Mi alapján fogadhatunk el egy elektronikus aláírást?[1]

Dr. Berta István Zsolt
istvan.berta@microsec.hu
Microsec Kft.

Az elektronikus aláírás elméleti alapjai régóta ismertek. E matematikai, kriptográfiai szempontból bevált technológia már a hazai jogrendszerbe is beépült, és ezzel az elektronikus aláírás a kézzel írott aláírással egyenértékűvé vált. Az elektronikus aláírás használatához mind a matematikai, mind a jogi alapok rendelkezésre állnak, de e technológia mégis csak az elmúlt években kezdett elterjedni hazánkban. A gyakorlati alkalmazás során számos probléma merült fel ezen új technológiával kapcsolatban. Ezek nagy része megjelenik a kézzel írott aláírások esetében is, de e problémák ott sokkal kisebb jelentőséggel bírnak.

1. Bevezetés

Elektronikus aláírás segítségével elektronikus dokumentumokat hitelesíthetünk. Ha egy dokumentumot elektronikusan írunk alá, az egyenértékű azzal, hogy a kézzel írott aláírásunkkal látjuk el. Az elektronikusan aláírt dokumentumról bármennyi másolatot készíthetünk, és tetszőleges számú helyre elküldhetjük úgy, hogy minden példány hiteles, az „eredetivel" egyenértékű, azonos bizonyító erejű lesz. Az elektronikus dokumentumokat papír alapú társaiknál sokkal gyorsabban elküldhetjük, és a fogadó fél – esetleg automatizáltan, számítógépes programok segítségével – sokkal gyorsabban feldolgozhatja őket. Ma sok ügyet azért lehet kizárólag papíron intézni, mert eredeti, hiteles dokumentumokra van szükség. Az elektronikus dokumentumok a papíroknál könnyebben kezelhetőek, a rendszer jobban kézben tartható, és az elektronikus aláírással ellátott iratok a papírokkal azonos bizonyító erővel rendelkeznek. Egy jól megtervezett informatikai rendszerben, amely értelmesen használja az elektronikus aláírásra épülő technológiát, gyorsan és gördülékenyen intézhetjük ügyeinket. Ezzel szemben, ha az elektronikus aláírást ügyetlenül alkalmazzuk, drága, szövevényes és bonyolult rendszerhez jutunk, amelyben az értelmetlenül használt elektronikus aláírások csak nyűgöt és költséget jelentenek, szélsőséges esetben akár bizonyító erejüket is elveszíthetik.

Az elektronikus aláíráshoz szükséges technológiák és kriptográfiai algoritmusok több évtizede rendelkezésre állnak. [BV2004] A 2001-ben megjelent, elektronikus aláírásról szóló törvény, az [Eat] a kriptográfiai algoritmusok nyújtotta *letagadhatatlanságot* jogi fogalomnak, *bizonyító erőnek* feleltette meg. E törvény „*minősített"* és „*fokozott biztonságú"* elektronikus

[1] E cikk a Híradástechnika című folyóirat 2006. májusi (LXI.) számában jelent meg.

aláírást különböztet meg. (Emellett „egyszerű” elektronikus aláírást is említ, de ezzel itt nem foglalkozunk.) A fokozott biztonságú aláírással hitelesített dokumentum *magánokirat* (tehát a kézzel írott aláírással azonos bizonyító erővel rendelkezik), míg a fokozott biztonságú aláírásnál erősebb minősített aláírással hitelesített dokumentum *teljes bizonyító erejű magánokirat* (ilyen például a két tanú előtt vagy közjegyző előtt aláírt dokumentum is). Minősített aláírással kapcsolatos jogvita esetén a bíróságnak vélelmeznie kell, hogy az aláírt dokumentum tartalma az aláírás elkészítésének időpontja óta nem változott meg, viszont a fokozott biztonságú aláírásra nem vonatkozik ilyen szabály. [Eat] Mind a technológia, mind a hozzá kapcsolódó jogszabályok rendelkezésre állnak, és a technológiát a jogszabályok szerint szolgáltató cégek is megjelentek. Négy olyan minősített *hitelesítés szolgáltató* is működik Magyarországon, akiktől bárki vehet minősített elektronikus aláíráshoz használható tanúsítványt.

Az elektronikus aláírás gyakorlatban történő alkalmazása számos olyan problémát vet fel, amelyet sem a technológia, sem a jogszabályok alapján nem könnyű megválaszolni. Cikkünkben az egyik ilyen problémakört, nevezetesen egy elektronikus aláírás elfogadásakor szükséges lépéseket gondoljuk végig. Emellett azt is megvizsgáljuk, hogy a közigazgatás által a közelmúltban közzétett elektronikus aláírás keretrendszer [Kozig] hogyan viszonyul e kérdésekhez.

2. Milyen formátumú az elektronikus aláírás?

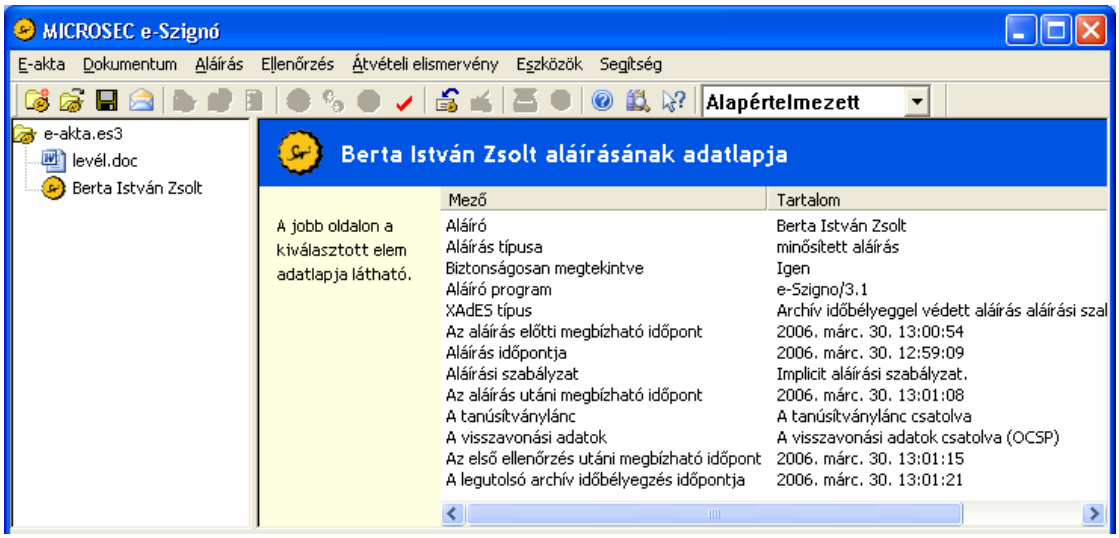
Tételezzük fel, hogy kaptunk egy elektronikusan aláírt dokumentumot. Első kérdés, hogy egyáltalán tudjuk-e értelmezni az elektronikus aláírást. Más szóval, van-e olyan szoftverünk, amely érti az adott formátumú aláírást? Nagyon sok különböző elektronikus aláírás formátum létezik: nemcsak e-mailek, de például Word dokumentumok és PDF fájlok is tartalmazhatnak aláírást, és a különböző szoftverek (illetve ugyanazon szoftver különböző verziói) által létrehozott fájlok különböző formátumú elektronikus aláírást tartalmazhatnak. Ezek közül a levelezőprogramok által készített S/MIME aláírások tekinthetőek valamelyest szabványosnak; ekkor gyakori, hogy az egyik levelezőprogrammal készített aláírást egy másik levelezőprogram is megérti. Sajnos, az általános célú alkalmazások – beleértve a levelezőprogramokat is – lényeges, alapvető műszaki követelményeknek sem felelnek meg a hosszú távon is letagadhatatlan elektronikus aláírással kapcsolatban. A legtöbb alkalmazás nem építi fel a tanúsítványláncot, sok nem ellenőrzi a lánc egyes elemeinek visszavonási állapotát, valamint nem vizsgálja meg, hogy a visszavonási állapotról beszerzett információ az aláírás időpontjára vonatkozik-e egyáltalán. (E kérdésekről a későbbi fejezetekben szólunk.)

