Kártya és Ügyfélkapu lehetőségek
Kártya és azonosítás problémakör

eGov Tanácsadó Kft.
1056 Budapest, Belgrád rkp. 27.
Tel.:+36(1)411-1668
Fax.:+36(1)411-1669
www.egc.hu

Dokumentum adatlap

Metaadatok

Cím	Kártya és Ügyfélkapu lehetőségek
Fájlnév	eGov_tanulmany_Kartya_es_ugyfelkapu_lehetosegek_v1.pdf
Verzió	1.1
Dátum	2011. 04. 05.
Szerző:	Kiss József, Kleinheincz Gábor
Szerkesztette:	Csomán Gábor
Jogok	eGov Tanácsadó Kft.

Hivatkozás

Kiss József et. all: *Kártya és Ügyfélkapu lehetőségek*. (eGov Tanácsadó Kft., 2011, http://hirlevel.egc.hu/tanulmanyok)

Kapcsolat

Csomán Gábor
+36 20 999 7985
gabor.csoman@egovconsulting.eu

Csomán Gábor
a dokumentumot
elektronikus aláírással
ellátta
2011.04.11 11:53:24 +02'00'

Tartalomjegyzék

1 Bevezető

Az elmúlt kormányzati ciklust végigkísérte egy nagy átfogó intelligens-kártya kiadási projekt szándéka. A kártyakiadással kapcsolatban két nagy hibát lehet elkövetni, ezek:

- ha támogatjuk a széleskörű kártyakiadást,
- ha elvetjük a kártyakiadást.

A **kártyakiadás feltétlen támogatása hiba**, mert a hazai és külföldi tapasztalatok is jelzik, sokkal rosszabb a hasznosulása, mintsem azt a projektek kezdetén beígérik.

> A hazai chipes diákkártya sorsa ismert (alig néhány helyen használják az elektronikus lehetőségeit). De a külföldi nagy közigazgatási kártya kiadásoknál sem rózsás a helyzet, még ha ezt kommunikáció jobban el is fedi. A finnek kezdték a kártyakiadást (önkéntes alapon) még a kilencvenes években, de most már a kártya kivonása folyik, annyira nem volt iránta társadalmi igény. Az osztrákok beígérték a széleskörű használatot, náluk az alapfunkcióra (társadalombiztosítás) használják is, de egyéb beígért felhasználási területein már korántsem igazi siker. Az észtek okosabbak voltak, kiadtak ugyan elektronikus személyit, de a közigazgatási rendszereknél a bankok azonosítási rendszerén keresztül is be lehet lépni, s igen sokan ma is ezt használják. A németekről olyan hírek jelentek meg, hogy az egészségügyi kártyaprogram kiterjesztésének felfüggesztését mérlegelik.
>
> A kártya terjedésének problémái igazából előre láthatók voltak, mivel az egész kártyamizéria dominánsan politika által vezérelt Európában. A legfejlettebb gazdaságok, Amerikai Egyesült Államok vagy délkelet Ázsia fejlett országai már egyre inkább túllépnek a „számítógép = a lakásban külön asztalon egy zajos masina képernyővel" felfogáson, s egyre általánosabb a helyfüggetlen számítógép használat. Itt a notebook kategória mellett rohamosan terjed a netbook, sőt egyes egyszerűbb funkciókra a mobiltelefonos internet használat. Az viszont elég nyilvánvaló, hogy az emberek nem cipelnek magukkal külön kártyaolvasót, amibe a plasztik kártyát még be lehetne dugni (ha előbb összekötötték a mobil-telefonjukkal, számítógépükkel az olvasót), ez nem életszerű. S akkor még nem is beszéltünk sok emberek azon természetes igényéről, hogy telefonon intézhesse ügyeit. De ez egyben azt is jelzi, az univerzális hagyományos kártyahasználat (ami feltételezi a speciális kártyaolvasók meglétét is), amiben a kormányzati informatikusok hisznek, csak azon területen működik, ahol kötelezik erre a polgárokat, de ez számukra inkább nyűgöt, mintsem hasznosnak ítélt szolgáltatást jelent. Nem véletlen, hogy Spanyolországban kormányzati kampányt szerveznek, hogy a kiadott elektronikus személyi használatát ösztönözzék, a kormány kiadta, de az embereknek nem igazán kell. Közpénzekből persze sok ország végrehajt politikai marketinget szolgáló

projekteket, de Magyarország mostani gazdasági helyzetében ilyenre pazarolni a pénzt a megszerzett tekintély jelentős erózióját okozhatná.

Hiba elvetni a kártyakiadást, mert a kártyák egy lehetséges hasznos eszközök konkrét problémák megoldására.

A készpénzfizetés visszaszorításában is óriási jelentősége van a bankkártyának, a francia és osztrák társadalombiztosítás belső adminisztrációjának hatékonyság növelésében is jelentős szerepe volt a kártyának. Általánosan elterjedt a kártya használata a különböző beléptető rendszerekben. A mobiltelefonok használhatósága, egyes speciális banki szolgáltatásokra alkalmassága is a bennük lévő kártyán alapul. A kártya (helyesebben chip) technológia nem hibás abban, hogy megalomán projektekkel rossz célokra akarják alkalmazni. Ettől még sok területen adekvát eszköz egy probléma kezelésére (például a személyes adatok megőrzéséhez helyenként szükséges titkosításhoz nem igen találni ennél egyszerűbb és hatékonyabb megoldást, de a személyazonosító okmányok – például útlevél - biztonságához is elengedhetetlen az elektronikus támogatás). Ugyanakkor nem szabad elfeledni, hogy a „kártya" megtévesztő megközelítés, hisz az elektronikus emlékezet nélküli sima igazolványtól a biometriát védetten kezelni tudó intelligens chipes megoldásig sokféle formában létezik. Az elektronikus megoldás is lehet érintkezős (mint a bankkártya) vagy érintkezés mentes (mint útlevél vagy a beléptető rendszerek), s a megszokott kártya forma sem kötelező (a pici SIM kártya is chipes kártya, s USB csatlakozású, közfelfogásban „kártya" funkcionalitásúnak tekinthető eszközök is léteznek).

Az egész témakör alapvető problémája, hogy a kormányzat rendre a projekt felől indul ki (ki akar adni kártyát), s nem a feladatokhoz keresi a legmegfelelőbb megoldást. Alapelvük, hogy kiadnak egy univerzális kártyát, amihez aztán hozzákeresik a felhasználásokat. Csak épp ez a feladat-egyesítés az, ami egyben a kártya valós hasznos felhasználását nehezíti, a felhasználók felé a tényleges értékét elveszíti, s marad a kötelezhető alkalmazások köre.

Németországban bölcsen sok pilot projektet hajtanak végre a szélesebb bevezetések előtt. Az elvben univerzális felhasználásra alkalmas egészségügyi kártyájuknál az alapfeladata mellé további alkalmazásokat kívántak elhelyezni, amelyeket természetesen a hazai adatvédelmi szabályokhoz hasonlóan elég szigorú német előírások miatt el kell választaniuk az alapszolgáltatásokhoz. Ehhez PIN kódok kellenek, amivel a páciens befolyásolhatja, milyen funkciót hajtson végre a kártya. A valós betegekkel végrehajtott pilot tapasztalata az volt, az emberek jelentős része a kártya használatakor nem emlékszik a PIN kódokra. Ez azzal jár, egy ilyen sok-mindent tudó kártyánál valójában vagy mellétűzi a kódokat a kártyához – ami a biztonság paródiája, ettől kezdve feleslegesek a milliárdos fejlesztések a magas védelemre -, vagy hagyományos módon kell kiszolgálni, mert az adatokhoz nem férnek hozzá. De a német esetben sem a

kártyával volt a baj, hanem azokkal, akik mindent kártyával, sőt egyetlen kártyával akarnak megoldatni, aminek eredménye a gyakorlati elfogadottság és alkalmazhatóság alacsony foka. Most már a németek is az eredeti tervek újragondolásával foglalkoznak.

Ha szakítunk azzal, hogy mindenáron kártyát akarunk kiadni, s a megoldandó feladatokból indulunk ki, akkor egy olyan igényvezérelt, több komponensre épülő rendszerhez jutunk, amiben a kártyáknak is megvan a maguk szerepe, de nem arra épül az egész, s ezáltal a bevezethetősége és hasznosulása jóval magasabb szintű lehet.

2 Mi a megoldandó feladat?

Az első tisztázandó kérdés, mi is a valódi probléma, amire megoldást keresünk. Itt gyakran keveredik egy személy azonosításának szükségessége bizonyos jogosultságok ellenőrzésének kérdésével. Itt két dolgot rögtön tisztázni kell:

- nem mindenhol a személy azonosítása a feladat (azaz egy kártya sem feltétlen kell, hogy embert azonosítson)
- nem biztos, hogy kártyával kell az azonosítást megoldanunk.

A kormányzat előszeretettel szeretne mindent személyhez kötött kártyával kezelni (ez tízmilliós lakossága alapján sokmilliárdos üzlet Magyarországon is), de a valós folyamatok ezt nem igénylik.

