyszerű eAláírások hamisíthatósága

A faxhoz legközelebbi szinten az egyszerű elektronikus aláírással ellátott dokumentum van.

Ennek az aláírásnak a definíciója szerint a legegyszerűbb eMail is megfelel, ha valaki az elküldendő megírt szöveg alá odaírja a nevét. Amellett, hogy ennek gyakorlatilag semmi joghatása nincs, igen könnyen át is írható, vagyis hamisítható. Természetesen lehet vizsgálni mindkét oldalon a (levelező) rendszereket, és egyezés esetén már nagy a valószínűsége, hogy az eMail úgy volt elküldve, ahogyan azt a vizsgálatra megkaptuk. Fontos persze, hogy ebben az esetben nem a személyt tudjuk megállapítani, hanem legfeljebb csak a gépet, ahonnan küldték. Ez nyilvánvalóan abból következik, hogy bárki beírhatta a levélbe bárki másnak a nevét.

Összegezve: az egyszerű elektronikus aláírással készült pl. eMail könnyen hamisítható.

PKI-s digitális elektronikus aláírások hamisíthatósága

A PKI-s aláírás folyamatát kell megnéznünk, hogy lássuk a hamisíthatóság lehetséges szintjeit.

1. Az aláírni kívánt elektronikusan aláírt dokumentumot először megnézzük, majd elkezdjük az aláírást. Ennek során az aláírást végző szoftverrel készítünk egy hash-t az aláírandó dokumentumról, majd ezt a hash-t az aláírást készítő eszköz (pl. MALE) az aláírókulcs segítségével legenerálja az aláírást, amit utána a szoftver hozzácsatol a dokumentumhoz.
2. Az aláírt dokumentumot kezeljük, vagyis tároljuk, átadjuk, elküldjük a másik félnek, archiváljuk vagy kezdhetünk vele bármit, csak nem szabad benne egyetlen bitet sem megváltoztatni.
3. A hozzánk került aláírt dokumentumot elolvasáskor ellenőrizzük, hogy azonos állapotban van-e, mint aláíráskor, illetve, hogy az aláíró beazonosítása rendben van-e.

Mivel az aláíráshoz használt kriptográfiai eljárás a matematika és technika mai állapotában feltörhetetlen, az aláírás nem hamisítható a 2. fázisban, vagyis az aláírt dokumentum kezelése során. Ha pedig akár egyetlen bitje is megváltozott, akkor az ellenőrzéskor az kiderül.

A 3.fázisban, vagyis az ellenőrzéskor egy szoftver eszköz segítségével megnézzük, hogy az aláírás sértetlen-e, és hogy az aláírás az aláírás pillanatában érvényes volt-e?

A sértetlenséget úgy ellenőrizzük, hogy a dokumentumról ismét elkészítünk egy hash-t és ellenőrizzük, hogy az aláírást a publikus kulccsal konvertálva, ugyanazt a hash-t kapjuk-e meg?

Az eljárás matematikai megalapozottsága miatt biztos eredményt ad. Az aláírás érvényességét pedig a hitelesítés szolgáltatótól történő lekérdezéssel lehet ellenőrizni.

Ennek a vizsgálatnak az eredménye teljes mértékben megbízható, de csak abban az esetben, ha az ellenőrző szoftver valóban azt csinálja, amit kell. Történt viszont már tavaly a valós életben, normál felhasználáskor, hogy az ellenőrző program nem jól végezte dolgát, és hitelesnek vélte az aláírt dokumentumot, pedig az aláírás után volt hozzáfűzve változtatás. A rendszer annyit mondott, hogy érvényes az aláírás (ami csak az eredeti dokumentumra vonatkozott), miközben a tartalma megmutatásakor már a változással együtt tette ember számára láthatóvá a dokumentumot. Ez egy .PDF dokumentum esetén történt, mert az az aláírás után - azon kívül - még tud hozzáfűzni változtatásokat. Az ellenőrző szoftvernek jeleznie kellett volna, hogy nem ugyanazt teszi olvashatóvá, mint amire az érvényes aláírás vonatkozik.

Ez tehát azt jelenti, hogy pl. megjelenítési hiba esetén tapasztalhatunk „hamisítást”.

Az 1. fázisban van a legkomolyabb lehetőség a hibára. Itt feltétlenül érintetlennek kell lennie a számítógépnek, amelyen az elektronikus aláírt elvégezzük. Ha egy (nem etikus) hacker esetleg átvette a felügyeletet a számítógépen, lehetséges, hogy más dokumentumot fog aláírni az aláíró, mint amit a számítógép emberileg láthatóvá tesz számára.