Ezen aláírás formátumok nem tartalmaznak időbélyeget sem, pedig ha nem tudjuk biztonságos módon megállapítani, hogy az aláírás mikor készült, akkor az aláírás letagadhatatlansága műszakilag nem biztosítható. (Lásd: 4. fejezet.) Léteznek olyan aláírás formátumok, amelyek alkalmasak az aláírás hosszú távú érvényességének biztosítására azáltal, hogy bennük az időbélyegek, a tanúsítványlánc és a tanúsítványra vonatkozó visszavonási információk is eltárolhatók. (Lásd: 6. fejezet.)

Aki elektronikusan aláírt dokumentumot szeretne fogadni, annak célszerű meghatároznia és a küldő fél tudomására hoznia, hogy milyen formátumú elektronikus aláírást fogad el. Különben abba a helyzetbe kerülhet, hogy olyan levelet kap, amelyet nem tud elolvasni. Az aláírás és az aláírt dokumentum többféleképpen csatlakozhatnak egymáshoz:

- Egyik lehetőség, hogy *az aláírás az aláírt dokumentum fájljába kerül*. Ilyen a .doc vagy .pdf fájlban lévő aláírás. E megoldásnak hátránya, hogy ilyenkor a felhasználó kénytelen az adott szoftver aláírás-ellenőrző mechanizmusát használni. E megoldás biztonsági szempontból nem egységes, mert lehet, hogy a befogadó az egyes fájltípusok esetén ellenőrzéskor más és más biztonsági követelményeket alkalmaz (a tanúsítványlánc felépítésére, a visszavonási információk összegyűjtésére stb). A befogadó kénytelen az adott típusú fájlt kezelő alkalmazás által nyújtott (gyakran igen alacsony) szintű biztonsággal beérni. Ugyanakkor, e megoldás sokszor praktikus lehet, mert egy meglévő informatikai rendszert nem szükséges jelentősen átalakítani az elektronikus aláírás bevezetéséhez; az eddig használt fájlformátumok (.doc, .pdf) továbbra is használhatóak.
- Az *aláírás(ok) és az aláírt dokumentum(ok) egy* aláírás-fájlban, például ún. *e-aktában* helyezkednek el (1. ábra). Ilyenkor a felhasználó az aláírás-fájlt kezelő, professzionális aláírás-létrehozó (vagy -ellenőrző) alkalmazás biztonsági beállításai szerint hozhatja létre és ellenőrizheti az aláírásokat, így e megoldás biztonsági szempontból testre szabható, és megfelelő aláírás-létrehozó és -ellenőrző alkalmazás esetén erős biztonságot jelenthet. Egyes esetekben e megoldás kényelmetlen is lehet, mert az elektronikus aláírást bevezető szervezetnek át kell alakítani a belső folyamatait, hogy minden folyamat aláírás-fájlokat használjon. Ekkor az aláírt fájlok olvasásához is aláírás-ellenőrző szoftverre van szükség.
- Az *aláírás és az aláírt dokumentum(ok) külön fájlokban vannak*. E megoldás egyesíti a két előző előnyeit: professzionális, testre szabható alkalmazást használhatunk, így tetszőleges fájlt aláírhatunk, és egyúttal a hagyományos fájlformátumokra épülő meglévő folyamatokat nem kell átalakítani. E megoldásnak van egy veszélye is: ha az aláírt fájlokat és az aláírásokat szétválasztjuk egymástól, és egy részük megsérül, vagy összekeveredik, akkor nagyon-nagyon nehéz lehet biztosítani az aláírások letagadhatatlanságát.

A magyar közigazgatás a [XAdES] szabvány által leírt XML elektronikus aláírás formátumot választotta. Ez egy nagyon jó választás – egy professzionális aláírás-formátum, amely alkalmas az aláírások letagadhatatlanságának hosszú távú biztosítására is. E szabvány szerint a második és a harmadik változat könnyen megoldható, az első változathoz az egyes szoftverek gyártóinak kell megvalósítaniuk a XAdES aláírások kezelését.



1. ábra – Elektronikus aláírás ellenőrzése az e-Szignó program ingyenes változatával

3. Érvényes-e az aláírás?

Ha szoftverünk ismeri az elektronikus aláírás formátumát, akkor meg tudja állapítani, hogy műszaki szempontból *érvényes*-e, tehát valóban kapcsolódik-e hozzá a jogszabályok szerinti bizonyító erő. Így, mielőtt egy aláírt dokumentum alapján fontos döntést hozunk, célszerű megvizsgálni, hogy az aláírás érvényes-e egyáltalán. Az [Eat] szerint ekkor meg kell néznünk azon *hitelesítési rendet*, amely szerint az aláíró tanúsítványát kibocsátották, és eszerint kell eljárnunk. Ha nem így teszünk, és esetleg érvénytelen aláírás alapján hozunk fontos döntést, akkor a felmerülő károkért sem az aláíró, sem az aláíró tanúsítványát kibocsátó hitelesítés szolgáltató nem vállal felelősséget. A hitelesítés szolgáltatók hitelesítési rendjei általában a nemzetközi szabványok (például a [CWA14171] és az [RFC3280]) által leírt lépéseket tartalmazzák:

1. Ellenőrizni kell, hogy az aláírás az aláíró tanúsítványához és az aláírt dokumentumhoz tartozik-e. (Ez a kriptográfiai ellenőrzés, amelyet szinte minden alkalmazás támogat.)
2. Ellenőrizni kell, hogy az aláíró tanúsítványa visszavezethető-e egy megbízható hitelesítés szolgáltató tanúsítványára. Ezt nevezzük a tanúsítványlánc felépítésének. (Erről bővebben az 5. fejezetben szólunk.)

