Gondolatok[1]

Alkalmazási példák a BioSM™ felhasználására:

A **BioSM™ -**ről **á**ltalánosan megállapítható tulajdonság, hogy alapesetben is 1Mbyte-os szabad felhasználású memóriával rendelkezik, melyhez a hozzáférési jogosultságot csak pozitív biometrikus azonosítással lehet megszerezni. Ezért kijelenthető, hogy egy személy(/ek)hez átruházhatatlanúl köthető igen magas biztonsági fokazatra minősíthető média-eszközzel állunk szembe.

- ***e-IDcard elektronikus igazolvány*** a felhasználói nem-felejtő (non-volatile) memória különböző jogosultság szerinti felosztásával és az egyes területek megfelelő személyes adatokkal való feltöltése, módositása, olvasása a különböző jogosultságú szervek számára ad lehetőséget személyazonosításra illetve jogosult adatok kezelésére. (pl. A rendőrség jogosult a személy digitális fényképét a kor előrehaladtával lecserélni.) Viszont a jogosulatlan adatokhoz való hozzáférést garantáltan kizárja. (pl. Egészségügyi adatokhoz nem fér hozzá a rendőrség, vagy adó-adatokhoz az útlevél-ellenörzés stb.)
- ***e-sign alkalmazás*** a PKI megoldások alapvető problémája a magánkulcsok titkosságának megörzése, védett helyen való tárolása, vagy az átruházahatatlanság biztosítása. Ez utóbbi jellemzőre tökéletes megoldást biztosithat a **BioSM™** alkalmazása akár mint önálló funkciót megvalósító megoldás, akár az e-IDcard egy kiegészítő opciójaként.

Egy szakértő véleménye:

„Mi a PKI gyengesége?

... A leggyakrabban ismételt felvetés a magánkulcsok kezelését illeti, különösképpen vonatkozik ez a magánkulcs illetéktelen használatára vagy ellopására. Vegyünk egy példát. Tegyük fel, hogy az Ön magánkulcsához való hozzáférés egy jelszó megadása után van lehetõség. Ez nem zárja ki az elvi lehetõségét annak, hogy más is küldhessen az Ön nevében digitális aláírással ellátott, tehát hitelesnek tûnõ levelet! ...

A biometria jelentősége

... Vegyük egy másik régi ismerõsünket, a chipkártyát, vagy a régebbi megnevezésén smartcard-ot. Ha a kulcs kezelését rábízzuk magára a kártyára, a magánkulcsot a kártya biztonságos területén tarjuk, akkor azt közvetlenül onnan érhetjük el, megoldva a magánkulcs számítógépen való tárolásának problematikáját. Ebben az esetben a felhasználónak abszolút kontrollja van a kulcs felett, viheti magával, õrizheti biztonságos helyen, mint pl. a lakáskulcsát. Na mármost, ha ebben az esetben védjük a hozzáférést biometrikus módszerrel, megteremtettük a biztonságnak azt a szintjét, amit a feladó és aláíró valódi identitásának megállapítása megkövetel. ....

.....A biometria, a chipkártyák és a PKI technológia integrációja tökéletes megoldást kínál a bizalmas adatcserére nem megbízható hálózatokon olyan alkalmazásokban, ahol a biztonság mindenek feletti kérdés." **Forrás:A PKI és a biometria - Adámi Gábor Login autonom Kft.**

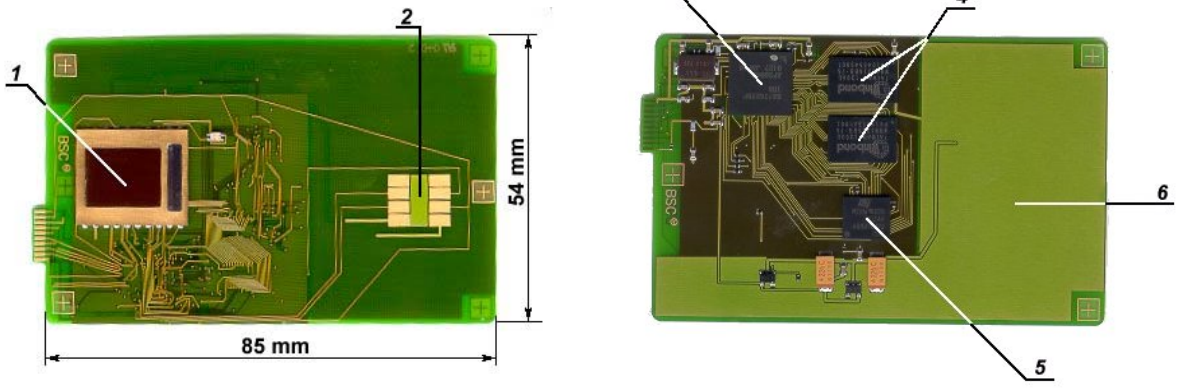
A fentiek szerzője természetesen nem ismerhette a **BioSM™** technológiát, ahol az említett integráció már megoldott kérdés és a biometriai azonosítás is saját erőforrásával müködik, ami chipkártya méretben merész elképzelésnek tünt.

