Szilágyi Károly Bálint
Szilágyi Ügyvédi Iroda
Pécs

Az elektronikus aláírásról szóló törvénytervezet egyes alapvető kérdéseinek elméleti vizsgálata

Miniszterelnöki Hivatal
Informatikai Kormánybiztosságának
Szabályozási Főcsoportfőnöksége részére
Pécs, 2000. november 18.

I. Az elektronikus aláírás szerepe

Jelen tanulmány tárgya a modern kommunikációs csatornák által felvetett hitelesítési és bizonyítási problémákra adható egyik adekvát válasz, az un. *elektronikus aláírás* jogi értékelése, valamint a felhasználásához kapcsolódó szabályozási modellek áttekintése. A tanulmány megállapításai a Miniszterelnöki Hivatal Informatikai Kormánybiztosságának Szabályozási Főcsoportfőnöksége által kidolgozandó elektronikus aláírási törvény egyes kérdéseiben való megalapozott döntést kívánja elősegíteni.

Napjainkban az információs társadalom, az Internet, az elektronikus kereskedelem fogalmai már nem a távoli jövőt, a várható lehetőségeket, hanem a mindennapi valóságot jelentik. Az a környezet, melyben ma a gazdaság, a jogtudomány, de legfőképpen maga a társadalom egésze él: hosszú és senki által nem vitatottan forradalmi változások következménye. A XX. század felfokozott gazdasági és tudományos fejlődésének eredményeként beköszöntő „digitális évezred" számos vívmánya – ugyanakkor árnyoldala is – hétköznapjaink részévé vált.

A fejlődés egyik legjelentősebb hozadéka az a körülmény, hogy az emberek közti kommunikáció egyre jelentősebb része zajlik teljes mértékben elektronikus formában. Ez egyaránt igaz a magánélet, az üzleti kommunikáció és az állam belső működése tekintetében. Fentiek következtében mind gyakrabban áll elő az a helyzet, hogy egy adott információ kizárólag elektronikus formában létezik, annak megformálásától a közvetítő folyamatokon át, egészen annak fogadásáig. Az ilyen úton közvetített információ végül elektronikus formában kerül tárolásra is. További, fontos körülmény, hogy a XX. sz. végére hasonlóan széles körben a számítógépek egymás közti kommunikációja is jelentős – gazdasági és társadalmi – szerephez jutott.

E gyors változások mára olyan gyökeresen új és komplex helyzetet teremtettek, melyben a több évszázada számos tekintetben az emberi kézírásra alapozó jogi kultúra és szabályozás bizonyos normák felülvizsgálatára kényszerül. E normák közül kiemelendőek azok, melyek bizonyos tények, körülmények hiteles rögzítéséhez kapcsolódnak, tehát a *hitelesség* feltételrendszerét alkotják. E szabályok:

- egyes formális eljárásokban való felhasználásra létrehozott iratokra, valamint
- formális eljárásokban tények vagy körülmények bizonyítására felhasznált eszközökre vonatkoznak.

Így a jogi szabályozás által tisztázandó kérdés különösen:

- az elektronikus formában tárolt iratok jogi megítélése, felhasználásuk körének kijelölése, bizonyító erejük meghatározása;
- az általános értelemben vett elektronikus adat felhasználási köre, bizonyító erejének meghatározása.

A hagyományos, emberi kéz által, papírra írt írás, és különösen a hagyományos értelemben vett aláírás jogi jelentősége közismert. Ennek bizonyos sajátosságait alapul véve volt képes a jog hosszú időn át meghatározni azokat a formális szabályokat, melyek megtartása egy tény vagy körülmény hiteles igazolását eredményezte. Az elektronikus környezetben azonban e normák helyett olyanok megállapítása szükséges, melyek bizonyos elektronikus adatok megléte esetén képesek a hitelességet biztosítani.

A dolgozatban később bemutatott tények és indokok miatt a fent említetteknek az elektronikus aláírás speciális szabályozásával lehet eleget tenni. Így a dolgozatban bemutatásra kerül:

- az elektronikus és a speciális elektronikus aláírásnak tekinthető un. digitális aláírás működése, a segítségükkel elérhető, hitelesítés szempontjából jelentős eredmények,
- az elektronikus környezetben fellépő, hitelesítéssel kapcsolatos jogi probléma,
- az elektronikus aláírás szabályozásának elméleti modelljei, ezekkel párhuzamosan
- egyes, már megalkotott nemzeti és nemzetközi szabályok és ajánlások, végül
- a hitelesítési probléma magyar jogban elfoglalt helye, az erre adható egyik elméleti válasz.

I.

Az elektronikus és digitális aláírás fogalma, a digitális aláírás működése

1. Az elektronikus aláírás fogalma

Az elektronikus aláírás általánosan elfogadott fogalma *elektronikus adathoz azonosítás céljából kapcsolt, vagy ahhoz logikailag hozzárendelt elektronikus adatot jelenti* [1]. Az „aláírás" kifejezés tehát nem fedi a módszer valódi funkcióját, használata az elektronikus aláírás kézi aláírást kiváltó jellege miatt terjedt el. Pontosabb megnevezés lenne az „elektronikus adatkapcsolás", vagy „ráírás", e dolgozatban az egyértelműség kedvéért mégis a már elterjedt fogalmat használja.

Az elektronikus aláírás tehát tág értelmű fogalom. Beletartozik minden olyan megoldás, melynek segítségével egy meglévő elektronikus adathoz egy további elektronikus adatot csatolnak[2] („*Electronic signature is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can "sign" an electronic record.*[3] "),. Így elektronikus aláírásnak nevezhetjük különösen az alábbi, technikai szempontból biztonságosnak nem nevezhető eljárásokat:

- a szövegek, elektronikus levelek végére írt név,
- a kézi aláírás képének elektronikus képként szövegekhez csatolása,
- számítógépes file-ba beírt név, azonosító,
- digitális képben elhelyezett un. digitális vízjel.

E megoldások jellemzője, hogy bárki által elkészíthetőek, megváltoztatásuk is viszonylag egyszerű feladat.

2. A digitális aláírás fogalma

Fentiek mellett ugyanakkor léteznek olyan elektronikus aláírások, melyekről a technika és tudomány mai állása szerint elmondható, hogy egyes körülményeket nagy fokú biztonsággal képesek tanúsítani. E módszerek közül kiemelendő az un. *digitális aláírás*. A digitális aláírás egy un. nyilvános kulcsú infrastruktúrát (public key

[1] Ld. többek között:
Thomas J. Smedinghoff - Ruth Hill Bro: Electronic Signature Legislation.
Megjelent: Findlaw oldalak, http://profs.findlaw.com/signatures/

[2] Külön jelölés hiánya esetén a továbbiakban az adat és irat fogalmakat elektronikus formában meglévőként értjük.

[3] „Az elektronikus aláírás általános, technológia független fogalom, mely mindazokat a módszereket jelenti, melyekkel valaki „aláírni" képes egy elektronikus adatot" (Tomas-Ruth, i.m.)

infrastructure, PKI[4]) használó titkosítási és hitelesítési rendszer. Megbízhatósága és könnyű kezelhetősége miatt mára igen elterjedtnek tekinthető, különösen az online, Internetes alkalmazások tekintetében[5]. Nagy előnye az un. titkos kulcsú megoldásokkal szemben, hogy a megbízhatósága nem csökken nyilvános kommunikációs csatornák (például Internet) használata esetén sem. E jellemzőjét annak köszönheti, hogy – mint neve is mutatja – két un. kulccsal operál. Ezek közül az egyik az un. titkos kulcs, a másik a nyilvános kulcs. Ezek létrehozása során a generálási folyamat a környezet egyes véletlen elemeit is felhasználja (véletlen-szám generálás), így biztosítva az egyediséget. A két kulcs közti kapcsolat jellege miatt a titkosítási és aláírási funkció aszimmetrikus módon zajlik. A titkos kulcs birokosa képes egy csak rá jellemző elektronikus aláírást létrehozni, illetve adatokat titkosítani. A nyilvános kulcs birtokában pedig bárki képes az elhelyezett aláírást ellenőrizni, valamint a titkos kulcs birtokosa számára adatokat titkosítani.

A digitális aláírás tehát titkosítási és aláírási funkciókat lát el. A hitelesség tekintetében a titkosítás kérdése irreleváns. Kiemelendőek azonban az aláírási funkció legfontosabb jellemzői, melyek az alábbiak[6]:

- kizárólag egy aláíró személyéhez kötődik,
- az aláíró személyét képes azonosítani,
- úgy kapcsolódik az elektronikus adatokhoz, hogy az aláírást követő minden – szándékos vagy véletlen – változása egyértelműen kimutatható,
- képes az aláírás időpontjának biztonságos megörökítésére,
- az aláírás ténye utólag le nem tagadható.

E jellemzők alapján a digitális aláírás sajátosságaira *fokozott biztonságú elektronikus aláírásnak* nevezhető.

3. A digitális aláírás működése

A digitális aláírás jellemzői jobban megérthetőek az aláírási és ellenőrzési folyamat áttekintésével[7]. A digitális aláírás egy bonyolult matematikai és kriptográfiai megoldás, azonban e területek részletes elemzése nem e dolgozat tárgya. Emiatt az alábbiakban e folyamat a felhasználó szemszögéből kerül bemutatásra, a háttérben meghúzódó technológiára csupán az un. HASH algoritmus tekintetében térünk ki.

[4] Az ismertebb nyilvános kulcsú titkosítási rendszerek: Elgamal (megalkotója: Taher Elgamal), RSA (feltalálói: Ron Rivest, Adi Shamir, and Leonard Adleman), Diffie-Hellman (mely szintén a feltalálókról kapta nevét), DSA, Digital Signature Algorithm (Digitális Aláírási Algoritmus, megalkotója David Kravitz).

[5] Ld. többek között a népszerű és ingyenes Pretty Good Privacy (PGP) software családot, http://www.pgpi.com.

[6] Ld. többek között: Sík Zoltán: Digitális aláírás, elektronikus aláírás. Megjelent: Magyar Távközlés, 2000/4. http://puskas.matav.hu/0009/digitalismt2.html;
Philip Zimmermann: Pretty Good Privacy, fordította Czakó Krisztián. Magyar Elektronikus Könyvtár, http://www.mek.iif.hu/porta/szint/muszaki/szamtech/wan/biztonsa/pgp.hun;
Valérie Sédallian: Preuve et signature électronique. http://www.juriscom.net/chronique/2/fr0509.htm

[7] Ld. továbbá: I. függelék.