A francia társadalombiztosítás első kártyás verziója családi szintű használatra épült, sok országban már elektronikus jeladásra képes (RFID) múzeumi belépőket használnak, de ezeket eszük ágában sincs személyhez kötni. A közlekedési jegyek esetében is csak egyes bérleteknél jelenik meg a személyhez rendelés, de ott sem egy schengeni útlevél-ellenőrzés szintű biztonsággal, azaz már a kötelező személyhez rendelés – ráadásul magas biztonsággal -, mint kiindulás is téves. A bevezetés alatt álló német jegyrendszerben – miközben az egészségügy területén univerzális kártya bevezetésére tettek kísérletet – egyértelműen a személyes adatot nem tartalmazó jegyrendszer mellett tették le a voksot. Jól példázza az autók elektronikus azonosításának kérdésköre (ami a követhetőség alapfeltétele), hogy nem szabadna csak a személyek azonosításának gondolatkörébe beragadni, a megtett úttal arányos díjfizetés bevezetése hatalmas bevétel többletet jelentene, de idehaza ezen a téren sem sikerült előre lépni.

A megoldandó feladatot ezért eleve pontosabban kell meghatározni, mivel nem feltétlen célszerű egyetlen eszközzel minden probléma megtoldását megkísérelni. **El kell különíteni egymástól egyrészt az azonosítást nem igénylő feladatokat** (az is igényelhet informatikai támogatást, s lehet, hogy többet hozna a konyhára a személyek azonosításánál, például elektronikus jegyrendszerek bevezetése), **az azonosításnál pedig**:

- **a nem természetes személy azonosítását** (cég, társadalmi szervezet stb.)
  Hibás a mostani kormányzati rendszerben kialakított nem természetes személyek kezelésére vonatkozó leegyszerűsítés, ami egy (ráadásul egyetlen) természetes személyre, mint képviselőre egyszerűsíti a kérdést, valójában egy informatikai megoldást próbál a másképp működő életre kényszeríteni. Ha belegondolunk, egy cég megbíz egy jogi irodát, vagy egy könyvelő céget a képviseletével. Ekkor az ügyfélkapu logikája szerint annak beosztottjait kellene bejelenteni, akár több száz személyt egy nagyobb cégnél, hisz a jogi iroda vagy könyvelő cég belügye, éppen melyik beosztottja foglalkozzon a megbízó ügyeivel. A cégek a postájukat is cégnevükön gyűjtik, s nem valamelyik alkalmazottjuk nevén nyittatnak postafiókot, mint ahogy most a kormányzati rendszer tárhely koncepciója működik.

- **az anonim ügyleteket**
  Az anonim ügyleteknél külön kell választani az azonosítást semmiképp nem igénylő ügyletet a végrehajtás során szükségtelen, de a visszaélések felderítéséhez szükségessé válható azonosíthatóságtól. Az azonosítást egyáltalán nem igénylő ügyleteknél az egyébként azonosításra szolgáló eszközök „korlátozása" az azonosításban igen költséges megoldás, vélhetőleg ezért nem igazán olvasni az ilyen jellegű felhasználási próbálkozások gazdasági hatásáról érdemi (tényadatokat tartalmazó) beszámolókat az egyes kormányoknál. Egy kártyahasználatnál ugyanis ellentmondó követelmény, hogy a kártya adja ki a szükséges adatokat az olvasónak, ugyanakkor ne adja ki, ahol nem szükséges.

  A megfelelő biztonsághoz például az útlevél ellenőrzésnél speciális kártyaolvasók vannak, speciális – az olvasókat felügyelő – on-line infrastruktúra, aminek kialakítása és fenntartása is sokba kerül. Látszólag (egy olyan informatikusnak, akit a megoldás ára nem érdekel) tehát jó megoldás, hogy kényes adatokat tartalmazó kártyát mellesleg egyéb célokra használnak, de az adatok védelmének ára jóval több lehet, mintha a feladatra egy adekvátabb eszközt használnának. Emellett a védendő adatokat tartalmazó eszköz (kártya) minden körülmények közti felhasználása az elvesztés, ellopás kockázatát is nagyban növeli. Gondoljunk bele, a személyi igazolványt most eltehetjük külön irattárcába, a táskában akár külön cipzározott rekeszbe. De ha ez kellene egy fizetéshez, vagy utazáshoz, bizony gyakran elő kell venni. (E megállapításhoz tudni kell, hogy az érintkezés nélkül megszólítható eszközök a gyakorlatban a tulajdonos tudta nélkül szólítgathatók, ezért egy túl „jó" megvalósítás, tehát ahol nem is kell közel tenni az olvasóhoz azt jelenti, a buszon ülve a szomszéd táskájából próbálkozhat a kártyánk feltörésével, ami a technika fejlődését is figyelembe véve komoly kockázat lenne. Emiatt (is) a gyakorlatban az érintésmentes rendszereket is viszonylag közel kell az olvasóhoz tenni a működtetéshez. Van ahol a táska oda tétele elég, de ez nem minden esetben működő képes. Emellett a bevezetett igazolványok szolgáltatásainak jó része

érintkezéses kapcsolatot igényel, ami szintén az igazolvány hozzáférhető elhelyezését, ki/bevételét, s egyben gyakoribb eltűnését eredményezheti.

A belgák például próbálkoznak vasúti jegyvásárlással, amit a személyi igazolványra lehet tölteni. A portugáloknál egy egyszerű, olcsó – néhány euro - elektronikus jegyet lehet venni (első jegyvásárlásnál), amire a további utazásokhoz rá lehet automatából tölteni akár busz, akár vonatjegyet (tömegközlekedésre is). Az érintésmentes jegy egyszerű utazást tesz lehetővé, s ha elveszik, sem igazán nagy a veszteség (nem beszélve arról, utazáshoz nem kell a személyi igazolványt elővenni, kockáztatva elvesztését). E két példa jól mutatja, egy igény alapú megközelítés – amit a közlekedési társaságok alakítottak ki a magasabb profit érdekében – s egy kormányzati PR vezérelt megközelítés – a belgák is kiadták az elektronikus személyit, muszáj valami alkalmazásokat kitalálni, hogy indokolt legyen a kiadás) közötti különbséget. De az is nyilvánvaló, hogy amíg az igényvezéreltet elfogadják, sőt megszeretik az alkalmazók (utasok), addig a másik egy nem igazán tömegsikert jelentő fejlődési pálya.

Nyomós érv az anonimitás ellen a visszaélések csökkentésének szándéka. De a visszaéléseket elkövetők felderítéséhez sem feltétlen kell az ügyleteknél a tényleges azonosítás. Ha belegondolunk, amikor a bankkártyával fizet valaki, valójában lehetővé teszi a személye utólagos meghatározását. De ehhez persze a vásárlási helytől a tranzakciószámmal el kell menni a bankhoz, aki a tranzakció alapján meghatározhatja az érintett számlát, majd következő lépésben az ahhoz rendelt személyt. Azaz felderíthető a személy, adatvédelmi gond a gyakorlatban még sincs, mivel több független intézmény olyan összejátszására lenne szükség a visszaéléshez, ami már a gyakorlatban nem valós veszély. Magyarán az elektronikus működésben kialakítható olyan modell is, ami valójában anonim a normál működés során, de ha szükséges, a személy kinyomozható (ennek egyszerű formája, ha az eszköz, kiadása személyhez rendelt, de ez az adat csak a kiadóhelyen – esetleg csak papíron vagy off-line nyilvántartásban – van meg, a használatnál csak az eszköz – például e-jegy - azonosítója jelenik meg)

- **a természetes személy azonosítását.**
  A természetes személy azonosítása messze nem egyszerűsíthető le a kártyahasználatra. Ezt a kérdést külön pontban részletesen kifejtjük.

3 Természetes személy azonosítása

Ha a természetes személyek azonosítását vesszük megoldandó feladatnak, akkor is több szempontot kell figyelembe vennünk. Lényeges szempont

a) a biztonsági szint
b) a felhasználás körülményei

3.1 A biztonsági szint meghatározása

A természetes személy informatikai azonosítására az informatikai közfelfogás szerint a három lehetséges komponenst szokás megnevezni, ezek:

- amit birtokol (például egy kártya, egyéb eszköz)
- amije van (képmás, ujjlenyomat)
- amit tud (jelszó, speciális információ)

Gyakran hallani, hogy két komponens kell a megfelelő azonosításhoz. Lényegében e logikára támaszkodik az elektronikus közszolgáltatásról szóló törvény, amikor bevezet három biztonsági szintet. A piac azonban, ahol a cégek ténylegesen megérzik a hibás döntéseiket, teljesen más utat jár, mint az e teoretikus elven építkezők. A kormányzat ugyanis lényegében „abszolút" biztonsági szintekben gondolkodik, megadva a legfelső szint követelményeit, s az alsóbb szintekkel is valójában azt sugallja, a biztonsági kérdéseket megfelelően kezelte. A kormányzat jelszavas védelmet használ, de betervezte egy chip-kártyás megoldás bevezetését is. Nézzük meg, mi ezekkel a valós helyzet.

