VAS Réka

VÁLASZÚTON AZ INFORMÁCIÓS TÁRSADALOM

A SZEMÉLYAZONOSÍTÁS AKTUÁLIS KÉRDÉSEI

Az elektronikus ügyintézés, a kormányzati és üzleti szolgáltatások együttesen az információs társadalom eléréséhez vezető út eszközei. Ezek megfelelő alkalmazásával hatás gyakorolható az ország versenyképességére, a hazai és nemzetközi elvárásoknak való megfelelésre. A gazdasági növekedés egyik alapfeltétele, hogy az intellektuális tőke megléte mellett biztosított legyen azon eszközök és szolgáltatások köre, amelyek katalizálják a gazdasági folyamatokat azáltal, hogy lehetővé teszik a racionális, hiteles és megbízható működést. Az elektronikus ügyintézés az elektronikus azonosítással kapcsolatos problémák megoldását is megköveteli. Ennek érdekében meg kell vizsgálni a lehetséges megoldások előnyeit és hátrányait, technológiai hátterét, valamint a beruházás és a fenntartás költségeit is.

Kulcsszavak: **információs társadalom, elektronikus ügyintézés, adatvédelem**

A kommunikáció és az elektronikus ügyintézés[1], valamint az elektronikus kormányzati szolgáltatások fejlesztésének egyik lényeges pillére az **elektronikus azonosítással** (azaz a felhasználók számítógépes hálózatokon történő azonosításával) kapcsolatos kérdések megoldása. Egyöntetű a vélemény, hogy a probléma áthidalása tovább nem halogatható. Sokan figyelmeztetnek arra is, hogy a személyazonosításon túl biztosítani kell a jogi személyek, intézmények, szervezetek stb. elektronikus azonosítását is.

Évek óta, sokszor egymással párhuzamosan, készülnek olyan fejlesztési tervek, sőt zajlanak konkrét projektek, amelyek valamilyen módon az elektronikus azonosítással, intelligens kártyákkal és egyéb eszközökkel célozzák meg a hatékonyságnövelést, modernizálást, megfelelő biztonsági szint elérését, költségcsökkentést (állampolgári kártya, diákigazolvány, munkakártya, elektronikus tb-kártya, közlekedési kártya, elektronikus jegyrendszer stb.).

Aktualitást ad ennek a kérdésnek egyrészről az egészségbiztosítókról szóló törvényben meghatározott **egészségügyi kártya** (2008. évi I. tv.), másrészről a MEH által az **elektronikus személyazonosítás**ról szóló kormány-előterjesztés munkálatainak állása.

Az elektronikus személyazonosítás stratégiai lehetőségei

Az elektronikus személyazonosításnak önmagában se gazdasági, se társadalmi haszna nincs, értelmet csupán a hozzá kapcsolódó alkalmazásokból nyer. Ezt a szempontot jelenítik meg az EU különböző stratégiai célkitűzései (pl. 20 kiemelt közigazgatási alkalmazás) (eEurope2002: Impact and Priorities, 2001). Az elektronikus személyazonosítás lehetséges stratégiáit önmagában az azonosítás technológiai megoldásából levezetni nem lehet, csak a lehetséges alkalmazások és alkalmazók körének, számosságának együttes figyelembevételével alkotható meg.

Alapvetően két stratégiai irány fogalmazható meg, melyek tekintetében az egyes tagállamok egymástól jelentősen eltérő utakat járnak be:

a) Az egyik stratégiai irány úgy foglalható össze, hogy a szubszidiaritás elvét követve, tagállami szinten, az állam egységes azonosítót bocsát ki, és az egyes szakrendszerek, illetve a verseny- és a magánszféra alkalmazásai erre az **egységes azonosítóra** épülnek.

b) A másik, az azonosítókibocsátás relatív autonómiájával élve, **egynél több azonosító rendszer** mellérendelt konstrukcióját feltételezi.

