INFORMÁCIÓS TÁRSADALOMÉRT ALAPÍTVÁNY BIZTONSÁGMENEDZSMENT KUTATÓCSOPORT

AZ ELEKTRONIKUS ALÁÍRÁS KÖTELEZETTSÉG-VÁLLALÁSI SZINTJEI ÉS KÖVETKEZMÉNYEI

AJÁNLÁS

1.2

OID: 1.3.6.1.4.1.29250.3.2.1.2

Erdősi Péter Máté, CISA
NJSZT Információrendszer-ellenőrzési szakértő
Elektronikus aláírással kapcsolatos szolgáltatási szakértő

2008

A kutatómunkát tanácsaikkal, észrevételeikkel segítették a Kutatócsoport tagjai:

Rajzó Gergő biztonsági szakértő, Budapest Bank Zrt

Dr. Székely Iván egyetemi docens, adatvédelmi szakértő

Valádi Zoltán informatikai biztonsági szakértő, a Bankkártya Zrt. biztonsági vezetője

Vasvári György CISM, informatikai biztonsági szakértő (a Kutatócsoport vezetője)

Tartalomjegyzék

1 A probléma.....4
1.1 A hitelesség hiánya.....4
1.2 Alkalmazási kérdések.....6
1.3 Az elektronikus aláírási szabályzat.....8
1.4 Elektronikus ügyintézési formák.....9
2 Szabványos elektronikus aláírások.....12
2.1 Az elektronikus aláírás típusai.....12
3 A jelenlegi megoldások.....15
3.1 Törvényi szabályozás és joghatások.....15
3.2 Hitelesítés-szolgáltatók tanúsítványaihoz kapcsolódó szintek.....19
3.3 Honnan szerezzük meg a tudást az elektronikus aláírás használatához?.....23
4 Következtetés.....25
5 Irodalomjegyzék.....28

1 A probléma

Ennek az ajánlásnak az a célja, hogy közelebb vigye az olvasót az elektronikus aláírás használatához szükséges tudás megszerzéséhez és megszerzésének miértjéhez, átfogóan ismertesse a terület részleteit – de nem részletekbe menően -, és iránymutatást adjon az érdeklődőknek arra nézve, hogy a probléma megoldásában hol lehet elindulni és hol lehet további tájékozódási pontokat találni az elektronikus aláírás kétségkívül széles, matematikai és technológiai részletekkel is átszőtt területein. A szerző véleménye – amely több éves elektronikus aláírással kapcsolatos szolgáltatási szakértői tevékenységen alapul – azonban az, hogy az elektronikus aláírás önmagában nemcsak műszaki-technológiai mutatvány, hanem vastagon kell hozzá szervezés, szabályozás és oktatás is. Az alábbiak megkísérlik mindezt alátámasztani. Kiemelten foglalkozunk továbbá az elektronikus aláírások tranzakciós értékhatáraival és a szolgáltatói felelősségvállalások mértékével, mint az elektronikus aláírás használatának lényeges és fontos garanciális elemeivel, illetve az ezekből adódó következményekkel, melyek első olvasatra talán nem teljesen explicit módon jelennek meg a digitális univerzumban.

1.1 A hitelesség hiánya

A felgyorsult és megnövekedett információ áramlásban - a nagy számok törvénye alapján is - egyre valószínűbb, hogy sokkal nagyobb számban jelennek meg olyan nem hiteles elemek, melyek a folyamatokon végigmenve már hitelesnek látszó eredményt produkálnak. Azonban a kiindulási alap hitelessége nélkül a végeredmény sem lehet hiteles, de esetenként jogtalan előnyökhöz juttathatja a küldőjét. A “személyazonosság-lopás”, “identity-theft” előtérbe helyezi az elektronikus személyazonosság kérdését, lévén azt – megfelelő használat esetén – nehezebb ellopni, hasonlatosan egy bankkártához és PIN-kódjához. A legfontosabb különbség egy bankkártya és egy aláírás-létrehozó eszköz között abban áll, hogy – műszakilag megfelelő algoritmusok használata esetén – az eszköz ellopásával sem lehet azt **PIN-kód nélkül** használni – ellentétben egyes bankkártyákkal.

Az internetes portálokon szinte nap mint nap megjelennek hírek a kiberbűnözés területéről, adathalászatról, kiberháborúról, on-line csalásokról, és más egyéb rosszindulatú

cselekményekről. A megtévesztés ellen az elektronikus aláírás használata sokat segíthet – habár természetesen meg lehet próbálkozni a sikeres megtévesztéssel aláírási környezetben is. De abban jónéhány szakértő egyetért, hogy a ma használatos bűncselekmények közül soknak megnehezítené a végrehajtását, ha használnának kriptográfiai védelmet, vagy ezen belül kriptográfiát alkalmazó elektronikus aláírást. Egyre több tanúsított eszközzel találkozhatunk az interneten, vagyis egyre több cég veszi a fáradságot, és megjelöli a saját eszközeit – azaz kinyilvánítja azt, hogy ő az eszköz birtokosa. Ennek nyilván nagyobb tranzakciók végrehajtásában közreműködő eszközök használatakor nagyobb jelentősége van (pl. internet-banking), de ma már minden, a biztonságra is kicsit odafigyelő vállalat honlapja biztonságos (https) módon érhető el.

A közelmúltbeli kapcsolódó események – [1] szándékosan választottunk könnyed témát itt – is megerősítették tehát, hogy elérkezett az idő az e-mailes üzenetek hitelességének is a biztosítására, mivel az e-mailek annyira beépültek már a mindennapjainkba, hogy automatikusan, látszatra elfogadjuk azok hitelességét is, kisebb-nagyobb kötelezettség-vállalásoknál egyaránt. A hitelesség azonban nem minden esetben áll fenn, és a biztonságtechnikai cégek felméréseit elemezve a statisztika romló képet mutat (terjedőben a phishing – adathalászat, mivel egyre több anyagi előnyhöz lehet jutni az Internet által). Másrészről szinte bizonyosak lehetünk benne, hogy mindig a legfontosabb, jelentős kötelezettséggel járó e-maileknél lesz a probléma. A napról-napra megjelenő példák megmutatták, hogy bizonyos esetekben súlyos jogi következményekkel is szembe kell néznie annak, aki nem hitelesített információt fogad el hitelesnek.

De nézzük meg, hogy mi lehet az oka annak, hogy nem hiteles levelek egyáltalán létezhetnek a levelező-rendszereinkben. A ma általánosan használtos internet-levelezést leggyakrabban az SMTP (Simple Mail Transfer Protocol) valósítja meg, melyet az RFC 821 (Request for Comments) [2] ír le, “de facto” szabványként. Az első leírás 1982-ben készült, több, mint 25 évvel ezelőtt. A levél (e-mail) úgy jön létre, hogy a felhasználó a levelező programja segítségével előállítja azt a formátumot, amit az SMTP-szerver fogadni képes, és átküld a fogadó oldali SMTP-szerverre.