3. Ellenőrizni kell, hogy nem vonták-e vissza a tanúsítványláncban szereplő tanúsítványok bármelyikét. (Erről a 6. fejezetben szólunk bővebben.)

Egy professzionális aláírás-ellenőrző alkalmazás a fenti lépések mindegyikét elvégzi. A fenti lépéseken túl azt is el kell dönteni, hogy az adott típusú tanúsítvány elfogadható-e az adott célra. Ez nemcsak műszaki lépéseket jelent, ennek a problémának jogi, gazdasági és szabályozási vonzatai is vannak. A 7., 8. és 9. fejezetek ilyen kérdésekről szólnak.

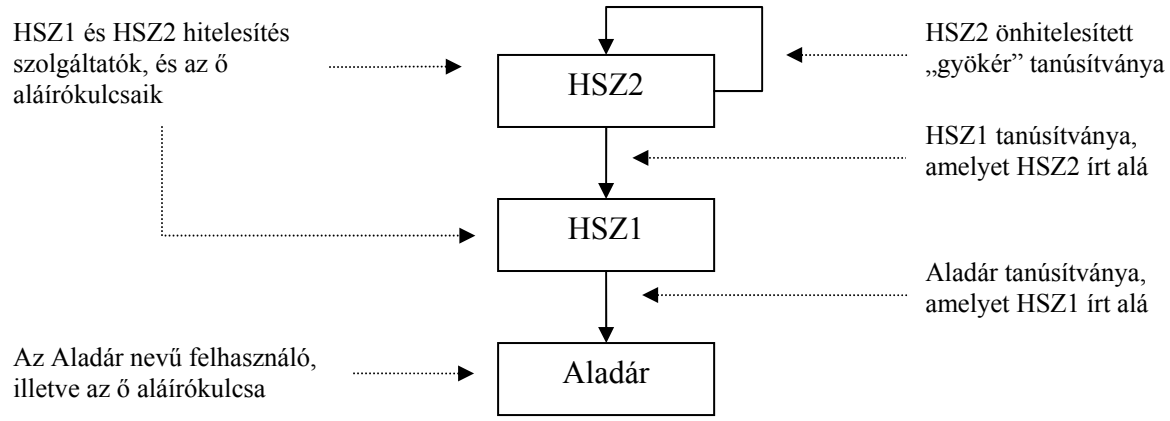
4. Bizonyítható-e, hogy mikor készült az aláírás?

Az aláírás akkor érvényes, ha az aláíró tanúsítvány érvényes volt az aláírás létrehozásának időpontjában. Ebből következően, ha nem bizonyítható az aláírás időpontja, akkor az aláírás érvényessége is megkérdőjelezhetővé válhat. Ez akkor fordulhat elő, ha az aláíró tanúsítványa később lejár, esetleg felfüggesztik vagy visszavonják. Ilyenkor később nem lehet majd bizonyítani, hogy az aláírás akkor készült-e, amikor a tanúsítvány még érvényes volt. Ez azt jelenti, hogy hiába győződünk meg egy aláírt dokumentum érvényességéről, *ha az aláírás időpontja nem bizonyítható, akkor az aláíró később letagadhatja az aláírását*. Többféle módon bizonyíthatjuk, hogy az aláírás mikor készült, de erre az *elektronikus időbélyeg* jelenti a legkézenfekvőbb módszert. Az időbélyeg az időbélyegzett dokumentum lenyomatát és az időbélyegzés időpontját tartalmazza. Ezen időpontot egy *időbélyegzés szolgáltató* – egy megbízható, bevizsgált és biztonságos szervezet – szolgáltatja, mielőtt aláírja az időbélyeget. Az időbélyeg valójában az időbélyegzés szolgáltató által aláírt igazolás arról, hogy az időbélyeggel ellátott dokumentum az időbélyegen szereplő időpontban létezett. Az aláíráson lévő időbélyeg azt igazolja, hogy az aláírás nem készülhetett az időbélyegen szereplő időpontnál később. Ha egy aláírt dokumentumon nincsen időbélyeg, akkor célszerű a legrövidebb időn belül elhelyezni rajta egyet (amíg érvényes a tanúsítvány); így meggátolhatjuk, hogy az aláíró később letagadja az aláírását.

Az időbélyegek jelentik az elektronikus aláírásokra épülő rendszer egyik alapkövét, így a közigazgatási keretrendszer is – nagyon helyesen – kimerítően foglalkozik az időbélyegekre vonatkozó követelményekkel. Ugyanakkor, nemcsak az [Eat.] szerinti időbélyeget, hanem az időjelzést is elismeri. Az *időjelzés* abban különbözik az időbélyegtől, hogy az időjelzést kibocsátókra nem érvényes az időbélyegzés szolgáltatókra vonatkozó erős követelményrendszer, így a közigazgatás az időbélyegnél sokkal olcsóbban állíthat elő – esetleg gyenge minőségű – időjelzést.

5. Melyik gyökér tanúsítványra vezetjük vissza az aláírást?

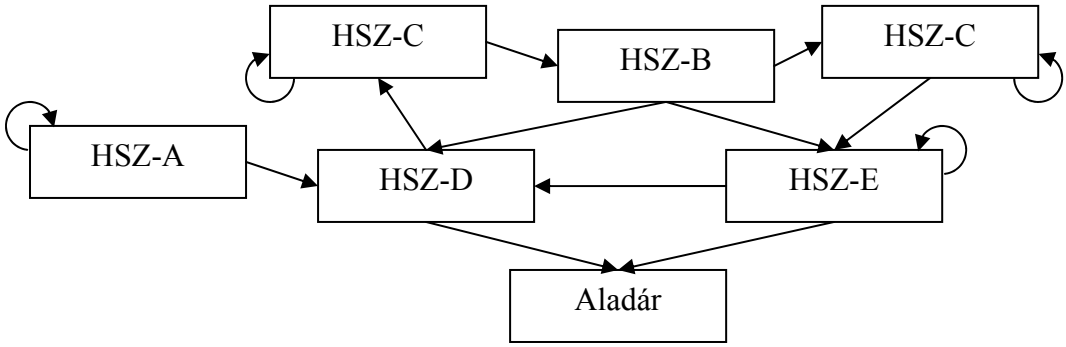
Tegyük fel, hogy az Aladár nevű felhasználó (akinek tanúsítványát a HSZ1 hitelesítés szolgáltató bocsátotta ki) elektronikusan aláírt üzenetet küld Bélának (2. ábra). Ha Béla a 3. fejezetben leírtak szerint *ellenőrzi Aladár aláírását, akkor egy „megbízható" tanúsítványra (gyökér tanúsítványra) próbálja meg visszavezetni az aláírást*. Béla akkor tekintheti egy hitelesítés szolgáltató tanúsítványát megbízhatónak, ha *ismeri* a hitelesítés szolgáltatót, és *megbízik benne*, valamint *hitelesen*, biztonságos módon *hozzájutott a* hitelesítés szolgáltató *tanúsítványához*. [BV2004] Könnyen előfordulhat, hogy Béla nem ismeri HSZ1 tanúsítványát. Ilyenkor Béla (pontosabban, a számítógépes program, amelyet Béla használ) egy olyan tanúsítványláncot keres, amely a Béla számítógépén (például a Béla Windowsában) lévő megbízható tanúsítványok egyikétől indul, és az Aladár tanúsítványát kibocsátó HSZ1 tanúsítványáig tart. (Ennek algoritmusát az [RFC3280] ismerteti részletesen.)