Közigazgatási szempontból az első stratégiának nagyon erős adatvédelmi korlátjai vannak (Magyarországon közismerten Európában az egyik legszigorúbb adatvédelmi törvény hatályos [1992. évi LXIII. tv.)]), míg a második stratégia előfeltétele az interoperabilitás megteremtése. Az egységes állampolgári azonosítóra épülő stratégia megvalósítása ugyanakkor nagyon nehezen skálázható, és koncentráltan nagy ráfordításigénye van.

A közigazgatásban ma is léteznek egységes azonosítómegoldások, melyek hosszú távú fennmaradása valószínűsíthető. Az egyik ilyen megoldás a személyi igazolvány **(1)**, amely az Európai Unió direktívájának (EU Directive 95/46/EC, EU Directive 97/66/EC) megfelelően intelligens személyi igazolvánnyá fejlődik ki, és elvben betöltheti az elektronikus személyazonosítás funkcióját is. A másik megoldás az útlevél **(2)**. Ezek bizonyosan sem egymással nem vonhatók össze, sem más szereptanúsítvánnyal nem bővíthetők. A harmadik egységes azonosítórendszer a tb által kibocsátott azonosító **(3)**, amely jellegét tekintve az államigazgatás egyik alrendszeréhez kapcsolódik (továbbiakban szakrendszerek), de egységesítésében fellelhető nagyon komoly összeurópai tendenciák miatt ez nemcsak országon belüli hatókörrel, hanem páneurópai karakterrel is rendelkezik.

A felsorolt megoldások mellett újabb megoldásként vezetik be az *önálló állampolgári azonosítót*, amely az elmondottak fényében rövid távon nagyon költséges, hosszabb távon pedig a redundancia veszélyét hordozza magában. A második stratégiai irányba sorolhatók azok a megoldások, amelyek az egyes szakrendszerekhez kötődnek (APEH, oktatás, foglalkoztatás stb.), illetve ugyanezt a szerepet a versenyszféra is elvállalhatja. Itt elsősorban a biztonsági követelményeknek maradéktalanul eleget tevő bankszektorra gondolunk. Ehhez a megoldáshoz társul az eltérő technológiai platformon, de ugyancsak PKI infrastruktúrával működő mobil azonosítás is. Külön figyelmet érdemel a személyazonosítás és a rádió frekvenciás (RF) technológia párosítása, elsősorban a kiterjedt közlekedési alkalmazási lehetőségek miatt (Mártonffy, 2006a).

A szakrendszeri azonosítók kidolgozása, bevezetése többféle előnnyel is jár. Két kiragadott példa:

- Nagyon erősen kötődnek az alkalmazásokhoz. Az első stratégiai iránnyal szemben, a szakrendszeri azonosítás esetében, fordított logika érvényesül. Míg az előzőben **(a)** a gondolatmenet szerint egy azonosító lenne, és majd ez húzná be az alkalmazásokat, addig utóbbi esetben **(b)**, a szükséges alkalmazásokból indulunk ki, amelyeknek előfeltétele az elektronikus személyazonosítás.
- Az utóbbi, alkalmazásorientált megközelítés nagyon jól fókuszált célcsoportokat lát maga előtt, ami egyben erős optimizmusra ad okot a kritikus alkalmazói tömeg[2] és tényleges eredmények elérésében.

Problémák, dilemmák

Ha létezne minden szempontot kielégítő és egyúttal megvalósítható megoldás, akkor minden bizonnyal már bevezették volna. A helyzet azonban ennél jóval bonyolultabb, számos probléma, dilemma nehezíti meg a döntéshozatalt.

Jó gyakorlatok hiánya

Sajnos az EU-s azonosítórendszerek közötti együttműködésre irányuló törekvések még nem rendelkeznek olyan eredményekkel, amelyeket műszaki szempontból használhatnánk.

Az EU-ban nincsen pontosan meghatározva, hogy egy adott ország milyen megoldást választ az elektronikus személyazonosításra. Itt a spektrum a legszélesebb határok között mozog, a minősített tanúsítványtól a jelszavas bejelentkezésig.