Az RFC 821 a 3.1 fejezetében részletesen ismerteti azt a három parancsot, melyet a levél küldésekor használni kell:

1).MAIL <SP> FROM:<reverse-path> <CRLF>

2).RCPT <SP> TO:<forward-path> <CRLF>

3).DATA <CRLF>

Ennek a három parancsnak a segítségével átverve a – nem megfelelően konfigurált – levelező szervereket, elméletileg bárki nevében (<reverse-path>) lehet nem hiteles feladóként bárkinek (<forward-path>) hamisított levelet küldeni. A levelező szerverek természetesen védekezhetnek ezek ellen. Az összes gyanús levelező szerver kiszűrése és tiltó listára rakása azonban nem feltétlenül járható út. Könnyen belátható a fentiek alapján tehát, hogy minden körülmények között nem lehetséges hitelesnek elfogadni az e-mail-eket, hiszen sajnos fennáll az egyszerű hamisíthatóság veszélye. Ebből következik, hogy kötelezettség-vállalások tételére sem javasolt ma már kizárólag normál e-mailekre hagyatkozni. Ezért javasolt a levelek hitelességéről a megfelelő mértékben gondoskodni, a kárkövetkezmények elkerülése érdekében.

1.2 Alkalmazási kérdések

A hitelesség kérdése tehát nem újkeletű, több száz év óta tudjuk, hogy bizonyos üzenetek, ígéretek, tranzakciók, kötelezettség-vállalások hitelességéről nem árt meggyőződni, különben könnyen előfordulhat, hogy “se pénz, se posztó”[3]. Az elektronikus tranzakciók hitelessége sem annyira újdonság már 2008-ban, hiszen több, mint 25 éve ismeretesek a digitális aláírás alapjául szolgáló aszimmetrikus kriptográfiai algoritmusok[1] is - sőt egyesek már meg is gyengültek [4]. Gyakorlati alkalmazása a PGP (Pretty Good Privacy) és a PKI (Public Key Infrastructure – nyilvános kulcsú infrastruktúra) rendszerek, azon belül is a hitelesítés-szolgáltatók megjelenésével széles körben is lehetséges, mégis úgy tűnik, hogy nehezen akar fejlődni az alkalmazási kör, és lassan szélesedik a felhasználói tábor is.

Megfogalmazódnak olyan kérdések a területet jól ismerőkben is, hogy:

- Kell-e ez nekünk?

1 Aszimmetrikus egy algoritmus, ha a rejtjelező és megfejtő kulcs különbözik egymástól.

- Nem túlságosan bonyolult ez nekünk?
- Elég biztonságos a használata?

Ha komolyan elgondolkodunk a kérdéseken, és válaszokat is akarunk keresni rájuk, előbb-utóbb be kell látnunk azt, hogy ez a kérdés nem intézhető el egy egyszerű “igen”-nel, vagy “nem”-mel. Ha ezt tennénk, nagy valószínűséggel beleesnénk az általános igazság keresésének hiábavalóságába, ami azonban a “tudatunktól független, objektív valósággá kövült állítások” hangoztatásával, vagy tagadásával lehet egyenértékű, és ez semmi esetre sem nevezhető tudományos szempontból célszerűnek. A követendő megoldás az igazság relativizálása [5].

Milyen következtetés vonható le ebből számunkra? Az, hogy a továbblépéshez szükséges a fenti kérdésekben megfogalmazott igazságok (és azok tagadásainak) relativizálása. Általánosságban mind a támogatók, mind az ellenzők találnak életszerű példát arra, hogy miért nekik van igazuk. Ebből azonnal következik, hogy a kérdés differenciálható, szintekre bontható, és elkülöníthetőek olyan esetek, melyekben igazolható, és amelyekben lehetőségként alkalmazható, ellenjavallott, vagy akár megtiltható az elektronikus hitelesség használata. A szintek összegzésével megkapjuk azt a teret, amiben a kérdést feltettük. A fenti kérdésekre adott válaszok már nem gondolati kövületek lesznek, hanem egy rendszerben értelmezett tételek vagy azok tagadásai, konkrét bizonyítással vagy bizonyítási lehetőséggel együtt.

Ha differenciáljuk az elektronikus hitelesség alkalmazási lehetőségeit, olyan kérdésekben kell gondolkodnunk, mint:

- hol használjuk? (és hol NEM)
- mikor használjuk? (és mikor NEM)
- mire használjuk? (és mire NEM)
- mit használunk? (és mit NEM)
- kivel használjuk? (és kivel NEM)
- hogyan használjuk? (és hogyan NEM)

A kérdésekre – a teljesség igényével – adott válaszok alapján kirajzolódhat előttünk az elektronikus kötelezettség-vállalások alkalmazásának feltétel-rendszere, az adott felhasználás aspektusából nézve. Ez magában foglalhatja a jogszabályi környezetet, a szervezeti és belső szabályozási feltételeket, a szerződéses jogviszonyok klauzuláit, és a technológiai feltétel-rendszereket egyaránt.

Gyakran szembesülünk azzal a kérdéssel, hogy vajon ha ezt használjuk, nem tudnak-e majd *mindent* rólunk megszerezni? A válasz az, hogy nem könnyebben, mint ma, a rengeteg külső és belső térfigyelő kamera, elektronikus és papír alapú nyomok (tranzakcók, e-mailek, mobil-telefonálás, böngészés, sütik, regisztrációk, konferencia-előadások, e-ügyintézés, szolgáltatás igénybe vételekor odaadott igazolvány-másolatok, egyéb elektronikus nyomaink) megfigyelésével. Másrészről a titkos kulcsunkhoz tartozó, de csak a nyilvános kulcsot tartalmazó tanúsítványunk élettartama korlátozott (minősített esetben legfeljebb két év), ami után új kulcsot kell kapnunk és hozzá új tanúsítványt. Ennek következtében a Szerző véleménye szerint a régi aláírásaink ellenőrizhetősége normál esetben megszűnik (illetve a Szolgáltatónál a tanúsítvány- és regisztrációs adatok őrzési idejéig korlátozottan fennmarad), csak komplex és archív esetben van erre később lehetőség – ahogyan a továbbiakban a szabványos aláírások erre rávilágítanak. Harmadrészt egyidőben több tanúsítványunk is lehet, és ezeket összekapcsolni csak a regisztrációkor megadott adatok ismeretében lehetséges 100%-os bizonyossággal. Ide kapcsolódik, hogy a tanúsítványban szereplő adatok egyes esetekben alkalmasak az olvasó számára az aláíró egyedi azonosítására, de nem általánosan (Melyik Tóth Béla?). Ha a Szolgáltatótól kérjük régi tanúsítványaink közzétételének megszüntetését, az aláírók későbbi azonosítása a nyilvánosság számára nem lehetséges a továbbiakban.

1.3 Az elektronikus aláírási szabályzat

A fentiek alapján tehát az elektronikus aláírás alkalmazása számos kérdést felvethet, melyekre explicit válaszokat kell megfogalmazni. A válaszoknak mind az aláírás készítői, mind pedig az elfogadói számára hozzáférhetőnek kell lennie. Erre célra szolgál tipikusan az Elektronikus Aláírási Szabályzat (EASZ), angolul Electronic Signature Policy. Az EASZ leírja a fenti kérdésekre adott válaszokat szabványos struktúrában.

