



## MELLÉKLET

### **Egy, az alkotmányos adatvédelmi elvárásokat teljesítő informatikai alternatíva**

Az adatvédelem jogszabályi feltételeinek kielégítéséhez az informatikai rendszerek kialakításánál szükség van négy tényező együttes figyelembevételére, ezek:

#### **1. Az AB<sup>1</sup> határozataival kialakult jogértelmezés maradéktalan betartása**

Az AB határozataival egyértelműen kijelölt egy adatvédelmi felfogást, amelynek megkerülési kísérletei rendre csak idővesztéséget és hosszabb távon jelentős többletköltséget jelentenek. El kell fogadni, hogy a célhoz kötöttség elvének gyakorlati megvalósításához architekturális garanciális elemekre van szükség, az egyszerű – kezelők vagy a gép felett felügyeletet szerző hacker által kiiktatható – védelmi rendszerek nem elégítik ki e követelményt. Hasonlóképpen tudomásul kell venni, hogy az önrendelkezés gyakorlati megvalósulásához általános érvényű meghatalmazások nem elegendők, a személyek megfelelő eseti tájékoztatása, hozzájárulásának megszerzése, illetve a kifogásolás lehetőségének biztosítása elengedhetetlen.

#### **2. A bevezethetőség**

Olyan megoldások jöhetnek csak szóba, amelyeket reális időn belül, alacsony kockázattal a közigazgatási alkalmazásokban be lehet vezetni. A K+F jellegű új ötletek nem jelentenek tényleges lehetőséget az üzemszerűen működő állam intézményrendszerének, amely kísérleti terepként semmiképpen nem kezelhető.

#### **3. A megfizethetőség**

Csak olyan megoldás jöhet szóba, amely nem jelent aránytalanul nagy költségterhet az államnak. Nagyon fontos az adatvédelem, de az adófizetők pénzéből erre való hivatkozással nem lehet irreális mértékben megterhelni a költségvetést. Természetesen ebből nem következik, hogy semmit sem kell költeni e feladatkörre. Néhány (akár 5-10) százalékos többletköltségnek egy-egy rendszer kialakításánál mindenképpen bele kell férnie a projektek költségvetésébe az alkotmányosság megtartásához, azaz nem fogadható el, hogy a rendszerek fejlesztése során a jogszabályi követelmények kielégítésénél semmilyen többletköltséget nem akarnak felvállalni, de az elfogadható, hogy mérsékelt költségű megoldásokra törekedjenek.

---

<sup>1</sup> Alkotmánybíróság

#### 4. A hatékonyság biztosíthatósága

Közvetve összefügg a megfizethetőséggel az alkalmazott megoldás hatása a hatékonyságra. Az informatikai rendszereknél kritikus tényező a „válaszidő”, vagyis hogy a képernyő mellett ülve mennyi időn belül kap választ a felhasználó (akár ügyfél, akár tisztviselő). A számítógépeknél az adatok kezelését hatékonyan biztosító megoldások a közvetlen összekapcsolhatóságon alapulnak. A megfelelő védelmi megoldásoknál arra is tekintettel kell lenni, hogy az igényelt többletfunkció bevezetése a működés hatékonyságát ne rontsa le olyan mértékben, hogy az elfogadható válaszidőkhöz megfizethetetlenül nagy számítástechnikai kapacitásra legyen szükség a hatékonyság leromlása miatt. A hatékonysági követelmény miatt nem lehet szoftveres titkosítási megoldásokkal élni az egész állomány vonatkozásában, mert adatbázis-műveletek, keresések szükségesek a működéshez, amelyek során a „minden egyes adatelem visszakódolása és összehasonlítása” típusú működés a gyakorlatban széles körben nem alkalmazható.