[1] Haraszti Pál fejl.mérnök, Dactylos Kft. társtulajdonosa

- ***Biometrikus személyes rejtjelző (BioPePy)*** pont-pont kapcsolat teremtés nyílt kommunikációs csatornán (telefon, internet stb.) a lehallgatás veszélyével jár. Különböző soft-, és hardware alapú rejtjelző (titkosító) eszközök elérhetőek ma a piacon a megfelelő védelem kialakitására, de egyetlen hardware-s eszköz se létezik, amely az átruházhatóság elleni védelmet is megoldja. A **BioSM™** technológiát ötvözni lehet (és már közös elképzelés is született) az „Álmok álmodói – Világraszóló Magyarok" című kiállításon is elhíresült PePy® (**Pe**rsonal **P**rivac**y**) titkosítóval.
- ***e-TÜK elektronikus titkos ügyirat kezelés*** egyedi azonosítóval ellátott digitálisan tárolt TÜK-ös iratokhoz a hozzáférést a **BioSM™** alkalmazásával lehetne biztosítani kétoldalú (hivatalt és egyént) igazoló nyilvántartással. A hivatal és a titokgazda számára is megvalósítható a TÜK-ös adatbankhoz fordulás egy ilyen eszközzel a biztonságos digitális ügyirat kezelés és annak bizalmas nyilvántartása. Például közjegyző elötti megszemélyesítés, és/vagy lajstromozott eszközhasználattal külön bizonyítási eljárást nem igénylő perdöntő bizonyitékként is minősíthető.
- ***BioSM™ mint OEM-es controller*** A **BioSM™** technológia olyan eszközökbe kerül beépítésre, ahol meg kívánjá valósítani az átruházhatóság elleni védelmet. Például az alábbi felsorolásban szereplő eszközöknél már felmerült ilyen igény: Pocket PC, Palmtop, mobiltelefon, kézi-lőfegyver, safe stb.

A **BioSM™** technológia műszaki jellemzése:
[1]

A BioSM™ memória egy mikroprocesszoros elektronikus egység, amelynek nem-felejtő (non-volatile) módon tárolt adataihoz való hozzáférés, vagy más hozzá kommunikatívan kapcsolódó elektronikai egység működtetése biometriai (ujjnyomat-) azonosítással szerzett jogosultsággal lesz engedélyezett. A felhasználó hozzáférésének biztosításához szükséges biometriai kóddal és nyílt és/vagy védett személyi adatokkal kell megszemélyesíteni a BioSM™ eszközt használatba vétel előtt. A megszemélyesítéssel járó jogi (pl. közjegyzői) procedúra keretében az egyedi eszköz azonosítójával elektronikus lajstromba-vételre is ad lehetőséget.
A BioSM™ memória, amely egyben egy önálló müködésű ujjnyomat-azonosító rendszert tartalmaz egy ujjnyomat-vételre alkalmas elemmel (*1*), melyet egy 32 bites CPU (*3*) egy a flash memóriában (*5*) a gyártó által védetten tárolt firmware program vezérel, ujjnyomat-képet vesz az SDRAM operativ memóriába (*4*), ahol a program ujjnyomat-azonosítást végez el megszemélyesítő procedúrával szerzett biometriai kóddal és az azonosságnak megfelelő döntés szerinti kommunikációt kezdeményez/folytat a különböző szabvány szerint kialakított villamos csatlakozáson keresztül (*2*) nevezetesen ISO7816 vagy USB. Az egység BGA és SMD technolóiával szerelt módon nem vastagabb 3mm-nél.



[1] Haraszti Pál fejl.mérnök, Dactylos Kft. társtulajdonosa