2. ábra – Egy egyszerű tanúsítványlánc

Sajnos a gyakorlatban a helyzet a 2. ábránál sokkal bonyolultabb. A 3. ábrán látható, hogy egy hitelesítés szolgáltató egy kulcsához egyszerre több tanúsítvány is tartozhat. Ha ezeket különböző időben bocsátották ki, akkor az egyes tanúsítványok különböző információkat tartalmaznak arról, hogy a hitelesítés szolgáltató adott kulcsához mely hitelesítés szolgáltatók mely kulcsaival bocsátottak ki tanúsítványt. Az 3. ábra alapján jogosan merül fel a kérdés, hogy melyik szolgáltató tanúsítványa a megbízható gyökértanúsítvány. Önhitelesített tanúsítványt – amely gyökér tanúsítványként is működhet – bárki bármikor kibocsáthat önmagának, de ettől ez még nem lesz megbízható tanúsítvány. *Egy tanúsítvány attól „megbízható", hogy mások megbíznak benne*, tehát elfogadják azokat az aláírásokat, amelyeket erre a tanúsítványra vezetnek vissza. Bizonyos szolgáltatók dönthetnek úgy, hogy bizonyos kulcsaikat önhitelesített gyökér tanúsítványként is közzéteszik, így lehetővé teszik, hogy mások aláírásokat vezessenek vissza e tanúsítványokra. A felhasználók, azaz a piac

dönti el, hogy megbízik-e ebben a tanúsítványban, és elismeri-e gyökértanúsítványnak. E döntés kimenetele függhet attól, hogy mekkora a bizalom a szolgáltató informatikai rendszere iránt, mekkora anyagi felelősséget vállal a szolgáltató a rendszer helyes működéséért, mennyire könnyen érhetőek el a visszavonási információk, mennyire könnyű hitelesen hozzáférni a gyökér tanúsítványhoz, és hány aláírás és időbélyeg vezethető vissza rá. Természetesen függ a jogszabályoktól is, például attól, hogy minősített tanúsítványokat bocsát-e ki a szolgáltató e tanúsítvány alapján. *Aláíráskor az aláíró visszavezetheti az aláírást valamelyik önhitelesített tanúsítványra, a befogadó pedig keres egy olyan gyökértanúsítványt, amelyikre az aláírás szintén visszavezethető.* A két gyökér nem feltétlenül ugyanaz.



3. ábra – Egy kusza, de realisztikus szituáció

Béla határozza meg, hogy mely gyökereket fogad el megbízható tanúsítványnak, de – attól függően, hogy milyen szoftvert használ az aláírás ellenőrzésére – szoftverében már eleve telepítve vannak bizonyos gyökerek. Sajnos nem általános, hogy a magyar hitelesítés szolgáltatók tanúsítványai szerepelnének a külföldi szoftverekben. Ezért az a jellemző, hogy az Aladár tanúsítványát kibocsátó HSZ1 tanúsítványa a jogszabályok szerint érvényes, de a Béla szoftverében lévő egyik megbízható tanúsítványra sem vezethető vissza. Ha egyáltalán visszavezethető Aladár aláírása egy olyan tanúsítványra, amelyben Béla megbízik, akkor sem nyilvánvaló, hogy Béla szoftvere megtalálja ezt a láncot. Megoldást jelent e problémára, ha Aladár, az aláíró maga építi fel a tanúsítványláncot, és az aláírásával együtt azt is elküldi Bélának. Ugyanakkor, ha Béla kizárólag az Aladártól kapott tanúsítványláncra hagyatkozik, akkor előfordulhat az a szerencsétlen eset, hogy Béla nem bízik meg abban a tanúsítványban, amelyikre Aladár visszavezette az aláírását, pedig van egy másik olyan megbízható tanúsítvány Béla tanúsítványtárában, amelyre az aláírás visszavezethető lett volna.

A [Ket] megjelenése előtt a magyar szolgáltatók önálló gyökér tanúsítványokkal rendelkeztek. Így csak az fogadhatta el az összes magyar elektronikus aláírást, aki minden magyar hitelesítés szolgáltató minden gyökér tanúsítványát megbízható tanúsítványnak fogadta el. A [Ket] szerint egy közigazgatási gyökér hitelesítés szolgáltató [KGYHSZ] jött létre, amely

tanúsítványt bocsát ki a közigazgatásnak is szolgáltató hitelesítés szolgáltatók bizonyos kulcsai számára. Így bizonyos aláírások esetén a KGYHSZ tanúsítványa közös megbízható gyökér tanúsítványt jelent. Sajnos a KGYHSZ időbélyegzőket és OCSP válaszadókat nem tanúsíthat felül, emiatt az ezeket tartalmazó aláírás (és hosszú távú aláírás mindig tartalmaz ilyet) ellenőrzésekor a hitelesítés szolgáltatók eddigi gyökér tanúsítványaira is szükség van. Tehát a KGYHSZ csak részmegoldást nyújt a problémára.