A **jelszavas védelem** csak laikusok ellen véd, mivel három súlyos elvi problémára nem ad megoldást:

- vizuálisan megfigyelhető
  Általában a munkahelyen, sőt még otthon sem biztosítható a rálátás, vagy egy kamerás rögzítés lehetőségének kizárása, közösségi hozzáférésnél pedig ez eleve nem biztosítható.
- elektronikusan megfigyelhető
  A számítógépes rendszerek biztonsága közismerten sok kívánni valót hagy maga után, még a vírusirtók futtatása sem ad teljes-körű garanciát egy rosszindulatú program, például egy billentyűzet leütés figyelő ellen. Ha nem saját gépünkön dolgozunk, még a gépi (hardveres) megfigyelés is előfordulhat, aminek felfedésére semmilyen eszköz nem áll a felhasználó rendelkezésére.
- automatával feltörhető (vagy a szolgáltatás blokkolható)
  A jelszóra épített beléptetésnél közvetlenül nem feloldható ellentmondó követelmény lép fel. Egy automata program az összes lehetséges karakterkombinációval meg tudja szólítani a szolgáltatást, tehát a jelszavas védelem igen egyszerűen feltörhető. Védelemként néhány sikertelen kísérlet után más megoldás szükséges. Van, ahol képi információt írnak ki (bár már ennek feltörésére is vannak megoldások), van ahol az adott címet adott ideig kitiltják (ezzel viszont a szolgáltatás jogos elérését akadályozhatja egy illegális akció), mindenesetre önmagában a jelszavas védelem nem elég.

Az informatikusok egy részének a válasza a biztonságnövelésre egy **„biztonságos" kártya** bevezetése. Ezzel azonban három baj van

- **megfejthető**
  A szokásos kártyák chipjeiben alkalmazott védelmi algoritmusok (a nyíltkulcsos architektúra) valójában egy egyszerűen megfejthető megoldás, lévén az algoritmus ismert (nyilvános). Gondoljunk bele, ha egy ismert algoritmussal (egy speciális kulccsal) előállítunk egy szöveget, ha a szintén ismert visszafordító algoritmusba belepróbáljuk az összes lehetséges kulcsértéket, akkor előbb-utóbb megkapjuk a megoldást (a matematikusok ráadásul ennél hatékonyabb heurisztikus megfejtő megoldásokat is tudnak, amelyek nem teszik szükségessé az összes lehetőség végigpróbálását). A mostani védelem az „elegendően hosszú" kódhossz választással arra épül, hogy a jelenlegi számítógépeken túl hosszú időt venne igénybe a kód feltörés (ez egy kompromisszum, mert a kódhossz egyben a feldolgozás idejét is befolyásolja, azaz papíron egyszerűen növelhető, a valóságban tetszés szerint nem növelhető, mert vagy nagyon sokáig tart egy kártyás azonosítás, vagy megfizethetetlen a kártya). Ez a védelem azonban sántít, mert egyrészt a közigazgatásban nem igazán életszerű a sűrű kártyacsere (amire a fenyegetettség csökkentése érdekében szükség lenne), másrészt a rendelkezésre álló kapacitás dinamikusan nő (nem beszélve az új elvű számítógépek várhat megjelenéséről, ami alapjaiban teszi használhatatlanná e megoldást).
- **megismerhető, másolható**
  Nem véletlen, hogy ilyen kártyára állam vagy komolyabb katonai titok védelmét sehol a világon nem bízzák. A probléma, hogy a kártyák (chipjei) a valóságban – persze kellő szakmai felkészültséggel - megismerhetők. Nemrég derült ki, hogy a számítógépekbe épített védelmi chip adattartalma, aminek a szerepe lenne a védettebb működés garantálása (például az ujjlenyomat olvasó viszonyítási adatainak, vagy a diszk titkosítás kulcsainak védelme), kiolvasható. Ehhez szinte házilagos eszközöket használt a szakértő (lemaratta a chip felső rétegét stb.), de ilyen módon is képes volt az adatok megismerésére. Egy magasabb védettségű chipnél ez nyilván bonyolultabb, de komolyabb felszereltséggel megtehető. Itt elég arra gondolni, hogy a COCOM lista idején az embargós chipeket keleten bizony – igaz, hogy fizikusok, anyagtechnológusok bevonásával – de szintén simán feltérképezték és visszafejtették. Magyarán az „abszolút" biztonságosnak hirdetett megoldások valójában nem azok, csak az a kérdés, kellően professzionális szervezet fel akarja-e törni azokat. (A katonai, nemzetbiztonsági védelmi rendszerek, ahol a teljes-körű védelem nem biztosítható, ott önmegsemmisítő megoldásokat is tartalmaznak, a kártyáknak nincs ilyen szolgáltatásuk)
- **a rendszer máshol is sebezhető**
  A kártya csupán egyetlen eleme az azonosítási folyamatnak. A biztonsághoz az összes elem egyenszilárdsága szükséges. Sőt, az azonosítás általában nem maga az ügylet, nem „öncélú". Ha egy azonosítás sikeres, attól még a teljes ügylet alatt gondoskodni kell arról, hogy a személy ne változhasson, aminek garantálása sem egyszerű feladat. Vannak informatikai megoldások, például védett csatornákkal, de ez sem a felhasználói oldali

alkalmazásnál, sem a szolgáltatónál lévő alkalmazásnál nem garantálja, hogy az alkalmazás belsejében ne történhessen valami meg nem engedett akció. A rendszer egy eleménél kialakított igen magas biztonság csak látszatmegoldás, a biztonsági szintet csak az egész rendszerre lehet értelmezni.

- **használati nehézségek miatt kockázat lép fel**
  A biztonság eléréséhez sokszor „rezsim" eljárások kapcsolódnak, amelyek terhesek a felhasználóknak. Ha az ügyvédnek naponta ötvenszer meg kell szakítania egy-egy megbeszélést, hogy lekérdezzenek valamit a közigazgatás adatbázisából, s csak ő kapott kártyát, alighanem a titkárnőjére fogja bízni Pin kódjával együtt, aki a lekérést ténylegesen intézi. Ha egy nem informatikusi beütésű ügyfélnek többféle PIN kódot is meg kell jegyeznie, alighanem vagy ráírja a kártyára, vagy mellé teszi. A papíron jónak tűnő biztonsági rendszerek rendre megbuknak azon, hogy a kitalálóik nem gondoltak bele a valós felhasználás körülményeibe. Elég gyakran látni „kitámasztott" biztonsági ajtókat, de ahol állandóan ki/be kell mászkálni csomagokkal, ott egy távoli érzékelős beléptető rendszer alkalmas lett volna, egy hagyományos kártya azonban csak akadályozhatja a munkavégzést, s ahol lehet, megkerülik használatát.

A fentiekből érzékelhető, hogy az elképzelt kormányzati fejlesztési irányok valójában szakmai oldalról megalapozatlanok. A helyes irány megválasztásához érdemes megnézni, hogy mit tesznek ezen a területen az olyan cégek, amelyeknek érdemi felelősségük van a döntéseikért, mert nem a közpénzeket költik.

A legszélesebb „azonosítók" a bankok, amelyek a bankkártyákkal igen nagyszámú ügyfél számláját kell azonosítaniuk, s a hozzáférés jogosságát kezelniük (komoly anyagi kockázattal)**.** Szemben a kormányzat központilag meghatározott biztonsági-szint felfogásával (amit az azonosítás technikai megoldására határoznak meg), a **bankok döntései teljesen más (három) alapelvre épülnek**:

- **kockázat alapján határozzák meg a szükséges megoldásokat**
  Igen lényeges hozzáállásbeli különbség, hogy nem teoretikus biztonsági modellekből indulnak ki, ahol egy hivatalban valakik kitalálják, milyen biztonság szükséges (mint ahogy a kormányzat tesz). A bankok folyamatosan figyelik a folyamatokat, értékelik az adatokat, s a tényleges biztonsági igényekhez igazítottan lépnek. Jó példa a bankok elektronikus chip-el ellátott kártyájának bevezetése. Az amerikai bankok még igen mérsékelten álltak át az új kártyára (kérésre adják, de főleg az Európába utazók miatt, otthon még a jó monitoring rendszereik miatt nincs igazán szükségük rá), de a hazai bankok közül is csak néhány vezette be. Az ok egyszerű, a chipes kártya drágább, mindaddig rontja a jövedelmezőséget, amíg a normál kártya hamisítási vesztesége a meglévő módszerekkel alacsony szinten tartható.
- **a biztonságot rendszerben kezelik**

Az egyik legfontosabb szemléletbeli különbség, hogy a bankok nem a kártyára alapozzák a védelmet, hanem a pénzügyi tranzakciók egészére építik ki a biztonsági rendszert. A védelmi rendszer első eleme a napi, heti limitek megadhatósága, amivel a felhasználó kellően alacsony szintre szoríthatja kockázatát. Emellett komoly szerepe van a monitoring rendszernek, amely valós időben figyeli a tranzakciókat, s felfedi a szokatlanokat (klasszikus példa, hogy ha például reggel Budapesten vesz ki pénzt, majd húsz perc múlva Londonban, akkor a második tranzakciót blokkolni és a felhasználóval – többnyire telefonon – egyeztetni kell, mert valamelyik tranzakció hamis). Már itt megjelenik a kormányzat által igen elhanyagolt eszköz, a telefon. A bankok a problémás esetekre telefonon keresik meg az ügyfelet, azonnali megoldásokat biztosítva. Tanulságos, hogy az internetes bankoláshoz kártya alapú megoldást az ismertebb bankok sehol sem alkalmaznak, pedig van, amelyik speciális eszközt (egyszer használatos jelszó generátort) biztosít. Ez nyilvánvalóan összefügg azzal, hogy az ügyfelek nem igazán vehetők rá kártyaolvasók beszerzésére, mobil eszközöknél ennek esélye még kisebb, ezért a bank – a kormányokkal szemben – a gyakorlati széleskörű alkalmazhatóságot tarja a szem előtt.

