MINŐSÍTETT ARCHIVÁLÁS SZOLGÁLTATÁS BEINDÍTÁSA MAGYARORSZÁGON

Dr. Berta István Zsolt, istvan.berta@microsec.hu
Endrődi Csilla Éva, csilla@microsec.hu
Microsec Kft.

Absztrakt

A papír alapú dokumentumokhoz hasonlóan az elektronikus (és elektronikusan aláírt) dokumentumokat is speciális körülmények között, biztonságosan kell tárolni, hogy a dokumentum (és a rajta lévő aláírás) ne sérüljön meg, és a dokumentum hitelessége hosszú távon – akár évtizedekig, sőt évszázadokig is – biztosítható legyen. Azért van erre szükség, mert a technológia hirtelen fejlődése, illetve bizonyos ritka (rövidtávon valószínűtlen, de hosszútávon már reálisan előforduló) események miatt a korábban biztonságos technológiával létrehozott aláírások később hamisíthatóakká válhatnak.

Az elektronikus aláírásról szóló törvényben definiált archiválás szolgáltatás az elektronikus aláírások hosszú távú érvényességének biztosítására szolgál. Az archiválás szolgáltató a jogszabályok szerint rendszeresen egyre erősebb technológia szerinti új időbélyeggel látja el a letétbe helyezett elektronikusan aláírt dokumentumokat, így biztosítja az archivált aláírások hosszú távú érvényességét.

A hitelesítés szolgáltatással, tanúsítványok kibocsátásával kapcsolatban létezik olyan nemzetközi gyakorlat, léteznek olyan nemzetközi szabványok és specifikációk, amelyekhez a magyar szolgáltatók alkalmazkodhatnak. Ezzel szemben, az elektronikus archiválással kapcsolatban nem beszélhetünk ehhez hasonlóan letisztult nemzetközi gyakorlatról.

Magyarországon 2007 elején indult el az első minősített archiválás szolgáltató. Cikkünkben az archiválás szolgáltatás megtervezésével, kialakításával és megindításával kapcsolatos tapasztalatainkat, valamint az új szolgáltatás jelentette kihívásokat mutatjuk be.

1 Letagadhatatlanság és bizonyító erő

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény [Eat] szerint az elektronikus aláírás megfelel az írásba foglaltság követelményeinek, a minősített elektronikus aláírással hitelesített dokumentum pedig a polgári perrendtartásról szóló törvény szerint teljes bizonyító erejű magánokiratnak minősül. Így az elektronikus aláírásról szóló jogszabályok a *letagadhatatlanság* néven ismert műszaki fogalmat a *bizonyító erő* nevű jogi fogalomra vezetik vissza.

Bármekkora bizonyító erővel is rendelkezik egy elektronikus aláírás, egy bíróság – indokolt esetben, egy esetleg igen bonyolult eljárás során – megkérdőjelezheti annak érvényességét. (Például, ha bizonyítható, hogy az aláírást nem az aláíró személy, hanem például az ő számítógépét irányító vírus hozta létre.) A letagadhatatlanság műszaki fogalom, azt jelenti, hogy gyakorlatilag kizárható, hogy egy adott tanúsítvány alapján elfogadható aláírást nem a tanúsítványhoz tartozó magánkulccsal hoztak létre. Jogi értelemben letagadhatatlanságról nem, hanem csak bizonyító erőről beszélhetünk.

Egy elektronikus aláírás kizárólag akkor rendelkezhet – jogi szempontból – bizonyító erővel, ha „érvényes”, tehát letagadhatatlansága műszaki szempontból bizonyítható.

2 Az elektronikus aláírások hosszú távú érvényessége

Egy tanúsítványhoz tartozó magánkulcs segítségével hozhatunk létre elektronikus aláírást. Ha aláíráskor érvényes a tanúsítványunk, akkor érvényes aláírást hozunk létre, és nem szeretnénk, hogy ez az aláírás később mégis érvénytelenné válhasson. Ha az aláírás később érvénytelenné válhat, akkor nem letagadhatatlan. Attól függ, hogy az aláírásunk érvényes marad-e később is vagy sem, hogy később is tudjuk-e majd bizonyítani – műszaki szempontból – az érvényességét. [Msc2007]

Előfordulhat, hogy a tanúsítványunk, amely alapján az aláírást létrehoztuk, érvénytelenné válik – lejár, vagy visszavonják. (A visszavonás történhet azért, mert később, az aláírást követően elvesztettük a tanúsítványhoz tartozó magánkulcsot, vagy mert valamely adatunk megváltozott.)

