DIGITÁLIS ALÁÍRÁS: EGYÜTTMŰKÖDÉSRE KÉPES ÉS BIZTONSÁGOS ALKALMAZÁSOK

Szabó Áron, aron@ik.bme.hu
BME Informatikai Központ
Szigeti Szabolcs, szigi@ik.bme.hu
BME Informatikai Központ

Az 1970-es évek végén kifejlesztett technológia, a digitális aláírás használhatóságának jogi háttere csak 1999-ben született meg az Európai Unió direktívája révén, amelyet 2001-ben követett a magyar törvény és az ahhoz kapcsolódó rendeletek.

A szakemberek nagy várakozással tekintettek az új lehetőségekre, a digitális aláírást használó webes szolgáltatásokra, dokumentumkezelő rendszerekre, azonban az érdeklődés csekély maradt. A több háttérben meghúzódó ok között technológiai problémák is szerepeltek. Az aszimmetrikus kriptográfiát használó technológia majdnem 30 éves kora ellenére most szembesültek a fejlesztők azzal, hogy a világméretű együttműködés nehezen megvalósítható, ha több szabvány, megoldás létezik. Ez az állapot lehet az oka annak, hogy olyan formátumú aláírást hozhat létre az egyik rendszer, amelyet egy másik nem tud értelmezni. Az alapok, a tanúsítványok és a kriptográfiai algoritmusok azonosak, viszont egy PGP, S/MIME, XMLDSig aláírás között már komoly eltérések vannak.

Az egységesítés, a formátumok egyértelművé tétele, azaz az alkalmazások együttműködési képességének biztosítása érdekében az IETF, W3C, illetve az ETSI szabványosító szerv kezdett komoly munkálatokba. A technológiai szabályozás mellett ügyeltek a jogi háttérhez való igazodásra is, így jutottak el az ETSI szakemberei a XAdES (TS 101 903) szabványban leírt sémához. Ez tekinthető azon aláírási formátumnak, amely minden szempontból megfelel a követelményeknek.

Az egységes aláírási formátum mellett azonban az alkalmazások működési logikája, illetve a fejlesztőkörnyezetek olykor pontatlanul megírt függvényei is okozhatnak együttműködési problémákat a különböző alkalmazásoknál. A szabványosító szervek felismerve a probléma komolyságát különböző együttműködőképességi-vizsgálatokat tartottak több fejlesztő bevonásával.

Az egymással versengő fejlesztők páratlan összefogása révén Magyarországon – az IETF, W3C és ETSI szabványosító szerv munkálatai után – a MELASZ (Magyar Elektronikus Aláírás Szövetség) és a BME Informatikai Központ független vizsgálólaboratóriuma végzett hasonló vizsgálatokat (MELASZ Ready program) 2005. őszén. A projekt sikere fontos a hazai elektronikus közigazgatási szolgáltatások terjedése szempontjából, ugyanakkor jó példával szolgál az Európai Unió és a világ számára is.

Az előadás során e hazai együttműködőképességi-vizsgálat eredményei kerülnek bemutatásra.