Az egyes tipikus adatvédelmi problémákra egy lehetséges egyszerű és (viszonylag) olcsó – de nem kizárólagos – megoldás a következő:

##### 1. Az adatok összevonhatóságának, illegális megszerzés esetére a felhasználásának megakadályozása

Az adatvédelem tekintetében az egyes informatikai rendszerek általában rendelkeznek olyan jogosultságkezelési rendszerrel, amely az egyes felhasználóknak csak a nekik engedélyezett adatokhoz teszi lehetővé a hozzáférést. Ez azonban nem elegendő garancia az adatok tényleges védelmére, az IT rendszerek rendre feltárt biztonsági rései, hazai példaként az ügyfélkapu üzemzavara ezt a megállapítást alátámasztja. Garanciális elem szükséges arra is, hogy személyes adatok (személyhez rendelt) az alábbi esetben se kerülhessenek nyilvánosságra:

- hacker kívülről behatol a számítógépes rendszerbe, és az adatokat kimásolja,
- a rendszerhez hozzáférő kezelő (operátor) másolatot készít az adatokról, amit ő vagy mások fel kívánnak használni,
- a számítógéphez jogszerűen hozzáférő egyéb személyzet (hardveres karbantartó, szervizes) másolatot készít az adatokról,
- programhiba az adatokhoz hozzáférést biztosít.

Mivel az adat kikerülését a tapasztalatok alapján nem lehet megakadályozni, így nyilvánvalóan annak értelmezhetőségét kell meggátolni. E témakörben figyelembe kell venni ugyanakkor, hogy észrevétlenül kialakult egy univerzális, állandó azonosító. A viselt név, leánykori név helyett a születéskori név alkalmazásával a természetes azonosítók hosszának és tárolási struktúrájának rögzítése egyben egy új univerzális azonosító bevezetését jelenti a számítógép számára. A természetes azonosítók ilyen használata logikus; nem indokolt, és nem is lehetséges a korlátozása. Az AB elvárásainak érvényesítéséhez azonban szükséges, hogy ez az univerzális azonosító (maguk az alapadatok, a természetes azonosítók) az IT rendszerekben elkülönülten (külön törzsadatállományban) tárolódjon, az alkalmazási alrendszerek ne ezzel azonosítsanak, hanem belső kóddal, s mind a belső feldolgozásnál, mind az intézményközi küldésnél ne ez legyen az azonosító. Ennek garantálását jogszabályban kellene rögzíteni. A kialakítandó IT rendszereknél a bevezetésben megfogalmazott szempontok figyelembevételére több lehetőség is van, ilyen technikák például az alábbiak:

## a) Célhoz kötött adatkezelésnek megfelelő nyilvántartás

A természetes azonosítók univerzális azonosítóként való használatának elkerülése érdekében a nyilvántartások kialakításánál szét kell választani magát a kifelé is használt (értelmes) azonosítást (természetes azonosítók, illetve ágazati azonosító) a rendszerek belső azonosításától. Azt kell elérni, hogy a személyazonosító adatok adatbázison belüli összerendelése az egyéb nyilvántartott adatokkal ne az azonos belső kódok letárolásán alapuljon, mert ekkor a megszerzett adatok egy egyszerű számítástechnikai művelettel összekapcsolhatók, a nevek az adatokhoz rendelhetők. A gyorsan bevezethető, költséges megoldás a titkosítás alkalmazása. Ennek leegyszerűsített elve, hogy ha pl. a névnél letárolunk egy kapcsolati kódot, akkor egy alrendszerbe (például labor vizsgálati adatok) a kapcsolati kód titkosított változata kerüljön, így a visszafejítő titkos kulcs ismerete nélkül az adatok nem kapcsolhatók össze.