A digitális aláírást lehetővé tevő eljárás igen fontos eleme az un. HASH függvény alkalmazása. Lényege, hogy egy tetszőleges hosszúságú dokumentumhoz egy belőle létrehozott, állandó hosszúságú un. stringet, sűrítményt fűznek. Az eredeti dokumentum a bemenet (input), a sűrítmény a kimenet (output). Minden dokumentumhoz más-más string tartozik és a string létrehozása gyors, egyszerű folyamat. A HASH a következő tulajdonságok miatt alkalmas aláírás („digitális ujjlenyomat") készítésére:

- gyakorlatilag nem létezik két olyan input, ami azonos outputot generál,
- egy létező outputhoz az eredeti inputtól eltérő inputot nem lehet konstruálni úgy, hogy a HASH függvény ahhoz is azonos outputot rendeljen,
- a dokumentumban eszközölt egy bit módosítás a kimenet több bitjét módosítja.

A leggyakrabban alkalmazott HASH függvény a Standard Hash Algoritmus, SHA. Itt az input tetszőleges hosszúságú (maximum 2^64 bit), a kimenet pedig 160 bit hosszú. Ez a hash érték (message digest, sűrítmény).

Az aláírási folyamat tekintetében a dokumentum létrehozásakor és annak feldolgozásakor (olvasás) végzett tevékenység vizsgálandó. Ebben a folyamatban három fél vesz részt:

- a dokumentum aláírója,
- a dokumentum olvasója,
- a hitelesítés szolgáltató.

Aláírónak nevezzük azt a személyt, aki saját aláírását az elektronikus iraton elhelyezi.

Az *olvasó* az a személy, aki az elektronikus iratot megkapja, és a más által elhelyezett aláírást ellenőrzi.

A *hitelesítés szolgáltató* (certificate provider, CP) az a személy vagy szervezet, amely az aláírás létrehozásához szükséges eszközök (software, hardware) és kulcsok kiadását végzi. Ezek kiadásakor az aláíró személyazonosságát ellenőrzi, és ennek eredményeként egy un. *tanúsítványt* állít ki. Fontos megjegyezni, hogy létezik olyan PIK, ahol nincs hitelesítés szolgáltató. Ilyen például a PGP rendszere. Az ilyen rendszerek – e hiányzó szereplő miatt – kevésbé megbízhatóak.

Az aláírás folyamata során:

a dokumentumot létrehozó személy:

- rendelkezik egy privát kulccsal (szigorúan titokban kell tartania, a fizikai hordozót biztonságos helyen kell tárolnia),

- nyilvánosságra hozza e kulcs publikus párját,

- a dokumentumból a fent megismert HASH függvénnyel stringet képez az aláíró,

- a stringet a privát kulcs segítségével aláírja,

- a stringet a dokumentumhoz csatolja.

A dokumentumot olvasó személy:

- kiszámítja a dokumentum eredeti ellenőrző kódját,

- a digitális aláírást a nyilvános kulcs segítségével dekódolja, így egy második kódot kap,

- a két kódot összeveti. Ha egyeznek, a dokumentum nem módosult aláírása óta.

- az aláíró személyt a nyilvános kulcs ismeretében a CP azonosítja, valamint igazolja, hogy a kulcs érvényes (tehát nem lopták el, nem járt le, stb.).

II.

A hitelesség problémája az elektronikus környezetben

Mint azt már a bevezetésben megfogalmaztuk, az elektronikus csatornákat használó kommunikáció és elektronikus adatkezelés hitelességének problémája jogi szempontból az emberi kézírás hiányára vezethető vissza. Technikai szempontból léteznek ugyan olyan eljárások, melyek segítségével bizonyos (eljárásonként változó) biztonsággal állapíthatóak meg egyes tények és körülmények, ezek értéke egy adott életviszonyban azonban a jogi szabályozás által meghatározott következményektől is függ. A hitelességi probléma, lényegét tekintve tehát, az alábbi kérdésekre adandó választ keresi:

- milyen következményeket és milyen célból fűz egy adott jogrendszer a kézzel történő írás használatához,
- mely technikai megoldások képesek e célok elérését elektronikus környezetben szavatolni, és végül:
- milyen jellegű jogi szabályozás szükséges e technikai megoldások eredményeinek érvényesítéséhez?

1. A kézi aláírás és a papír-alapú írásbeliség jelentősége

A jogi normák egyik legfontosabb funkciója a szervezetek és az állampolgárok jogérvényesítésének és kötelezettségeik teljesítésének biztosítása. E funkció egyik fontos eszköze abban áll, hogy bizonyos formális szabályokat állapít meg mind egyes informális tevékenységek (például szerződés) elemei tekintetében, mind a jogérvényesítés illetve kötelezettség teljesítés formális útjai (eljárások) vonatkozásában.

E követelmények közül témánk szempontjából azok jelentősek, melyek tények és körülmények hiteles[8] igazolásához kapcsolódnak. E szabályok széles körén belül is azok a normák kerültek az elektronikus környezetben problematikus helyzetbe, melyek az általános értelemben vett *nyilatkozatokra* vonatkoznak. A nyilatkozat fogalma alatt tág értelemben az akaratnyilatkozatokat, kijelentéseket, valamint az emberi gondolatok rögzítésének eszközeit értjük. A nyilatkozatok hitelesség azt jelenti, hogy a nyilatkozat nem hamis és nem hamisított[9].

[8] Hitelesség alatt a

[9] Vö.: Kengyel Miklós, Magyar polgári eljárásjog, Osiris Kiadó, 1998, Budapest, 272. oldal [529]: “Hamis az az okirat, amely nem a benne feltüntetett kiállítótól származik.”, “Hamisított iratról beszélünk akkor, ha az okirat valódi, de szövegét megváltoztatták.”. A terminológia mutatis mutandis alkalmazandó a nyilatkozatokra is.

A hagyományos, tehát az elektronikus környezetet figyelembe még nem vevő szabályozás a nyilatkozatok hitelesítése tekintetében az emberi kézírást veszi alapul[10], ennek segítségével állapít meg bizonyos vélelmeket. Ennek oka az a tudományos tapasztalat, hogy egy ember saját aláírását más azonos módon nem képes megismételni.

A fenti jelenséget a kézi aláírás *egyediségének* nevezzük, mely alkalmas az aláíró egyedi *azonosítására*. Ez alapján fennáll az a vélelem[11], miszerint a nyilatkozatban megnevezett kibocsátó megegyezik az aláíróval.

További vélelemként kapcsolódik az aláíráshoz az *integritás* vélelme, mely szerint az aláírást megelőző nyilatkozat tartalma az aláírás óta nem változott meg (nincs meghamisítva).

Tehát a kézi aláírás létezése esetén vélelmezi kell azt, hogy

- a nyilatkozat nem hamis,
- a nyilatkozat nem hamisított.

E két feltétel teljesülése esetén tehát a nyilatkozatot *hitelesként* kell kezelni.

Az aláíráson túl, a jogi szabályozás két további sajátosságot is mutat az írásbeliséggel kapcsolatban:

- egyrészt a szóbeliségtől elválasztja az írásbeliséget, kialakítva az „írásba foglalás” alaki szabályát,
- megkülönbözteti és előre megadja az eltérő biztosítékokkal rendelkező „írásbeli”, vagyis „írásba foglalt” nyilatkozatok eljárásonkénti bizonyító erejét.

Az *írásbeliség* (mely papírra való kézi vagy nyomdai jellegű írást jelent) problémája abban jelentkezik, hogy elektronikus környezetben nem létezik a klasszikus jogi normák által megkövetelt papír és íróeszköz. Meg kell tehát találni azokat a lehetőségeket, melyek ezek kiváltására alkalmasak.

Az előre meghatározott bizonyító erő tekintetében a probléma papír alapú írásbeliség és a kézi aláírás egyidejű hiányából ered. Ennek feloldása tehát akkor lehetséges, ha mindkét hiányzó elemet pótolni tudjuk.

[10] A szabály alól természetesen léteznek kivételek, például a zárt körben történő iratkezelés esetén.

[11] Fontos kiemelni, hogy az itt használt fogalmak nem azonosak a magyar polgári perrendtartás fogalmaival. A bemutatott vélelmek általában jellemzőek a kontinentális jogrendszerekre.

2. A kézi aláírást helyettesíteni képes technikai megoldások

Az, hogy egy adott technikai megoldás alkalmas-e a kézi aláírás helyettesítésére, eldönthető az alapján, hogy az adott megoldás használata esetén felállíthatóak-e a megismert vélelmek. A vizsgálat célja tehát annak eldöntése, hogy egy technikai megoldás képes e önmagában, papír-alapú aláírás és nyilatkozat nélkül a hitelességet biztosítani.

Nagyon fontos, hogy az elektronikus nyilatkozatokkal kapcsolatban kizárólag az önmagukban is hitelesítésre képes módszereket válasszuk ki. Amennyiben ugyanis az elektronikus nyilatkozat használatával párhuzamosan papír-alapú nyilatkozat használata is szükségesnek mutatkozik, az elektronikusa hitelesítés nem tudja a modernizációt elősegíteni.

A ma elterjedt technológiák közül, figyelembe véve a korábban bemutatott előnyeit, a digitális aláírás vizsgálatát érdemes elvégezni[12]. Az alábbiakban megvizsgáljuk, hogy a kézi aláírás mely jellemzőit képes a digitális aláírás kiváltani, jelezve azt, hogy ezt melyik tulajdonsága teszi lehetővé, és e tulajdonsága alapján mely vélelmeket lehet a digitális aláírással ellátott nyilatkozat tekintetében megállapítani.

A kézi aláírás és a digitális aláírás összehasonlítása

a kézi aláíráshoz kapcsolt vélelem	**kiváltható a digitális aláírással?**	**a kiváltást megalapozó digitális aláírási tulajdonság**
egyediségen alapuló vélelem: a nyilatkozat nem hamis	*igen*	a titkos kulcs egyedi
integritás: a nyilatkozat nem hamisított	*igen*	a HASH algoritmus minden utólagos változást kimutat

A fenti táblázat azt mutatja, hogy a digitális aláírás alkalmas a nyilatkozatok hitelességének biztosítására.