Ha egy aláírás esetén azt látjuk, hogy az aláíró tanúsítványa már nem érvényes, önmagában az aláírásból többé nem tudjuk megállapítani, akkor érvényes volt-e, amikor az aláírást elkészítették. Lehet, hogy azt meg tudjuk mondani, hogy a tanúsítvány mikor vált érvénytelenné[1], de azt nem tudjuk biztosan megmondani, hogy az aláírás mikor készült. (Előfordulhat, hogy az aláírás tartalmaz ugyan utalást az elkészítésének időpontjára, de ezt nem fogadhatjuk el megbízható időpontnak. Egy személyi számítógép órája egyrészt nem pontos, másrészt nagyon könnyű átállítani, manipulálni.) Ha nem tudunk valamilyen más módon meggyőződni arról, hogy az aláírás mikor készült, akkor műszaki szempontból nem tudjuk bizonyítani az aláírás érvényességét, tehát az aláírást érvénytelennek kell tekintenünk.

Ha az aláíráson időbélyeget helyezünk el, akkor – egy időbélyegzés szolgáltató, tehát egy megbízható harmadik fél állítása alapján – bizonyíthatjuk, hogy az aláírás mikor (pontosabban, mely időpont előtt) készült.

Az időbélyeg egy megbízható időbélyegzés szolgáltató által kibocsátott, aláírt igazolás arról, hogy az időbélyegzett adat (esetünkben az aláírás) az időbélyegzés pillanatában már létezett. Az időbélyegzés szolgáltatók nagyon vigyáznak az időbélyegek aláírására használt magánkulcsukra, de mégis előfordulhat, hogy ez illetéktelen kezekbe kerül. Mi történik ilyenkor? A támadó, aki megszerezte az időbélyegzés szolgáltató magánkulcsát, ezentúl tetszőleges időpontot beleírhat az időbélyegekbe. Így hiába vonják vissza egy időbélyegzés szolgáltató tanúsítványát: ha a támadó visszadátumozott időbélyegeket bocsát ki, azokról már nem lehet megállapítani, hogy a visszavonás után készültek. Hasonló helyzet áll elő, ha az időbélyegzés szolgáltató tanúsítványa lejár: ha a magánkulcs valahogy mégis illetéktelen kezekbe kerül, a támadó visszadátumozott időbélyegeket bocsáthat ki.

Ha egy időbélyegzés szolgáltató tanúsítványa már nem érvényes (mert lejárt vagy visszavonták), az adott tanúsítvány szerinti időbélyegek érvényessége PKI alapon nem, legfeljebb csak az időbélyegzés szolgáltató naplófájljai segítségével bizonyítható.

Ha egy aláíráson időbélyeget helyeztünk el, az időbélyegen új, esetleg más forrásból származó időbélyeget kell elhelyeznünk, ha azt szeretnénk, hogy az aláírás érvényessége hosszú távon is bizonyítható maradjon.

Ha hosszú távú archiválásban gondolkozunk, számolnunk kell azzal, hogy a tudomány és a technológia fejlődése miatt az aláírás készítésekor még biztonságosnak tekintett (aláíró vagy hash) algoritmusokban megrendülhet a biztonság, és egy korábban még biztonságos aláírás

[1] Ez például a visszavonási listában szereplő visszavonási időpontból állapítható meg.

(évekkel, évtizedekkel) később hamisíthatóvá válik. Ha azt szeretnénk, hogy az aláírás érvényessége hosszú távon is bizonyítható maradjon, az aláírt dokumentumon és a rajta lévő időbélyegeken új, fejlettebb technológiával készült időbélyeget kell elhelyeznünk, mielőtt a korábbi technológiában megrendül a biztonság. [Msc2006]

Összefoglalva:

- Az aláírás érvényessége akkor bizonyítható, ha az aláíró aláíráskor használt tanúsítványa még érvényes, vagy
- ha más módon, például érvényes időbélyeg segítségével bizonyítani tudjuk, hogy az aláírás akkor készült, amikor az aláíró tanúsítványa még érvényes volt.
- Az időbélyegen is (műszaki szempontból nézve) aláírás van, így egy időbélyeg érvényessége akkor bizonyítható, ha az időbélyegző tanúsítványa még érvényes, vagy
- ha más módon, például, egy másik érvényes időbélyeg segítségével bizonyítani tudjuk, hogy az időbélyeg akkor készült, amikor az időbélyegző tanúsítványa még érvényes volt.
- Az időbélyegzők lejárta és a technológia fejlődése miatt rendszeresen – néhány évenként – újra kell időbélyegeznünk az aláírásokat, hogy érvényességük bizonyítható maradjon.