Egy kártya vagy több kártya, központi vagy decentralizált megoldás

A jogosultságok[3] központosított kezelése – amennyiben teljes mértékben megfelel az adatvédelmi előírásoknak – nagyon költséges, mert több, egymástól független rendeltetésű rendszer hatékony együttműködését kívánja meg.

Elképzelhető a különböző kártyakiadó rendszerek működésében központi szereplő, akár a lakcímnyilvántartó bevonása, de ez pillanatnyilag nincs kitalálva, nincs előkészítve, nincs egyeztetve.

El kell különíteni a közhiteles személyazonosítást, ahol csak egy központi állami tanúsítás fogadható el, illetve a többi személyazonosítást, amelyeket sikerrel használnak az üzleti élet szereplői. Például az egészségpénztárak kiadhatnak olyan kártyát az ügyfeleiknek, amelyeket a saját rendszerükön belüli azonosításra használnak, és esetleg nem közhitelesek, mint az állami kártya, de azért az ő céljaikra (lásd bankok) megfelelnek. Ha minden ilyen üzleti kártyát államivá akarunk tenni, akkor például az egészségügyi kártya esetében lényegesen meghaladjuk az indokolt biztonsági szintet, vagyis lassan és drágán történhet csak a bevezetés.

Szükséges biztonsági szint

Az elektronikus azonosítási rendszerek nem nyújtanak 100%-os biztonságot, hanem bonyolultságukkal és költségükkel arányosan, ehhez egyre közelebb jutnak a 100%-hoz. Például az egészségügyi kártya, az elektronikus személyi igazolvány vagy a fénymásoló kártya másmás biztonsági szintet igényel, és feleslegesen költséges mindenhol a legmagasabb szintet megvalósítani. Tökéletesen biztonságos elektronikus megoldás nem létezik a személyazonosításra, még az útlevelek másolását, védelmének feltörését sem lehet teljesen kizárni.

Általában a számítógépes biztonság és a biztonságot szolgáló rendszerek tervezésének alapja a kockázatelemzés (ISO/IEC 15408), ennek hazai szabványai is léteznek. A gazdasági szférában alkalmazott biztonsági eljárások és rendszerek költsége arányos a kockázatelemzés során kapott várható károkkal. A bankok sem tartják égető szükségnek az intelligens debit/credit kártya bevezetését, mert az elérhető kockázatcsökkenés nem áll arányban a bevezetés költségeivel.

Az államigazgatás ugyanakkor a zéró kockázatot szeretné elérni, ami egyrészt nem reális kiindulási alap, másrészt a költségek szükségtelen növelését jelenti. Az elektronikus azonosítás szintjénél alkalmazni kellene a célhoz kötöttség elvét, azaz minden rendszer-használat biztonságát a kockázatokkal kellene arányosítani. (Ne kelljen drága eszközöket használni ott, ahol az olcsó is kellően biztonságos.)

Hivatalos kontra üzleti kártya

Problematikusnak látszik a hivatalos kártya és az üzleti kártya összeférhetősége. Az üzleti szereplők (utazási, banki, biztosítói stb.) általában ragaszkodnak ahhoz, hogy az azonosítókártyákat ők adják ki, saját arculatukkal stb. (Vanamali, 2004), ami általában nem valósítható meg, ha hivatalos okmányról, például elektronikus személyi igazolványról van szó. Fordítva, az okmányjellegű, személyazonosításhoz szükséges adatokat tartalmazó kártyáknál adatvédelmi kérdéseket vethetnek fel az üzleti alkalmazások.

Az üzleti kártyák esetében alaposan végig kellene gondolni, hogy mi a viszonya az államnak ezekhez. Megfelelő esetben ezeket a kártyákat az állam elfogadhatja, információkat helyezhet el rajta stb., miközben ez a költségcsökkentést és a bevezetés gyorsaságát is szolgálja. Magyarországon lényegében nincs szó az ilyen azonosítási modellekről, sőt inkább kizárják ezeket a jelenlegi elképzelések.