Az „írásbeliség”, mint a papír-alapú írás használatának kiváltása elméletileg nem jár jelentős nehézséggel. A fentiekre tekintettel elmondható, hogy a digitális aláírással ellátott nyilatkozat írásbeliként való értelmezése nem jelent a hitelesség tekintetében hátrányt.

[12] E technikán kívül természetesen más megoldások is léteznek, melyek felsorolását kisebb jelentőségük miatt mellőzzük.

A bizonyító erő kérdése azonban további vizsgálatokat tesz szükségessé a hagyományos és elektronikus iratok (mint a nyilatkozatok speciális formái) tekintetében. A fokozott bizonyító erővel bíró iratok, a klasszikus szabályok szerint, sajátos jellegüket az írásbeliség meglétén túl további, alaki feltételek jelenlétéből nyerik. Ezek jellemzően tanúk, vagy „hiteles személyek", tehát például ügyvéd közreműködését, vagy meghatározott szerv speciális eljárását jelentik.

E feltételek minden esetben azt a célt szolgálják, hogy az írásbeliség alapvető biztonságát meghaladó mértékben biztosítsák az irat kibocsátójának kilétét, valamint az irat integritását.

Ez ilyen jellegű, magasabb szintű garancia a PKI keretében *hitelesítés szolgáltatók*[13] segítségével valósítható meg. E szolgáltatók feladatuk ellátása során sajátos szabályok megtartásával ellenőrzik a kibocsátó személy vagy szervezet azonosságát. Amennyiben az erre irányuló jogi szabályozás adekvát biztosítékokat követel meg a CP-k eljárása során[14], az azonosítás és az ez alapján kiadott tanúsítvány segítségével megadható a digitális aláírás tekintetében is a fokozott bizonyító erő lehetősége. Az ilyen elektronikus aláírást *minősített elektronikus aláírásnak* nevezzük.

Fentiek értelmében tehát:

- az elektronikus aláírás mint mérlegelhető bizonyítási eszköz alkalmazható,
- a digitális aláírás – mely, tekintettel sajátosságaira *fokozott biztonságú elektronikus aláírásnak* nevezhető – alkalmas az írásbeliség kiváltására,
- a *minősített elektronikus* aláírás pedig a fokozott bizonyító erővel bíró iratok felváltását teszi lehetővé.

III.
A szükséges jogi szabályozás vázlata

Az alábbiakban az elektronikus nyilatkozatok hitelességével kapcsolatban szükségesnek vélt jogi szabályozás rövid vázlatát adjuk[15]. A vázlat kidolgozása során olyan szempontok érvényesülnek, melyek a bevezetésben megjelölt cél - tehát az elektronikus csatornákon folyó kommunikáció által létrehozott elektronikus iratok (mely fogalom megegyezik a fent használt nyilatkozat fogalmával) hitelességének biztosítása és azok megbízhatóságuktól független, kötelező jogi értékelésének kimondása – elérését hivatottak elősegíteni.

A célirányos szempontok közül a legfontosabbak a következők:

- az elektronikus nyilatkozatokat, hitelességi szintjüktől függetlenül, nem lehet kizárni a formális eljárásokban bizonyítási eszközként való felhasználásból,

[13] Ld. I.3. vonatkozó része

[14] Az adekvát azonosítás érdekében a CP számára meg kell adni a központi nyilvántartások használatának lehetőségét.

[15] Vö.: az elektronikus aláírás közösségi kereteiről szóló 1999/93. EK irányelv (1999. december 13.) rendszerével.

- meg kell alkotni azokat a szabályokat, melyek a kézzel történő, papír alapú „írásbeliség”, mint formai követelmény elektronikus helyettesítését teszik lehetővé,
- meg kell határozni, hogy mely elektronikus iratok nyernek egyes eljárásokban fokozott bizonyító erőt.

A korábbi fejezetek alapján kijelenthető, hogy egy, a fenti célokat megvalósító jogi szabályozás az elektronikus aláíráshoz kötődő problémákat hivatott rendezni. A célok elérése érdekében azonban szükségesek a megfelelő környezet kialakítása. E környezet célja, hogy biztosítsa a fenti célok megvalósítására kiválasztott technológiák zavartalan és biztonságos működését. Ehhez – mint erre már korábban utaltunk – hitelesítés szolgáltatók működése szükséges. Mivel a hitelesítés szolgáltatók megbízhatósága igen nagy jelentőségű egy ilyen rendszerben, szükséges a CP-k felügyeletét és működésük ellenőrzését ellátó állami szerv kijelölése is. Összefoglalva tehát elmondhatjuk, hogy az elektronikus környezetben hitelességet biztosítani hivatott szabályozás hatálya az alábbi fő pontokra terjed ki:

a, a hitelességet biztosító *alapvető* körülmények szavatolására:

- az elektronikus nyilatkozatok,
- az „írásbeliség”, valamint a
- bizonyító erő kérdéseire;

b, a technológia megbízható működését szavatoló környezet kialakítására, tehát

- a hitelesítés szolgáltatók működésének, valamint
- ezek állami ellenőrzésének kérdéseire.

A kívánatos szabályozás tehát az alábbiak szerint foglalható össze:

A. *Az alapvető rendelkezések kiterjednek:*

- az elektronikus aláírás és az elektronikus irat fogalmának meghatározására,
- a fokozott biztonságú és minősített elektronikus aláírás és elektronikus irat fogalmának meghatározására,
- a velük szemben támasztott követelmények előírására,
- a papír-alapú egyszerű magánokirat és a teljes bizonyító erejű köz- és magánokirat kiváltására alkalmas elektronikus iratok megjelölésére.
- azon az életviszonyok meghatározására, melyekre vonatkozó jognyilatkozatok elektronikus formában nem tehetők. Ilyen lehet a

    - családjog,
    - öröklési jog területére vonatkozó, valamint
    - a közjegyzői vagy ügyvédi ellenjegyzéshez kötött jognyilatkozat.

- az elektronikus iratok diszkriminációjának alapelvi szintű tilalmára,

- az elektronikus irat alapjogokat érintő eljárásokban való kötelezővé tételének tilalmára,
- az közigazgatási valamint igazságügyi szervek esetén a minősített elektronikus okiratok elfogadásának kötelezővé tételére.

B. *A digitális aláíráshoz szükséges eszközök megszerzésével összefüggésben szabályozandó kérdések:*

Az elektronikus aláírást hitelesítő intézményekre (CP-k) vonatkozó előírások:

- általános követelmények megfogalmazása,
- annak biztosítása, hogy e tevékenység piaci alapon, piaci szereplők lássák el,
- a közigazgatási szervek esetén saját, állami CP létrehozása,

a piacon működő CP-k tekintetében:

- piacra lépésük feltételeinek meghatározása,
- működési rendjük szabályozása,
- a minősített elektronikus aláírás hitelesítésére jogosult intézményekhez tapadó speciális követelmények megfogalmazása.

Szükséges szabályozni az állami felügyeleti rendszer felépítését és működését. Ehhez kapcsolódóan meg kell határozni:

- a hitelesítés szolgáltató minősítést végző szerv,
- az ellenőrzést és felügyeletet gyakorló szerv jogkörét, feladatait, kötelezettségeit,
- meglévő állami szervek közül ki kell választani, vagy új szervet kell létrehozni ennek ellátására.

C. *A digitális aláírás alkalmazása során érintett felek jogai és kötelességei:*

1. Az aláírás jogosultjának

- kizárólagos joga az aláírását elhelyezni
- az aláíráshoz szükséges kulcsokat képviselőjének átadni
- a képviselő irányában a felhasználás körét megállapítani

- kötelessége a visszaélések elleni intézkedéseket megtenni,
- a kulcs őrzéséről megfelelő szinten gondoskodni,
- a kulcs elvesztése, vagy,
- annak eltulajdonítása esetén köteles a CSP-nél a kulcs letiltása és érvénytelenítése végett haladéktalanul intézkedni.

2. Az irat címzettje

- jogosult a CP-től az aláíró személy azonosítását kérni,
- az irat hitelességének, integritásának ellenőrzését igényelni.
- visszaélés észlelése esetén a kulcs tulajdonosával azonos kötelezettségek terhelik.

3. A hitelesítés szolgáltató

- jogosult jogszabály által megállapított körben a kulcsok biztonságos kezelését ellenőrizni,
- köteles a nyilvános kulcsot nyilvánosan elérhetővé tenni,
- kérelemre arról információkat adni,
- azt rendelkezésre bocsátani,
- az ehhez szükséges nyilvántartást vezetni,
- a birtokában lévő adatokat törvényesen, a speciális szabályok szerint kezelni,
- a kulcs tulajdonosának kérelmére a kulcsot érvényteleníteni, törölni.

4. A fenti szereplők felelőssége tekintetében:

- a szerződéses viszonyok bizonyos részét törvényileg szabályozni (felelősség kizárásának, korlátozásának eseteit meghatározni)
- szerződésen kívüli viszonyukban célszerű általános polgári felelősséget megállapítani,
- ezt azonban ésszerű mértékben részletszabályokkal konkretizálni.
- a CSP előírásokat megszegő magatartása esetén speciális felelősséggel bír a minősített tanúsítványokkal kapcsolatban felmerült károk tekintetében.

D. *A szabályozás módja, jogforrási szintje:*

- az általános szabályokat törvényben kell meghatározni,
- a szűk értelemben vett technikai normákat és a felügyeleti szabályokat rendeleti szinten érdemes rendezni,
- a szükséges, már létező anyagi és eljárásjogi jogszabályokat célszerűen módosítani kell,
- a polgári jogi viszonyokra, valamint a polgár és az állam viszonyában jelentkező területeket törvényben kell szabályozni,
- az állami (kormányzati, közigazgatási) szférán belüli szabályokat differenciált jogforrásokkal kell szabályozni.

E. *Nemzetközi átjárhatóság*

- Meg kell állapítani azokat a minősítési elveket, amely alapján egy külföldi CP tevékenységét a magyar szabályoknak megfelelőnek lehet kimondani,
- elő kell írni, hogy a fentieknek megfelelő külföldi CP azonos jogokkal működhet a magyar piacon, mint a magyar CP-k,
- a külföldi szabványok megismerésével és – ha célszerűnek látszik –alkalmazásával lehetővé kell tenni a külföldi digitális aláírások magyarországi feldolgozhatóságát.