Két lehetőség áll előttünk:

- Archív aláírást hozunk létre, és rendszeresen archív időbélyegeket helyezünk el rajta.
- Elektronikus archiválás szolgáltatót bízunk meg a feladattal.

A későbbiekben ezen utóbbi megoldásról írunk.

3 Mi az az archiválás szolgáltatás?

Az elektronikus archiválás szolgáltatást az elektronikus aláírásról szóló 2001. évi XXXV. törvény definiálja. Az archiválás szolgáltató feladata az elektronikusan aláírt dokumentumokon lévő elektronikus aláírások hosszú távú érvényességének biztosítása.

Az archiválás szolgáltatónak aláírásokat, illetve aláírt fájlokat küldhetünk be, és a szolgáltató megbízható, bevizsgált rendszer segítségével ellenőrzi az aláírásokat a vonatkozó szabványok, előírások szerint. [CWA14171] Az archiválás szolgáltató az archiválás időtartama alatt a jogszabályi előírások szerint folyamatosan biztosítja az archivált aláírások hitelességét. Ez többek között azt jelenti, hogy rendszeresen időbélyegeket helyez el rajtuk. Az archiválás szolgáltató ügyfelei kérésére igazolást állít ki arról, hogy egy adott aláírás érvényes. Az elektronikus aláírásról szóló törvény szerint, ha minősített archiválás szolgáltató archivál egy aláírást, vélelmezni kell, hogy az aláírás érvényes. A minősített archiválás szolgáltatókról a Nemzeti Hírközlési Hatóság vezet nyilvántartást, felügyeli őket, és éves rendszerességgel helyszíni ellenőrzést tart náluk.

Az elektronikus archiválás szolgáltatást a magyar elektronikus aláírásról szóló törvény [Eat] határozza meg. E szolgáltatás külföldön is ismert fogalom, de ott nem vonatkozik rá a hazaihoz hasonló szintű szabályozás. Az archiválás szolgáltatás nemzetközi viszonylatban is ritka jelenség, nagyon kevés szervezet foglalkozik ilyen tevékenységgel. Viszonylag új területről van szó, amely nem rendelkezik a hitelesítés szolgáltatáséhoz hasonló letisztult, és általános elfogadott követelményrendszerrel. [KOV2006], [CW2004]

A Microsec Kft. 2007 elején indította el minősített elektronikus archiválás szolgáltatását, és Magyarországon ma ez jelenti az egyetlen példát az elektronikus archiválás szolgáltatásra. [Msc2007a] A szerzők a Microsec Kft. munkatársai, jelen cikkben ezen új szolgáltatás

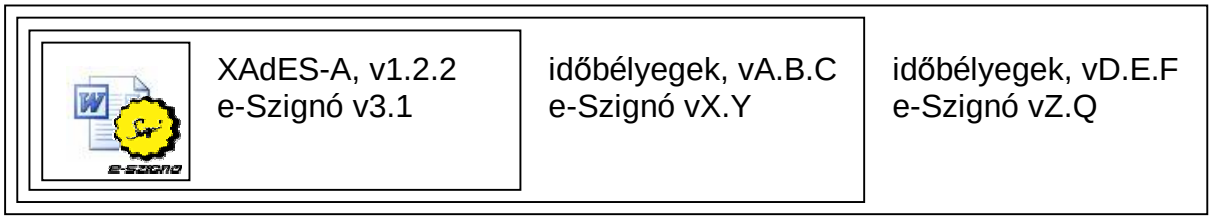
megindításával kapcsolatos tapasztalataikról, és a felmerülő főbb elvi kérdésekről számolnak be.