Az 1. és 3. fázisban lehetséges hibás működésre igaz az a kijelentés, hogy nem az eljárás okozza a hamisítás lehetőségét, hanem a használt számítógép-rendszer, vagy eszköz.

Ez viszont nem rosszabb állapot, mint a papíron aláírt dokumentum esetén. Gondoljunk csak a következő példára: Vannak olyan tinták, amelyek a megírás után valamennyivel elhalványodnak, majd teljesen eltűnnek.

Fontos még megjegyezni a PKI-s rendbe vetett bizalom fenntartása érdekében, hogy az említett .PDF-et kezelő szoftver implementációs hibát már kijavították, és a visszaellenőrzéskor egyetlen hibakihasználó esetet sem találtak, pedig milliós nagyságrendű volt az ellenőrzendő dokumentumok mennyisége!

Biometrikus elektronikus aláírások

A biometrikus elektronikus aláírás 1. szintje, amikor az aláírást beszkennelve tesszük rá az aláírandó dokumentumra. Könnyen belátható, hogy ennek hamisíthatósága semmivel nem tér el a fénymásoló, vagy telefax hamisíthatóságának szintjétől, vagyis nem ajánlott elfogadni komoly ügyekben, mivel nincs valós joghatása.

A biometrikus aláírások 2. szintje, amikor - ahogyan azt pl. az MPL, DHL is teszik - saját maguk által működtetett, és rendszerbe bekötött aláírópadokon íratják alá a szükséges dokumentumokat, miközben a rendszerelemek nem zártak hitelesen. Ennél a megoldásnál a megmutatott - általában igen kisméretű - dokumentum elolvasása után azt egy pálcával kell aláírni az aláírópadon. Ezen aláírást, vagyis annak dinamikus adatsorát kapcsolja hozzá a dokumentumhoz az aláírópad. Ezt az aláírt dokumentumot utána feltöltik egy központi rendszerbe.

Ennek a megoldásnak problémája - azon kívül, hogy az egyik fél saját felügyelete alatt működik -, nincs biztosíték arra, hogy az aláírás dinamikus adatsorát nem csatolják hozzá más dokumentumhoz is, akár rögtön, akár eltárolva az adatsort a későbbiekben.

Természetesen a PKI-nál már tárgyalt hackelés lehetősége is fennáll ennél a rendszernél is.

Lényeges volt az egyik ezt a módszert alkalmazó csomagszállító cégnél a rendszer bevezethetőségének megvitatásakor, hogy csak limitált értékű csomagokat lehet feladni, mégpedig maximum 2MFt-osat.

A biometrikus aláírások 2½. szintje, amikor - ahogyan egyes bankok szeretnék elfogadtatni - először aláíratják az ügyféllel az aláírópadon, majd 'rögtön' utána rátesznek egy PKI-s aláírást is. Természetesen ez sem különbözik lényegesen a 2.szintű megoldástól, hiszen semmi nem bizonyítja, hogy a biometrikus és PKI-s aláírások között nem történik semmi, ráadásul a már begyűjtött biometrikus aláírást később is bármikor hozzá lehet csatolni egy másik dokumentumhoz. Az egyetlen nehézséget csak a CAdES-T/XADES-T aláírásnál szereplő időbélyeg jelenthet, az időzítés eltérése miatt.

A biometrikus aláírások 3. szintje az a megoldás, amikor kontrolokkal körbevesszük a 2.szintű megoldást. (Ez egyébként nem is ördögtől való ötlet, hiszen önmagában a PKI-s megodások sem önmagukban a technikát alkalmazzák, hanem ott is igen komoly kontolok vannak beépítve az eljárásokba.) Ennél a megoldásnál olyan eszközt és háttér rendszert kell alkalmazni, amelybizonyos feltételek teljesítését ellenőrző tanúsítvánnyal rendelkeznek. A legfontosabb, hogy az aláírópadról levett biometrikus aláírás dinamikus adatait csak az éppen kijelzett dokumentumhoz lehessen hozzácsatolni és csak az aláírópadról közvetlenül levett aláírást tudja a dokumentumhoz hozzácsatolni!

Ennél a megoldásnál hasonló problémák (biztonsági rések) elvileg lehetnek, mint a PKI-s megoldásnál, viszont itt ellenőrzöttek az eszközök. A meghackelés persze itt is szóba jöhet, ha pl. vírusok elérhetik, de ezeket az eszközöket ellenőrzik, míg a személyek PC-it, laptopjait nem ellenőrzik és az internetes barangolások miatt nagy veszélynek vannak kitéve.Fontos egyébként azt is tudni, hogy nem csak két ember aláírása nem tud azonos lenni, de egy személy sem tud kétszer pontosan ugyanolyan aláírást létrehozni.