Személyes azonosítás kontra távoli ügyintézés

A (továbbfejlesztett) személyi igazolvány alapfunkciója a természetes személy megjelenésekor történő hivatalos személyazonosság megállapítása (igazoltatás). Ekkor a fénykép és egyéb adatok (ujjlenyomat stb.) alapján győződnek meg arról, hogy kicsoda az illető. Nem mindenhol szükséges azonban ez az azonosítási erősség. Az utazási igazolványok vagy céges belépőkártyák az adott kontextusban személyazonosításra szolgálnak, csak nem ilyen biztonsági szinten.

Míg a személyes megjelenésnél indokolt lehet egy rendkívül magas biztonsági szint, addig az ügyek jelentős részében – különösen távoli intézésnél – már erősebben támaszkodni lehetne az élet más területén, önkéntesen választott biztonsági megoldásokra (a banknál az ügyfél dönt, mire és milyen mértékben használ kártyát, telefonos ügyintézést).

A probléma elsődlegesen a távoli (például telefonos, internetes) eléréskor történő azonosításnál jelentkezik. Alapkérdés a más intézményrendszer azonosítási megoldásainak elfogadása. Több példa van arra, hogy a bankok azonosítási rendszerét az elektronikus (távoli) ügyintézésben az állam elfogadja (például Észtország, pedig van kiadott elektronikus személyi) (Kő – Vas, 2004).

A távoli elérésnél lényeges kérdés a telefonos kapcsolatban használt azonosítás. Az üzleti életben (például bankok, közműszolgáltatók, távközléscégek) széles körben elterjedt a telefonos ügyintézés lehetősége, sokkal hozzáférhetőbb az internetesnél, sok ügytípusra ez is elégséges. Hasonló szolgáltatást az állam is nyújthatna, de ehhez szolgáltatást és telefonos azonosítást kell kiépíteni.

Egy konkrét példa: egészségügyi (biztosítói) kártya

A fenti általánosabb megjegyzések jelentősége jól értelmezhető az egészségügyi, biztosítói kártyával kapcsolatban, amely az egészségügyi reform miatt is aktuális (Mártonffy, 2006b).

A korábban említett **a)** megoldás, az egységes azonosítás esetén ez úgy nézne ki, hogy valamilyen központi szervezet kiadja, és egy alkalommal hitelesíti az elektronikus azonosítókártyát (ez az Elektronikuskormányzat-központ jelenlegi elképzelése, okmányirodák bevonásával). Ezt követően a kártyabirtokos elmegy a saját biztosítójához, ahol elhelyezik kártyáján az egészségügyi adatokat, TAJ-számot stb. Így a kártya biztonsági szintje megfelelne az elektronikus személyinek, viszont lényegesen költségesebb és bonyolultabb lenne, mint az szükséges. A gyors bevezethetőséget tönkreteszi ez a bonyolult terítés (Ausztriában postán küldték ki mindenkinek az e-egészségügyi kártyát). Tömeges kiadásnál elő-megszemélyesítésre, adatok nagyüzemi feltöltésére lehet szükség, amelyhez rugalmas eljárási

rend kell. Kérdéses, hogy ebben az esetben az üzleti szereplők hogyan tudnak rugalmasan saját alkalmazásokat elhelyezni a kártyán, a saját arculatról pedig valószínűleg le kellene mondaniuk.