3.1 Követelményrendszer

Míg a hitelesítés szolgáltatásra és az időbélyegzés szolgáltatásra létezik általánosan elfogadott nemzetközi gyakorlat, és e területen léteznek átfogó, elfogadott szabványok, elektronikus archiválás szolgáltatás esetén nem beszélhetünk ehhez hasonlóan letisztult követelményrendszerről. Két olyan „legjobb gyakorlatot" találtunk, amely segítségével e probléma megközelíthető:

- Az *archív aláírás* hasonló célt tűz ki, mint az archiválás szolgáltatás; szintén az elektronikus aláírások hosszú távú érvényességének biztosítására szolgál. Az archív aláírások létrehozását, gondozását, ellenőrzését már létező nemzetközi specifikációk (ETSI TS 101 903, [XAdES]) írják le, ezek megfelelő alapot biztosíthatnak az archiválás szolgáltatás számára. Ugyanakkor, *az archív aláírás* csupán egy fájlformátum, *egy eszköz*, és közel *nem fedi le az archiválás szolgáltatás minden aspektusát*.

  Az archív aláírás arra biztosítana lehetőséget, hogy ha valaki letölt egy aláírt dokumentumot egy archiválás szolgáltatótól, akkor maga is „könnyen" meggyőződhet annak hitelességéről. Sajnos, ez a helyzet nem ennyire egyszerű.



1. ábra

  Ha egy archiválás szolgáltató hosszú ideig tárol egy archív aláírást, rendszeresen új archív időbélyegekkel kell kiegészítenie. Előfordulhat, hogy az archiválás időtartama alatt változások következnek be, könnyen lehet, hogy az archív aláírás formátumára vonatkozó specifikáció is megváltozik. A 1. ábrán látható példa szerint az eredeti archív aláírás XAdES v1.2.2 szerint készül el, de egyes archív időbélyegek már más XAdES verzió szerint (az e-Szignó aláírás-létrehozó program más változatával) kerülnek az archív aláíráshoz. Ha hosszú ideig tárolunk egy archív aláírást, több ilyen változás is bekövetkezhet, és nagyon nehézzé válhat egy aláírás ellenőrzése[2]. (Például, nem lesz egyetlen olyan XAdES verzió, amelynek az archív aláírás megfelelne, és nem lesz egy olyan e-Szignó verzió, amely ilyen formátumú aláírást hozna létre.) Eszerint *az archív aláírások fenti előnye nemigen használható ki*, és egyéb *súlyos hatékonysági kérdések* is felmerülnek az archív aláírásra alapuló archiválás szolgáltatóval kapcsolatban.

  Úgy láttuk, az archív aláírás egy nagyon hasznos eszköz az archiválás szolgáltatáshoz, merítettünk az archív aláírással kapcsolatos ismeretekből, de arra jutottunk, *nem szabad egyenlőséget tennünk az archív aláírás és az archiválás szolgáltatás közé*.

- Létezik egy „*Long-Term Archive and Notary Services*" (LTANS) elnevezésű munkacsoport, amely kifejezetten elektronikus archiválás szolgáltatásra vonatkozó követelményrendszer kidolgozásával foglalkozik. E követelményrendszer nem archív aláírás alapú, itt az archiválás szolgáltató egy adatbázist épít az aláírásokból és visszavonási információkból, és az aláírás hitelességét ezen adatbázis biztosítja (nem pedig az egyes archivált fájlok). [LTANS]

[2] Úgy látjuk, az archiválás szolgáltató által kiállított igazolásoknak lesz majd hosszú távon jelentősége.

Itt az jelentette a legnagyobb problémát, hogy – a felkészítésünk ideje alatt – az LTANS munkacsoport mindössze internet draftokat publikált, és anyagaik még RFC-ig sem jutottak el. (2007 márciusában jelent meg az első RFC-jük, de ez is csak az alapvető követelményeket írja le, ezek megvalósításával nem foglalkozik. [RFC4810])

Az általunk tervezett archiválás szolgáltató olyan megoldást alkalmaz, hogy befogadáskor archív aláírássá konvertálja az aláírásokat, de a későbbiekben nem egyenként terjeszti ki az archív aláírásokat, hanem az LTANS-éhoz hasonló megközelítéssel dolgozva, egységesen védi meg az összes archivált aláírást. Elfogadtuk és átemeltük az LTANS által megfogalmazott alapvető követelményeket. [Msc2007a]

3.2 Dokumentum vagy lenyomat archiválása?

Az Eat. két megközelítés szerinti archiválás szolgáltatást tartalmaz. Az egyik megközelítés szerint az archiválás szolgáltató az aláírt dokumentumot is megkapja és archiválja az aláírással együtt, míg a másik megközelítés szerint az archiválás szolgáltató csak az aláírást kapja meg, és magát a dokumentumot nem.