- **választható lehetőségeket kínálnak**
  A banki megoldások jellegzetessége, hogy a vállalandó kockázatot nem maguk határozzák meg (s arra kötelezik az ügyfelet), hanem megadják számára a választás lehetőségét. Eleve egy választási lehetőség az elektronikus ügyintézés, a pénzügyi feltételekkel (díjak) persze tudják ösztönözni az ügyfeleket a korszerű megoldásokra, de nem olyan durván köteleznek, mint amivel a magyar kormányzat kísérletezik az elmúlt időszakban (például az adózásnál, vagy az egyéni vállalkozóknál). Teljes értékűen biztosítják a telefonos ügyintézést, s csak egy lehetőség az internet. A sima jelszavas védelem már a legtöbb banknál nem elegendő, valamilyen kiegészítő eszközt biztosít az internetes bankolást választóknak. Az internetes alkalmazásoknál éppúgy, mint a bankkártya használatnál választható az alternatív értesítés (általában SMS) egy választható biztonságnövelő elem. Van bank, ahol egy független csatorna használata a biztonságnövelő eszköz (SMS-ben küldött egyszer használatos kód). A telefonos ügyintézéshez szükséges azonosítási rendszerük is van (van, ahol hiányos kódmegadásra épül, van ahol változtatható PIN kód, de többnyire az azonosításhoz az ügyintéző további személyes adatot is bekér).

Összefoglalva a biztonsági szinttel kapcsolatos kormányzati és piaci felfogást megállapítható, hogy amíg a kormányzati felfogás teoretikus, valójában szakmai és gazdasági oldalról nem alátámasztott („tud, amit tud, kerül, amibe kerül”), a piaci szereplők felfogása pragmatikus, amely a valós kockázathoz és igényhez igazodik, s a gazdaságilag rentábilis megoldásra törekszik.

3.2 A felhasználás körülményei

Annak érzékeltetésére, hogy az azonosítás korántsem egy kártya olvasóba helyezéséből áll, egy táblázatba foglaljuk a tipikus eseteket, az eltérő jellegük szerint. A táblázat szerkezete:

- Az első (technikai) oszlop a sorok sorszáma, ami a későbbi magyarázatokban a hivatkozáshoz szükséges.

- A második (az első érdemi) oszlopban az szerepel, **a személyt egy automata azonosítja-e, vagy egy ember**.
  Ez önmagában jelentős különbség. Egészen más helyzetet jelent egy fizikai találkozás (akárcsak telefonon), ahol akár az elbeszélgetés, a helyzethez illő kérdések segítik a személyt az azonosításban, a visszaélés felderítésében. Egy telefonos automatának egészen más lehetőségei vannak, de egy belépést engedélyező rendszernél is más helyzetet jelent egy automata beléptető rendszer, mint ha a belépést végső soron egy ember engedélyezi (még ha használ is az ellenőrzéshez segédeszközt). Még telefonos elérés esetén is az ember más jelleggel képes az azonosításra, kellő tapasztalattal a megkülönböztetés azért lényeges, mert a folyamatok hatékonysága értelemszerűen lényegesen magasabb lehet, ha megfelelő hibaarányon belül automata képes az igények kiszolgálására. Érdemes ezért az automatizálásra törekedni, de ez az azonosítás alkalmazható technikáira kihatással van.

- A harmadik (második érdemi) oszlopban az szerepel, hogy az **azonosítás távolról történik** (például telefonon, interneten), **vagy közelről** (például ott áll előtte a határőr, és azonosítja, az érzékelő előtt megjelenik a személy, amely a képmását is rögzíteni tudja stb.).
  A távolról történő azonosítás lényegesen megnöveli a kockázatot, hisz a helyszíni ellenőrzésnél a visszaélő számára egy azonnali retorzió következhet be (lebukik, rendőrt hívnak, vagy a határőr egyből lefogja), míg távolról lehet „kísérletezni”, azaz a fenyegetettség sokkal nagyobb). Másrészről viszont az ügyfél felé a szolgáltatás színvonalában minőségi változást jelent, ha nem kell valahova bemennie, hanem otthonról, vagy ami a még magasabb szint, bárhonnan képes intézkedni.

- A negyedik oszlopban található szempont, hogy az **ellenőrzési közeg teljes mértékben ellenőrzöttnek tekinthető** (pl. határ-állomás ellenőrzési rendszere), **vagy nyílt** (pl. internet kávézóból jelentkezik be valaki).
  A biztonságot mindig csak egy teljes rendszerre érdemes értelmezni. Hiába van páncél bejárati ajtaja egy családi háznak, ha a teraszajtó sima üvegből van. A kártyahívők előszeretettel bíznak az eszközükben, miközben a teljes rendszer biztonságát (s ebben nem csak maga a kártya, kártyaolvasó, de az egyes futtatott alkalmazások, sőt a személyzet, és a szolgáltatás oldali alkalmazások esetében is azonos biztonsági szintre

lenne szükség. Ez a valóságban legtöbbször nincs így, a világban eltérő biztonságú megoldások, helyzetek, környezetek vannak, ezt a mérlegelésnél szintén illik figyelembe venni.

- Az ötödik oszlopban található szempont az, hogy **az azonosítás speciális eszközzel történik-e**, **vagy külön eszköz nélkül.**
  Ez a szempont – a gyakorlati bevezethetőség vizsgálhatóságához - némileg eltér az előző háromtól. Itt nem azt nézzük, kell-e eszköz az azonosításhoz, hanem azt, kell-e olyan, ami a gyakorlatban nem tekinthető elterjedtnek, amit az azonosítás miatt kellene elterjeszteni. Ezt azért vesszük figyelembe, mert a tapasztalatok azt mutatják, egy megoldás elterjesztése igen erősen függ attól, mennyiben kötődik valamilyen specialitás a széleskörű elterjesztéséhez. A bankkártyáknál is kezdetben a terjedés komoly gátja volt az elfogadóhelyek hiánya, ami nagyban összefüggött az elfogadás technikai feltételeinek hiányával. Nem véletlen, hogy elvben a dombornyomásos bankkártya még ma is – sokkal szűkebb körben, az elfogadó nagyobb felelőssége mellett – használható hálózat nélküli környezetben is, a bankoknak először olyan megoldást kellett kialakítaniuk, amit a kereskedők be tudtak fogadni. Valószínű, ha a bankkártya elfogadás kezdeti feltétele a számítógépes kapcsolat megléte lett volna, talán még ma sem használnák széles körben. S az is egy „elfogadási" folyamat része, hogy a speciális elemet az ügyfél magánál tartsa, a bankkártya hordozása sem volt természetes a kezdeti időben. Mindezek miatt külön szempontként vizsgáljuk a speciális eszköz nélküli azonosítás eseteit, mivel ennél valószínűsíthető a leggyorsabb bevezetés, a legszélesebb ügyfélkör elérése. Jelenleg hazánkban például egy telefon „birtoklása" már egy szokásos közigazgatási alkalmazásnál általánosan elterjedt eszköznek tekinthető, a számítógép (és internet) megléte egy határozottan szűkebb (de még elég széles) felhasználói körre értelmezhető, a kártyaolvasó megléte viszont nem tételezhető fel, az egyértelműen speciális, elterjesztendő eszköz lenne, ami a széleskörű bevezetés idejét igencsak kitolja, kockázatát növeli. Mindezek alapján például egy nyugdíjjal, idősebbek ellátással kapcsolatos szolgáltatásnál a telefon ügyintézést segítő eszközként igen széles kör elérésénél meglévő lehetőségként figyelembe vehető (a leszakadt legalsó réteg kivételével!), a számítógépes elérés viszont nem, az ebben a feladatkörben speciális eszköznek számít. A közösségi pontokban vetett hit nem igazán igazolódott, ha kötelező az elektronikus út, persze használatára nagy nehezen rávehető az ügyfél, de az elektronikus ügyintézést ilyen feltételekkel mindenképpen nyűgnek érzi majd). Ha az értelmiség felső rétegének kínált szolgáltatásokról van szó, ott a számítógép már nem speciális eszköz, mint ahogy a bankkártya sem.