6. Minek a visszavonási állapotát ellenőrizzük és hogyan?

Ha egy tanúsítványhoz tartozó titkos aláírókulcs elvész vagy illetéktelen kezekbe kerül (például, ha a tanúsítványhoz tartozó kártyát ellopják), szólni kell a hitelesítés szolgáltatónak, és az visszavonja a kibocsátott tanúsítványt. A visszavonás azt jelenti, hogy a hitelesítés szolgáltató közzéteszi, hogy a tanúsítvány érvénytelen. Ezért mielőtt elfogadunk egy tanúsítványt, meg kell győződnünk róla, hogy a tanúsítvány nincs visszavonva (vagy felfüggesztve). Magyarországon két technológia terjedt el, amelyek segítségével megtudhatjuk egy tanúsítvány visszavonási állapotát: az egyik a visszavonási lista (CRL), a másik pedig a kérdés-válasz alapú online tanúsítvány-állapot szolgáltatás (OCSP). A visszavonási lista a visszavont tanúsítványok sorozatszámát tartalmazza. Minden magyar hitelesítés szolgáltató bocsát ki visszavonási listát, és a visszavonási listák ingyenesen elérhetőek. Az online tanúsítvány-állapot szolgáltatás egy olyan protokollt jelent, amellyel rákérdezhetünk, hogy egy tanúsítvány az adott pillanatban érvényes-e, és kérdésünkre a szolgáltató azonnali hiteles választ ad, így sok esetben gyorsabb, praktikusabb, mint a CRL. A négy magyar kereskedelmi hitelesítés szolgáltatóból három nyújt OCSP szolgáltatást.

Két okból van szükség visszavonási információkra (CRL-ekre és OCSP válaszokra): Egyrészt, aláírás befogadásakor a visszavonási információk alapján állapítjuk meg, hogy a tanúsítvány az aláírás pillanatában érvényes volt-e. Másrészt, később a visszavonási információk segítségével igazolhatjuk, hogy az aláírást valóban megalapozottan fogadtuk el. Ezáltal a visszavonási információk védik az aláírás befogadóját, és biztosítják az aláírás letagadhatatlanságát. A gyakorlatban előfordulhat, hogy a visszavonási információkat később nem könnyű összegyűjteni (például azért, mert az [RFC3280] szerint CRL nem feltétlenül tartalmazza a már lejárt tanúsítványokat), így elterjedt, hogy a visszavonási információkat nem a befogadó gyűjti össze, hanem az aláíró csatolja őket az aláírásához. Ezt általában a befogadó kényszeríti ki: kijelenti, hogy csak olyan aláírásokat fogad, amelyek tartalmazzák az aláírásra vonatkozó visszavonási információkat. Milyen információk tartoznak ide? Az aláíró tanúsítványától a megbízható gyökér tanúsítványig tartó tanúsítványlánc minden elemére

vonatkozó visszavonási lista vagy OCSP válasz, amely igazolja, hogy az adott tanúsítvány az aláírás időpontjában érvényes volt. Ha az aláírás időbélyeget is tartalmaz (lásd 4. fejezet), akkor az időbélyegre vonatkozó visszavonási információkra is szükség van. Emellett, a visszavonási információkon is aláírás szerepel, így az aláírás ellenőrzéséhez a visszavonási információkon lévő aláírásokra vonatkozó visszavonási információk is szükségesek.

Ha azt szeretnénk eldönteni, hogy elfogadhatunk-e egy aláírást, akkor arra a kérdésre keressük a választ, hogy a tanúsítvány *az aláírás időpontjában érvényes volt-e*. Ebből következően, pusztán az aláírás időpontja előtt kibocsátott visszavonási listák és OCSP válaszok alapján nem fogadhatunk el aláírást, hanem az aláírás időpontját követő visszavonási listára vagy OCSP válaszra van szükségünk. Tegyük fel, hogy egy szolgáltató minden nap éjfélkor bocsátja ki a CRL-ét. Ilyenkor, ha egy aláírás délután 2-kor jön létre, akkor egészen addig nem lehet CRL alapján megállapítani, hogy érvényes-e, amíg a következő CRL meg nem jelenik. Lehet, hogy a tanúsítványt reggel 9-kor visszavonták, de CRL alapján várhatóan csak éjfélkor szerzünk tudomást erről. Ez azt jelenti, hogy az aláírt dokumentummal kapcsolatban érdemi döntést éjfél előtt nem hozhatunk. A szakirodalom „kivárási időnek” (grace period) nevezi azt az időszakot, amikor az aláírás már rendelkezésre áll, de a visszavonási információk beszerzéséig nem lehet megállapítani az érvényességét. OCSP használata esetén a fenti probléma esetleg meg sem jelenik. OCSP segítségével a délután 2-kor létrehozott aláírás érvényességét akár 2:01-kor is megkérdezhetjük, és a kérdésre a hitelesítés szolgáltató azonnali, aláírással hitelesített választ ad. Egyes szolgáltatók vállalják, hogy soron kívül kibocsátanak egy új CRL-t, ha egy tanúsítvány visszavonási állapota megváltozik. Ha azt látjuk, hogy nem jelent meg új CRL, akkor a tanúsítvány érvényes ugyan, de nem rendelkezünk olyan visszavonási információval, amelyet az aláíráshoz csatolhatnánk, hogy később bizonyíthassuk annak érvényességét. OCSP esetén nincsen ilyen probléma, mert érvényes tanúsítvány esetén is hiteles OCSP választ kapunk, amelyet csatolhatunk az aláíráshoz. További probléma a CRL-lel, hogy a szabványok nem írják elő, hogy az alkalmazásoknak figyelnie kell a soron kívül kibocsátott CRL-eket, így nem biztos, hogy minden szabványos alkalmazás mindig ugyanarra az eredményre jut, ha tanúsítványt CRL alapon ellenőriz.

A szabványok szerint *a tanúsítványláncban szereplő minden tanúsítvány visszavonási állapotát ellenőriznünk kell*. Ezen ellenőrzés történhet *elektronikusan* CRL vagy OCSP alapján, vagy *manuálisan*, amikor a szolgáltató vállalja, hogy például újsághirdetést tesz közzé, ha aláírókulcsa illetéktelen kezekbe kerül. Ha sok embernek gyakran kell elvégeznie az ellenőrzést, akkor az elektronikus megoldás mindenképpen olcsóbb. A manuális megoldás

viszont néha elkerülhetetlen, az önhitelesített gyökér tanúsítványok visszavonási állapotát például kizárólag így lehet ellenőrizni. Egy nagy rendszerben az a jó, ha a lehető legkevesebb olyan tanúsítvány van benne, amelyet csak manuálisan lehet ellenőrizni, s amelyekre a többi tanúsítványt visszavezetjük. *Ha több szolgáltatói tanúsítvány szerepel a tanúsítványláncban, akkor az egyes szolgáltatóknál jelentkező kivárási idők legnagyobbika számít.* Tegyük fel, hogy a 2. ábrán szereplő HSZ1 naponta bocsát ki visszavonási listát, HSZ2 pedig havonta (amely igen gyakori gyökér hitelesítő egységek esetén). Ekkor, ha Aladár aláírását HSZ2 gyökér tanúsítványára szeretnénk visszavezetni, és a tanúsítványlánc elemeit CRL alapján ellenőrizzük, akkor akár 1 hónapot kell várnunk Aladár aláírásának ellenőrzéséhez. OCSP segítségével ez az ellenőrzés is mindössze néhány másodperc. Ha gyorsan szeretnénk ellenőrizni egy aláírást, akkor az OCSP egyértelműen jobb technológia a CRL-nél, de ha sok aláírt dokumentumot szeretnénk tárolni, akkor a CRL a praktikusabb megoldás: ilyenkor egyetlen CRL sok aláírás érvényességét igazolhatja, míg OCSP esetén külön OCSP válasz szükséges minden egyes aláíráshoz. [Msc2005], [R1998]