Ez a második megközelítés arra az esetre nyújt megoldást, ha az ügyfél nem szeretné, hogy az archiválás szolgáltató hozzáférjen a nyílt dokumentumhoz. E megoldásnak van egy nagyon súlyos gyenge pontja: Hogyha (például) az aláíráskor használt hash függvény elavul, előfordulhat, hogy valaki előállít egy másik olyan dokumentumot, amelyhez ugyanaz az aláírás tartozik. Ekkor az aláírás hitelessége elvész – nem lehet megállapítani, hogy eredetileg melyik dokumentumot írták alá. Ezért az Eat azt írja elő, hogy a dokumentumból rendszeresen (újabb és újabb algoritmusok segítségével) lenyomatot kell képezni, és a lenyomatokat rendszeresen be kell küldeni az archiválás szolgáltatónak. Ezt a megoldást egyrészt bonyolultnak, nehézkesnek tartjuk, másrészt több súlyos problémát is látunk vele kapcsolatban:

- Ha a hash algoritmus „hirtelen” avul el (vagy hirtelen derül fény arra, hogy már régen elavult), előfordulhat, hogy az ügyfélnek nincs ideje beküldeni az új lenyomatot, és az archivált aláírások hitelessége elvész.
- Ha az ügyfél – véletlenül vagy szándékosan – nem jó lenyomatot küld be (vagy összekeveri a beküldött lenyomatokat), szintén elvész az archivált aláírások hitelessége, és ez lehet, hogy csak sokára, akár évtizedekkel később derül ki.

A fentiek alapján azt a döntést hoztuk, hogy *a Microsec Kft. kizárólag azt a változatát nyújtja az archiválás szolgáltatásnak, amely során magát a dokumentumot is archiválja*.

3.3 Az érvényességi lánc felépítése

Ha az archiválás szolgáltató befogad egy dokumentumot, fel kell építenie az *érvényességi láncot*, vagyis össze kell gyűjtenie minden olyan információt, amely igazolja az aláírás érvényességét. Ide tartozik a tanúsítványlánc (a végfelhasználói tanúsítványtól valamely megbízható gyökértanúsítványig), valamint a tanúsítványlánc minden elemére[3] vonatkozó visszavonási információ (CRL vagy OCSP válasz), amely igazolja, hogy az adott tanúsítvány az aláírás pillanatában érvényes volt. Az aláíráshoz időbélyeg is tartozik (ha nem, akkor az archiválás szolgáltatónak kell rátennie), és az időbélyeg (vagy időbélyegekre) vonatkozó tanúsítványlánc és visszavonási információk is az érvényességi lánchoz tartoznak.

A feladatot nagyban megnehezíti az a jogszabályi követelmény, hogy az érvényességi láncot három napon belül be kell szerezni. [IHM 3/2005] Így három napon belül kell olyan CRL-

[3] a gyökértanúsítvány kivételével

eket vagy OCSP válaszokat összegyűjteni, amelyeket az aláírás időpontját követően bocsátottak ki. A legtöbb hitelesítés szolgáltató naponta bocsát ki CRL-t, de egyes szolgáltatók – különösen a gyökér hitelesítés szolgáltatók – ritkábban, a Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) például 35 naponta. (Így például KGYHSZ-re visszavezethető aláírást elvileg sem lehet értelmes módon archiválás szolgáltatóba helyezni.)

Azt tapasztaltuk, hogy CRL alapján történő ellenőrzés esetén nagyon nehéz elvi problémákkal állunk szemben. [EB2007] Az okozza a problémát, hogy a CRL-ek periodikusan jelennek meg, méghozzá az archiválás szolgáltatótól független módon. Míg az aláírások többsége nem okoz problémát, igen egzotikus speciális esetek is előfordulhatnak. OCSP esetén jelentősen egyszerűbb problémával állunk szemben, és ekkor – az OCSP sajátosságai miatt – nem jelent problémát a 3 napos korlát sem. Azt a döntést hoztuk, hogy az archiválás szolgáltató kizárólag OCSP alapon ellenőrzi a beérkező fájlokon lévő aláírásokat. (Ez sajnos kizárja a csak a KGYHSZ-re visszavezethető aláírásokat, de a KGYHSZ amúgy sem alkalmazható gyökérként a 3 napos korlát miatt.)