- A hatodik oszlop néhány tipikus példát tartalmaz az adott sorra jellemző azonosítási szituációkra

A táblázat a következőképpen néz ki:

	személy vagy automata ellenőriz	**közelről vagy távolról**	**ellenőrzött vagy nyílt környezet**	**eszközzel vagy eszköz nélkül**	**példa**
1	A	T	NY	EN	telefonról számlaérték (pl. adótartozás) összegének lekérése, telefonos ügyfélszolgálathoz belépés
2	A	T	NY	E	banki utalás token használattal, kártyával aláírt igazolás-kérés otthonról, amire automata adja ki az igazolást
3	A	T	E	EN	hivatalnál felállított önkiszolgáló állomáson intézett ügy,
4	A	T	E	E	hivatalnál, postán felállított önkiszolgáló állomáson intézett ügy kártyahasználattal,
5	A	K	NY	EN	képmásrögzítéssel kombinált nyilvános önkiszolgáló állomás
6	A	K	NY	E	
7	A	K	E	EN	automata beléptető biometriával (ujjlenyomat olvasóval), képmásrögzítéssel kombinált önkiszolgáló állomás hivatalnál, postánál
8	A	K	E	E	automata kártyás beléptető rendszer, bankautomata, képmásrögzítéssel kombinált önkiszolgáló állomás kártyaolvasóval
9	SZ	T	NY	EN	telefonos ügyfélszolgálat, ügyintéző
10	SZ	T	NY	E	
11	SZ	T	E	EN	belső hivatali telefonrendszeren megkeresés
12	SZ	T	E	E	
13	SZ	K	NY	EN	boltos, orvos azonosít
14	SZ	K	NY	E	boltos vagy orvos azonosít e-kártya használattal
15	SZ	K	E	EN	tisztviselő (mint bankfiókban) azonosítja az ügyfelet belső nyilvántartásokat is felhasználva (aláírás minta, fényképtár)
16	SZ	K	E	E	határátlépés engedélyezése, vagy közjegyzőnél hitelesítés igazolvánnyal (biometriával ellenőrizve)

Néhány példa a táblázat értelmezésére. A 16. sor a személy általi közeli azonosításról szól ellenőrzött környezetben, speciális eszközzel. Tipikusan ilyen feladatot végez a határőr a beléptetési ponton, amikor a biometrikus adatot tartalmazó útlevelet ellenőrzi. Persze az egyes fogalmak nem pontos definíciók, jelentésük rendszerenként eltérő lehet. például

az, hogy mit tekintünk ellenőrzött környezetnek, az adott rendszertől függ. Itt beleütközünk megint egy elvi nézetkülönbségre a kormányzati informatikusok és a társadalmi igények között.

A táblázat az azonosítás eseteit vizsgálja. **Arról semmit nem mond, az egyes esetekben milyen erősségű azonosítás kell**. Ez nem csak a táblázatban elfoglalt helytől, de a konkrét szituációtól függ! Van, ahol ezt az államnak kell eldöntenie, ilyen az előbb említett határátlépés engedélyezése. Ott nemzetbiztonsági kérdés, hogy csak arra jogosult lépjen be az országba, így a technikai követelményeket az állam szabja meg. Ezért kötelező a biometrikus útlevél, de még ez sem mindenhol elegendő, Amerikában tízujjas ujjlenyomatot is vesznek (ami nincs az új útlevélben sem) a megfelelő szűrés érdekében. Az 1. sor viszont olyan távoli azonosítás, ahol például telefonon akar valaki ügyet intézni egy automata rendszerben, minden segédeszköz nélkül. Itt már a felelősség megfordulhat. Ha az ügy csak az illetőre vonatkozik, a saját kockázatvállalásának a kérdése lehet, milyen szintű biztonságot igényel, azaz nincs reális indok a biztonsági szintek kőbe (jogszabályba) vésésének, mint amivel most a kormányzat kísérletezett. Lesz, aki mindent csak kiemelt szinten mer intézni (sokan bankkártyával sem fizetnek, legfeljebb bankfiókban vesznek fel vele pénzt), s lesz, akit zavar, ha rugalmasabb használatban gátolják.

Ebből a szempontból nézve tehát nem lehet az egyes sorokhoz elvárt biztonsági szintet hozzárendelni, egy azonosítási lehetőség portfóliót célszerű biztosítani (lásd később), amit aztán az egyes konkrét esetekhez hozzá lehet rendelni (többnyire választhatóan, de ahol szükséges – például nemzetbiztonsági okból -, ott kötelező jelleggel).

Visszatérve a besorolásra, egy közjegyzői irodában végrehajtott személyazonosításnak vélhetőleg olyannak kell lennie, mint amilyen a határon van, azaz feltételez biometrikus információt. A kisméretű fénykép alapján, ami egy igazolványban van, gyakorlatban nem lehet elfogadható hibahatáron belül azonosítani egy személyt, ez régóta ismert, ezért ha valóban közhiteles igazolása szükséges egy személy nyilatkozatnak, akkor a személyt érdemben kell azonosítani. Egy orvosi rendelőben is szükséges az azonosítás, hogy a beavatkozást valóban az érintett személy nevében végezzék el (ennek elsődleges etikai - orvosi indokai vannak, nem függ közvetlenül a társadalombiztosítástól, nem véletlen, hogy egyes speciális esetekben van csak anonim ellátás, például az AIDS-nél). Itt azonban önáltatás lenne rávágni, hogy ellenőrzött környezetben történik, s szükségessége is vitatható. Az ellenőrzött környezet azt jeleni, az eszközökhöz idegen nem fér hozzá. De mibe kerülne minden rendelőben, mentőautóban olyan biztonság megteremtése riasztórendszerrel, fegyveres őrséggel, ami a határőrizethez hasonlóan megvédené az ellenőrzésben alkalmazott rendszert (azaz feltétlen bízni lehet benne, hogy nem manipulálták, illetéktelen nem tudja akár ideiglenesen is használatba venni stb.)? És mi értelme ilyen szintű ellenőrzést kialakítani? A bankok esetében jóval nagyobb értékekkel történhet visszaélés, mint egy vizsgálat ára, mégsem célozták meg a kiemelt biztonsági szintet. Az orvos-beteg kapcsolat jellege olyan, hogy értelmetlen kriminalisztikai szintű

ellenőrzéseket beiktatni azért, mert elméletileg elképzelhető, hogy valahol talán valaki másnak adja ki magát. Itt keveredik a társadalombiztosítás (elszámolás) szempontja, az orvosi ellátás (etikai) szempontja – más nevében ne lehessen foglalkozási korlátra vezető beavatkozást elvégeztetni, hogy mondjuk a valódi személynek megmaradhasson a jogosítványa). A kétféle megközelítés azonban nem kell, hogy azonos platformon oldódjon meg, az orvosi azonosítás azoknál kell, akiket nem ismer, ott viszont személyazonosításra alkalmas okmánnyal, míg az elszámoláshoz a biztosítási jogviszonyt naprakészen mindenkinél ellenőrizni kell. Mindez nem azt jelenti, nem kell azonosítás az orvosnál, de az elszámoláshoz bevezetett azonosítás biztonsági szintje jóval alacsonyabb lehet, mint egy repülőtéri ellenőrzésnek.

Már itt ki kell emelnünk, hogy a bankok példáján jól látszik, **az egész rendszerre kell értelmezni a biztonságot és a kezelt kockázatot, s nem kiragadva egy elemre, az azonosításra.** A bank a megszabható limitekkel, kérhető azonnali (SMS) értesítésekkel és tranzakció-figyelő kockázatelemző rendszerekkel tarja megfelelő szinten a kockázatát, s ez a modell szemmel láthatóan jól működik. Nem véletlen, hogy még a chipes bankkártyára átállás is igen vontatottan halad, hisz a visszaéléseket olyan jól kézben tudják tartani, hogy nem volt okuk a folyamatot siettetni. A kormányzatok hajlamosak egy kiragadott elem (kártya alapú igazolvány) biztonságával letudni a kérdést, ami egyrészt a rendszer egészére nem kellő garancia, emellett igen rossz költséghatékonyságot és a használóknak sokszor kifejezetten terheket jelent (azaz nem véletlen az alacsony használati elfogadottsága több külföldi országban).

Visszatérve a táblázatra, a (rendelői) orvosi rendszereket a gyakorlatban a 13-14. sorba is be lehet sorolni, azaz az eszközeik inkább nyíltnak tekinthetők. Lényeges – sok milliárdot jelentő - különbség, hogy van-e speciális saját elem, amit az azonosításhoz felhasználnak. A 13. sorba tartozónak tekinthetjük a normál személyi igazolvánnyal történő vizuális azonosítást, s a TAJ szám ismeretét (ahol maga az igazolvány valójában nem biztonsági tényező), a 14. sorba sorolódik az osztrák, illetve francia megoldás, ahol elektronikus társadalombiztosítási kártya van. E külföldi rendszerek bevezetésekor tapasztalt előnyök azonban nem a kártyákból, hanem az elszámolási rendszer elektronizálásából adódtak, amelynek csak – hasznos – kelléke volt maga a kártyakiadás. Ugyanilyen hasznosulást például az osztrákok a kártya más célú felhasználásánál nem tudtak kimutatni, ami jelzi, a kártya jó eszköz lehet egy konkrét probléma megoldásánál, de azon túlmutató várakozások rendre nem igazolódtak.

Ez a látszólag kis különbség (nem a 16., hanem 13-14. sor) a határőrizeti pontok költségeihez képest egészen más megközelítést eredményezhet, milliárdos megtakarítást jelenthet a fejlesztésben, üzemeltetésben, s persze reálisabbá, a gyakorlatban megvalósíthatóbbá teheti egy egészségügyi kártya alkalmazását. Persze valamit valamiért, nyilván azért takarít meg, mert valamit nem azonos színvonalon tud. De kérdés, szükséges-e egy rendelőben a határőrizeti szintű biztonság? A gyógyítás eleve

bizalmi viszony, a szereplők gyakran ismerik egymást. A visszaélést nem olyan szinten kell kiszűrni, mintha terroristák ellen kellene védekezni. S itt jön be a korábban említett rendszerszemlélet szükségessége. A visszaélések kiszűrését rendszer szinten, s nem egy eleménél kell biztosítani, amiben a bankok mintájára egy elfogadható mértékű hiba is beletartozik. Például nem érdemes milliárdokért fenntartani egy szuper receptkezelő rendszert, ami lehetetlenné teszi, hogy valaki jogosulatlanul váltson ki egy receptet, akár biometriával azonosítva a felvevőket. Bőven elég, ha a hamisítást szűrik ki (ami megoldható egyszerű központi vénynyilvántartással, aminek jogosultsággal nem is kell foglalkoznia, csak egy vény érvényességével), s az esetleges visszaélések utólagos felderítését teszik lehetővé.