Erre találhatunk nagyon jó példát a Pénzügyi Szervezetek Állami Felügyeleténél (PSZÁF), az elektronikus közzétételek oldalon [9]. A szabályzat az alábbi fő fejezetekből áll (kirészlezetve az aláírással kapcsolatos rendelkezéseket):

1. Általános rendelkezések
2. Az elektronikus aláírással kapcsolatos érvényesítési rendelkezések
   a) Az aláíró tanúsítványra vonatkozó megkötések
   b) Az érvényesítő adatokra vonatkozó szabályok
   c) Az aláírás létrehozójára vonatkozó szabályok
   d) A kötelezettségvállalás elfogadott típusai
   e) A hitelesítés szolgáltatók használatára vonatkozó szabályok
   f) Az időbélyegzésre vonatkozó megkötések
   g) Az aláírás elfogadójára vonatkozó szabályok
   h) A végfelhasználói tanúsítványokra vonatkozó kivárási idő
   i) A használható aláíró algoritmusokra vonatkozó szabályok
   j) Az elektronikusan aláírt adatszolgáltatás értelmezése, ellenőrzése
3. Az adatszolgáltatásra/bejelentésre kötelezett bejelentkezési kötelezettsége
4. Vitás esetek rendezése

A fentebb feltett kérdésekre itt válaszokat kap minden érintett fél. Megemlítjük továbbá, hogy az elektronikus aláírási szabályzat kidolgozásakor érdemes figyelembe venni az RFC 3125-öt is [10] és az ETSI TR 102 038-at is [11].

1.4 Elektronikus ügyintézési formák

Tipikus mai prioritás az elektronikus ügyintézési formák megjelenése. De vajon mi az Európai Unió véleménye a dologról? Idézzük az EU i2010 eGovernment cselekvési terv dokumentumból [6] az alábbiakat:

“A közszféra nyitottságában és hatékonyságában, illetve az elektronikus kormányzatra való felkészültségben élen járó országok az elsők között találhatók a gazdasági teljesítményben és versenyképességben is. A nemzeti versenyképesség, az erős innovációs képesség és a közigazgatás minősége között fennálló szoros kapcsolat azt jelzi, hogy a világgazdasági versenyben a jó kormányzás

elengedhetetlen. Az elektronikus kormányzattal a közigazgatás nagyban hozzájárulhat a lisszaboni stratégiához.”

A terv továbbá nagyon jól foglalja össze ennek a területnek a prioritásait is. A cselekvési terv középpontjában öt, az elektronikus kormányzattal összefüggő fő célkitűzés áll, és mindegyikhez 2010-ig elérendő konkrét célok társulnak:

1. **a hátramaradtak felzárkóztatása**: a társadalmi integráció felgyorsítása az elektronikus kormányzaton keresztül, hogy 2010-re minden polgár élvezhesse a megbízható, innovatív szolgáltatásokat és az azokhoz való könnyű hozzáférést;
2. **az eredményesség és a hatékonyság elérése** – a magas felhasználói elégedettség, az átláthatóság és az elszámoltathatóság, valamint az adminisztratív terhek könnyítésének és a hatékonyság növelésének jelentős mértékű elősegítése 2010-ig;
3. **nagy hatóerejű alapszolgáltatások** a polgárok és a vállalkozások javára – 2010-re a közbeszerzések 100%-a elektronikusan is elérhető lesz, és 50%-uk elektronikus úton fog lezajlani; együttműködési megállapodásokat kell kötni a polgároknak szóló további nagy hatóerejű online közszolgáltatásokra is;
4. a legfontosabb összetevők rendszerbe állítása – lehetővé tenni a polgárok és a vállalkozások számára, hogy **a közszolgáltatásokhoz 2010-re kényelmes, biztonságos és interoperábilis, hitelesített hozzáférést élvezhessenek egész Európában**;
5. **a részvétel és a demokratikus döntéshozatal** erősítése – a hatékony közvita és a demokratikus döntéshozatalban való részvétel eszközeinek demonstrációja 2010-re.”

Továbbá ide vonatkoztatható az Európai Parlament és a Tanács 2006/123/EK belső piaci szolgáltatásokról [7] szóló irányelvének (2006. december 12.) 8. cikke is az elektronikus eljárásokról:

„(1) A tagállamok biztosítják, hogy a szolgáltatási tevékenység nyújtására való jogosultsággal, valamint a szolgáltatási tevékenység gyakorlásával kapcsolatos **minden eljárás és alaki követelmény egyszerűen teljesíthető legyen távolról és elektronikus úton** az érintett egyablakos ügyintézési pontoknál és az érintett illetékes hatóságoknál.

(2) Az (1) bekezdés nem alkalmazható a szolgáltatás nyújtásához használt helyiség vagy a szolgáltató által használt eszközök ellenőrzésére, továbbá a szolgáltató vagy felelősséggel rendelkező alkalmazottai képességét vagy személyes képességét érintő fizikai vizsgálatra sem.

(3) A Bizottság a 40. cikk (2) bekezdésében említett eljárással összhangban az információs rendszerek interoperabilitásának és az elektronikus eljárások tagállamok közötti használatának elősegítése érdekében részletes szabályokat fogad el e cikk (1) bekezdése végrehajtására, figyelembe véve a közösségi szinten kialakított közös szabványokat.”

Láthatjuk, hogy az e-demokrácia sem nélkülözheti a hitelességet. A hitelesség pedig elektronikus aláírással biztosítható, az 1999/93 Irányelv [8] 2. cikk (1) pontja szerint:

- “elektronikus aláírás": olyan elektronikus adat, amely más elektronikus adathoz van csatolva, illetve logikailag hozzárendelve, és amely **hitelesítésre** szolgál; illetve angolul:
- "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and **which serve as a method of authentication.**

Fontos információval szolgálhat a tárgyban az Európai Közösségek Bizottságának [15] jelentése, mely az elektronikus aláírásra vonatkozó, már ismertetett 1999/93. EU Irányelv közösségi szintű működéséről fogalmazott meg megállapításokat 2006-ban. Az elektronikus aláírásnak a piacra tett hatásáról idézzük az alábbi bekezdéseket:

„A minősített elektronikus aláírás használata jelentősen elmaradt az előrejelzésektől, a piac jelenleg nem túl fejlett. A felhasználónak jelenleg nincs meg a maga egyetlen tanúsítványa, amellyel iratokat vagy ügyleteket írhat alá a digitális környezetben, ahogy ezt papíron teszi. Ezért a mostani szakaszban még nem lehet értékelni az irányelv belsőpiaci célkitűzését, amely a minősített elektronikus aláírás szabad forgalmára irányul.

A piac fellendülése elsősorban gazdasági okból lassú: a szolgáltatók kevés ösztönzést kapnak arra, hogy többalkalmazásos elektronikus aláírást fejlesszenek ki, ehelyett inkább saját szolgáltatásaikhoz kínálnak megoldásokat, ahogy

ezt például a banki ágazat tette. Ez lassítja az átjárható megoldások kifejlesztésének folyamatát. Hiányoznak alkalmazások, például nincs átfogó megoldás az elektronikus archiválásra, ami szintén akadálya lehet a többcélú elektronikus aláírás kifejlesztésének, mivel ehhez a felhasználóknak és felhasználási területeknek el kellene érniük bizonyos kritikus tömeget.

A jövőben azonban több olyan alkalmazás is lesz, amely a piacot növekedésre készteti.(…)„

2 Szabványos elektronikus aláírások

2.1 Az elektronikus aláírás típusai

Az elektronikus aláírás típusait két szabvány dokumentum, az ETSI TS 101733 (CMS Advanced Electronic Signature - CAdES) és az ETSI TS 101 903 (XML Advanced Electronic Signature - XAdES) alapján járjuk körbe. Mindkét szabvány hasonló aláírás típusokat fogalmaz meg gyakorlatilag, de más leíró nyelvvel.