A **b)** megoldás, tehát a több azonosítórendszer párhuzamos létezése esetén meg kell alkotni egy egységes műszaki szabványt (ennek alapjai rendelkezésre állnak). Ezt implementálva a biztosítók saját maguk adhatják ki az egészségügyi kártyát, az országos TAJ-szám-nyilvántartás adataival ellenőrizve. Az így kiadott kártyára ezt követően további tanúsítványok, azonosításra alkalmas adatok helyezhetők el. Ha a kártyabirtokos olyan elektronikus kormányzati szolgáltatásokat is igénybe kíván venni, ahol szükséges az okmányirodai hitelesítés, akkor a kártyájával elmegy az okmányirodába, és elhelyezik rajta a megfelelő közhiteles azonosítás után a szükséges adatokat. Továbbmenve, bármilyen más, a szabványoknak megfelelő alkalmazásra „élesíteni" tudja a kártyát, például a közlekedésre. Ebben az esetben a gyors bevezetés is tartható, hiszen akár postán is ki lehet küldeni az új kártyákat. A felhasználók pedig el tudják dönteni, hogy milyen egyéb szolgáltatásokra kívánják igénybe venni kártyájukat.

Lehetséges megoldás: a federatív modell

Az eddigiekből úgy látszik, hogy a magyar viszonyokban a **b)** megoldás, vagyis a több azonosítási rendszer párhuzamos létezése alkalmazható jobban. Több ilyen szakrendszeri azonosító esetében előfeltétel az **interoperabilitás** (CompTIA, 2004). Ezalatt azt kell érteni, hogy az egyik szakrendszer által kibocsátott azonosítóval az állampolgár hitelesen tudja azonosítani magát egy másik szakrendszerben is. Ezt a feltételt úgy lehet kielégíteni, hogy az azonosítórendszerek működése fölé egy olyan federatív elven működő hálózatot hozunk létre, amely lebonyolítja a különböző szakrendszerek közötti kommunikációt.

Az úgynevezett **federatív modell** az elsődleges azonosításszolgáltatót és jellegét meghagyva, egy „gateway" architektúrát (réteget) helyez a rendszer fölé, amivel biztosítható a konstrukció kialakítása, illetve az ahhoz történő csatlakoztatás. Ez az architektúra már létezik, működőképességét nemzetközi tapasztalatok is bizonyítják (*GUIDE Creating a European Identity Management Architecture for eGovernment (IST-2003-507498) is part funded by the European Commission's 6th Framework Programme*).

A federatív modell előnye, hogy ha valamilyen okból kifolyólag (adatvédelmi, időkorlát, kapacitáskorlát stb.) az egy központi szolgáltató mellett esetleg más szolgáltatók is létrejönnek, akkor a létrejövő más szolgáltatók saját „gateway"-en keresztül azonnal csatlakozni tudnak a federációban részt vevő többi azonosításszolgáltatóhoz.

A megoldás előnye, hogy miközben nem zárja ki az uralkodó álláspont érvényesülését, lehetőséget biztosít, hogy szükség esetén ettől eltérő koncepció mentén megvalósított megoldásokat emeljünk be a rendszerbe.

Az azonosítási folyamat meghatározása nemzeti hatáskörbe tartozik, nem várható olyan kötelező érvényű irányelv, mely egységesítené ezeket a protokollokat.