Tekintve, hogy idegen hitelesítés szolgáltatók által kibocsátott tanúsítványok esetén nagyon szövevényes felelősségi kérdések is felmerülnek, induláskor a Microsec Kft. által kibocsátott tanúsítványokat fogadjuk be, és később terjesztjük ki a szolgáltatást más, OCSP-t támogató szolgáltatókra.

3.4 Értelmezhetőség biztosítása

Aláíráskor műszaki értelemben mindig egy bitsorozatot írunk alá, amely valamely számítógépes programmal létrehozott, a program segítségével látható, olvasható, értelmezhető állomány. Ha az aláírt bitsorozatot ezzel a programmal megnyitjuk, akkor a program *értelmezi* a bitsorozatot, és valamilyen *értelmes tartalmat* jelenít meg nekünk. Előfordulhat, hogy ha ugyanazt a bitsorozatot másik programmal (vagy ugyannak a programnak egy másik verziójával, esetleg ugyanannak a programnak egy másképpen konfigurált változatával) nyitjuk meg, a bitsorozat másképpen jelenik meg, esetleg más tartalommal rendelkező értelmes dokumentum jelenik meg. Hiába bizonyítható, hogy milyen bitsorozatot írtunk alá, az aláírásunk „letagadhatatlanságához” az is szükséges, hogy az aláírt tartalmat hogyan kell értelmezni, megjeleníteni.

A fejlett aláírás-formátumok szerint éppen ezért nemcsak magát a dokumentumot kell aláírni, hanem például a dokumentum megjelenítésére vonatkozó információkat (pl. mime típus) is. Ez néhány éven belüli archiválás esetén (jellemzően) elegendő, viszont hosszú távú – több évtizeden átívelő – archiválás esetén nem feltétlenül igaz. Előfordulhat, mint ahogy korábban már többször előfordult, hogy a használt fájlformátumok „kihalnak”, és a jövőben megjelenő platformokon nem lehet majd megjeleníteni őket. Az Eat. szerint az archiválás szolgáltató olyan szolgáltatást is nyújthat, amely szerint bizonyos fájlformátumok esetén vállalja, hogy az archivált dokumentumokat hitelesen meg tudja jeleníteni. Ehhez a szolgáltató meg kell, hogy őrizzen a fájl hiteles megjelenítéséhez szükséges szoftver és hardver eszközöket.

A Microsec Kft. archiválás szolgáltatása az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól szóló *12/2005-ös IHM rendelet 1. számú mellékletében szereplő formátumok esetén vállalja az értelmezhetőség biztosítását*. (Ez txt formátumok mellett a pdf és az rtf egyes verziót sorolja fel.) Más formátumú dokumentumok is archiválhatóak, viszont ezek esetében az archiválás szolgáltató nem vállalja az értelmezhetőség biztosítását, ekkor mindössze az aláírt bitsorozat megőrzését és az elektronikus aláírás érvényességének fenntartását vállalja.

3.5 Az archivált dokumentumok bizalmassága

Az Eat szerint az archiválás szolgáltató (az ügyfél felhatalmazása nélkül) nem ismerheti meg az archivált dokumentumok tartalmát. Ezt a követelményt úgy értelmeztük, hogy *a szolgáltató munkatársai nem ismerhetik meg a dokumentumok tartalmát*, hiszen a szolgáltatónak mindenképpen kezelnie kell a nyílt dokumentumot, ugyanis az [Eat] szerint ellenőriznie kell a dokumentumon lévő elektronikus aláírást.

Megoldást jelenthetne, ha az archiválás szolgáltató olyan fájlokat archiválna, amelyeket először titkosítottak, és utána helyeztek el rajtuk elektronikus aláírást, de ekkor nagyon nehéz lehet például annak a bizonyítása, hogy milyen nyílt fájlt írt valaki alá.

Olyan megoldást választottunk, hogy az ügyfél SSL csatornán küldi el a nyílt e-aktát az archiválás szolgáltatónak. Az archív szolgáltató ellenőrzi az aláírást, kiterjeszti archív aláírássá, időbélyeget helyez el rajta, majd titkosítja az e-aktát. A titkosítás olyan módon történik, hogy a titkosított e-aktát csak az arra jogosult ügyfél és az archiválás szolgáltató fejtheti vissza. Az archiválás szolgáltató magánkulcsa visszaállítható módon nincs jelen az archiválás szolgáltató rendszerében, ezt egy különleges eljárás során, több, bizalmi munkakört betöltő munkatárs együttes jelenlétében állítja vissza. Így, ha egy támadó fizikailag hozzáfér az archiválás szolgáltató archívumához, akkor sem képes elolvasni az archivált e-aktákat. Az archiválás szolgáltatónak nagyon ritkán van szüksége a titkosított e-akták visszafejtésére szolgáló magánkulcsra, kizárólag azért fér hozzá, hogy jogszabályi kötelezettségeinek eleget tegyen.