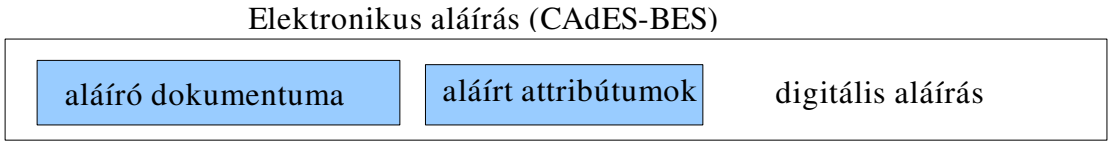
Mind a CAdES, mind pedig a XAdES formátumú elektronikus aláírások kielégítik a 1999/93 Irányelv [8] által az “advanced” vagy “fokozott biztonságú” elektronikus aláírásokkal szemben támasztott definíciókat. Az Irányelv három aláírás-fajtát különböztet meg, különböző joghatások kiváltására alkalmasságuk szempontjából:

1. normál aláírás, melynek nincsenek követelményei a definíció kielégítésén túl, a meg nem tagadhatóság vonatkozik rá

2. fokozott biztonságú aláírás, melynek komolyabb követelményei vannak, és így alkalmas az írásbeliség követelményének kielégítésére. A követelmények az alábbiak:
   a) alkalmas az aláíró azonosítására,
   b) egyedülállóan az aláíróhoz köthető,
   c) olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak, és
   d) a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető.

3. minősített aláírás, mely olyan fokozott biztonságú aláírás, amelyet biztonságos aláírás-létrehozó eszközzel készítettek, és amelyhez minősített tanúsítványt bocsátottak ki, ezért alkalmas a kézírással egyenértékű jogok biztosítására.

Ebből következik, hogy ahol a jogszabályok legalább fokozott biztonságú aláírásokat kötnek ki, ott a fenti két formátumú aláírások biztonsággal használhatóak. A szabványos aláírások közül a normál és az archív aláírásokat ismertetjük, jelen dokumentumban. A szabványban szereplő angol és magyar elnevezéseket egyaránt használjuk, hogy az elektronikus aláíráshoz kapcsolódó kifejezések mindkét nyelven ismerősek lehessenek.

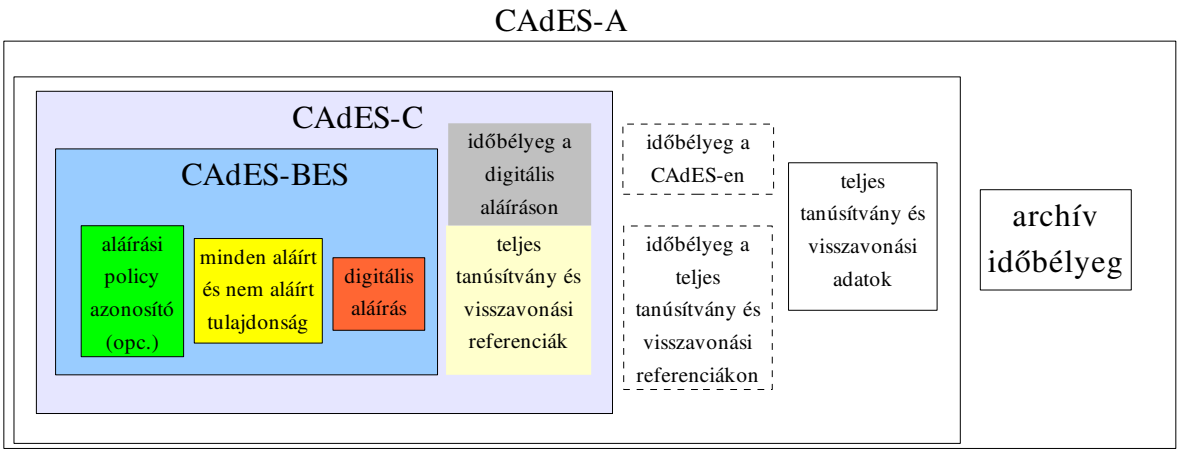


1. ábra: CAdES-BES (Basic Electronic Signature)

A normál CAdES-BES aláírás látható az 1. ábrán. Az aláírás az alábbi komponenseket tartalmazza:

1. **Aláíró dokumentuma (Signer's Document)**: más szóval az aláíró aláírt adatai (ahogy az RFC 3824-ben definiált [12]), azaz tetszőleges adatból, adatokon az aláíró által generált aláírás,
2. **Aláírt attribútumok (Signed Attributes)**: szintén az RFC 3824 [12] által meghatározott kötelezően beszerzendő és az aláíráshoz csatolandó adatok, tipikus példa az adatok kivonatolásához használt algoritmusok azonosítója,
3. **Digitális aláírás (Digital Signature)**: A digitális aláírás készítésének módját itt is az RFC 3824-ben rögzített módon kell elvégezni, minden olyan adaton, amelyik szerepel az aláírásban – tehát az aláírt adatokat és az aláírt atribútumokat egyaránt be kell vonni a digitális aláírásba.

A normál aláírás tartalmazhat még opcionálisan aláírt további adatokat (például időjelet) és opcionálisan aláíratlan adatokat is (például egy másik szekvenciális aláírást). A továbbiakban még vizsgáljuk meg – az ettől kicsit bonyolultabb struktúrájú – archív aláírást is.



2. ábra: CAdES-A (Archive Electronic Signature)

Láthatóan további elemekkel bővült az archív aláírás, melyeket az alábbiakban röviden ismertetünk:

1. **Aláírási Policy azonosítója – opcionális (Signature Policy ID):** az aláírással kapcsolatos szabályokat tartalmazó dokmentum azonosítója (tipikusan OID száma),
2. **Minden aláírt és aláíratlan tulajdonság (All signed and unsigned Attributes):** minden olyan adat, melyet az aláíró az aláírásban felhasznált, akár elhelyezett rajta digitális aláírást, akár nem,
3. **Digitális aláírás (Digital Signature):** a digitális aláírás készítésének módját itt is az RFC 3824-ben rögzített módon kell elvégezni, minden olyan adaton, amelyik szerepel az aláírásban,
4. **Időbélyeg a digitális aláíráson (Timestamp over digital signature)**: a normál aláíráson elhelyezett időbélyeg (aláíró által nem aláírt attribútum), mely a dokumentum adott időpnt előtti létezését bizonyítja,
5. **Teljes tanúsítványi és visszavonási referenciák (Complete certificate and revocation references)**: az aláírás érvényesítési adatainak azonosítói hivatkozás formában (tanúsítvány-ID, visszavonási lista-ID),
6. **Időbélyeg a CAdES-en (Timestamp over CAdES)**: a teljes aláíráson elhelyezett időbélyeg, mely a hiteles időt rendeli az aláíráshoz,
7. **Időbélyeg a teljes referenciákon (Timestamp over complete certificate and revocation references)**: a referenciákon elhelyezett időbélyeg, mely a referenciákhoz rendeli a hiteles időt,

8. **Teljes tanúsítványi és visszavonási értékek (Complete certificate and revocation values)**: az aláírás érvényesítéséhez szükséges adatok (tanúsítványok, visszavonási listák) elhelyezése az aláírásban,
9. **Archív időbélyegzés (Archive Timestamp)**: az aktuális dátum és a kor műszaki színvonalának megfelelő kriptográfiai eljárások használatával lehetővé teszi a hitelesség hosszú távú megőrzését. Az archív időbélyeget szükség szerint – a kriptográfiai eljárások gyengülése esetén – meg kell ismételni az új, megbízhatónak tartott kriptográfiai eljárásokkal.