A szükséges védelemhez ennél kissé bonyolultabb (mindkét oldalon titkosított) megoldás kell, és több alrendszer esetén különböző kapcsolati kódokat és titkosító kulcsokat kell használni. Mindez azonban normál piaci technológián alapul, bevezetése sem költségben, sem időben nem érdemi probléma. A megoldás az, hogy a (természetes) személyazonosító (illetve ágazati azonosító) adatok egy elkülönült törzsadatárba kerülnek. A törzsadatár a személy azonosítójához minden külön kezelendő adatalrendszerhez tartozóan egy-egy külön kapcsolati kódot tárol. A törzsadatárhoz és minden alrendszerhez külön-külön titkosítási kulcspár is tartozik.<sup>2</sup> Ezekre azért van szükség, mert a kapcsolati kódokat sehol sem eredeti formájukban tárolják, hanem a törzsadatár a kapcsolati kódoknak az egyes alrendszerek nyilvános kulcsával titkosított változatait tárolja, az alrendszerek pedig a saját kapcsolati kódjaiknak a törzsadatbázis nyilvános kulcsával titkosított változatát tárolják. Ezáltal az egy személyhez tartozó törzsadatokat és a különböző alrendszerbeli adatokat csak az tudja összevonni, aki ismeri a törzsadatárhoz és az alrendszerekhez tartozó titkos visszafejítő kulcsokat. Ha egy névhez tartozó alrendszerbeli adatra van szükség (például X.Y. laborletétét kéri a természetes azonosítói alapján), akkor a program a törzsadatárban tárolt (az alrendszer nyilvános kulcsával titkosított) kapcsolati kódot küldi meg az alrendszernek, az visszafejti (dekódolja) saját titkos kulcsával, majd titkosítja a törzsadatár nyilvános kulcsával, így megkapja a nála tárolt azonosítót, amivel kikérheti az adatot. Ha egy alrendszerben lévő adathoz kell személyazonosító adatokat (törzsadatokat) párosítani (felismernek egy ujjnyomatot, és elő kell keresni pl. a tulajdonos nevét), az alrendszer elküldi a nála tárolt (a törzsadatár nyilvános kulcsával titkosított) kapcsolati kódot a törzsadatárnak, a törzsadatár azt először visszafejti a saját titkos kulcsával, majd a visszafejtett kapcsolati kódot titkosítja az alrendszer nyilvános kulcsával, s így végül megkapja a kapcsolati kód nála letárolt azon változatát, amivel megtalálhatja a keresett személyazonosító adatokat.

## b) Eseti intézményközi adatközlés össze nem vonható adatokra

Ez a technika arra az esetre vonatkozik, amikor független intézmények közötti adatszerről van szó, és a két adatbázis együttes védelméről nem (ebben az eljárásban) kell gondoskodni. Ilyenkor a cél, hogy a két intézmény ne ismerhesse meg a másik fél által használt azonosítót (például az OEP az adóazonosító jelet). A megoldás egyik módja, hogy a küldő a mindkét félnél meglévő azonosító adatból (ez természetes személynél gyakorlatilag csak a természetes azonosítók együttese) egyedi algoritmussal képez kapcsolati kódot, az adatokon és a kapcsolati kódokon kívül átadja az algoritmust és a paramétereit is, a fogadó pedig az algoritmus ismeretében a kapcsolati kódból visszafejti a közös azonosító adatot, aminek segítségével aztán megtalálja a saját adatbázisban a megfelelő adatcsoportot. Most ezt a megoldást alkalmazzák az információs szabadságról szóló törvényből adódó ad-hoc (eseti) összekapcsolásokra. Ez elvi megoldásként megfelelő, de a gyakorlatban igen körülményes. Mivel a kapcsolati kódok nincsenek letárolva,

---

<sup>2</sup> A legegyszerűbb megoldás a nyilvános kulcsú infrastruktúra (PKI), amelynél az adat megismerésére jogosult nyilvános titkosító kulcsával történik a titkosítás, és a jogosult a nyilvános kulcshoz tartozó titkos kulcsával fejt vissza a titkosított adatot.

legrosszabb esetben az állomány összes elemére el kell végezni a kódolást (a kapcsolati kódok előállítását), s így kell egyezéseket keresni a küldött állomány elemeivel, ami komolyabb méretű küldött, illetve tárolt állományok esetében igen rossz hatékonyságot eredményez. A gyakorlatban csak a természetes azonosítókból képezhető a kapcsolati kód (ez az egyetlen közös tudás a két nyilvántartás között), és a módszer biztonsági szintje is korlátozott.