4 Mire jó az archiválás szolgáltatás?

Az elektronikus dokumentumok hiteles archiválásáról szóló [IHM 7/2005] rendelet szerint ha elektronikus aláírás segítségével hosszú távon szeretnénk biztosítani egy dokumentum hitelességét, két dolgot tehetünk:

- archiválás szolgáltatót bízunk meg e feladattal, vagy
- saját magunk látjuk el az archiválás szolgáltató feladatkörét (pl. archív aláírással) .

Bármelyik megoldást is választjuk, az aláírás mind műszaki, mind jogi szempontból hiteles marad, ilyen szempontból nincsen különbség e két megoldás között. Az jelent különbséget, hogy *ha egy aláírt dokumentumot minősített archiválás szolgáltató archivál, akkor egy bíróságnak ellenkező bizonyításig vélelmeznie kell, hogy az aláírás valóban érvényes*. A „házi” megoldásokhoz nem kapcsolódik ilyen jogkövetkezmény, ott előfordulhat, hogy az archiválónak kell bizonyítania, hogy valóban helyesen végzi az archiválást, és egy adott aláírás valóban érvényes.

Az elektronikusan aláírt dokumentumok hitelességének megőrzése nehéz feladat, nemcsak szakértelmet, de jelentős erőforrásokat igényel; többek között folyamatosan figyelemmel kell kísérni az elektronikus aláírással kapcsolatos technológiák fejlődését. Egy minősített archiválás szolgáltató egységesen, a jogszabályoknak megfelelő módon végzi el mindezt, teljes körű szolgáltatást nyújt az aláírt dokumentumok megőrzésével kapcsolatban. Ha valaki minősített archiválás szolgáltatónál helyez el egy dokumentumot, semmilyen további teendője nincs a dokumentum hitelességével kapcsolatban. Az archiválás szolgáltató egységesen felelőssé tehető az archiválásért, és egyúttal arra is garanciát jelent, hogy az archiváló nem járt el hanyagul: az elérhető legmagasabb szintű, bevizsgált, professzionális megoldást választotta.

5 Hivatkozások

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

[CW2004] Chokhani, S., Wallace, C.: Trusted Archiving, 3rd Annual PKI R&D Workshop, April 12-14, 2004, NIST, Gaithersburg MD, http://middleware.internet2.edu/pki04/proceedings/trusted_archiving.pdf, 2004.

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

[EB2007] Endrődi, Cs. – Berta, I.: Mire jó az archív aláírás, Networkshop, 2007.

[IHM 3/2005] 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

[IHM 7/2005] 7/2005. (VII. 18.) IHM rendelet a digitális archiválás szabályairól, valamint az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos elektronikus archiválás szabályairól

[K2005] Krasznay, Cs.: Hosszútávú hiteles archiválás elektronikus aláírás segítségével, Networkshop, 2005.

[KOV2006] Kunz, T. and Okunick, S. and Viebeg, U.: Long-term security for signed documents: services, protocols and data structures, http://www.dzi.tu-darmstadt.de/fileadmin/content/veranstaltungen/20060606-09_etrics/kunz_okunick_viebeg.pdf ETRICS, 2006.

[LTANS] Long-Term Archive and Notary Services, http://ietfreport.isoc.org/ids-wg-ltans.html, 2007.

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

[Msc2006] Miért szükséges az elektronikus archiválás szolgáltatás?, http://www.e-szigno.hu/wp_archivalas.html, 2006.

[Msc2007] A XAdES aláírás-típusok összehasonlítása, http://www.e-szigno.hu/wp_xades.html, 2007.

[Msc2007a] e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – szolgáltatási szabályzat, Microsec Kft., http://www.e-szigno.hu/docs/szolgaltatasiSzabalyzatASZ--v1.1.pdf, 2007.

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

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

[RFC4810] Long-Term Archive Service Requirements, 2007 http://www.rfc-archive.org/getrfc.php?rfc=4810