3 A jelenlegi megoldások

3.1 Törvényi szabályozás és joghatások

1999. december 13.-án az Európai Tanács Irányelvet fogadott el az elektronikus aláírás szabályozásáról [8]. Az Irányelv kötelezte a tagállamokat, hogy legkésőbb 2001. július 19-ig az Irányelv rendelkezéseire figyelemmel szabályozzák az elektronikus aláírások használatát, vagy ha korábban már létezett tagállami szabályozás, akkor teremtsék meg az Irányelv rendelkezési és a saját szabályozásuk közötti összhangot. Az Irányelv rendelkezési alapvetően két csoportra oszthatók. Az első csoportba sorolhatók azok a rendelkezések, amelyek az áruk és szolgáltatások, konkrétan az elektronikus aláírási termékek és a hitelesítés szolgáltatók által nyújtott szolgáltatások[2] Közösségen belüli szabad mozgását, illetőleg a fogyasztók érdekeinek védelmét hivatottak biztosítani. A másik csoportba pedig azok a rendelkezések sorolhatók, amelyek az elektronikus kereskedelemben rejlő lehetőségek kiaknázhatósága érdekében az elektronikus aláírások jogi elismerésére kötelezik a tagállamokat [13].

Nemcsak az EU-ban, hanem a világban is elindult az elektronikus aláírás szabályozásának folyamata, melyről 2002-ben az ISACF közzétett egy tanulmányt [14], amelyből az alábbi adatokat felhaszálva bemutatjuk a világ törvényi szabályozásait az elektronikus aláírás vonatkozásában.

2 A fogalmak angol megnevezései sorrendben: electronic signature product(irányelv 2. cikk 12. pont) és certification service provider (irányelv 2. cikk. 11. pont)

Régió	Felmért országok	Létezik elektronikus-digitális aláírási törvény	Készül, vagy nincs törvény
Ázsia	13	10	3
Közép/Dél-Amerika	10	8	2
Európa	33	26	7
Afrika	4	1	3
Észak-Amerika	4	4	0
Közel-Kelet	6	1	5
Összesen:	**70**	**50**	**20**

1. táblázat: Elektronikus aláírás jogi szabályozása – ISACF felmérés

A táblázat legfontosabb következménye az, hogy a vizsgált országok 71,42%-ában (amelyek láthatóan lefedik a világ nagyobbik részét) törvényi szabályozás létezik – létezett már 2002-ben is – az elektronikus aláírás használatára, tehát ennek jogi akadálya ma már nincs gyakorlatilag sehol a világ információs társadalmaiban. Európában ma már minden ország rendelkezik elektronikus aláírásra vonatkozó jogszabállyal. A probléma inkább a használathoz szükséges tudásban és ellenérzésben kereshető, mivel az eszközök viszonylag alacsony ára (pár ezer forint évente) sem lehet igazán indoka a gyér használati gyakoriságnak.

A magyarországi jogszabályi háttér alapvetően a 2001. évi XXXV. törvény köré csoportosul. A főbb jogszabályokat az alábbiakban soroljuk fel:

1. 2001/XXXV. törvény az elektronikus aláírásról (módosítva a 2004. évi LV. törvénnyel)
2. 3/2005 IHM rendelet a hitelesítésszolgáltatókra vonatkozó követelményekről
3. 193/2005. Kormányrendelet az elektronikus ügyintézés részletes szabályairól
4. 194/2005. Kormányrendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről

5. 195/2005. Kormányrendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról
6. 13/2005 IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól
7. 114/2007. GKM rendelet az elektronikus archiválásról

A törvényi szabályozás az alábbi fontosabb vélelmeket fűzi az elektronikus aláírásokhoz:

1. Eat: 3. § (1) **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 (Polgári Törvénykönyvének 598-684. §-aiban szereplő, illetve a házasságról, a családról és a gyámságról szóló 1952. évi IV. törvény szerinti jogviszonyok) - **nem lehet** kizárólag amiatt, hogy az aláírás, illetve dokumentum elektronikus formában létezik.
2. Eat. 3. § (5) A (3)-(4) bekezdés szerinti esetekben (a bírósági eljárások különböző típusaiban), ha a vonatkozó jogszabály **írásos formát** ír elő, e követelménynek **elektronikusan aláírt elektronikus dokumentum** használatával is eleget lehet tenni.
3. Eat. 3. § (8) Minősített tanúsítványt bármely - a (3)-(4) bekezdés szerinti - bírósági vagy közigazgatási hatósági eljárásban el kell fogadni.
4. Eat. 4. § (1) Ha jogszabály a 3. § (2)-(4) bekezdésében foglaltakon kívüli jogviszonyban **írásba foglalást ír elő**, e követelménynek **eleget tesz** az elektronikusan aláírt elektronikus dokumentumba foglalás is, ha az elektronikusan aláírt elektronikus dokumentumot **fokozott biztonságú elektronikus aláírással** írják alá.
5. Eat. 4.§ (2) Ha az elektronikusan aláírt elektronikus dokumentumon **minősített elektronikus aláírás** szerepel és az aláírás ellenőrzésének eredményéből más nem következik, **vélelmezni kell**, hogy a dokumentum tartalma az aláírás óta **nem változott**.

A Polgári Perrendtartásról szóló 1952. évi III. törvény az alábbiakat írja elő a közokiratok és a magánokiratok vonatkozásában:

1. Ppt. 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 elektronikus aláírást, valamint - ha jogszabály így rendelkezik - időbélyegzőt helyezett el. Az eredeti közokiratéval azonos bizonyító ereje van annak az elektronikus okiratnak is, amelyet a közokirat kiállítására jogosult külön jogszabályban meghatározott eljárási rend szerint készített el, illetve amelyet törvény elektronikus közokiratnak nyilvánít.
2. Ppt. 195.§ (4) A magánokiratról a közokirat kiállítására jogosult által ügykörén belül, a megszabott közokirati alakban készített okirat - ideértve az elektronikus okiratot is - teljesen bizonyítja, hogy annak tartalma az eredeti okiratéval megegyezik. **Elektronikus okirat esetében** e bizonyító erő megállapításának feltétele az is, hogy a közokirat kiállítására jogosult az okiratot **minősített elektronikus aláírással** és - ha jogszabály így rendelkezik - időbélyegzővel lássa el, vagy azt külön jogszabály által meghatározott eljárás szerint készítse el. A magánokiratról közokirati alakban készített okirat bizonyító ereje - a magánokirat tartalmát illetően - megegyezik az eredeti okiratéval.
3. Ppt. 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:

   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, illetőleg a kiállító minősített elektronikus aláírásával aláírt elektronikus okirat tartalma az ügyvéd által készített elektronikus okiratéval megegyezik;

f) az elektronikus okiraton kiállítója minősített elektronikus aláírást helyezett el.

Mindezekből látható, hogy a jogszabályaink elfogadták és használják az elektronikusan aláírt dokumentumokat, tehát ezek használatának semmilyen jogi akadálya nincs már.

Megismételjük, hogy – összhangban az ETSI szabványokkal – a magyar jogszabályok is úgy tekintik az aláíró által aláírt elektronikus dokumentumot, hogy az aláíró abban foglalt nyilatkozatot megtette, illetőleg elfogadta, vagy magára nézve kötelezőnek ismerte el. Ezt jelenti tehát az elektronikus aláírás, hasonlóan a kézírásos aláíráshoz.