A közigazgatási keretrendszer mind a CRL, mind az OCSP technológiát elismeri. Kötelezi a hitelesítés szolgáltatókat, hogy egy visszavonás bejelentésétől számított 4 órán belül új CRL-t tegyenek közzé, ezzel felgyorsítja a CRL alapú ellenőrzést. Sajnos egyúttal az aláírás formátumáról szóló specifikációban mind a CRL, mind az OCSP használata esetén 4 óra kivárási időt ír elő. Ezen előírás akkor is érvényes, ha a hitelesítés szolgáltató 4 óránál sokkal gyorsabban fel tud dolgozni egy visszavonási kérelmet. A felhasználónak ekkor is 4 órát kell várnia, mert csak ekkor tudja később igazolni, hogy egy aláírást valóban jogosan fogadott el. A keretrendszer nem ösztönzi a hitelesítés szolgáltatókat, hogy versenyezzenek, hogy melyik biztosít gyorsabb, megbízhatóbb, jobb minőségű visszavonás kezelést. Ehelyett rákényszeríti a felhasználókra a gyenge technológiákat alkalmazó hitelesítés szolgáltatók nyújtotta minőséget. Ez azt eredményezi, hogy az elektronikus aláírással történő közigazgatási ügyintézés legalább 4 óráig mindenképpen eltart, pusztán az elektronikus aláírás ellenőrzése miatt. Eközben a négy magyar kereskedelmi hitelesítés szolgáltató közül három is (Microsec, Magyar Telekom, Máv Informatika) felelősséget vállal azért, hogy azonnal (azaz nem 4 óra alatt) tudja megváltoztatni az általa kibocsátott tanúsítványok visszavonási állapotát.

A keretrendszer szerint minden aláírást a KGYHSZ tanúsítványára kell visszavezetni. Így a tanúsítványláncban három tanúsítvány szerepel: az aláíró tanúsítványa, az „első szintű” hitelesítés szolgáltató tanúsítványa és a KGYHSZ gyökér tanúsítványa. Az első szintű hitelesítés szolgáltatók 24 óránként adnak ki CRL-t, és közülük három OCSP szolgáltatást is nyújt. A KGYHSZ (amely csak az első szintű hitelesítés szolgáltatóknak ad tanúsítványt) 35

naponta, de visszavonás esetén 1 napon belül bocsát ki új CRL-t. A KGYHSZ nem nyújt OCSP szolgáltatást, igaz, a tanúsítványában – nagyon bölcsen – elhelyezték egy később bekapcsolható OCSP szolgáltatás elérhetőségét. Ha a KGYHSZ tanúsítványára vezetünk vissza egy aláírást, akkor esetleg csak 35 nap után tudjuk igazolni, hogy valóban gondosan ellenőriztük az aláíró tanúsítványának érvényességét.

7. Ki írta alá a dokumentumot?

Az aláíró személyéről az aláírásban szereplő aláírói tanúsítvány révén kaphatunk információt. Sajnos – ahogy erre [ES2000] is rámutat – a tanúsítványban szereplő adatok alapján nem feltétlenül könnyű feladat megállapítani, hogy ezen adatok pontosan mely személyt jelentik. A magyar hitelesítés szolgáltatók adatvédelmi okok miatt csak akkor írhatnák bele a tanúsítványba az aláíró valamely igazolványának számát, ha az aláíró ebbe beleegyezik. Ez azt jelenti, hogy az aláírást befogadó fél nem várhatja el, hogy az aláíró tanúsítványában igazolványszám szerepeljen. Így az elektronikus aláírásból – a kézzel írott aláíráshoz hasonlóan – egyetlen egy információ derül ki biztosan az aláíróról: a neve.

Tovább bonyolítják a problémát az úgy nevezett *álneves tanúsítványok*. Az [Eat] lehetővé teszi, hogy a tanúsítványban ne az aláíró valódi neve, hanem „álnév” szerepeljen. A magyar hitelesítés szolgáltatóknak kötelező lehetővé tenni, hogy ügyfeleik álneves tanúsítványt is igényelhessenek, így ha elektronikusan aláírt dokumentumot kapunk, célszerű megvizsgálni, hogy nem álneves-e a tanúsítvány. Ha a tanúsítvány álneves, a benne lévő név nem az aláíró neve. Az [Eat] szerint az álneves tanúsítványban jelölni kell, ha a tanúsítvány álnevet tartalmaz. Sajnos a magyar hitelesítés szolgáltatók ezt többféle módon jelölik, így ahány szolgáltató, annyi módon lehet ellenőrizni, hogy a tanúsítvány álneves-e. Az álneves tanúsítvánnyal aláírt minősített aláírás azonos bizonyító erővel bír, mint az, amelyiket nem álneves tanúsítvánnyal hoztak létre, csupán az nem derül ki belőle, hogy pontosan ki hozta létre az aláírást, ki vállalt az aláírással kötelezettséget. Bíróság elkérheti a hitelesítés szolgáltatótól az álnevet viselő személy adatait, de senki nem tudja megállapítani az aláíró személyazonosságát, amíg eddig nem fajul az ügy. Így az álneves aláírás hiába érvényes, hiába bír jogilag bizonyító erővel, általában senki nem hajlandó elfogadni azt.