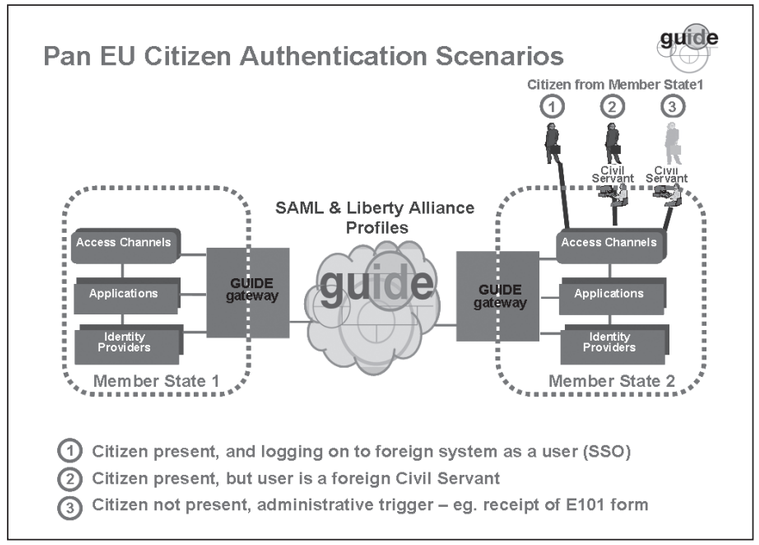
A federatív (szövetségi) modell meg tudja oldani, illetve kezelni tudja azt a problémát, amely a PKI infrastruktúra alapértelmezésű megvalósításának sajátossága. A tanúsítvány, a hardvereszközön elhelyezett személyes adatok nem lehetnek nagyon részletesek, egyértelmű azonosításra alkalmasak, sem adatvédelmi, sem biztonsági okokból. Nyilvánosan elérhető helyen (tanúsítványtárakban, címtárakban) tárolt személyes azonosításra használható adatok nem lehetnek nagyon részletesek, és ezért az informatikai biztonság jelenlegi helyzetében, illetve a technológia jelenlegi állása szerint megint nem célszerű és nem is lehet az előbbi okok miatt egyértelmű azonosításra, hitelesítésre és a jogosultságok, jogosítványok megadására felhasználni az esetleg nyilvánosan elérhető adatokat.

A közigazgatásban egyértelműen felmerülő nagyfokú biztonságú és helyességű személyazonosítási igény és a jogi szabályozásban – olykor önkényesen – meghatározott, alkalmazható technológiai lehetőségek között feszülő ellentmondás egyik lehetséges feloldása a federatív megközelítés szellemében a következő:

- Az elektronikus azonosításra alkalmas tanúsítvány az adatvédelmi és célszerűségi szempontok alapján a minimálisan szükséges személyes adatot tárolja olyan formában, amely kriptográfiailag viszonylag gyengén védett.
- A hardver adathordozó eszközön kriptográfiailag erősen védett formában sem célszerű nagyon sok adatot tárolni, mivel a kriptográfiai kulcsok eléréséhez, aktiváláshoz általában egy sokkal egyszerűbb PIN-kód vagy jelszó szükséges, amely a leggyengébb pontja az egész rendszernek. Az erős kriptográfiai védelem ezzel a jelszóval felbontható, és sokkal kevesebb számítási erőfeszítés kell hozzá, mint a kriptográfiai védelem alapját alkotó kulcs megszerzéséhez.
- A tanúsítvány azonosítóját vagy valamilyen azonosítót lehet arra felhasználni, hogy a kriptográfiailag védett kommunikáció során az azonosító alapján a tanúsítványokat és a regisztrációs adatokat tároló

1. ábra

GUIDE – A federatív elvű megközelítés (GUIDE, 2006. p.33.)



adatbázisból egy helyesség-ellenőrzést lehessen elvégezni. Azaz a személy által közölt adatok, a hardvereszközön tárolt adatok és a hitelesítő/regisztráció szervezet adatbázisában tárolt adatok egyeznek. Ezt a viszontazonosítást a federatív rendszer résztvevői önként alkalmazzák, interoperábilis, együttműködő protokollokat alkalmaznak azért, hogy lehetőleg vonalon és valós időben (on-line, interaktív, real-time) az azonosítást hitelesítsék.

A federatív elvű azonosítás a legkülönbözőbb alkalmazástípusokat kezeli *(1. ábra).*