3.2 Hitelesítés-szolgáltatók tanúsítványaihoz kapcsolódó szintek

A magyarországi hitelesítés-szolgáltatók különböző paraméterekkel bocsátják ki tanúsítványaikat 2008. első negyedévében. Ez további indoka annak, hogy van értelme differenciálni az elektronikus aláírásokat.

Az aktuális nyilvános szolgáltatókat[3] két szintre (minősített és nem minősített) és ezen belül további két altípusra tagolhatjuk (közigazgatási, nem közigazgatási – itt a 194/2005. Kormány-rendeletben foglaltaknak megfelelő tanúsítvány-kibocsátókra gondolunk), és ezekben az NHH nyilvántartásában szereplő szolgáltatók az alábbi módokon jelennek meg (megjegyezzük, hogy további kategóriák is léteznek az egyes kategóriákon belül, a táblázat egyszerűsített módon ábrázolja a szolgáltatókat):

Kategóriák	minősített	nem minősített
közigazgatási	Magyar Telekom, MÁV INFORMATIKA, Microsec, Netlock	EDUCATIO, MÁV INFORMATIKA, Microsec, Netlock
nem közigazgatási	IHM Biztonsági (nem működik), Magyar Telekom, MÁV INFORMATIKA, Microsec, Netlock	*Giro Elszámolásforgalom* Magyar Telekom, MÁV INFORMATIKA, Microsec, Netlock

2. táblázat: Magyarországi hitelesítés-szolgáltatók

3 Ez a táblázat a 2008. május 15-i állapotot tükrözi. Az aktuális szolgáltatókat mindig megtalálhatjuk a http://webold.nhh.hu/esign/ címen, a nyilvántartásokban.

A fenti szolgáltatók különböző tanúsítványokat bocsátanak ki, melyek fontos tulajdonságai közül kettőt emelünk itt ki:

1. **tranzakció mértéke**: a szolgáltató javaslatot tesz arra nézve, hogy ebben a tanúsítványban szereplő nyilvános kulcshoz tartozó aláíró kulccsal mekkora kötelezettség-vállalást javasolnak aláírni.
2. **felelősség-vállalás mértéke**: a szolgáltató a saját hibájából eredő károkért mekkora mértékben vállal felelősséget, azaz mekkora mértékben hárítható ez – adott esetben – legfeljebb rá?

A használathoz mindkét paraméter ismerete szükséges lehet, hiszen többször előfordulhat az, hogy különböző értékű elektronikus tranzakciókat bonyolítunk le, kezdve például egy egyszerű újságvásárlástól az elektronikus banki tranzakciók aláírásán keresztül egy nagyértékű elektronikus közbeszerzési kötelezettség felvállalásáig.

Mindehhez a szolgáltatók az alábbi szintű tanúsítványokat biztosítják – csak az aláírásra használható tanúsítványokat figyelembe véve:

1. Netlock (csak minősített tanúsítványhoz határoz meg ügyleti értéket):
   a) Személyes minősített közjegyzői tanúsítványok (Class QA) segítségével készített aláírások kötelezettség-vállalásának ügyleti értéke lehet:
      - 5.000.000 Ft
      - 20.000.000 Ft
      - 50.000.000 Ft
   b) Munkatársi minősített közjegyzői tanúsítványok (Class QA) segítségével készített aláírások kötelezettség-vállalásának ügyleti értéke lehet:
      - 5.000.000 Ft
      - 20.000.000 Ft
      - 50.000.000 Ft

A felelősségbiztosítás a Szolgáltató hibájából eredő károknál lép életbe, amelynek nagysága a tanúsítványban szereplő érték, de maximálisan 50.000.000 Forint.

2. MÁV INFORMATIKA

a)Nem minősített tanúsítványok

- *személyes tanúsítvány*:
  - 0 Ft tranzakciós limit, 50.000 Ft Szolgáltatói felelősség-vállalási limit
  - 250.000 Ft tranzakciós limit, 125.000 Ft Szolgáltatói felelősség-vállalási limit
  - 1.000.000 Ft tranzakciós limit, 1.000..000 Ft Szolgáltatói felelősség-vállalási limit
  - 5.000.000 Ft tranzakciós limit, 2.500.000 Ft Szolgáltatói felelősség-vállalási limit
- *szervezeti és munkatársi tanúsítvány*:
  - 0 Ft tranzakciós limit, 500.000 Ft Szolgáltatói felelősség-vállalási limit
  - 1.000.000 Ft tranzakciós limit, 1.000.000 Ft Szolgáltatói felelősség-vállalási limit
  - 5.000.000 Ft tranzakciós limit, 2.500.000 Ft Szolgáltatói felelősség-vállalási limit
  - 10.000.000 Ft tranzakciós limit, 5.000.000 Ft Szolgáltatói felelősség-vállalási limit

b)Minősített tanúsítványok

- *magánszemélyes tanúsítvány*:
  - 0 Ft tranzakciós limit, 125.000 Ft Szolgáltatói felelősség-vállalási limit
  - 1.000.000 Ft tranzakciós limit, 1.000.000 Ft Szolgáltatói felelősség-vállalási limit
  - 5.000.000 Ft tranzakciós limit, 2.500.000 Ft Szolgáltatói felelősség-vállalási limit
  - 10.000.000 Ft tranzakciós limit, 5.000.000 Ft Szolgáltatói felelősség-vállalási limit
  - 25.000.000 Ft tranzakciós limit, 20.000.000 Ft Szolgáltatói felelősség-vállalási limit
- *szervezeti személyek tanúsítványa*:
  - 0 Ft tranzakciós limit, 1.000.000 Ft Szolgáltatói felelősség-vállalási limit
  - 5.000.000 Ft tranzakciós limit, 5.000.000 Ft Szolgáltatói felelősség-vállalási limit
  - 20.000.000 Ft tranzakciós limit, 20.000.000 Ft Szolgáltatói felelősség-vállalási limit

- 100.000.000 Ft tranzakciós limit, 40.000.000 Ft Szolgáltatói felelősség-vállalási limit
- 250.000.000 Ft tranzakciós limit, 50.000.000 Ft Szolgáltatói felelősség-vállalási limit

3. Magyar Telekom:

a) Nem minősített

- *standard személyi tanúsítvány*: 100.000 Ft kötelezettség-vállalás, 1.500.000 Ft Szolgáltatói felelősség-vállalási limit
- *fokozott személyi tanúsítvány:* 5.000.000 Ft kötelezettség-vállalás, 2.000.000 Ft Szolgáltatói felelősség-vállalási limit
- *standard üzleti tanúsítvány*: 100.000 Ft kötelezettség-vállalás, 1.500.000 Ft Szolgáltatói felelősség-vállalási limit
- *fokozott üzleti tanúsítvány*: 5.000.000 Ft kötelezettség-vállalás, 2.000.000 Ft Szolgáltatói felelősség-vállalási limit
- *egyedi tanúsítványok*: megállapodás szerinti kötezettség-vállalás, 3.000.000 Ft Szolgáltatói felelősség-vállalási limit

b) Minősített – csak üzleti - tanúsítványok

- *“Arany”*: 500.000.000 Ft kötelezettség-vállalás, 15.000.000 Ft Szolgáltatói felelősség-vállalási limit
- *“Ezüst”*: 100.000.000 Ft kötelezettség-vállalás, 10.000.000 Ft Szolgáltatói felelősség-vállalási limit
- *“Bronz”*: 10.000.000 Ft kötelezettség-vállalás, 5.000.000 Ft Szolgáltatói felelősség-vállalási limit

4. Microsec:

a) Minősített tanúsítványok

- *Bronz*: 1.000.000 Ft ügyleti érték, 0 Ft Szolgáltatói felelősség-vállalás
- *Ezüst*: 20.000.000 Ft ügyleti érték, 5.000.000 Ft Szolgáltatói felelősség-vállalás
- *Arany*: 80.000.000 Ft ügyleti érték, 20.000.000 Ft Szolgáltatói felelősség-vállalás
- *Platina*: 200.000.000 Ft ügyleti érték, 50.000.000 Ft Szolgáltatói felelősség-vállalás

b) Nem minősített tanúsítványok esetén az aláírói szerződés fogja tartalmazni az aktuális értékeket (a HSZSZ előírása szerint).