### c) **Rendszeres intézményközi adatközlés össze nem vonható adatokra**

Ahol rendszeres adatkapcsolat áll fenn (például APEH<sup>3</sup> – KeK KH<sup>4</sup> közti adatátadás), ott az előbbinél hatékonyabb megoldást kell kialakítani. Az olyan megoldás, ahol ismerik egymás azonosítóit, vagy ahol egy állandó kapcsolati kódot alkalmaznak (mint ami a jelenlegi gyakorlat), az valójában az AB határozatának a megkerülése (ténylegesen összekapcsoltak az adatbázisok, ezért ha az állományok kikerülnek, az adatok egyszerűen összekapcsolhatók). A megoldás itt is egyszerű. Az az elve, hogy a fogadó (akinek adatot küldenek) minden küldőnek (akitől adatot vár) elkészít egy kapcsolati kódot minden személyre (eddig hasonlít a most alkalmazott megoldásokhoz), de nem a kódot adja át, hanem csak a majdani küldőhöz tartozó nyilvános kulccsal titkosított változatát, amit a küldő a nála nyilvántartott személyhez hozzácsatol. Amikor a küldő küldeni akar, ezzel a titkosított kapcsolati kóddal küld, de ebből a tényleges, a fogadónál tárolt kapcsolati kód csak visszafejtés után ismerhető meg. Ezeket a kapcsolati kódokat időszakosan cserélik, ami az időbeni összekapcsolást (személyiségprofil építését) is megakadályozza.

A tényleges megvalósításnál - nagyobb védelmet igénylő adatok esetén - ennél magasabb védeltséget érdemes kialakítani. Fogadó minden küldő partneréhez egy-egy PKI technológiájú titkosító kulcspárt generál, amiket saját nyilvános kulcsával titkosítva tárol el. (Ez azért kell, mert minden partnerre külön hardveres titkosító modul (HSM) alkalmazása túl költséges lenne, így inkább a kulcsokat a saját adatbázisában tárolja, de saját nyílt kulcsával titkosítja, lehetőleg egy gépi - HSM - modulban tárolva a visszafejtő kulcsot). Kezdetben a küldő és a fogadó nyilvántartást egyszer szinkronizálni kell. Ehhez a fogadó küldő partnerenként minden személyhez képez egy-egy kapcsolati kódot, letárolja a természetes azonosítókhoz vagy saját ágazati azonosítójához (törzsadataihoz), a küldő számára korábbiakban generált nyílt kulccsal titkosítva átadja a küldőnek, amit az a saját törzsadataihoz letárol. Ezt az előkészítési műveletet, amit csak egyszer kell végrehajtani, szinkronizálásnak nevezik. (Ennek során a természetesen személyazonosító adatokat is át kell adni a kapcsolati kóddal, hogy lehessen tudni, hogy melyik kapcsolati kód melyik személyhez tartozik.) A tényleges küldéskor (ez az ismétlődő művelet) a küldő a nála letárolt kapcsolati kóddal (amit kezdetben a fogadó a küldőhöz tartozó nyilvános kulccsal titkosított) azonosítva küldi meg az adatot (tehát nem adja át saját azonosítóját). A fogadó a küldő partnerhez tartozó visszafejtő kulcsot (titkosított állapotban) kiveszi a nyilvántartásából, azt – lehetőleg a HSM modul segítségével az abban tárolt saját titkos visszafejtő kulcsával – visszafejti (dekódolja), és az így hozzáférhető visszafejtő kulccsal visszafejti magát a kapott kapcsolati kódot. Így megkapta a saját törzsadattárban használt kapcsolati kódját, ami a törzsadattárban megmutatja, hogy a küldött adatok kire vonatkoznak. Célszerű a kulcsot sűrűn cserélni (új kulcspárt képezni), és megküldeni a küldőnek a korábbi és az új kapcsolati kódokat, persze mindkettőt az aktuális nyilvános kulccsal titkosított formában. A küldő megkeresi a régi kapcsolati kódot, és helyébe az új kapcsolati kódot tárolja le. A fogadó oldali többlétszámú titkosításra csak azért van szükség, mert a normál PKI eszközök a nyilvános kulcsot nem védik, így egy hacker vagy rendszergazda a titkosítás nélkül letárolt kapcsolati kódokat az ugyancsak védtelen nyilvános kulccsal kódolva megkapná a küldő partnereknél használt kapcsolati kódokat, ami túlzott kockázatot jelentene az összekapcsolásra. Ahol nincs szükség az erős védelemre, ott a HSM modulós védelem és titkosítás szükségtelen.