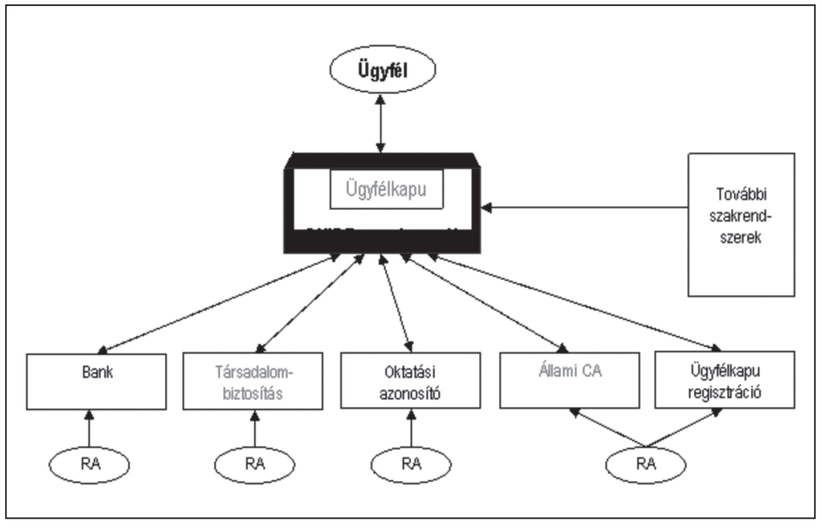
A federatív modell bevezetésének ma is megvannak az alapjai, az eddig megtett fejlesztéseket nem kell lecserélni. Az Ügyfélkapu és az állami CA (tanúsítás) jóváhagyott kiemelt projektjei mellett a tervezett pénztári kártya a federatív modell csirája lehet. Az EKOP-ból az Ügyfélkapu és az állami CA finanszírozása megoldott, a pénztári kártya bevezetésére is van forrás. Később – főként a technológiaváltás ütemének megfelelően – a magánbiztosítók ezt a szolgáltatást átvehetik (finanszírozzák). A tanúsítás állami monopóliumát sem szerencsés fenntartani, egyrészt több állami tanúsítószervezet is lehetséges, másrészt a versenyszféra versenyképes árakon tud szolgáltatást nyújtani[4] *(2. ábra).*

Sokféle platform együttes működésének technológiai korlátja nincs. A federatív megoldás automatikusan biztosítja a személyazonosításnak páneurópai dimenzióra való kiterjesztését is, hiszen a tagállamok közötti együttműködés, illetve személyazonosítás problémája teljesen analóg a szakrendszerek közötti együttműködés problémájával.

Az állampolgár döntésén és lehetőségén múlik, hogy a saját személyazonosítását mely hordozó igénybevételével oldja meg. A lehetséges skála a mobil megoldásoktól a szoft tokenig (pl. Ügyfélkapu-azonosító és PIN-kód) terjed. Szintén állampolgári döntés, hogy egy kártyára több tanúsítvány elhelyezését kéri, vagy szakrendszerenként külön-külön kártyát tart a zsebében.

2. ábra

A séma alkalmazása a magyar helyzetre



Külön ki kell emelni a személyazonosítás megvalósításában a versenyszféra, illetve a bankok szerepét. Minthogy mindenre, erre is lehet találni Európában számos példát, elsősorban a skandináv országokban. Ha a bankok által kibocsátott személyazonosító kártya alkalmas fokozott biztonságú elektronikus aláírásra, akkor ezzel egy igazi PPP konstrukció hozható létre. Az előzőekben leírtakhoz képest – melyben a beruházási költségeket az államigazgatás különböző alrendszerei között kellene szétterhelni – a bankok által kibocsátható kártyák költségeit egyértelműen a bankoknak kellene állni, hiszen azok megtérülését az általuk nyújtott szolgáltatások-ban fogják realizálni.

A fenti okfejtésből következik, hogy bármelyik kiválasztásra kerülő megoldásnak technológiai akadálya nincsen, azonban a választásnál együttesen kell mérlegelni a bevezetés és az érzékelhető pozitív hatások megjelenése között eltelő időt, a megvalósítás egyszeri beruházási költségeit, a bevezetett rendszer életciklusa alatti fenntartásának költségeit. Ezek együttes figyelembevételével a ma asztalon fekvő megvalósítási javaslatok közül egyértelműen lehet választani, illetve a megvalósításhoz szükséges politikai akarat is egyértelműen jól argumentálható.