VI.
Az elektronikus aláírás nemzetközi szabályozása

Az információs társadalom kihívásaira adott nemzeti és nemzetközi válaszok között számos esetben megtaláljuk az elektronikus aláírással vagy általában az elektronikus hitelesítéssel foglalkozó szabályozást is. Számos ország készítette már el nemzeti jogszabályát, és számos nemzeti vagy nemzetközi szervezet dolgozott ki ajánlásokat e tárgykörökben. Az alábbiakban bemutatjuk azokat a szempontokat, melyek alapján a megalkotott szabályozások egymástól jellegüknél fogva elválaszthatóak. Az áttekintés során a jelentősebb normák részletesebb bemutatására is kitérünk.

Vizsgálódásunk során az alábbi szabályozási technikákat különböztetjük meg[16]:

1. technológia független és egy adott technológiára alapozó szabályozás,

2. nemzeti és nemzetközi szabályozás,

3. állami szabályozás és ipari önszabályozás,

1. Technológia független és technológia függő szabályozás

Az elektronikus aláírás szabályozása tekintetében két, részben egymás ellen ható törekvés jellemző. A jogalkotó egyrészt célként tűzi maga elé a hosszú távon adekvát szabályozás megvalósítását, tehát azt, hogy a technika fejlődése miatt nem váljon szükségessé túlzottan gyakran a normák felülvizsgálata. A másik szempont a szabályozás egyértelműsége és az elektronikus aláírásokhoz fűzött jogi hatások maximális biztosítása.

Egy olyan szabályozási tárgykörben, mint az elektronikus aláírás, e két cél a technika rohamos fejlődése miatt ellentétbe kerül egymással. A technológia függő szabályozás ugyanis egy bizonyos elektronikus aláírási technológia jogi hatályának elismerését valósítja meg, a technológia független szabályozás ezzel szemben az alkalmazott technológiától függetlenül, bizonyos előre meghatározott tulajdonságok alapján biztosít jogi hatást a technológiák számára. A két szabályozás előnyeit és hátrányait az alábbi összefoglalás hivatott bemutatni.

[16] B.P. Aalberts & S. van der Hof, Digital Signature Blindness, Analysis of legislative approaches toward electronic authentication, November 1999, http://cwis.kub.nl/~frw/people/hof/ds-fr.htm .

A technológia független és a technológia függő szabályozás előnyős és hátrányos vonatkozásai

	Technológia függő szabályozás	**Technológia független szabályozás**
előnyök	◆ erősíti a jogbiztonságot, ◆ a jogi hatások megbízható rendszerét alakítja ki, ◆ a bíróságok jogértelmező szerepe kisebb szerephez jut, ◆ a kiválasztott technológia ismert képességeihez igazítva képes cizellálni a szabályozást	◆ jól alkalmazkodó szabályozást jelent, ◆ felváltása későbbi időpontban válik szükségesség, ◆ helyt ad új technológiák kifejlődésének, ◆ képes több technológia számára is jogi hatásokat biztosítani
hátrányok	◆ a technika fejlődésével egyidejűleg gyakori felülvizsgálatot igényel ◆ a kiválasztott technológia fejlődését visszavetheti annak bizonyos tulajdonságainak kiválasztása, ◆ zavarokat okozhat a piaci folyamatokban	◆ csökkenti a jogbiztonságot, ◆ a valódi függetlenség csupán bizonyos korlátok között igaz

A technológia függő szabályozások közül kiemelendő az Európában elsők között megalkotott német Informations- und Kommunikationsdienste-Gesetz, IuKDG[17]. A technológia független szabályozás egyik példája pedig a japán szabályozás lehet[18].

Az Információs és Kommunikációs Szolgáltatásokról szóló német törvény az olasz szabályozás[19] mellett az egyik első európai törvény, mely felvállalta az információs társadalom jogi problémáinak rendezését. 1997. augusztus 7-én lépett hatályba az Informations- und Kommunikationsdienste-Gesetz, IuKDG, amely a digitális aláírások

[17] http://www.iid.de/rahmen/iukdgebt.html
[18] CA Working Group of the Electronic Commerce Promotion Council of Japan szabványai:http://ecom.ecom.or.jp/ecom_e/cag-smry.htm
[19] http://www.aipa.it/english[4/law[3/pdecree51397.asp

jogi rendezése mellett többek között jelentős adatvédelmi, szolgáltatói-felelősségi és szerzői jogi szabályokat tartalmaz. A 16.§ felhatalmazása alapján készült el a Digitális aláírás rendelet (Signaturverordnung - SigV), mely 19 bekezdésben rendezi a digitális aláíráshoz szükséges kulcsok kiadásának, a hitelesítés ellenőrzésének szabályit. A rendelet 1997. november 1-én lépett hatályba, tehát jóval megelőzi az EU direktíva[20] kiadását.

2. Nemzeti és nemzetközi szabályozás

A nemzeti és nemzetközi szabályozás közti választás különös jelentőséget kapott a modern, határokon átívelő kommunikációs csatornák miatt, mely jelenség kétségtelenül a nemzetközi szabályozás előtérbe helyezését indokolja.

Az eddigi tapasztalatok azonban azt mutatják, hogy bár a nemzetközi reguláció rövid távon képes lenne egységes normák kialakítására, ez mégsem valósulhat meg teljes mértékben. Ennek oka a nemzeti jogrendszerek és kultúrák nagyfokú eltérésében keresendő.

Ennek következtében – a nemzetközi egységesség célját szem előtt tartva – a nemzeti szabályok megalkotásakor fontos a nemzetközi tendenciák áttekintése, a szabályozások közös jegyeinek felismerése és ezek nemzeti szintű megvalósítása.

Jelenleg egy nemzetközileg kötelező, az elektronikus aláírást szabályozó norma létezik. Ez az elektronikus aláírások közösségi kereteiről szóló 1999/93/EK irányelv. E norma – az EK sajátosságaiból következően – jelenleg 15 tagország nemzeti jogalkotásának kereteit szabja meg. Ennek hatása kettős: egyrészt egységes módon rendezi a közösségi tagállamok nemzeti regulációját, másrészt – tekintettel az EK világpolitikai és gazdasági súlyára – más országok számára is irányadóvá válhat. Közelebbi vizsgálata a magyar jogalkotás európai-integrációs kötelezettségei miatt is indokolt.

A 2000. január 19-én közzétett irányelv jogilag kötelező előírásokat tartalmaz. Az EU tagállamoknak 18 hónap áll rendelkezésükre a jogharmonizációra. Jelenleg ez a jogforrás tekinthető a legmagasabb szintű és legújabb közösségi normának ezen a területen.

Az irányelv saját céljaként a belső piac „megfelelő működése” érdekében az elektronikus aláírások használatának megkönnyítését és jogi elismertetésének elősegítését jelöli meg (*I. cikkely*).

A *II. cikkelyben* található 13 alapvető fogalom meghatározása. Ezekhez igazodik a dolgozat végén megjelölt néhány alapvető kifejezés magyarázata is. Ésszerűnek tűnik ezek átvétele, részben Magyarország jogharmonizációs kötelezettsége, részben az átjárhatóság feltételeinek megteremtése érdekében[21].

---

[20] Az elektronikus aláírás közösségi kereteiről szóló 1999/93. EK irányelv (1999. december 13.)

[21] A direktíva szóhasználatától két esetben térünk el: „fokozott biztonságú elektronikus aláírás” fogalmát használjuk a direktíva „fejlett elektronikus aláírás” fogalma helyett.

A *III. cikkely* rendelkezéseinek célja a hitelesítés szolgáltatók (CP-k) piacra lépési szabadságának biztosítása, valamint az egységes, a direktíva előírásait megtartó állami felügyeleti rendszer kiépítése. A piacra lépés szabadságát hivatott biztosítani az a megoldás, hogy a szolgáltatók nem engedélyezési eljárás után kezdhetik meg tevékenységüket, hanem csupán a tevékenység elindításának bejelentése a kötelezettségük. További lényeges szabály, hogy az államok külön előírásokat tehetnek a működéssel kapcsolatban, de ezeknek minden esetben objektívek, átláthatónak, arányosnak és diszkriminációmentesnek kell lenniük[22].

Az *V. cikkely* szerint elektronikus dokumentumon elhelyezett *minősített elektronikus aláírás* ugyan olyan jogi hatállyal kell, hogy bírjon, mint a papír-alapú dokumentumokon elhelyezett kézi aláírás, valamint előírja a bizonyítékként való felhasználás feltételeinek megteremtését. Fontos körülmény, hogy e cikkely tiltja a *minőségi elektronikus aláírás* diszkriminációját is.

3. Állami szabályozás, ipari önszabályozás

A modern telekommunikációval kapcsolatos jogalkotás rövid története alatt már bizonyosság vált, hogy egyes kérdések szabályozása kizárólag állami eszközökkel nem lehetséges. Ennek okait abban jelölhetjük meg, hogy a szabályozás tárgyköre a gyorsan változó és speciális szakértelmet[23] igénylő technikai jelenségekhez kötött.

E problémára megoldást jelenthet, ha a szabályok egy részét a technológiákat kidolgozó és azokat alkalmazó piaci szereplők határozzák meg. Ebben az esetben az állami reguláció csupán a szabályok kialakítására való felhatalmazást és ezek kialakításának bizonyos eljárási feltételeit adja meg. Ezek jellege, a felhatalmazás keretei, nagyban függenek az adott ország önszabályozási hagyományaitól.

Az ipari önszabályozás „termékeit” gyakran nevezik „puha jognak”, vagy „best practices”-nek.

A piaci szereplők önálló, elektronikus hitelesítésre vonatkozó normaalkotására nemzetközileg különösen a PKIX Working Group of the Internet Engineering Task Force (IETF)[24] és az Internet Law & Policy Forum (ILPF)[25] tevékenysége jelent példát.

A kormányzat és a piaci szereplők együttműködése egy további módon valósulhat meg. Ezt együttes szabályozásnak nevezzük (co-regulation). Ez a szabályalkotási technika minimálisan annyival jelent többet az önszabályozásnál, hogy a normák kialakítása a kormányzattal folytatott rendszeres konzultációkkal egészül ki. Az együttes szabályozás kétségtelen előnye, hogy képes lehet kialakítani a kormányzati és ipari érdekek kompromisszumát.

---

[22] „Such requirements shall be objective,transparent,proportionate and non-discriminatory…” (III. cikkely 7. pont)

[23] Mellyel a gyors fejlődés következtében általában az ezt alkalmazó szervezetek rendelkeznek.