<sup>3</sup> Adó- és Pénzügyi Ellenőrzési Hivatal

<sup>4</sup> Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala

#### **d) Többes bejelentést kezelő űrlap**

Ha egy tényt több szerv részére be kell jelenteni, és valamely okból lényeges annak fenntartása, hogy az ügyfél dönthessen arról, mely szerveket kívánja értesíteni, és melyeket még nem, akkor erre igen egyszerű megoldást jelenthet egy megfelelő űrlap kialakítása. Az űrlapon csak egyszer adja meg az adatot az ügyfél, de a lap tartalmazza mindazon szervek nevét, ahova az adat elküldésre kerülhet. Az ügyfél bejelölheti, hogy mely szervekhez nem kívánja az adatot továbbítani. Ha olyan szervek vannak a listán, amelyekhez külön azonosító kell a bejelentéshez (például a TAJ<sup>5</sup> az OEP<sup>6</sup> felé, az adóazonosító jel az APEH felé), s az intézményközi továbbítás hivatalból nem valósul meg, ezt az űrlap jelzi. Az ügyfélnek meg kell adnia ezeket az azonosítókat (ha mindnek küldi, minden szükségeset). Emiatt azonban nem jön létre az összekapcsolás lehetősége, mert az űrlapkitöltő program a jelenleg az adóbevallásnál (ill. az általános nyomtatványkitöltőnél) alkalmazott módon csak az ügyfél számítógépén fut (akár hálózati kapcsolat nélkül is), közvetlenül nem küld adatot, az állami rendszer kitöltéskori állapotában nem fér hozzá. A kitöltés után az űrlapkitöltő előállítja az érintett szervek számára a bejelentéseket (az azonos azonosító használatára jogosultaknál közösen), azokat az ügyfél hitelesíti (értelemszerűen ahány elkülönült azonosító szerepelt, annyi hitelesítendő üzenet lesz). Ezt követően a program címzettenként összeállítja, és ha szükséges, az érintett szervek kódjával titkosítja az üzeneteket, amelyek ezután már elküldhetők.

## **2. A cenzúra, az állam illegális adatmegismerése veszélyének csökkentése**

A magántitok védelme alkotmányos jog. Ennek érvényesülését súlyosan megkérdőjelezi, ha egy ellenőrzésre, másolásra alkalmassá tehető ponton az állampolgárnak kötelező az üzenetét keresztülküldenie. Ebben az esetben több okból nem helytálló az üzenetek titkosítására hivatkozás. A jelenleg alkalmazott – és a széles körben reálisan alkalmazható – titkosítási megoldások jellegzetessége, hogy idővel védelmi erejük csökken, és ugyan az állampolgárok üzeneteinek letárolásával egy központ most nem tud a titkosított adatokhoz hozzáférni, de akár tíz év múlva már a mostani titkosítások visszafejthetővé válnak számára a gépi eszközök fejlődése miatt. Az alkotmányos védelem azonban a személyek múltjára is kiterjed. További elvi gond, hogy egy állami ponton történő keresztülvezetés az államnak manipulálási lehetőséget ad (visszatarthat üzenetet, hamis üzenetet kreálhat). A gyakorlatban az üzenetek titkosítása az űrlapkitöltőkben még biztosítható, de a szervek által az ügyfélnek küldött hivatalos értesítéseknél már a titkos üzenetek kezelése (visszafejtése), egyáltalán az, hogy az ügyfél saját kulcsot készíttessen, már csak egy igen szűk társadalmi rétegnél reális elvárás (értelmiség egy része, fiatalok), azaz durván sérül az esélyegyenlőség. Mindezeket túl a megoldás költséges is. Az állam ezzel egy párhuzamos rendszert épít ki a meglévő piaci szolgáltatások mellé, hisz minden internet-előfizetéssel postafiók és tárhely jár, emellett más nagy ingyenes információküldő szolgáltatások is elérhetők, tehát az állampolgár egyszer megfizeti az üzenetváltáshoz és -tároláshoz szükséges költségeket a szolgáltatójának, másrészt ugyanazt az adóján keresztül még egyszer az államnak. A megoldás nem is piackonform, hisz pont a piaci megoldások használatának mellőzésére ösztönöz az információs társadalom kialakulásához szükséges mindennapos használat ösztönzése helyett. Mindez a hátrány azonban egyszerűen elkerülhető egy rugalmasabb megoldás kialakításával.