4 Következtetés

A táblázatból láthatóan az esetek eltérő jellege miatt **az egy közös megoldásban gondolkodás, a „majd a szuperkártya megoldja" felfogás téves irány. Célszerű a bankokhoz hasonlóan egy szolgáltatás portfólióban gondolkodni,** ami jelentős-részben választható lehet az ügyfelek által.

5 Járulékos szempontok

Az azonosítási probléma kezelésénél a szakmai megfontolásokon túl természetesen egyéb szempontokat is figyelembe kell venni. Ezek közül a leglényegesebbek:

5.1 Beruházásvédelem

A kormányzat kialakított egy központi azonosítási rendszert (ügyfélkapu) néhány kapcsolódó szolgáltatással. Ez szakmai szempontból rendkívül primitív, alacsony szintű, de mégiscsak milliárdokat öltek bele, így valamilyen átmentése beruházás-védelmi megfontolásból indokolt.

A primitív jelező magyarázatra szorul. Ha belép valaki egy egyszerű, ingyenes Gmail levelező rendszerbe, az azonosító/jelszó párost a rendszer már egy védett (https) kapcsolat keretében kéri be, a kormányzati megoldás csak a jelszóbekérés után vált védett módra. A legtöbb rendszer védekezik az automata támadások ellen, a bankok rendszerei pedig ma már nem csak az egyszerű jelszavas védelemre építenek (pl. van, amelyik SMS-ben küld véletlen kódot, van, amelyik egyszer használatos kódgeneráló eszközt biztosít), a kormányzati rendszer semmi ilyesmit nem nyújt. A bankok a telefonos ügyintézéshez is nyújtanak azonosítási lehetőséget, a kormányzati rendszer ezt sem

tudja (az APEH bevezetett ilyen szolgáltatást, de annak semmi köze a központi rendszerhez).

5.2 Finanszírozhatóság (nincs pénz)

A kormányzati stratégiák gyakori jellemzője a realitások figyelmen kívül hagyása, a PR jellegű szárnyalás. Ennek következménye viszont az igen alacsony szintű megvalósulás. A kialakítandó megoldásnál - ahhoz, hogy ténylegesen megvalósuljon – kiemelten kell figyelembe venni a reális finanszírozhatóságot.

5.3 Digitális szakadék kiküszöbölése

Érdemi lépések szükségesek a társadalmi egyenlőtlenségek felszámolására. Ez eddig főleg PR jelleggel próbálták kezelni. Egy közösségi internet elérési hely nem jelent érdemi segítséget a 85 éves néninek, vagy a 8 általános sem elérő munkanélkülinek az ügyei intézésében. Ha az állam tényleg törődni akar velük, a közvetlenebb formák alkalmazását alakítja ki. ennek egy jó formája lehetne, ha a posta vállalna át funkciókat. Egyik lehetőség, hogy telefonon megbeszélik a problémát az ügyintézővel, az kiküldi az űrlapot „előkitöltve", a postás kiviszi, aláíratja, elviszi, majd kiviszi az eredményt. Ahol lehet, törekedni kell az első lépés kiküszöbölésére (például telefon alapján van határozat, de csak akkor kapja meg a postástól, ha fizet és aláír, egyébként nem lesz jogerős). Mindez nem teszi feleslegessé az internet terjesztési programokat, közösségi helyeket, de azok elsősorban az internet általános szolgáltatásainak megszerettetésére kell, hogy irányuljanak, a közigazgatási szolgáltatások azokra alapozása tévút, a leszakadó rétegeknek nem valós segítség.

5.4 Gyors eredmény

A kormányok jellegzetessége az ígérgetés. Szó volt már elektronikus jegyről, útdíj-fizetésről, kormányzati negyedről, eTAJ kártyáról, új elektronikus diákigazolványról, egyikből sem lett semmi. Fontos, hogy az azonosítás területén ne ígérgetés, sok év alatt – talán – megvalósítható nagy tervek szülessenek, hanem az emberek által akár fél év múlva már érzékelhető, számukra javulást jelentő konkrét eredmények.

6 Megoldási javaslat

Egy gazdaságos, bevezethető, társadalmi elismerést hozó megoldáshoz a jelenlegi alapelvektől célszerű elszakadni, s a piaci szféra bevált gyakorlatához igazodni, csak a közigazgatás sajátosságai miatt feltétlen mértékű eltéréssel.

Az új alapelvek a következők:

6.1 Közvetlen kapcsolattartás lehetőségének biztosítása

A közvetlen kapcsolattartás lehetősége tehermentesíti az államot (nem kell mindenfajta kapcsolattartás minden feltételéről saját pénzén gondoskodnia), s egyben katalizálja a piacot, így az adatvédelmi követelményeken túl a gazdaságossági megfontolások miatt is ezt az utat célszerű megengedni. Ez nem azt jelenti, az állam teljesen kivonul erről a területről! S azt sem jelenti, minden szerv mindenféle külső megoldásra fel kell, hogy készüljön. De azt mindenképpen jelenti, hogy az elektronikus aláírás elmúlt kormányzati ciklusban tapasztal bojkottját meg kell szüntetni – anakronisztikusságát jelzi a Belsőpiaci Szolgáltatási Irányelv alapján kötelezően elfogadandó „Trusted list" miatt a teljes mellőzést nem is tudták fenntartani), s a hitelesített dokumentumok közvetlen benyújthatóságát érdemes biztosítani

Ez a gyakorlatban a következőket jelenti:

- Érdemi funkciót kap a **gyökértanúsító**, az általa tanúsított szolgáltatók szolgáltatásaira épülő elektronikusan aláírt dokumentumokat mindenhol el kell fogadni
- Kialakításra kerül az **on-line** eléréseknél használt azonosításokhoz használt **tanúsítványok gyökértanúsítása** is (azaz rendeződik az azonosítás jogi és technikai háttere, ami most csak az aláírásra terjed ki). Ezeket azon intézmények fogadják el, amelyek a párbeszédes szolgáltatásnál a kihívásos (tanúsítvány alapú) ellenőrzést nyújtják (magyarán, ha nyújt ilyen ellenőrzésű on-line szolgáltatást egy szerv, akkor nem válogathat, minden szolgáltató gyökértanúsítványra visszavezethető tanúsítását el kell fogadnia)
- A gyökértanúsítási rendszer részét képezi az EU szintű **„trusted list" kezelésének biztosítása**
- kialakításra kerül a **megbízható közigazgatási szolgáltatások hitelesítése**, s az ehhez szükséges tanúsítási rendszer (részeként a korábbi Biztonsági Hitelesítés Szolgáltató egyes funkciójának tényleges megvalósítása). Ez jelenti mind az eszköztanúsítások központilag kézben-tartott rendszerét, s a közzétett információk hitelesítésének biztosítását is
- bevezetésre kerül az attribútum tanúsítvány, de alkalmazható – a szolgáltatónál történő ellenőrzés („viszontazonosítás") is

Közvetlen megkereséskor az ügyfél az ügyintézésre vonatkozó igényéről közvetlen rendelkezhet (például elektronikus választ elfogad-e). Az egyes hivatalok ugyanakkor nem kell, hogy felkészüljenek a központi szolgáltatásokkal összemérhető szolgáltatási szintre a közvetlen kapcsolattartásnál, ezért itt valószínűleg (nem kizárva egyes

szervezetek ennél szélesebb kínálatát) alapvetően a kártya alapú kapcsolattartásra (elektronikus aláírás, tanúsítvány alapú azonosítás) épülnek.

Ez a központi szolgáltatástól független megkereshetőség alapvetően az EU elektronikus aláírásra vonatkozó direktívájára épül, de az ottani követelmények miatt belátható ideig feltételezi a kártyát vagy tokent, ami elterjedését nagyban lassítja, s alkalmazhatóságát is korlátozza (aki mobiltelefonján akar gyorsan egy felmerült problémát megoldani, az nem erre vágyik). Mint a táblázatból látszik, igen nagyszámú egyéb eset van, s ha az egyes sorokhoz a tényleges igényt (esetszámot) is hozzávesszük, akkor akár nagyságrendi különbség is kialakulhat (ha telefonon is lehet egyszerűen ügyet intézni, alighanem sokkal nagyobb lesz iránta az érdeklődés, mint amihez speciális eszközök, felkészültség szükséges).

6.2 Azonosítási monopólium felszámolása

A kormányzat által kiválasztott szabványoknak megfelelő on-line belépés azonosításnál is indokolt a piaci lehetőségek elfogadása. Nem szerencsés az a megközelítés, amivel a kapcsolattartást a kormányzat „hungarikumokkal" oldja meg. Semmiben sem épít piaci megoldásokra, így mindent magának kell – a teljes fejlesztési költséget állva és a fejlesztési kockázatot viselve – megvalósítania. Mivel az azonosításra és a hitelesítésre vannak bevált piaci megoldások, és hozzáférhetők szolgáltatások, az állam monopóliumát – mind hatékonysági, mind alkotmányossági megfontolásból – célszerű felszámolni.