[24] http://www.ietf.org, valamint http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html.

[25] Ld.: http://www.ilpf.org. Az eredményekről a http://www.ilpf.org/digsig/principles.htm oldal számol be.

E konzultációk kiszélesítésével kialakulhat egy többszereplős normaalkotási folyamat, melyben a piaci és kormányzati érdekek mellett például a sajátos fogyasztói szempontokat is érvényesíteni tudják az erre szakosodott érdekképviseletek.
Ilyen folyamatot példáz a holland Electronic Commerce Platform in the Netherlands (ECP.NL)[26] tevékenysége, valamint az ausztrál Australian Internet Industry Association (IIA)[27] által kialakított „Code of Practice" is.

A különböző normaalkotási folyamatok jellemzői az alábbiak szerint foglalható össze:

	állami szabályozás	**önszabályozás**	**együttes szabályozás**
előnyök	◆ jogilag precízebben kidolgozott reguláció, ◆ piaci érdekeken képes felülemelkedni	◆ képes gyors válaszokat adni a fejlődés által kiváltott problémákra, ◆ általában az ipari szereplők rendelkeznek a szükséges technikai, speciális ismeretekkel	◆ a piaci szereplők érdek-érvényesítését a kormányzati felügyelet korlátok közé szoríthatja, ◆ bevonhatóak további érdekképviseleti szervek
hátrányok	◆ a szabályozás lassan születik meg, ◆ új technikai eredmények esetén hiányozhat a megfelelő szakértelmű tanácsadók köre	◆ jogtudományi szempontból nem megfelelő normát adhat, ◆ erősen érvényesíti a normaalkotásba bevont felek üzleti érdekeit	◆ csak a komoly érdekképviseleti és önszabályozási múlttal rendelkező országokban képes eredményeket elérni, ◆ lassú normaalkotással jár

[26] http://www.ecp.nl
[27] Ld.: http://www.iia.net.au/, http://www.iia.net.au/code.html.

V.
Az elektronikus aláírás problémája a magyar jogban

Az előző fejezetekben írtakat figyelembe véve, megkíséreljük a hitelesítési problémát a magyar jog szabályaira tekintettel feloldani. A logikai levezetés érdekében egyes pontokat röviden újra felvázolunk. Ennek során a korábban használt nyilatkozat fogalmat az irat fogalmával váltjuk fel. Ezt a magyar jogi szabályozásban való konkretizálás szükségessége indokolja.

1. Általános összefoglalás

A jogi életben alkalmazott dokumentumok, iratok tekintetében mind anyagi, mind eljárásjogi jogszabályok irányadóak A polgári anyagi jog alapvető intézményeit a Polgári Törvénykönyv szabályozza. Számos esetben írja elő írásbeliség használatát, amikor írásos formát tesz kötelezővé.

Az „írásban", „írásbeli", „írásba foglalás" jelentését azonban nem definiálja. Ezek a fogalmak

- az okirat létrehozásához használt eljárást,
- az okiratban foglaltak rögzítésének, tárolásának jellegét,
- adott esetben az okirat továbbításának módját jelölik.

Ezt figyelembe véve az *elektronikus irat* fogalmát egy már létező magyar jogszabály[28] alapján így határozhatjuk meg:

Számítástechnikai program felhasználásával - elektronikus formában rögzített - elektronikus úton érkezett, illetve továbbított irat, amelyet számítástechnikai adathordozón tárolnak[29].

Ezzel szemben a *hagyományos értelemben vett iratot* a következők jellemzik:

- papír alapú hordozóra ritkábban kézzel, általában nyomdai eljárással felvitt írást tartalmaz,
- a felvitt tartalom papíron tárolódik,

[28] *40/1998. III.6. Korm. Rendelet* A minisztériumok és az országos hatáskörű államigazgatási szervek iratkezelési mintaszabályzatáról, melléklet, I. fejezet.

[29] E meghatározás előnye, hogy az elektronikus iratot dinamikusan írja le. Az általunk használt „digitális adat" meghatározás ezzel szemben csak egy tulajdonságot vesz figyelembe, ezzel azonban szélesebb körben (ezért pontosabban)

- továbbításra csak az eredetileg használt papír hordozón alkalmas, az erről készült másolat jellemzően nem hiteles, illetve csak további biztosítékok mellett.

Az elektronikus irat egyes jellemzői tehát jelentősen eltérnek a hagyományos iratétól. Ezt foglalja össze az alábbi táblázat.

	papír alapú irat	**elektronikus irat**
az irat létrehozásának módja	◆ kézzel vagy nyomdai eljárással papírra felvitt	◆ elektronikus eszközökkel elektronikus jelek létrehozása
az irat tartalmi rögzítésének és tárolásának módja	◆ az eredeti papíron marad	◆ elektronikus formában marad
az irat továbbításának, másolásának módja	◆ a tároló eszköz (papír) fizikai áthelyezése, ◆ papírra történő átmásolás, ◆ esetleg az átmásoláshoz elektronikus átviteli csatorna használata[30]	◆ a továbbítás és a másolás általában szinonim fogalmak, ◆ fizikai hordozó és elektronikus csatorna is használható, ◆ a másolat teljesen azonos az eredetivel[31]

A gyakorlatban való *teljes értékű*, *általános alkalmazhatósághoz* biztosítani kell azokat a feltételeket, melyek nélkül az elektronikus iratok kiszorulnak a gazdasági életből, a közigazgatási és polgári eljárásjogokból (*elektronikus iratok diszkriminációja*).

Ezek a feltételek:

- a hitelességet biztosító technikai normákat tartalmazó jogszabályok megalkotása, amelyek hiánya a jelenlegi fogyatékosságokat okozza,
- a teljes bizonyító erőt lehetővé tevő szabályok,
- ezekkel párhuzamosan a papír alapú iratokkal megegyező általános értelemben vett jogi hatály kimondása.

A korábban a jogérvényesítési funkcióról írottak alapján az okiratok bizonyító erejének kérdése kerül a vizsgálat fókuszába. Ezeket a magyar jogban az eljárási jogok határozzák meg. Ezek közül a legfontosabb[32] a polgári perrendtartásról szóló 1952. évi III. tv.

[30] Pl. telefax.

[31] Azonos, hiszen a másolat minden bitje azonos az eredetiével.

[32] E jogszabály a polgári eljárás tekintetében állapít meg szabályokat, de a bizonyító erővel kapcsolatos rendelkezései a közigazgatási eljárásban is irányadóak. A büntető eljárásjog a bírói mérlegelés széles megengedése miatt nem alkalmaz a polgári eljárásjoghoz hasonló, bizonyító erőhöz kapcsolódó vélelmeket.

2. Az elektronikus okiratok bizonyító ereje

A dokumentum hamisítatlanságában vetett bizalom és az ezzel összefüggő vélelmek jelentik a bizonyító erő különböző fokait. Az elektronikus iratok esetén is célszerű két fokozat szabályozása, melyekből kiindulva kimondhatóak a klasszikus felosztás szerinti teljes bizonyító erejű közokirat és magánokirat, valamint az egyszerű magánokirat digitális megfelelőinek ismérvei.

Az *egyszerű magánokirat* elektronikus megfelelője az *elektronikus aláírás.* Ezeket a bíróság a Pp. 3.§ (5). bekezdésben meghatározott szabad mérlegelés elvének megfelelően ítéli meg:

> **„3.§. (5) Ha törvény másként nem rendelkezik, a bíróság a polgári perben alakszerű bizonyítási szabályokhoz, a bizonyítás meghatározott módjához vagy meghatározott bizonyítási eszközök alkalmazásához nincs kötve, szabadon felhasználhatja a felek előadásait, valamint felhasználhat minden egyéb bizonyítékot, amely a tényállás felderítésére alkalmas. E rendelkezések nem érintik a törvényes vélelmeket, ideértve azokat a jogszabályokat is, amelyek szerint valamely körülményt az ellenkező bizonyításáig valónak kell tekinteni[33].”**

Ezzel kapcsolatban azonban törvényi előírásnak kell kimondania, hogy papír-alapú és az elektronikus aláírással ellátott elektronikus iratok azonos megítélés alá esnek. Az ilyen elektronikus irat bizonyítékként való felhasználása nem utasítható el csak azon az alapon, hogy nem hagyományos eljárással készült irat (*elektronikus iratok diszkriminációjának felszámolása).*

Az előzőnél magasabb szinten meghatározható bizonyító erővel bíró dokumentum a *minősített elektronikus aláírással* ellátott okirat.

A digitális aláírást, amennyiben egy hitelesítés szolgáltató tanúsítványával van összekapcsolva, *minősített elektronikus aláírásnak* kell tekintenünk. Ennek jellemzői a következők:

- egyedülállóan köthető az aláíró félhez (adott aláírást csak egy személy képes dokumentumon elhelyezni)
- alkalmas az aláíró fél azonosítására,
- olyan eszközökkel hozták létre, amelyek kizárólag az aláíró fél befolyása alatt állnak,
- olyan módon van hozzákapcsolva az adatállományhoz, hogy minden későbbi adatmódosítás érzékelhető.

A kérdés az, hogy ezek a jellemzők kielégítik-e a teljes bizonyító erejű magánokirat fogalmához tartozó követelményeket? E fogalmat a polgári perrendtartás adja meg[34]:

---

[33] Ld. továbbá I.1.
[34] 1952. évi III. törvény 196-197.§§.

„196. § (1) A magánokirat az ellenkező bebizonyításáig teljes bizonyítékul szolgál arra, hogy kiállítója az abban foglalt nyilatkozatot megtette, illetőleg elfogadta, vagy magára kötelezőnek ismerte el, feltéve, hogy az alábbi feltételek valamelyike fennáll:

a) a kiállító az okiratot saját kezűleg írta és aláírta;

b) két tanú az okiraton aláírásával igazolja, hogy a kiállító a nem általa írt okiratot előttük írta alá, vagy aláírását előttük saját kezű aláírásának ismerte el; az okiraton a tanúk lakóhelyét (címét) is fel kell tüntetni;

c) a kiállító aláírása vagy kézjegye az okiraton bíróilag vagy közjegyzőileg hitelesítve van;

d) a gazdálkodó szervezet által üzleti körében kiállított okiratot szabályszerűen aláírták;

e) ügyvéd (jogtanácsos) az általa készített okirat szabályszerű ellenjegyzésével bizonyítja, hogy a kiállító a nem általa írt okiratot előtte írta alá, vagy aláírását előtte saját kezű aláírásának ismerte el.