5. EDUCATIO (felelősségvállalása tanúsítványonként és káreseményenként nem haladhatja meg a 10.000 Ft-ot – a HSZSZ szerint):

   a) *személyes (végfelhasználói) tanúsítvány*: 0 Ft tranzakciós limit

   b) *szervezeti képviseletre alkalmas (végfelhasználói) személyes tanúsítvány*: 0 Ft tranzakciós limit

   c) *szolgáltatói tanúsítvány (végfelhasználói és eszköz tanúsítványok)*: 0 Ft tranzakciós limit

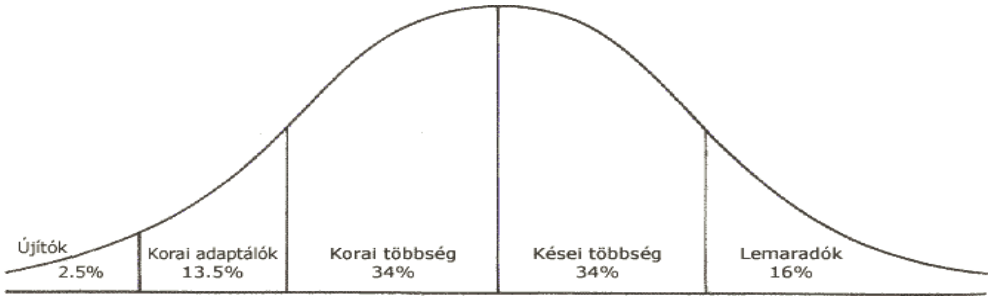
3.3 Honnan szerezzük meg a tudást az elektronikus aláírás használatához?

De egy kérdésre még mindig nem kaptunk választ. Elfogadjuk, hogy kell ez nekünk – bizonyos korlátok között. Elfogadjuk, hogy használni kell (kötelező), ahol előírják. De ha használni szeretnénk, honnan szerezzük meg azt a tudást, ami segítségével már tudjuk is használni az elektronikus aláírást?

A társadalomtudományban több vizsgálódás és elmélet született az innovációk elterjedési mechanizmusának vizsgálatára. Ezek közül Everett M. Rogers adaptációs elméletét ismertetjük[4], mely az innovációt olyan gondolatként, gyakorlatként vagy tárgyként definiálja, amelyet az egyén vagy más alkalmazó újnak értékel. Tapasztalatai szerint az adaptálás ütemét jelentősen megszabják az adott innováció jellegzetességei. A potenciális adaptálók szempontjából az újítások az alábbi öt fő kategóriában jellemezhetők (a kategóriák ismertetésétől eltekintünk):

a. Relatív előny (egyenes arány)
b. Kompatibilitás (egyenes arány)
c. Komplexitás (fordított arány)
d. Kipróbálhatóság mértéke (egyenes arány)
e. Megfigyelhetőség (egyenes arány)

4 Forrás: Internet.hu A magyar társadalom digitális gyorsfényképe 1. kötet pp39-46



1. ábra: Rogers adaptációs görbéje

Az ajánlás írásának idején kicsit több, mint 8.000 személy használta a nyilvános és ellenőrzésre kötelezett magyarországi szolgáltatótól vásárolt tanúsítványához tartozó aláíró-kulcsát Magyarországon, ami kisebb, mint 1 ezreléke a népességnek. Azaz még az "újítók" szakasz elején tartunk ezek szerint – habár a képet természetesen árnyalhatják a nem nyilvános szolgáltatások (belső vállalati, zárt körű szolgáltatások) felhasználói.

A korai és késői adaptálók jellemzőire vonatkozó megfigyeléseket Rogers három nagyobb dimenzióba csoportosítva foglalja össze. Eszerint a két csoport közti különbségek megfogalmazhatók

- gazdasági-társadalmi státusz,
- személyes jellemzők, valamint
- kommunikációs viselkedés terén.

A korai adaptálók általában iskolázottabbak, magasabb társadalmi státusszal és jövedelemmel rendelkeznek, valamint társadalmilag mozgékonyabbak, mint a többiek. Továbbá empatikusabbak és racionálisabban gondolkodnak. Ha a kommunikációs kapcsolatokat és viselkedést figyeljük meg, a korai adaptálókra jellemző, hogy több kapcsolattal, tömegkommunikációs eszközökhöz való hozzáféréssel rendelkeznek, mint a többiek. Érdekességképpen megjegyezzük, hogy Rogers felfigyelt arra a paradoxonra, hogy az utolsóként adaptálók csoportjába tartozók általában azok, akik a legtöbbet profitálhatnának az innovációból.

Felmérések alapján kijelenthetjük[5], hogy tudomásunk szerint ma Magyarországon nincs olyan átfogó koncepció, mely arra irányulna, hogy az elektronikus hitelesség fogalom-rendszerébe, technikáiba bevezesse az érdeklődő felhasználókat, hálózat-használókat, újkeletű szóhasználattal "netizen"[6]-eket. Ezért ez a tudás ma kizárólag önképzés útján

5 Lásd: http://www.melasz.hu Magyar Elektronikus Aláírási Szövetség honlapja
6 Lásd Z. Karvalics László: Fogpiszkáló a hálózaton

szerezhető meg. Azonban meg kell említeni, hogy elindultak olyan folyamatok és projektek, melyek ennek a helyzetnek a megváltozására irányulnak, így hát bízunk benne, hogy a jövő változást tartogat a hitelesítéssel kapcsolatos tudás elterjedése területén is.

A tudás-átadásnak ki kell terjednie az alábbi területek mindegyikére – így nem elképzelhetetlen, hogy előbb-utóbb ECDL-modul is készül hozzá:

1. alsófokú közoktatás
2. középfokú közoktatás
3. felsőfokú közoktatás
4. poszt-graduális intézményi oktatás
5. felnőtt-képzés
6. senior képzés

Csak így képzelhető el minden érintett fél tájékoztatása.

4 Következtetés

Az elektronikus aláírásokat tehát az alábbi dimenziók mentén tipizálhatjuk:

1. **joghatások**: meg nem tagadhatóság, írásbeliség, teljes bizonyító erő
2. **szabványos típusok**: normál, időbélyegzett, komplex, nagyon komplex, archív
3. **felelősségvállalás**: 0-tól megállapodás szerinti összegig (több százmillió is lehet akár)
4. **tranzakció értékhatár**: 0-tól megállapodás szerinti összegig, többszázmillió vagy milliárd is lehet.

A fentiek ismerete fontos az aláírások rendeltetésszerű és rendszeres használata érdekében, ezért minden aláírási rendszer kialakításánál erre tekintettel kell lenni. Ebből következik, hogy talán a tervezési kérdések megválaszolása több időt vehet igénybe a komplexitás miatt, de a kérdésekre adott válaszok után a megvalósításhoz már minden szükséges infrastruktúrális elem a rendelkezésre áll, tehát az implementálási fázis viszonylag gyorsan kivitelezhető.