A közigazgatási keretrendszer meghatározza, hogy milyen formátumú tanúsítványokat használhatnak a közigazgatást képviselő személyek, és azt is, hogy a közigazgatáshoz milyen formátumú tanúsítványokkal fordulhatunk. E keretrendszer határozott útmutatást ad arra, hogy mely mezőbe pontosan milyen értékek kerülhetnek, láthatóan a szolgáltatók hajlandóak tanúsítványprofiljaikat a közigazgatás által megadott, a szabványoknak és nemzetközi

ajánlásoknak is megfelelő profilra alakítani. Így e keretrendszer rendet tesz a hazai kusza tanúsítványprofilok között. A keretrendszer – nagyon helyesen – kizárja az álneves tanúsítványok használatát is. Adatvédelmi okok miatt csak az aláíró neve derülhet ki az elektronikus aláírásából, így az aláírást befogadó fél két módon járhat el: Feltételezheti, hogy az aláíró az, akinek mondja magát. Amennyiben e feltételezés hamisnak bizonyul, akkor bíróság előtt felelősségre vonhatja, és a bíróság már jogosult utánajárni, hogy pontosan ki készítette az aláírást. Másik lehetőség, hogy különböző trükkös módszerekkel igyekszik meggyőződni az aláíró kilétéről. Ma többen használják azt a módszert, hogy egy szervezettől papíron kiállított, cégszerűen aláírt igazolást kérnek arról, hogy az adott (kiállítójú és sorozatszámú stb.) tanúsítvány birtokosa jogosult elektronikusan eljárni a szervezet nevében. A közigazgatás egy „viszontazonosítás” névre hallgató protokollt dolgozott ki, amelyben az aláírást befogadó közigazgatási szerv XML alapú kérdéseket tehet fel a hitelesítés szolgáltatónak. Az aláíró természetes azonosító adataira (neve, anyja neve, születési ideje) kérdezhet rá, amelyre a hitelesítés szolgáltató csak „igen” vagy „nem” választ adhat. A világon egyedi PKI-megoldásról van szó, amely a „barkohba” nevű játékra emlékezetet.

8. Jogosan írta-e alá az aláíró a dokumentumot?

Ha tudjuk, hogy az aláíró kicsoda, akkor is felmerül a kérdés, hogy jogosan írta-e alá a dokumentumot. Ugyanez a probléma merül fel a kézzel írott aláírások esetében is, csak a papíron történő ügyintézés esetén sokkal lassabb, valamint a kézzel írott aláírásokat ellenőrző emberek sokkal kevésbé hajlamosak szarvashibákat elkövetni, mint az automaták. Így e probléma nem az elektronikus aláírás technológiából, hanem az automatizált elektronikus ügyintézésből, a gyors elektronikus kommunikáció támasztotta követelményekből ered.

A tanúsítványban fel lehet tüntetni, hogy az aláíró mely szervezethez tartozik. Az jelenti a nehéz kérdést, hogy az aláíró jogosult-e az adott szervezet nevében aláírni és amennyiben igen, akkor pontosan milyen feltételek mellett. Sok hitelesítés szolgáltató feltünteti a tanúsítványban az aláírási jogosultságot, de itt sem beszélhetünk egységes jelölésrendszerről. Ennek megfelelően a közigazgatás – logikusan – megtiltja, hogy kizárólag a tanúsítvány alapján állapítsák meg a közigazgatás egy ügyfelének képviseleti jogosultságát. A keretrendszer külön hitelesítési rendeket definiál a közigazgatás szereplői és a közigazgatás ügyfelei számára, így a hitelesítési rend alapján számítógép is el tudja dönteni például azt, hogy egy adott aláírást valóban köztisztviselő hozott-e létre. Praktikus megoldásról van szó, amely reális, elérhető célt tűzött ki, és a szabványoknak megfelelő módon éri el azt.

9. Mi a biztosíték arra, hogy bízhatunk a tanúsítványban?

Ha elfogadunk egy elektronikus aláírást, akkor – a hitelesítés szolgáltató által kibocsátott tanúsítvány alapján – elhisszük, hogy az aláírás létrehozásához használt aláírókulcs az aláírás pillanatában az aláíró birtokában volt. A hitelesítés szolgáltató garantálja, hogy a tanúsítvány kibocsátásakor az aláírókulcs az aláíró birtokában volt, és amint tudomást szerez róla, hogy ez már nem így van (például az aláíró bejelenti, hogy elveszítette az intelligens kártyáját), a hitelesítés szolgáltató haladéktalanul visszavonja a tanúsítványt. Természetesen előfordulhat, hogy a hitelesítés szolgáltató hibázik. Bármilyen erős biztonsági intézkedések is működnek nála, előfordulhat, hogy valaki megtéveszti a szolgáltatót, és valaki egy másik ember nevében igényel tanúsítványt, de az is lehet, hogy a szolgáltató nem elég gyorsan von vissza egy kibocsátott tanúsítványt. Ekkor előfordulhat, hogy az aláírást nem a tanúsítványban szereplő aláíró hozza létre, és ez nem derül ki a tanúsítványra vonatkozó visszavonási információkból. *Ha a hitelesítés szolgáltató hibájából valakinek kára keletkezik, a szolgáltató köteles megtéríteni a kárt – az adott tanúsítványra vonatkozó feltételek szerint.* Az [Eat] szerint *a hitelesítés szolgáltató korlátozhatja* az egyes tanúsítványokkal egy alkalommal vállalható kötelezettség mértékét. Ezzel a szolgáltató az egy aláírással okozható kár mértékét, és így *saját kártérítési kötelezettségét* korlátozza. Az [Eat] szerint e korlátozást fel kell tüntetni a tanúsítványban. Ez az érték az ún. *tranzakciós limit*.

A kézzel írott aláírást tipikusan személyi igazolvány vagy aláírási címpéldány alapján szokás ellenőrizni. Általában attól függ, hogy milyen alaposan ellenőrzünk egy kézzel írott aláírást, hogy mekkora kárunk származhat abból, ha az aláírás nem érvényes. Ha elektronikus aláírással kötjük a szerződést, akkor is mérlegelnünk kell, hogy mennyire fontos, hogy a másik fél aláírása érvényes legyen. Elektronikus aláírás esetében is léteznek különféle szintek (pl. a teljes tanúsítványlánc megkövetelése, az aláírás időpontja után kibocsátott visszavonási információk megkövetelése), de bármilyen gondosan is járunk el az aláírás ellenőrzésekor, a hitelesítés szolgáltató hibája ellen egyedül a szolgáltató kártérítési kötelezettsége véd bennünket. Ez biztosít bennünket arról, hogy nem lesz anyagi kárunk abban az (egyébként rendkívül kis valószínűségű) esetben sem, amikor a hitelesítés szolgáltató hibát követ el. A kártérítési kötelezettség egyúttal arra ösztönzi a szolgáltatót, hogy saját informatikai rendszerét és belső szabályzatait úgy alakítsa ki, hogy a hiba valószínűsége a lehető legkisebb legyen. Például, a 2. ábrán szereplő tanúsítványlánc a következőket jelentheti: A „HSZ2” tanúsítványról tudom, hogy a HSZ2 szolgáltatóé, és HSZ2-ben megbízom. HSZ2 azt állítja, hogy a „HSZ1” tanúsítvány a HSZ1 szolgáltatóé. HSZ1 pedig azt állítja, hogy az „Aladár”

tanúsítvány Aladáré. Nemcsak az számít, hogy Aladár mennyire megbízható; az „Aladár” tanúsítvánnyal történő aláírás semmit sem ér, ha HSZ1 vagy HSZ2 állítása hamis. *Mennyire bízhatunk HSZ1 vagy HSZ2 állításában?* Mekkora kárt hajlandóak megtéríteni, ha kiderül, hogy hibáztak? *Mennyire biztonságosan kezelik a tanúsítványaikat*: mit mondanak*, milyen értékű tranzakciókhoz használhatóak?*