(2) Gazdálkodó szervezet által kiállított vagy őrzött okiratról készült felvétel [195. § (2) bek.], továbbá bármilyen adathordozó útján készített okirat bizonyító ereje az eredeti okiratéval, közokiratról készült másolat esetében pedig a teljes bizonyító erejű magánokiratéval azonos, feltéve, hogy a gazdálkodó szervezet, amely a felvételt készítette vagy az okiratot kiállította, illetve őrzi, a felvétel vagy az okirat azonosságát szabályszerűen igazolta.

(…)

197. § (1) A magánokirat valódiságát csak akkor kell bizonyítani, ha azt az ellenfél kétségbe vonja, vagy a valódiság bizonyítását a bíróság szükségesnek találja.

(2) Ha a magánokiraton levő aláírás valódisága nem vitás, vagy be van bizonyítva, az aláírást megelőző szöveget az ellenkező bebizonyításáig meg nem hamisítottnak kell tekinteni, kivéve ha az okirat rendellenességei vagy hiányai ezt a vélelmet megdöntik."

Fenti rendelkezésekből két jellemző olvasható ki[35], melyek

- a bizonyító erőre, és
- a hamisítatlanságra vonatkoznak.

Először tehát: a teljes bizonyító erejű magánokiratok az ellenkező bizonyításig teljes bizonyítékul szolgálnak arra, hogy a bennük foglalt nyilatkozatot a *kiállító megtette, magáénak elfogadta, vagy azt magára kötelezőnek ismerte el*.

Másodszor: a teljes bizonyító erejű magánokirat aláírást megelőző része élvezi a *hamisítatlanság vélelmét*, amennyiben az aláírás bizonyított vagy nem vitás, illetve az okirat rendellenességei e vélelmet nem döntik meg.

Az aláírási technikák bemutatott jellegzetességei miatt megállapítható, hogy a *fokozott biztonságú elektronikus aláírás* használata esetén érhetjük el a teljes bizonyító erőhöz megkövetelt feltételeket.

A fokozott biztonságú elektronikus aláírás jellemzik az alábbiak:

[35] Vö.: Kengyel Miklós, Magyar polgári eljárásjog, Osiris Kiadó, 1998, Budapest 237. oldal, [532]-[533]

- egyedülállóan köthető az aláíró félhez – tehát kétségtelenül megállapítható, hogy ki volt az aláíró fél. A hamisítás szándékával elhelyezett aláírás nem eredményez más személyhez köthető jelsorozatot (hamis okirat[36]). Úgy is fogalmazhatunk, hogy egy ember csupán egyféle, csak rá jellemző aláírást képes létrehozni.

- alkalmas az aláíró fél azonosítására, hiszen a privát kulcs,

- olyan eszközökkel hozták létre, amelyek kizárólag az aláíró fél befolyása alatt állnak. Ez a feltétel azt jelenti, hogy nem állt módjában senkinek az aláírás folyamatát befolyásolni. Az aláíró fél képes volt saját nevében aláírni, és azt a dokumentumot írja alá, amelyiket ő akarta.

- olyan módon van hozzákapcsolva az adatállományhoz, hogy minden későbbi adatmódosítás érzékelhető. Ez a fogalmi elem pedig kizárja annak lehetőségét, hogy az egyszer már aláírt dokumentum később más tartalmat öltsön, nincs mód arra, hogy – a Pp. szavaival – az aláírást megelőző szöveget átírják (hamisított okirat[37]). Egy ilyen beavatkozás *biztosan* ellenőrzési hibát fog eredményezni.

- ki kell egészíteni a fentieket még egy sajátossággal: amennyiben e feltételek teljesültek, úgy az aláírás ténye nem tagadható le.

A fenti pontokban található ismérvek azonban csak akkor tekinthetők adottnak és csak akkor biztosíthatóak általánosan, ha *minősített elektronikus aláírást* alkalmaznak.

Ez az aláírás típus két vonatkozásban jelent eltérést, többletbiztosítékot a *fokozott biztonságú elektronikus aláíráshoz* képest:

- megfelel a minősített tanúsítványokkal, és a
- biztonságos elektronikus aláírást előállító eszközökkel szemben támasztott követelményeknek.

E követelményeket részletesen sorolja fel a II. függelék. Itt elégségesnek látszik ezek rövid, lényeges ismérvekre szorítkozó jellemzése, illetve indoklása.

A hitelesítés szolgáltató (CSP) szerepe és a minősített tanúsítványok:

A nyilvános kulcsú titkosításon alapuló digitális aláírások használatához egy privát és egy nyilvános kulcs szükséges. E két kulcsot együtt *kulcspár*-nak nevezzük. Az egyszerű digitális aláírás esetén a kulcspár létrehozását akár a kulcs tulajdonosa is elvégezheti. A hitelességet biztosító előírások betartatása végett azonban szükség van un. *hitelesítés szolgáltatók (CSP)* működésére. Ezek szervezetek kulcspárokat és hozzájuk tartozó tanúsítványokat bocsátanak ki. Minden kulcspárhoz egy tanúsítvány tartozik, mely a kulcspár tulajdonosának azonosítására szolgál.
A minősített tanúsítvány garanciális különbségének lényege, hogy

[36] I.m. 272.oldal [529] "Hamis az az okirat, amely nem a benne feltüntetett kiállítótól származik."
[37] I.m. 272. oldal [529] "Hamisított iratról beszélünk akkor, ha az okirat valódi, de szövegét megváltoztatták."

- több adatot tartalmaz a kulcs jogosultjáról (tulajdonosáról),
- az adatokat megbízható forrásból szerzik be,
- a tanúsítvány kiállítója magasabb szakmai előírások betartására köteles.

A biztonságos aláírást létrehozó eszköz

E minősített eljárást jelentő szabályok azt a célt szolgálják, hogy külső hatások és harmadik személyek nem legyenek képesek befolyásolni az aláírás folyamatát. Ennek biztosítás a legmegfelelőbben technikai szabályok betartatásával érhető el.

Amennyiben tehát egy elektronikus okiratot *minősített elektronikus aláírással* látnak el, álláspontom szerint eleget tesz azoknak a feltételeknek, melyeket a Pp. jelenlegi szabályozása a papír-alapú dokumentumokkal kapcsolatban előír. Ebben az esetben tehát, a minősített elektronikus aláírás alkalmazását feltételezve, a teljes bizonyító erejű magánokiratokkal egy szintre, azonos bizonyító erőt szerezve beszélhetünk az elektronikus iratok diszkriminációjának felszámolásáról.

Tekintettel arra, hogy az elektronikus hitelesítés a közigazgatás területén is fontos szerepet képes játszani, ki kell térni a *teljes bizonyító erejű közokirat* fogalmára. A Pp. a következőket mondja ki ezzel kapcsolatban[38]:

> **„195. § (1) Az olyan okirat, amelyet bíróság, közjegyző vagy más hatóság, illetve közigazgatási szerv ügykörén belül a megszabott alakban állított ki, mint közokirat teljesen bizonyítja a benne foglalt intézkedést vagy határozatot, továbbá az okirattal tanúsított adatok és tények valóságát, úgyszintén az okiratban foglalt nyilatkozat megtételét, valamint annak idejét és módját. Ugyanilyen bizonyító ereje van az olyan okiratnak is, amelyet más jogszabály közokiratnak nyilvánít."**

Látható, hogy a fenti meghatározás az okirat létrehozásának körülményeit, a hitelességet biztosító szervek közreműködését tekinti olyan biztosítéknak, melyek megléte esetén
- teljes bizonyító erő (ellenkező bizonyításig az okiratban foglalt intézkedés, adat, nyilatkozat valódisága), és
- a valódiság vélelme (az okirat nem hamis és nem hamisított)
kapcsolódik az okirathoz.

Ezek megfelelnek a teljes bizonyító erejű okiratokról mondottaknak, így ahhoz, hogy ezeknek a feltételeknek az elektronikus „közokirat" irat is megfeleljen, értelem szerűen a *minősített elektronikus aláírás* alkalmazása indokolt. Tehát az elektronikus irat akkor válik teljes bizonyító erejű közokirattá, ha azt a Pp. 195.§-ban megjelölt szervek eljárásuk során *minősített elektronikus aláírással* látják azt el.

[38] 1952. évi III. tv. 195. §. Ld. továbbá Kengyel i.m. 271-272. oldal.

Bibliográfia

A felhasznált szakirodalom és normaszövegek

1. **Thomas J. Smedinghoff - Ruth Hill Bro: Electronic Signature Legislation**
Megjelent: Findlaw oldalak, http://profs.findlaw.com/signatures/

2. **Sík Zoltán: Digitális aláírás, elektronikus aláírás**
Megjelent: Magyar Távközlés, 2000/4. http://puskas.matav.hu/0009/digitalismt2.html

3. **Philip Zimmermann: Pretty Good Privacy**
fordította Czakó Krisztián. Magyar Elektronikus Könyvtár,
http://www.mek.iif.hu/porta/szint/muszaki/szamtech/wan/biztonsa/pgp.hun

4. **Valérie Sédallian: Preuve et signature électronique**
http://www.juriscom.net/chronique/2/fr0509.htm

5. **Kengyel Miklós, Magyar polgári eljárásjog**,
Osiris Kiadó, 1998, Budapest

6. Az elektronikus aláírás közösségi kereteiről szóló **1999/93. EK irányelv**

7. **B.P. Aalberts & S. van der Hof, Digital Signature Blindness**, Analysis of legislative approaches toward electronic authentication, November 1999,
http://cwis.kub.nl/~frw/people/hof/ds-fr.htm

8. **Informations- und Kommunikationsdienste-Gesetz**
http://www.iid.de/rahmen/iukdgebt.html

9. **CA Working Group of the Electronic Commerce Promotion Council of Japan**
szabványai
http://ecom.ecom.or.jp/ecom_e/cag-smry.htm

10. **Az 1997. november 10-én kelt 513. sz. dekrétum (Olaszország)**
http://www.aipa.it/english[4/law[3/pdecree51397.asp

11. **PKIX Working Group of the Internet Engineering Task Force (IETF)**
dokumentumai

http://www.ietf.org

12. **Internet Law & Policy Forum (ILPF)** dokumentumai
http://www.ilpf.org

13. **Electronic Commerce Platform in the Netherlands** (ECP.NL) dokumentumai
http://www.ecp.nl

14. **Australian Internet Industry Association** (IIA) egyes dokumentumai
http://www.iia.net.au/

15. **40/1998. III.6. Korm. Rendelet** A minisztériumok és az országos hatáskörű államigazgatási szervek iratkezelési mintaszabályzatáról

16. **Dr. Nemetz Tibor: Kriptográfiai mondanivaló újonnan beinduló adatvédelmi rendszerek szervezői számára**
Magyar elektronikus könyvtár,
http://www.mek.iif.hu/porta/szint/termesz/matemat/nemetz.hun

17. **Pásztor Miklós: Nyilvános kulcsú titkosítás, digitális aláírás akadémiai hálózatokban**
Magyar Elektronikus Könyvtár,
http://www.mek.iif.hu/porta/szint/muszaki/szamtech/wan/netwshop/netwsh97/pasztor.hun

18. **Simon Géza: Authentikáció a World Wide Weben**
Magyar Elektronikus Könyvtár,
http://www.mek.iif.hu/porta/szint/muszaki/szamtech/wan/netwshop/netwsh98/simon/simon.mek

Alapfogalmak

Az alábbi fogalmak a feldolgozott terület sajátos terminológiájához tartoznak, ezért ismeretük nélkülözhetetlen.