6.3 Az azonosítás koordinációjának és magának a szolgáltatásnak a szétválasztása

Jelenleg az ügyfélkapu és maga a személyazonosítás egy összefolyó funkció, holott itt több logikailag elkülönülő feladat azonosítható. Az, hogy az ügyfél milyen azonosítást kíván alkalmazni, célszerű központilag kezelni, ezzel nagyban tehermentesíteni az intézményrendszert (az intézmény készíthet saját megoldást is, de a központi mindig rendelkezésére áll). Az azonosíthatósághoz elkülönült azonosítás szolgáltató, illetve regisztrációs szervezet kialakítása javasolható. A piaci azonosítás szolgáltatók ügyfélkapu azonosítóra vonatkozó tanúsítványon keresztül rendelik a személyt a regisztrációjukhoz, illetve az azonosításhoz szükséges egyéb tanúsítványokkal („attribútum tanúsítvány", vagy az elektronikus ellenőrzés biztosításával („viszontazonosítás") teszik lehetővé a személy azonosságának garantálhatóságát. Természetesen megmarad az állami szolgáltatás is (a jelenlegi jelszavas, ezt néhány technikával azért továbbfejlesztve), de az is elkülönül az ügyfélkaputól, külön központi szolgáltatásként, amit az ügyfélkapu – de a szakrendszerek is – igénybe vehetnek. Ennek ott van jelentősége, hogy például egy

telefonos ügyfélszolgálatnál közvetlenül igénybe vehető az azonosítási szolgáltatás, az internetes ügyfélkapu nélkül. A nem természetes személyek azonosítása is egyszerűsödik ezáltal, hisz lehet rájuk más regisztrációs szerv, miközben alkalmazhatják ugyan azt az azonosítási módot. Az ügyfélkapu igazából azt tisztázza, az ügyfél milyen előírásokat tett a kapcsolattartására (például kikötötte, tőle csak kártyás azonosítást fogadjon el az állam, akár a hitelesítés szolgáltatót is megszabva), s egy külön lépés a választott azonosítással a személy ellenőrzése (aminél vagy a tanúsítványokból kideríthető a személy azonossága, akkor maga az ügyfélkapu képes az ellenőrzésre, ha nem, akkor bizony a szolgáltatónak kell ezt megtennie). Ez a gyakorlatban azt jelenti, ahogy most egy szakrendszer az ügyfélkapuhoz fordul, ha személyt azonosíttatni akar, a jövőben az ügyfélkaputól azt tudja meg, milyen azonosítást fogadhat el, s magát az azonosítást vagy közvetlenül végezteti el a piaci szolgáltatóval, vagy a központi rendszer azonosítás szolgáltatását használja, ami azonban már elkülönül az ügyfélkaputól. Mindez nem zárja ki, hogy a folyamatosság érdekében átmenetileg létezzen olyan közös szolgáltatás, ahol az ügyfélkapu a profilnak megfelelő azonosítást maga intézi, azaz a szakrendszereket rövidtávon nem kell módosítani.

6.4 Központi biztonsági profil bevezetése

Az ügyfélkapu központi funkciójánál célszerű az azonosítás feltételrendszerén lényegesen túllépni, s egy személyre vonatkozó – általa önkéntesen megadott – biztonsági előírás halmazt (profilt) célszerű kezelni. A profilban rendelkezhet arról, milyen ügytípusokban engedi meg a kapu használatát (például az egészségügyet kizárja), az egyes ügytípusokhoz milyen biztonsági megoldásokat kíván alkalmazni (például a jelszón túl vállalja, hogy bejelentett telefonszámról a belépéskor felé közölt véletlen-számot SMS-ben beküldi, s az azonosítás csak akkor sikeres, ha az adott számról a kód beérkezik). Emellett a kapcsolattartási csatornákat is kijelölheti (bejelentett e-mailt kíván használni, a tárhelyes továbbítást fogadja vagy elutasítja stb.).

6.5 Az ügyfélkapu átalakítása három kategóriára

Az ügyfélkapu a valós felhasználási környezethez illeszkedve az alábbi típusként nyitható:

- **természetes személyhez rendelten**
- **egyéb személyhez (jogi személy, társadalmi szervezet stb.) rendelten**
- **anonim módon**

A személyhez rendelt ügyfélkapu jellegzetessége:

- **egy személynek több is lehet**, s több (de rögzített számú, például 5) ingyenes

- hozzá rendelődik egy általa megadott **biztonsági profil**, ahol megadja, hogy ezen ügyfélkapun történő azonosításánál milyen előírása van az állammal szembeni kapcsolattartásra, ilyen előírás különösen:
    - milyen ügytípusokra, szervezetek felé használható (például csak adózásra)
    - az egyes ügytípusoknál, szervezeteknél a jelszó mellett (eszköz használatakor akár helyette) milyen további azonosítást követeljenek meg tőle (például hiányos kódú azonosítás, SMS-ben bekérése a regisztrált telefonszámról a megküldött véletlen számnak, megnevezett hitelesítés szolgáltató által adott eszköz használata stb.)
    - milyen formában fogad üzenetet (SMS küldhető-e neki, email-t fogad, tárhelyet használ-e)
    - milyen formában küld üzenetet (például kizárja az emailt, akkor csak tárhelyén keresztül fogadnak, de rendelkezhet fordítva is)
    - legalább a nem természetes személynél akár több kód, több telefonszám stb. megadható, hogy a különböző képviselő személyek eltérő azonosítást használjanak (megkülönböztethetők legyenek).
- az ügyfélkaput tanúsított rendszerek szólíthatják meg (a központi portál is az, nem kitüntetett), kérésre beléptet egy személyt és megküldi a személyre vonatkozó biztonsági profil adott szervezetre vonatkozó részét. Az alkalmazás által küldött kérés is azonosított (szenzitív adatoknál hitelesített, azaz aláírt), az ügyfélkapu a kérés és kérő azonosítását – ahol adatot kér le – az azonosítás szolgáltató (beleértve a központi azonosítás szolgáltatást) felé megadja.
- **a természetes személy ügyfélkapuhoz rendelése valamilyen regisztrációs szerv azonosításán keresztül történik**. Az ügyfélkapuhoz rendelt egyedi felhasználónevet (most is van ilyen) a regisztrációs szerv (is) letárolja a regisztrált személy adataihoz, ezzel rendeli ügyfélkapuhoz. Lehetne ügyfélkapu azonosító is, de most már ezt így szokták meg. Az ügyfélkaput kezelő rendszer nem tudja, egy kapu kihez tartozik. Különböző regisztrációs szervek is lehetnek, a különböző ügyfélkapuk így egy szervnél sem futtathatók össze. Ha például valaki (gyökértanúsított) hitelesítés szolgáltató azonosítását kívánja alkalmazni, annak eszközének birtokában nem kerül „állami" regisztrációba a személyes adata, a regisztrációs szerv lehet a hitelesítés szolgáltató (ha például a tanúsítványba az ügyfélkapu belépési nevet belefoglalja, illetve az ellenőrzéshez szükséges elektronikus szolgáltatásokat vállalja).
- A használatnál az ügyfélkapu tényleg csak beléptet, s ellenőrzi, létező ügyfélkapu azonosítóra hivatkoznak-e. Ha igen, a kapuhoz rendelt profilban előírt azonosítási követelmények szerint jár el, például a jelenleginek megfelelő alapesetben egy (központi) azonosítás szolgáltatást kér, ami az ügyfélkapuhoz tartozó jelszót bekéri, ellenőrzi, s visszajelez a kapunak. Ekkor a kapu tudja, az ügyfélkaput nyitó személlyel azonos–e a belépő (ismeri a jelszót, a hiányos kódot, a kapuhoz megadott telefonról küldi meg a kódot stb.), de hogy ténylegesen ki az a személy, azt csak az ügyfélkaput létrehozó regisztrációs szervezet ismeri. A beléptetés után ezért csak annyit tudni, az

adott ügyfélkapu azonosítójú személy sikeresen belépett, ha ennél több kell (például neve) azt már a regisztrációs szervtől kell lekérni. Felülvizsgálható az a megközelítés, hogy a nevet/email címet küldi meg, általánosabb, ha az ügyfélkapu nem kérdez le automatikusan személyes adatot.