Összefoglalóan, a 21. században az elektronikus hitelesség helyes megvalósítása alapvető követelmény a digitális univerzumban. Komoly társadalomformáló ereje lehet annak, ha a hiteles (valaki által hitelesített) információkat el tudjuk választani a nem hiteles információktól. Ha *minden* releváns információ hitelessége valamilyen szinten fennállna, hamar létrejöhetnének olyan bizalmi közösségek, melyek az egymás hitelesített információiban – saját belátásuk szerint természetesen – megbíznak. A bejövő információ ebben az esetben az alábbi – szinte automatikus - döntési folyamatot követheti:

1. Elektronikusan aláírt az információ? Ha nem -> eldobás
2. Ha az 1. kérdésre a válasz „igen”, akkor megyünk tovább. Következő kérdés: megbízható-e a tanúsítvány és a tanúsítvány-lánc? Ha nem -> eldobás.
3. Ha eddig minden kérdésre a válasz „igen”, más szóval az információk megbízható és az elfogadó számára megfelelő módon alá vannak írva (elektronikusan), ekkor és csak

ekkor használhatjuk az információt, a saját elfogadási szintünknek megfelelően.

Az elektronikus hitelesség ismerete azonban egy ember számára “kis lépés”, de ha egy információs társadalom (majdnem) minden tagja ismeri és tudja használni a hitelességet, akkor az “nagy ugrás” bekövetkezéséhez vezethet[7].

Paradigmaváltás bekövetkezésére számítunk tehát, de nem lehetünk teljesen optimisták. Úgy látszik, hogy jónéhány tévhit a gátja az elektronikus hitelesség terjedésének – egyet emelünk ki ezekből: “azért hiteles, mert számítógépben van”. A számítógépes rendszerekbe egyszer bekerült adat hitelessége azonban nem automatikus, hanem komoly műszaki-informatikai és szervezési intézkedésekkel biztosítható csak. Ezen intézkedések hiányában az egzakt hitelesség gyakorlatilag minden esetben megkérdőjelezhető.

Az elektronikus aláírás használata – mindezekből következően – tudás-intenzív feladat, de a mai meglévő tudásunkkal a korrekt használat kevésbé valószínűsíthető, tehát mindenképpen szükségesnek látszik egy olyan modell kialakítása és végrehajtása, amely a használathoz szükséges tudást – a fentebb felvázoltak szerint – teríti az információs társadalom szélességében és mélységében egyaránt.

Ennek a változásnak a bekövetkezéséhez konstruktívan és nyitottan kell majd hozzáállni, hiszen az elektronikus hitelesség megvalósítása számos olyan kaput nyithat meg az e-világban az e-polgárok számára, amivel a saját életüket tudják könnyebbé és egyszerűbbé tenni, továbbá a velük történtek felett gyakorolhatnak nagyobb ellenőrzést (példának okáért említhetjük az e-ügyintézést; vagy az adóadatbázis, egészségügyi adatbázis, munkaügyi adatbázisokhoz való hozzáférést). Az elektronikus folyamat-elemek – erőforrás-igényüktől függően – pedig csökkenthetik a folyamatok energia-igényeit és költségeit, amivel környezetbarátabb világot teremthetünk magunk számára – legalább lehetőség szinten.

7 Felhasználtuk itt Neil Armstrong híres mondását: ”That's one small step for [a] man, one giant leap for mankind.” 2:56 UTC July 21, 1969, Hold

Az elektronikus hitelesség hatása tehát az alábbi területeken lehet kézzelfogható:

1. ügyintézési folyamatok gyorsulása
2. megtévesztések csökkenése
3. rosszindulatú módosítások hatásainak kivédése
4. költséghatékonyság
5. energia-megtakarítás
6. számonkérhetőség, auditálhatóság magasabb szintre emelése

Az elektronikus aláírások szintjeinek van egy további következménye is, mégpedig a használati modellek kialakulásának lehetősége. Két modell (és ezek keveredése) képzelhető el a többszintű elektronikus aláírások használatakor:

1. egy aláíró kulcsot használ az aláíró mindenre
2. több aláíró kulcsot használhat az aláíró, területtől függően

Az “egy kulcs mindenre” elv következménye, hogy a lehető legnagyobbra kell venni mind a tranzakció, mind a felelősségvállalás mértékét, és egy kis értéknél is nagy értékre meghatározott kulcsot használnak – ez ugyan nem tűnik hiányosságnak rendeltetésszerű használat esetén, de rosszindulatú használatkor már vethet fel problémákat.

A “több kulcs több célra” pedig az értékhatárt jobban differenciálja, viszont a megfelelő kulcs és a hozzá tartozó PIN-kód kiválasztása – és eltévesztése – nagyobb kockázattal járhat.

Hogy melyik fog elterjedni? A technológia mind a kettő használati filozófia megvalósulását támogatja, ez a kérdés ezért már nem technológiainak, hanem társadalom-filozófiainak látszik, így ennek tárgyalásától itt eltekintünk. De töretlenül bízunk az elektronikus aláírás használatának gyors hazai elterjedésében.

5 Irodalomjegyzék

[1] Hamis e-mail a Spice Girls turnéjához kapcsolódóan
http://www.educafe.hu/index.php?cikk=8398

[2] RFC 821 Simple Mail Transfer Protocol (http://www.ietf.org/rfc/rfc0821.txt)

[3] O. Nagy Gábor: Mi fán terem? - magyar szólásmondások eredete, 9, kiadás, Akkord kiadó, 2005. ISBN 963 9429 65 1; pp307-308.

[4] SHA-1 is broken (http://www.schneier.com/blog/archives/2005/02/sha1_broken.html)

[5] Surányi László: Metaaxiomatikai problémák, Typotex kiadó 1992, ISBN: 963 7546 19 7; pp99-100

[6] Az Európai Közösségek Bizottsága Brüsszel, 25.04.2006 COM(2006) 173 végleges, a Bizottság közleménye a tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának i2010 eGovernment Cselekvési Terv: az elektronikus kormányzat létrehozásának felgyorsítása a társadalom egészének javára (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0173:HU:HTML)

[7] Az Európai Parlament és a Tanács 2006/123/EK irányelve (2006. december 12.) a belső piaci szolgáltatásokról (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:01:HU:HTML)

[8] Az Európai Parlament és a Tanács 1999/93/EK irányelve (1999. december 13.) az elektronikus aláírásra vonatkozó közösségi keretfeltételekről (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:01:HU:HTML)

[9] Elektronikus Aláírási Szabályzat (https://www.kozzetetelek.hu/engine.aspx?page=easz)

[10] RFC 3125 Electronic Signature Policies (http://tools.ietf.org/html/rfc3125)

[11] ETSI TR 102 038 V1.1.1 (2002-04) TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies

[12] RFC 3852 Cryptographic Message Syntax (CMS) (http://tools.ietf.org/html/rfc3852)

[13] Dr. Rátai Balázs Az elektronikus aláírás szabályozásának kulcskérdései az 1999/93/EC irányelv alapján 2001. március 18. (http://www.jogiforum.hu/publikaciok/16)

[14] Electronic and digital signatures. A Global Status Report. *Information Systems Audit and Control Foundation™.* 2002.

[15] Az Európai Közösségek Bizottsága, Brüsszel, 15.3.2006 COM(2006) 120 végleges; Jelentés az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló 1999/93/EK irányelv működéséről ;