CA, Certification Authority:

olyan szakosodott szervezet vagy cég, amely tanúsítványokat adhat ki kliensek és szerverek számára, vagy akár megfelelő jogosítvánnyal rendelkező más CA alközpontok számára

Elektronikus aláírás:

elektronikus formában tárolt adat, amely hozzá van kapcsolva, vagy logikailag hozzá van rendelve más elektronikus adathoz, amely így egy azonosítási eljárást alkot.

Fokozott biztonságú elektronikus aláírás:

elektronikus aláírás, amely megfelel az alábbi követelményeknek:
- egyedülállóan köthető az aláíró félhez;
- alkalmas az aláíró fél azonosítására;
- olyan eszközökkel hozták létre, amelyek kizárólag az aláíró fél befolyása alatt állnak; és
- olyan módon van hozzákapcsolva az adatállományhoz, hogy minden későbbi adatmódosítás érzékelhető.

Minősített elektronikus aláírás:

elektronikus aláírás, amely megfelel a minőségi elektronikus aláírással, a minősített tanúsítványokkal és a biztonságos elektronikus aláírást előállító eszközökkel szemben támasztott követelményeknek.

Digitális aláírás:

olyan titkosított karaktersorozat, melyet igen nagy valószínűséggel csak az aláíró kódolhatott, és ez magából a kódolásból következik. Keltezést (dátumot, pontos időpontot), sorszámot, a küldött üzenetből képezett ellenőrző összeget tartalmazhat.

Aláíró fél:

aláírás létrehozó eszközzel rendelkező személy, aki saját maga, vagy egy általa képviselt természetes vagy jogi személy nevében jár el.

Aláírás létrehozó adat:

egyedi adat, mint például a jelszavak vagy magánkulcsok, amelyeket az aláíró fél az elektronikus aláírás létrehozásához használ.

Aláírás létrehozó eszköz:

konfigurált hardware vagy software, amelyek az aláírás létrehozó adatot reprezentálják.

Biztonságos aláírás létrehozó eszköz:

olyan aláírás létrehozó eszköz, amely megfelel a II. függelék 2. pontjában felsorolt követelményeknek.

Aláírás ellenőrző adat:

adatok, mint például kódok, vagy nyilvános kulcsok, amelyet az elektronikus aláírás ellenőrzésének céljára használnak.

Aláírás ellenőrző eszköz:

konfigurált hardware vagy software, amelyek az aláírás ellenőrző adatot reprezentálják.

Elektronikus irat:

tág értelemben minden elektronikus formában tárolt adat.

Minősített tanúsítvány:

tanúsítvány, amely kielégíti a IV. függelékben 1. pontjában megjelölt követelményeket, és amelyet olyan hitelesítés-szolgáltató biztosít, amely megfelel a 3. pontban meghatározott követelményeknek.

Hitelesítés szolgáltató:

természetes vagy jogi személy, amely tanúsítványokat bocsát ki, illetve más, elektronikus aláírásokkal kapcsolatos szolgáltatásokat nyújt.

Elektronikus aláírás termék:

hardware vagy software eszközök, amelyeket egy hitelesítés-szolgáltató elektronikus aláírási szolgáltatások nyújtásához kíván felhasználni, illetve amelyek elektronikus aláírások létrehozására vagy ellenőrzésére szolgálnak.

Magánkulcs:

nyilvános kulcsú infrastruktúra esetében, az aláíró által kizárólagosan használt aláírás létrehozó eszköz.

Nyilvános kulcs:

nyilvános kulcsú infrastruktúra esetében, az aláírás ellenőrző adat szerepét tölti be.

Nyilvános kulcsú kriptográfia:

kriptográfiai rendszer, amelynek a résztvevői közös algoritmust használnak rejtjelezésre, és az algoritmusnak két kulcsa van. Ezek egyikét (nyilvános kulcs) nevükkel együtt nyilvánosságra hozzák, ezzel történik a kódolás. A másikat titokban tartják (titkos kulcs), ezzel történik a dekódolás.

Nyilvános kulcsú infrastruktúra:

az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére szolgáló infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.

Tanúsítvány:

egy használó nevét, nyilvános kulcsát, a kulcs érvényességi idejét rögzítő adatsor, amelyet egy CA a saját titkos kulcsával aláír.

Címtár szolgáltatás:

szolgáltatás, amely az aláírás ellenőrző adatok megfelelő módon történő automatikus hozzáférését biztosítja.

Visszavonás címtár szolgáltatás:

szolgáltatás, amely a már nem érvényben lévő aláírás ellenőrző adatok megfelelő módon történő automatikus hozzáférését biztosítja.

Időbélyegző:

a dokumentumhoz - hitelesítés-szolgáltató által - hozzárendelt időadat, amely egyértelműen és megbízhatóan jelzi a dokumentum elektronikus aláírásának időpontját, valamint azt, hogy az adott időpillanatban az elektronikus irat milyen tartalommal bírt.

Hash algoritmus:

olyan transzformáció, amely egy meghatározott szövegből egy digitális jelsorozatot állít elő. Tulajdonsága, hogy gyakorlatilag lehetetlen eltérő szövegből azonos digitális lenyomatot készíteni. A szöveg egyetlen bitjének megváltoztatása a lenyomat nagymérvű megváltoztatását eredményezi. Ismertebb Hash algoritmusok: MD5, SHA, CRC.

I. számú függelék

A Hash algoritmus szerepe és a digitális aláírás menete

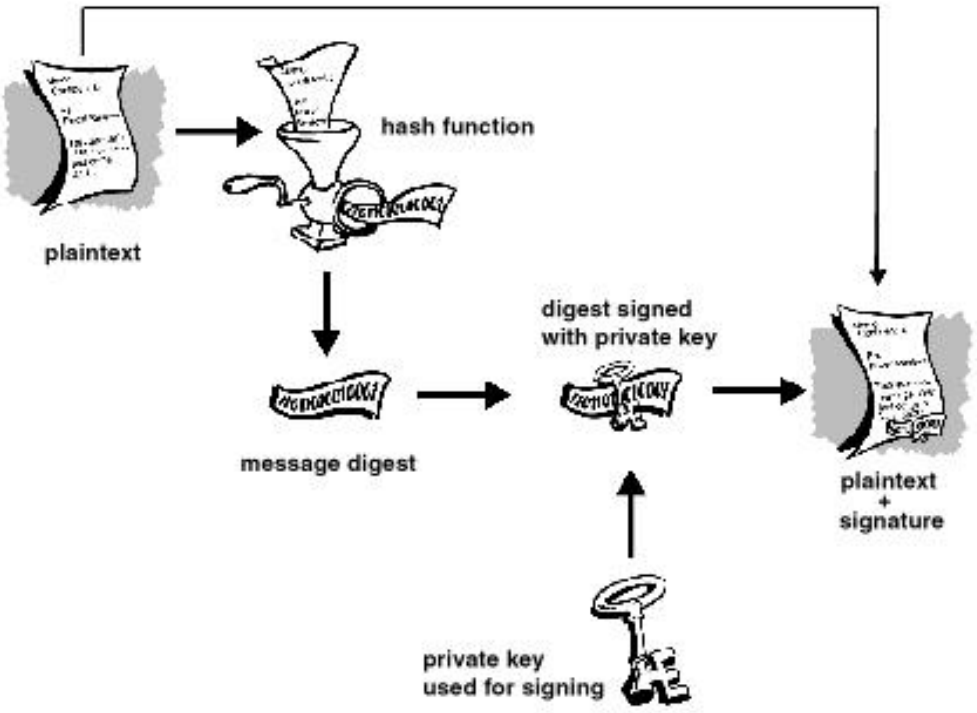


Figure 1-7. Secure digital signatures

(eredeti szöveg)

(sűrítmény)

(eredeti szöveg + aláírás)

(az aláíráshoz használt privát kulcs)