- Az azonosítás eszközei ne módosítását az ügyfél nem az ügyfélkapunál, hanem az azonosítás szolgáltatásnál végzi (például jelszó módosítást). Ha a biztonsági helyzet (kockázatelemzés eredménye) megköveteli, külön állami szolgáltatások állíthatók fel például a jelszóra, a hiányos kódra, az SMS kezelésre, ekkor több lépcsős az azonosítás, de a több szervezet megjelenése nagyban növeli a belső visszaéléssel szembeni toleranciát.
- A sikeres belépés után egy **időleges tranzakciós kód** rendelődik a belépéshez, ami addig tárolódik, míg ki nem lép, vagy ha ezt központ nem észleli, amíg újra be nem jelentkezik. Ez a kód kerül megküldésre a beléptetést kérőnek az ügyfélkapuhoz rendelt biztonsági profil további – kapcsolattartásra vonatkozó - részével együtt.
- A sikeres beléptetés egy ügyfélkapu azonosítójú személyre vonatkozik, az alkalmazás (portál, adózás stb.) a megkapott tranzakciós kód és biztonsági profil alapján teszi fel további kérdéseit. Itt nyilvánvalóan eltér a természetes és nem természetes személy kezelése (de ez lehet csak a biztonsági profil paraméterezése). A nem természetes személy esetében az ügyfélkapu (illetve az azonosítás szolgáltatás) a regisztrációs adatokat akár belépéskor bekérheti és rögtön megküldheti, a természetes személynél csak akkor, ha a profil így rendelkezik. Ügyfél rendelkezhet úgy is, hogy adatait közvetlen küldjék meg, azaz nem igényli a viszontazonosítást, az profilban megadott szerveknek, ügytípusokra az adatai kezelését a nyilvántartott szervek számára megengedi.
- A regisztrációs szervnek az ügyfél további adatokat is – önként – megadhat, például TAJ számot, adóazonosítót stb. A biztonsági profilban rendelkezhet arról, ez kinek továbbítható.
- Az ügyfélkapu rendszer a regisztrációs szervezetektől is hitelesített kérésekkel kér a biztonsági profil vonatkozó részének megküldésével, az ügyfélkapu azonosítóval.
- Az alkalmazás és regisztrációs szerv között az ügyfélkapu rendszer képez átjárót, a tranzakciós kóddal az alkalmazás, az ügyfélkapu azonosítóval a regisztrációs szerv felé. Ha ügyfél úgy rendelkezik, hogy ügyfélkapu azonosítója a szervnek (alkalmazásnak) kiadható – egy jogi személynél ez aligha gond -, akkor az alkalmazás azt is megkaphatja, de ezt követően már választhat, hogy az ÜK rendszeren keresztül vagy közvetlenül tartja a regisztrációs szervezettel a kapcsolatot. Itt meg kell jegyezni, hogy az elvi lehetőség gyakorlati problémákat felvethet, a regisztrációs szerv számára nem mindegy, hogy csak az ÜK rendszerrel (esetleg néhány kritikus nagy rendszerrel) tart kapcsolatot, vagy változó – bővülő – számú rendszer szólongatja, magyarán a gyakorlatban azért nem minden esetben érdemes biztosítani ezt a választást (nem éri meg, egy kicsit túllihegése lenne az adatbiztonságnak).

- A biztonsági profilt létrehozásakor elektronikusan hitelesíteni kell (időbélyeg, aláírás ügyintéző által, szegmentáltan, ha egyes részek elkülönülten küldhetők), s ez a kérésekhez mellékelt, kizárandó az ügyfélkapu rendszer operátorainak esetleges visszaélési lehetőségét.
- Az igényelt azonosítási szolgáltatásoknál harmadik fél szolgáltatása is kérhető (ez egyes azonosítási típusoknál – például kártyás kihívás – alkalmazható, általánosságban azonban az interoperabilitáshoz szükséges szabályok kialakulása szükséges hozzá).
- az ügyfélkapu csak belépésre (azonosításra) szolgál, nem tartozik hozzá semmi féle tárhely, postafiók stb. A tárhely nyitás külön opcionális funkció, amit ügyfélkapuval rendelkező végezhet. Egy ügyfélkapuhoz egy „tulajdonolt" tárhely tartozhat, de a tulajdonos más ügyfélkapus belépésnek az ügyfélkapu azonosító megadásával (biztonsági profilban) hozzáférést engedélyezhet (azaz családon belül egyet használhatnak kapcsolattartásra, nem kell külön-külön mindenkinek létrehozni, s figyelni). Természetesen egyes esetekben létrehozása lehet kötelező (például cégnek kell, hogy legyen). Cégeknél a tárhely a másodlagos értesítés abban az esetben, ha az elsőre fogadottként e-mailt adott meg, de nem igazolt vissza. Természetes személynél a másodlagos a papír.

Az anonim ügyfélkapu lényege, hogy a személy adatai csak papíron kerülnek rögzítésre a regisztrációs szervezetnél. Ez a kapu tehát alacsonyabb funkcionalitáshoz elég, de mivel visszaélés esetén a személy igazságszolgáltatási úton (a papíron rögzített adatai alapján) megtalálható, így sok esetben, ahol most is a bejelentőről elhitték nyilatkozata alapján, hogy kicsoda, ott ez a kapu is elegendő.

A fenti rendszer lényege tehát, hogy megtartja az ügyfélkapu központi szolgáltatást, de valós szolgáltatási rendszerré szervezi át. ebben a modellben a központi azonosítási rendszer lényeges – de egyszerű, kézbentartható költségű - bővítése szükséges (hiányos jelszó generálhatósága, SMS fogadásos megerősítés). E modell már befogadja a hitelesítés szolgáltatók azonosítási megoldásait (kártya, token).

6.6 Rendszeres jelentés bevezetése

A fentiekben ismertetett koncepció lényeges eleme még a biztonsági rendszer egyéb elemeinek kialakítása – tanulva a bankoktól. **Ennek fontos eleme az időszakos (például a fellebbezési időkre tekintettel kétheti) adatkezelési jelentés – például e-mailben - , amiben az ügyfél mindazon adatkezelési akciók tényéről (nem magáról az érintett adatról) értesül, ami az adott időszakban folyt**. Így megtudja, nevében mikor hova jelentkeztek be, milyen iratot küldtek be. Ezáltal alacsonyabb biztonsági szintet is elfogadhat, mivel illegális akciót felfedezve időben reklamálhat.

6.7 Dokumentum hitelesítés szolgáltatássá alakítása

A központi rendszer elkülönült szolgáltatásává válik a dokumentum hitelesítés is (a mostani feltöltésnél használthoz hasonló). Ezt a biztonsági profilban az ügyfél megengedheti, de ki is zárhatja. Mindenképpen elkülönülő funkció, a továbbítási rendszerekkel nem vonódik össze, önálló szolgáltatás. Értelemszerűen helyette alkalmazható a szolgáltatókra épülő elektronikus aláírás.

6.8 Tárhelyhasználat opcionális szolgáltatássá alakítása

A továbbítási rendszerben a tárhelyre töltés is opcionális elkülönült szolgáltatás, ami függetlenedik a hitelesítéstől, az azonosítást is ügyfélkapu meghívásával végzi, mint egy önálló alkalmazás.

6.9 Kártyakiadás

A kártyák kiadásánál – a friss német visszavonulásra is tekintettel – semmiképp nem egy gyors, nagy állami kártyarendszer bevezetése a célszerű a közeljövőben. **Helyette az önfinanszírozó, ahol lehet, piaci alapú kártyák használatának elfogadására tevődjön át a hangsúly.** Ilyen lehet egy postakártya kiadása, nem állampénzen ingyenes kártyaként, hanem olyan postai szolgáltatáshoz kötődve, ami miatt az ügyfél téríti a díját (de ez kapcsolódhat az utánvétes közigazgatáshoz, interneten vagy postásnál ezzel is fizethet, igazolhat). Az egészségügyben első lépésben a hivatásos (orvos) kártya kiadása látszik fontosabbnak, de ez akár a kamarákra is bízható (ha visszakapják nyilvántartás vezető, de legalább felügyelő funkciójukat). Hasonló előrelépési lehetőség egy korszerűbb diák kártya (de ennek sem kell mindent tudó szuperkártyának lennie), itt akár a bankok kártyáinak befogadása is elképzelhető. A cégek esetében az elektronikus kereskedelmi kapcsolatokban is használható üzleti kártyáknak juthat nagyobb szerep (hitelesítés szolgáltatók kínálata). Ezeket azonban nem kell erőltetni, csak a lehetőséget kell megadni, hogy ahol kimutathatóan gazdaságos, ott előre léphessenek (ne kelljen egy központi szupermegoldásra várva mindenhol várakozni). Lényeges, hogy központi szuperkártya elképzelések ne akadályozzák a gazdaságosan kialakítható rendszerek bevezetését, (abban, hogy a hazai közlekedésben a külföldi bevált gyakorlatokkal szemben még mindig papíralapú jegyek vannak, komoly visszahúzó szerepe volt a kormány szuperkártya elképzeléseinek).

Alapos átgondolást igényel a személyi igazolvány kérdésköre. Sok országban erre építve adtak ki többfunkciós elektronikus kártyát. A személyazonosításnál az elektronikus biztonságnövelés – mint az útlevélnél bebizonyosodott – várhatóan elkerülhetetlen lesz. Egy felmenő rendszerű korszerűsítésre tehát előbb utóbb szükség lesz. Az azonban

erősen kérdéses, hogy a lakosság teljeskörű e-személyi igazolvánnyal való ellátása indokolt-e? Mivel a lakosság ma már nem lebecsülhető része gépkocsival jár, számukra a jogosítvány hordozása kötelező, de akkor e kör számára egy másik igazolvány felesleges és csak zavaró tényező. A legutóbbi hírek szerint a briteknél is igen kemény ellenérzés alakult ki a személyazonosító bevezetési projektjükkel kapcsolatban, s ott is az vetődött fel, miért nem jogosítvány, útlevél? A multifunkcionalitással kapcsolatban sincs egyértelmű pozitív tapasztalat. Mindezek alapján e területen még alaposabb előkészület szükséges, nem javasolható egy még át nem látott fejlesztésbe való beleugrás.