IKTA5-160/02.

Biometriával ötvözött digitális aláírás

Magyar nyelvű szakmai összefoglaló a projekttervről

A számítástechnika rohamos fejlődése megkövetelte, hogy a csupán elektronikus formában létező dokumentumokat a papíralapú iratokkal azonos elbírálás alá helyezzünk, és azok *eredetiségét bizonyítani tudjuk*. Az elektronikus iratok hitelességét igénylik az e-business alkalmazások, az elektronikus ügyintézés, adóbevallás, illetve egyéb ügyfél-kapcsolattartó megoldások. Szükséges tehát, hogy biztonságos elektronikus aláírási technikák álljanak rendelkezésünkre, amelyek erős kriptográfiai módszerek révén biztosítják, hogy a dokumentum aláírója *azonosítható*, az aláírás ténye *letagadhatatlan*, valamint az aláírt dokumentum tartalma *sértetlen* legyen.

A projektjavaslat alapját képező *biometriával ötvözött digitális aláírás* technológia alapvetően az aláíró fél azonosításának, és az aláírás letagadhatatlanságának *megerősítésére* koncentrál. A jelenlegi elektronikus aláírás technológia a nyilvános kulcsú rejtjelezésre épül, melynek lényege, hogy erős kriptográfiai algoritmusok garantálják, hogy egy dokumentum aláírását csak a megfelelő titkos kulcs segítségével lehet előállítani, valamint a nyilvános kulccsal csak a titkos kulcs-pár felhasználásával készített aláírásokat lehet sikeresen leellenőrizni. Az aláíró személy nyilvános kulcshoz rendelését pedig tanúsítvány-kibocsátó szervezetek igazolják.

Figyelembe véve, hogy a kriptográfiai algoritmusok – tipikusan a használt kulcshossz segítségével – szinte tetszőlegesen erőssé tehetők, egy elektronikus aláírás ellenőrzése során a rendszerben a leggyengébb, nem erősíthető láncszemet a valódi személy és az őt azonosító titkos kulcs közötti kapcsolat képezi. A titkos kulcsot tartalmazó eszköz eltulajdonítható, míg a kulcshoz való hozzáférés a mai megoldásokban csupán jelszavas megoldással védhető, ami a növekvő számítási kapacitás mellett már nem tud érdemben ellenállni a támadásoknak.

Vagyis a jelenlegi megoldásokban a hiteles aláírás azt igazolja, hogy az aláíró személy *birtokában* volt a titkos kulcs, azt viszont nem lehet ellenőrizni, hogy ez így is volt, és valóban a jogos tulajdonos használta-e azt fel.

Az általunk javasolt módszer alapötlete az, hogy az aláíró felet azonosító titkos kulcsot olyan *kódolt formában* tároljuk, hogy csak a kulcs tulajdonosának ujjlenyomatából kiolvasható adat segítségével legyen visszaállítható, és csak így lehessen aláírást készíteni vele. Ilyen módon a kódolt titkos kulcs, vagyis a kártya eltulajdonítása révén sokkal nehezebb visszaélni, hisz az aláírás elkészítéséhez szükséges még – a jelenlegi PIN kód mellett – a tulajdonos ujjlenyomata is. Fontos megjegyezni, hogy ez a módosítás nem befolyásolja a nyilvános kulcs használatát, így teljesen *kompatíbilis a jelenlegi PKI ajánlásokkal és a meglévő alkalmazásokkal*.

A konzorciumban résztvevő tudásközpont már évek óta folytat kutatást a fenti algoritmus kidolgozásával kapcsolatban. Az elméleti eredmények elérkeztek arra a szintre, amikor az alapkutatásra építve érdemes megvizsgálni a gyakorlati megvalósíthatóság kérdéseit is építve az adott iparág neves résztvevőinek tapasztalataira.

A gyakorlati megvalósítás feltételeit, illetve az eredmények hasznosítását a technológiai központ biztosítja, amely cég egy, a magyarországi ujjlenyomat alapú személyazonosítás terén méltán elismerté vált társaság. Tapasztalatuk és termékeik skálája kiterjed az ujjlenyomat alapú felhasználó-azonosítás mind hardveres, mind pedig szoftveres támogatására. A megcélzott eljárás jól kiegészíti jelenlegi szolgáltatásaik körét.

A tudásközpont alapkutatási eredményeire, és a technológiai központ tapasztalataira építve a 20

hónapos projekt végére olyan prototípus alkalmazást tervezünk létrehozni, amely már kisebb befektetés árán piacképes termékké válhat. Létrehoznánk továbbá e termékből egy szabadon elérhető változatot is, amely alkalmat nyújthat mindenkinek, hogy megismerkedjen ezen újszerű technológia biztonságával és kényelmével. Tudományos eredményeinket pedig szakmai konferencián, előadás formájában tervezzük közismerté tenni.