A digitális aláírás és ellenőrzés folyamata

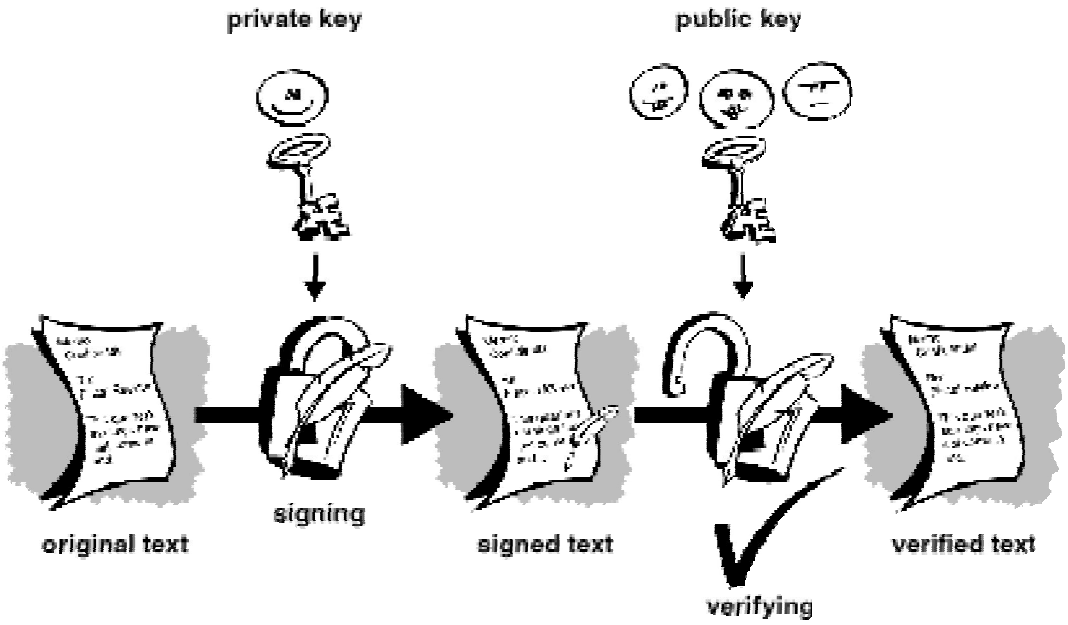
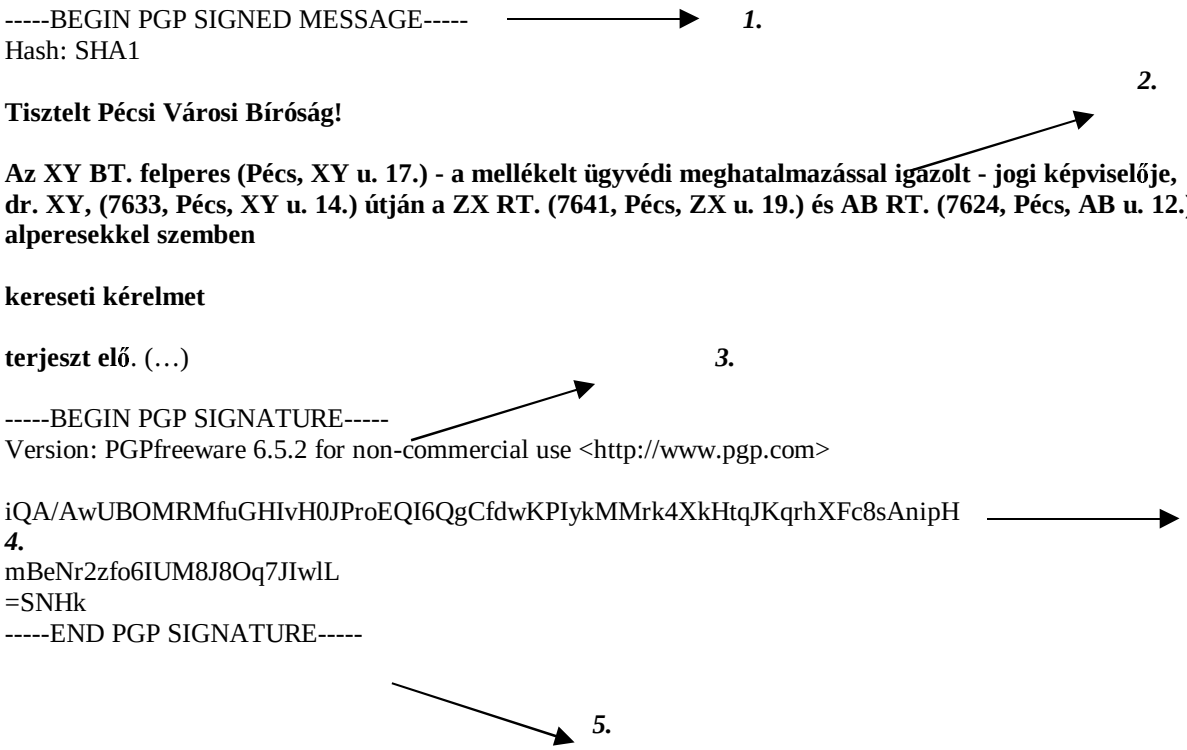


Figure 1-6. Simple digital signatures

privát kulcs nyilvános kulcs

Eredeti szöveg → aláírás → aláírt szöveg → ellenőrzés → ellenőrzött szöveg

Egy digitálisan aláírt dokumentum (dokumentumrészlet).



1. Az aláírt dokumentum kezdetének jelölése, alatta az alkalmazott Hash eljárás megnevezése.

2. Az aláírt dokumentum.

3. A digitális aláírás (a sűrítmény) kezdete.

4

5 4. A sűrítmény.

5. A digitális aláírás végének jelölése.

Az alkalmazott software a PGP 6.5.2. A megjelenési forma más software használata esetén ettől eltérő lehet, itt azonban jól szemléltethetőek a leglényegesebb elemek.

II. számú függelék[39]

1. A minősített tanúsítványokkal kapcsolatos követelmények

A minősített tanúsítványnak tartalmaznia kell
- annak jelölését, hogy a tanúsítványt, mint minősített tanúsítványt adták ki;
- a kiállító hitelesítés-szolgáltató azonosítását és alapításának országát;
- a kulcstulajdonos megnevezését, vagy a tulajdonos álnevét. Ez utóbbi tényt külön jelölni kell;
- az aláíró speciális megjelölését, ha rendelkezik a tanúsítvány kiállítása céljának megfelelő megjelöléssel;
- az aláírás ellenőrző adatot, amely megfelel az aláíró aláírás létrehozó adatának;
- a tanúsítvány érvényességének kezdő- és végső időpontját;
- a tanúsítvány egyedi azonosító kódját;
- a hitelesítés-szolgáltató minőségi elektronikus aláírását;
- a tanúsítvány felhasználási területének korlátozását, ha van ilyen;
- a tranzakció értékének korlátozását, amelyre a tanúsítvány használható, amennyiben van ilyen.

2. A biztonságos aláírás létrehozó eszközzel kapcsolatos követelmények

a, A biztonságos aláírás létrehozó eszközöknek megfelelő technikai és eljárási módszerekkel biztosítaniuk kell:
- az aláírás generálásához használt aláírás létrehozó adat gyakorlatilag csak egyszer fordul elő és a titkossága - ésszerűen biztosított;
- az aláírás generálásához használt aláírás létrehozó adat megfelelően védett a visszafejtéssel szemben és az aláírás nem hamisítható a rendelkezésre álló technikai lehetőségekhez képest;
- az aláírás generálásához használt aláírás létrehozó adatot jogos tulajdonosa megbízhatóan védheti mások használata ellen;

b, A biztonságos aláírás létrehozó eszközök nem változtathatják meg az aláírásra szánt adatot, és nem akadályozhatják meg az ilyen adat aláírónak történő megmutatását az aláírási folyamatot megelőzően.

3. A minősített tanúsítványokat kiadó hitelesítés-szolgáltatókkal kapcsolatos követelmények

A hitelesítés-szolgáltatók kötelességei:

a, a szolgáltatás nyújtásához szükséges megbízhatóságának bizonyítása;

b, gyors és biztonságos címtár szolgáltatás működésének biztosítása, és biztonságos, és azonnal rendelkezésre álló visszavonás címtár szolgáltatás működésének biztosítása;

c, annak biztosítása, hogy a tanúsítvány kiadásának vagy visszavonásának dátuma és időpontja pontosan meghatározható legyen;

d, megfelelő eszközökkel köteles ellenőrizni annak a személynek az azonosságát, és - ha ilyennel rendelkezik - specifikus jellemzőit, aki részére a minősített tanúsítványt kiállítja;

e, olyan alkalmazottak foglakoztatása, akik megfelelő szakértelemmel, gyakorlattal és a szolgáltatással kapcsolatos végzettséggel rendelkeznek, különösen vezetői szinten. Elengedhetetlen a hozzáértés az elektronikus aláírás technológiájával kapcsolatban, megfelelő ismeretek birtoklása a biztonsági eljárásokban, továbbá olyan adminisztratív és igazgatási eljárások alkalmazása, amelyek összhangban vannak az elfogadott szabványokkal;

f, megbízható rendszerek és elektronikus aláírás termékek használata, amelyek megfelelő védettséggel rendelkeznek módosítás ellen, és amelyek biztosítják a technikai és kriptográfiai biztonságot az eljárások során;

g, intézkedéseket kell tenni a tanúsítványok hamisítása ellen, és abban az esetben, amikor a hitelesítés-szolgáltató készíti a magánkulcsot biztosítani kell a folyamat bizalmasságát;

h, megfelelő pénzügyi források biztosítása a törvényben lefektetett követelmények teljesítése érdekében, különösen tekintve a károkozási felelősség kockázatának elviselésére, például megfelelő biztosítások alkalmazásával;

i, az összes lényeges, a minősített tanúsítványokkal kapcsolatos információ tárolása megfelelő időtartamra, különös tekintettel arra, hogy a tanúsítványok jogi eljárásokban bizonyítékként szerepelhetnek. Ez az információtárolás történhet elektronikusan is;

---

[39] Forrás: KHVM Digitális Aláírás Munkacsoport dokumentumai: *http://www.dbassoc.hu/khvmea/khvmeas.html*.

j, a hitelesítés-szolgáltató kulcskezelési szolgáltatását igénybevevő személy aláírás létrehozó adatait nem tárolhatja, és nem másolhatja a szolgáltató;

k, a szolgáltatást igénybe venni kívánó személyt még a szerződéses kapcsolat létrejötte előtt megfelelő módon tájékoztatni kell a szolgáltatás igénybevételének pontos feltételeiről és kikötéseiről, beleértve a használat korlátozásait, az önkéntes minősítést, reklamációs eljárásokat, a vitás kérdések elintézésének módjait. Ezt az információt írásban, akár elektronikus formában, érthető nyelvezettel kell megadni. Lényeges részeit ennek az információnak kérésre elérhetővé kell tenni a kibocsátott tanúsítványban bízó harmadik fél számára is;

l, Megbízható rendszerekben kell tárolni a tanúsítványokat, olyan ellenőrizhető módon, hogy

- csak a feljogosított személyek készíthetnek új bejegyzéseket és végezhetnek módosításokat,
- az információ hitelessége ellenőrizhető legyen,
- a tanúsítványok nyilvánosságra hozatala csak a tulajdonos hozzájárulásával történhet; és
- bármilyen technikai változás, amely ezen biztonsági követelményeket veszélyezteti nyilvánvaló kell legyen a kezelő számára.