Fontos lehet itt azt is hangsúlyozni, hogy a nem biztonságos megoldások is terjednek, hiszen akárcsak a korábbi faxnál, az üzleti kockázatszámítások alapján itt is bevállalják a piaci szereplők a kockázatokat, pl. a 2MFt-os értékhatárig.

VII. Biztonság - Hamisíthatóság - Hasznosság

Az előző fejezetekből jól látható, hogy a világban felhasznált technológiák/technikák nem csak a műszakiak, a mérnökök gondolkodásmódja szerint van felhasználva.

Alapvetően három szakma befolyásolja a technikák/technológiák elterjedését.

Az első - természetesen ☺ - a technikaiak, mérnökök, akik meg tudják alkotni és műszakilag értékelni tudják az lehetőségeket, a megvalósult megoldásokat.

Második a gazdasági szakemberek - ideértve a menedzsereket is -, akik kihasználják az új technikákban rejlő gazdasági előnyöket, pl. az ügyintézések gyorsítási lehetőségeként.

Harmadik csapat a jogászoké, akik a két előző szakma által összehozott konfliktusokat próbálják meg rendezni. [Vagy még jobban összekuszálni. ☺]

A mérnökök kitalálták a faxot, ami először teljesen beazonosítható volt és bár az ellenmérnökök kitalálták a beazonosíthatóság hamisítását, a gazdasági embereknek a postánál nagyságrendekkel gyorsabb intézkedéssekkel hatalmas hasznot realizáltak a fax használatával.

A normál eMail-eket is megalkották mérnökök és világrendszer lett belőle, mégpedig a gazdasági életben is igen aktívan felhasználva. Igaz ugyan, hogy még csak mérnöknek sem kell lenni ahhoz, hogy hamisítani lehessen egy

eMail-t, mégis széles körben használják, komoly gazdasági következmények esetén is. Természetesen ennek a megoldása még gyorsabb és kényelmesebb, mint a fax, így még nagyobb hasznot lehet vele realizálni.

A mérnökök hivatása az, hogy a technikai problémákat megoldják, így az eMail biztonságára is kialakítottak megoldásokat. A ma legelterjedtebben használt biztonságos megoldás a PKI-s aláírás. Ez már nem olcsóbb és gyorsabb, mint a sima eMail, ezért lassabban terjed.
Sőt, van a normál eMail, vagy egyszerű elektronikus dokumentum és PKI-s aláírás közötti szint is, a biometrikus aláírás. Ez már sokkal gyorsabban terjed, mert mint a PKI, mert ez is gyors, és mindenki számára érthető, hiszen jobban „érezhető" az átlag ember által is. Igaz, kevésbé biztonságos és jobban hamisítható, mint a PKI, de szintén sok nyereséget lehet vele realziálni.

Ezek után nézzük, hogy hol is jön elő a harmadik szakma, a jogászoké?
Mivel minden megoldásnál lehet hamisítani - még a PKI-nál is, de az egy külön téma lesz -, természetesen vannak olyanok akik ezt meg is teszik. Itt lép be a társadalmi szabályozás, a jog. A fax idejében még csak utólag próbálta meg valamilyen szinten szabályozni a használatát, az elektronikus aláírásnál már befolyásoló módon „előre" próbál meg szabályozni.

Összefoglalóként érdemes megjegyezni, hogy a biztonság mindig fejlődik, és a hamisíthatóság egyre nehezebb, de tökéletes biztonság nem létezik, főleg, ha a leggyengébb láncszemet, az embert nem lehet kivenni a rendszerből.

VIII. Hivatkozások

[1] http://www.deol.hu/main.php?c=3592

[2] https://hu.wikipedia.org/wiki/A_miskolci_távközlés_története

[3] Balogh – Berkes – Kovács : A számítógépes távközlés telematikai szolgálatai (teletex, faximile, videotex), LSI Alkalmazástechnikai Tanacsadó szolgálat, 1988.

[4] Berkes – Gonda – Szabó – Verebélyi: Adatátvitel számítógép felhasználóknak, Ipari Informatikai központ, 1989.

[5] Dr. Berta István Zsolt: NAGY E-SZIGNÓ KÖNYV, Amit az elektronikus aláírásról tudni akartál, csak féltél megkérdezni, 2011.

[6] Az informatikai biztonság kézikönyve, szerkesztő: Muha Lajos, Verlag Dashöfer Szakkiadó, 2000. (folyamatosan aktualizált kiadvány)