Aláírás befogadásakor meg kell vizsgálnunk, hogy az aláíráshoz tartozó tanúsítványért mely hitelesítés szolgáltató vállal felelősséget. Ha a tanúsítványláncban több szolgáltató is szerepel, akkor célszerű egészen a gyökér tanúsítványig ellenőrizni, hogy mely tanúsítványért mekkora kártérítési kötelezettséget vállal a tanúsítványt kibocsátó szolgáltató. Emellett mérlegelnünk kell, hogy az aláíró az aláírt dokumentumban mekkora kötelezettséget vállal (nem pénzügyi jellegű dokumentum esetén ez nem könnyű feladat), és ennek függvényében kell döntenünk, hogy az adott esetben az elfogadjuk-e az adott aláírást. Sok szolgáltató 0 Ft tranzakciós limittel is bocsát ki tanúsítványt. Az ilyen tanúsítványokkal elvileg semekkora anyagi kötelezettség nem vállalható, így elképzelhető, hogy a szolgáltató egyáltalán nem vállal anyagi felelősséget a tanúsítvány helyes kezeléséért. Nehéz megítélni, hogy ez pontosan mit jelent, várhatóan az ezzel kapcsolatos bírói ítéletek alakítják majd ki, hogy a tranzakciós limit hogyan viszonyul a szolgáltatók kártérítési kötelezettségéhez.

A KGYHSZ minden felelősséget elhárít a hitelesítési rendjében az általa kibocsátott szolgáltatói tanúsítványokkal kapcsolatban. [KGYHSZ] Ez igen bizarr esetet eredményez: a közigazgatás egy olyan szolgáltatóra vezette vissza minden elektronikus aláírás biztonságát, amely semmilyen pénzügyi garanciát nem tud vállalni a saját biztonságos működéséért. Így gazdasági erő nem ösztönzi a KGYHSZ-t biztonságos működésre. Míg a közigazgatási szervek számára előírás a KGYHSZ gyökér-tanúsítványának használata, a magánszférára ez nem vonatkozik. Ha egy vállalat a KGYHSZ tanúsítványára visszavezetett aláírást kap, akkor azt látja, hogy ha a KGYHSZ hibát követ el, abból olyan kára származhat, amelyet senki nem köteles neki megtéríteni. Így nem várható, hogy egy gazdasági szempontból racionálisan gondolkodó szervezet elfogadja a KGYHSZ tanúsítványára visszavezetett aláírásokat.

10. Összefoglalás

Egy elektronikus aláírás elfogadásához számos feladatot kell elvégeznünk. Ezek jelentős részét szoftver is megoldhatja helyettünk, egy másik részéhez azonban emberi döntés szükséges – akárcsak a papíron történő aláírások esetében. A közigazgatás által kidolgozott keretrendszer ezen lényeges problémákra ad egyfajta választ. E keretrendszer szükséges: aki úgy dönt, hogy elektronikus aláírást is elfogad, az jól teszi, ha meghatározza, hogy pontosan

milyen aláírást fogad el. Ugyanakkor, ha később egy másik közösség – például a bankok, vagy az EU – hasonló szintű elvárásokat – például saját gyökeret – határoz meg, az nagyon könnyen előidézheti, hogy a két követelményrendszer kölcsönösen kizárja egymást és az egyik rendszerben használt tanúsítványokat, aláírásokat a másik rendszer nem fogadja el. A közigazgatás alaposan kidolgozott, a nemzetközi szabványoknak megfelelő specifikációt készített, amely – egy-két szerencsétlen megoldástól (pl. a kötelezően 4 órás kivárási idő, és az OCSP nélküli, minden felelősséget kizáró KGYHSZ) eltekintve – hasznos, mert várhatóan összefogja, egységesíti a hazai elektronikus aláírás piacon használt technológiák sokaságát.

Nem véletlen, hogy az elektronikus aláírás csak lassan kezdett terjedni. A gyakorlati alkalmazás számos olyan problémát vetett fel, amelyre sem a technológia, sem a jogszabályok nem adnak közvetlen választ. Ha pusztán a rendszer egyes elemeit nézzük – például a hitelesítés szolgáltató, vagy egy PKI-ra épülő alkalmazás fejlesztőjének szemszögéből – e problémák gyakran nem látszanak. Egy hitelesítés szolgáltatónak sokkal egyszerűbb dolga van, ha nem nyújt OCSP szolgáltatást, és az alkalmazásfejlesztőnek is egyszerűbb a dolga, ha nem foglalkozik a kivárási idővel, vagy esetleg a felhasználóra bízza a szolgáltatói tanúsítványok visszavonási állapotának ellenőrzését. Talán az a helyes, ha egy PKI-ra épülő rendszert a legfontosabb résztvevője, a *felhasználó* szemszögéből nézzük. Fontos, hogy a felhasználó értelmes, elfogadható választ kapjon az itt felsorolt kérdésekre, kizárólag ekkor jelenthet számára hasznos, költség-hatékony megoldást az elektronikus aláírás technológiája.

11. Hivatkozások

[BV2004] Buttyán L., Vajda I., *Kriptográfia és alkalmazásai*, Typotex Kiadó, 2004.

[CWA14171] CWA 14171, General guidelines for electronic signature verification, 2004.

[Eat] 2001. évi XXXV. törvény az elektronikus aláírásról.

[ES2000] Ellison, C. & Schneier, B.: Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, Computer Security Journal, v 16, n 1, 2000.

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

[Kozig] A közigazgatás elektronikus aláírással kapcsolatos ajánlásai www.ihm.gov.hu/jogszabalyok/kapcsolodo_ajanlasok?ayear=2006&amonth=0

[KGYHSZ] A Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) honlapja, hitelesítési rendje, 2006., http://www.kgyhsz.gov.hu/

[Msc2005] Berta I., A CRL és az OCSP összehasonlítása, Microsec Kft., 2005. http://www.e-szigno.hu/wp_crl_vs_ocsp.html

[R1998] Rivest, R.: Can we eliminate Certificate Revocation Lists?, Financial Cryptography, 1988., http://citeseer.ist.psu.edu/rivest98can.html

[RFC3280] Certificate and Certificate Revocation List (CRL) Profile, 2002.

[XAdES] ETSI TS 101 903 XML Advanced Electronic Signatures, V1.2.2 2004.