MIRE JÓ AZ ARCHÍV ALÁÍRÁS?

Endrődi Csilla <csilla@microsec.hu>
Dr. Berta István Zsolt <istvan.berta@microsec.hu>
MICROSEC Kft.

A papír alapú aláírásokhoz hasonlóan elektronikus aláírás esetén is fennáll az a probléma, hogy a „régen" készült aláírások hitelességét nem könnyű megbízhatóan ellenőrizni. Általánosságban igaz az, hogy minél több idő telik el az aláírás létrehozása és ellenőrzése között, annál nehezebb feladattal állunk szemben.
Problémát okozhat egyrészről, hogy egyszerű (időbélyeget nem tartalmazó) aláírás érvényessége kizárólag addig bizonyítható, amíg az aláíró tanúsítványa érvényes. Azaz az ilyen aláírás hitelessége elvész, ha az aláíró tanúsítványa lejár vagy visszavonják. Emiatt, amennyiben ennél hosszabb távon van szükségünk az aláírás felhasználhatóságára, az aláírás elkészítését követően időbélyeget kell rá kérnünk egy időbélyegzés szolgáltatótól.
Jelentős gondot okozhat továbbá a későbbi ellenőrzéskor az, hogy idővel az ellenőrzéshez szükséges információk (visszavonási információk, tanúsítványok, aláírási szabályzatok) elérhetetlenné válhatnak. Ezt azzal előzhetjük meg, ha még időben az aláíráshoz csatoljuk ezeket az információkat.
Mindezeken túl a használt időbélyegzés szolgáltatók tanúsítványai is lejárnak valamikor, amely a kapott időbélyeg érvénytelenségét vonja maga után. Valamint természetesen az sem zárható ki, hogy az alkalmazott kriptográfiai algoritmusok a használt kulcshosszal elavulhatnak, törhetővé válhatnak, azaz az aláírás hamisíthatóvá válik. Utóbbi két problémát azzal lehet áthidalni, hogy az aláírásra rendszeresen újabb és újabb ún. archív időbélyeget helyezünk el.
Láthatjuk tehát, hogy a hosszú távú érvényesség biztosításához különböző érvényesítési adatok beszerzésére és csatolására van szükség. A csatolandó adatok köre függ attól, hogy az aláírásnak milyen időtávlatban kell ellenőrizhetőnek maradnia, illetve az ellenőrző milyen szintű bizonyosságot szeretne kapni az aláírás hitelességét illetően. Ezeknek a szinteknek megfelelően különböző aláírás formátumokat dolgoztak ki. Az ETSI (European Telecommunications Standards Institute) TS 101 903 ajánlása tartalmazza az XML formátumú aláírások felépítésére vonatkozó követelményeket, ebben nyolc aláírás formátumot határoztak meg. A Magyarországon az IHM által kiadott „*a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációja*" című ajánlás is alapvetően erre építve definiálja „pillanatnyi", „rövid távú", „hosszú távú" és „archív" aláírási formátumokat.
A legnagyobb biztonságot adó aláírási formátum az archív aláírás, ennek használatával a legalapvetőbb problémák – hosszú távon is – megoldottnak tekinthetőek. Azonban még ennek az aláírási formátumnak a használata esetében is akadhatnak olyan speciális esetek, amikor egy aláírás ellenőrzése – az ajánlás pontos alkalmazása ellenére – vitatott eredményre vezethet. Az ilyen helyzetek alapvetően az alkalmazott PKI megoldás (pl. CRL technológia, kivárási idő alkalmazása) hiányosságából, negatívumából adódnak, amelyek megoldására egyelőre nem találták meg az egységesen alkalmazható, jó megoldást.
Előadásunkban röviden áttekintjük az egyes aláírás formátumokat. Bemutatjuk az archív aláírást felépítő adatelemeket, a létrehozására és kezelésére vonatkozó szabályokat és az általa elérhető biztonsági szintet. Ismertetjük azokat a PKI megoldásokat, amelyek használata esetlegesen gondot okozhat még az archív aláírás alkalmazása esetében is. Ezek ismeretében megválaszolható a kérdés, hogy mikor, mi ellen véd, mire jó az archív aláírás.