Összegzés

A megoldás megtalálásához több lehetőséget kell megvizsgálni, s egyeztetni az érintett kormányzati szereplőkkel. Megvalósíthatósági tanulmányokat, kockázatelemzéseket kell végezni.

A kidolgozatlan részletkérdések valójában koncepcionális döntésekre vonatkoznak, részletesebb kidolgozás és egyeztetés nélkül felelős döntés a kérdésben nem tud születni.

Elvi probléma a megjelenéskori azonosítás és a távoli kapcsolattartásnál használt azonosítás keverése, s ez utóbbinál különösen hiányzik az egyéb lehetőségek megjelenítése Magyarországon (amelyek egymás mellett is élhetnek). A túlzottan magasra tett követelményszint, túlzott központosítás a pénztári kártya gyors, reális költségű bevezetését nem tenné lehetővé, s emellett gyakorlatilag kizárná más, egyszerűbb, gyorsan bevezethető megoldások alkalmazását is.

Nemcsak személyek, hanem intézmények/cégek/szervezetek elektronikus azonosítására is fel kell készülni.

Összefoglalva, a jelenlegi helyzetben nem megfelelő egy központi megoldás gyorsnak vélt bevezetése, hanem az érintett szereplők közös egyetértésben elfogadott, kidolgozott koncepciójára és megvalósítási tervére van szükség.

Lábjegyzet

[1] Ideértve minden lehetséges tranzakciót, a regisztrációt, a jogosultságok megállapítását, a szolgáltatások igénybevételét stb.

[2] Kritikus alkalmazói tömeg úgy értendő, mint a felhasználók azon minimális száma, amely mellett a szolgáltatások TCO alapon számítva rentábilissá válnak. Tekintettel arra, hogy a szakrendszeri azonosító létrehozatalának beruházási költségei alacsonyabbak, ezek a szolgáltatások már rövidebb távon, viszonylag alacsonyabb alkalmazói szám mellett is rentábilisabbá válnak, az egységes állampolgári azonosítóhoz képest. A társadalmi költség szintjén a második stratégia esetén várható gazdaságosság még akkor is jobb lehet, ha beruházási oldalon az egymás mellett létező szakrendszeri azonosító megvalósítása összességében több mint az egyegységes azonosítóé.

[3] A webes alkalmazások többsége megköveteli, hogy felhasználóikat megkülönböztethessük abból a szempontból, hogy a rendszer mely szolgáltatásait, funkcióit használhatják. A jogosultság azt határozza meg, hogy az adott felhasználónak milyen interakciókra van lehetősége az alkalmazással szemben.

[4] A monopólium ellen szólnak a magas költségek, a verseny kizárása és a korrupció nagy valószínűsége.

Felhasznált irodalom

CompTIA (2004): *European Interoperability Framework*, White Paper, Brussels

eEurope2002- Impact and Priorities: A communication to the Spring European Council in Stockholm, 23-24 March 2001 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2001&nu_doc=140

GUIDE (2006): *Policy and Research Implications of GUIDE for eGovernment in the EU*, White Paper

ISO/IEC 15408 1, 2 , 3 Informatikai biztonsági szabvány

Kő, A. – Vas, R. (2004): Research and assessment of existing IdM systems for eGovernment in the EU, EU IST E-government: GUIDE Report

Mártonffy, A. (2006a): Érintkezés nélkül, IT-Business, IV. évfolyam 42. szám,15. old.

Mártonffy, A. (2006b): Kártyacsat az egészségügyben, IV. évfolyam 46. szám, 14–19. old.

Vanamali, S. (2004): Identity Management Framework: Delivering Value for Business, Information Systems Control Journal, Vol. 4., ISACA

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról

2008. évi I. törvény az egészségbiztosítási pénztárakról

Cikk beérkezett: 2008. 3. hó
Lektori vélemény alapján véglegesítve: 2008. 5. hó.