---

<sup>5</sup> társadalombiztosítási azonosító jel

<sup>6</sup> Országos Egészségbiztosítási Pénztár

## a) **A meglévő központi rendszer tárhelyes csatorna tartalékkénti használata**

A kapcsolattartás az állami közléseknél az ügyfél választása szerint a mindenki által használt e-mailen vagy az állami tárhelyen történik. Az elektronikus kapcsolattartáshoz minden azt kérő számára kialakításra kerül az állami tárhely „biztonsági” csatornaként. Ha e-mailt választ az ügyfél, elvárás, hogy a kapott üzenetekről visszaigazolást küldjön (a 2004. évi Ket.<sup>7</sup> még erre a megoldásra épült). Ha ez nem történne meg adott időn belül, akkor – ha van az ügyfélnek érvényes ügyfélkapuja, és a hivatal ismeri az ügyfél központi rendszer címét – az ügyfél központi rendszerbeli értesítési tárhelyére küldik meg az iratot, ahol már a kézbesítési vélelem beáll, ha viszont nincs az ügyfélnek ügyfélkapuja, akkor marad a papíralapú (postai) út. A megoldás előnye, hogy az az ügyfél, amelyik reagál a megkeresésekre (visszaigazol), ezzel egyúttal azt is biztosíthatja, hogy üzenetforgalma nem kerül be az állami tárhelybe, így az állami központi rendszer adatait nem tudja megszerezni, kapcsolatrendszerét sem tudja feltárni (hogy milyen ügyei vannak). Emellett az állam számára megvan az ügyfél hivatalos elérhetősége, s a kialakított rendszert sem kell kidobni, ami beruházásvédelmi szempontból előnyös (és a rendszer fejlesztését a reális felhasználói igényekhez lehet illeszteni, csak akkora kapacitásra kiépítve, amennyit ténylegesen igénybe vesznek).

A tényleges megvalósítás a fent leírtánál kicsit bonyolultabb. Azoknál az értesítéseknél (de csak azoknál), ahol az értesítés átvételének időpontja az ügyintézés szempontjából lényeges, a küldemény az e-mailés küldésnél sem azonnal olvasható. Két megoldási lehetőség van (akár választhatóan): vagy csak értesítést küldenek, s a küldeményt csak visszaigazolás után küldik, vagy hogy elmegy a küldemény titkosítva, s az ügyfél a visszaféjtő kulcsot csak visszaigazolás után kapja meg, ill. töltheti le harmadik féltől, például hitelesítésszolgáltatótól. Ez utóbbi megoldás előnye a küldés titkosítottasága, az átviteli csatorna korlátainak jobb kezelése, hátránya, hogy a feloldáshoz program kell, amelynek használata nem minden felhasználónak egyszerű, még leggondosabb kialakítás esetén sem.

Az ügyfél közléseinél szintén indokolt a választható csatorna biztosítása, ez esetben is fennáll (itt a hivatal részéről) a visszaigazolási kötelezettség. Természetesen e területre is biztosítani kell a központi rendszeren keresztül történő (a beadási időt igazoló) benyújtási lehetőséget, amivel az ügyfél saját döntése szerint élhet (illetve, ha nem kap időben visszaigazolást, élnie kell).

## b) **Ügyfél hozzájárulásának kezelése adatátkéréshez**

A különböző szerveknél kezelt adatok átkérésének jogosságát célszerű valamilyen ellenőrzési rendszerrel garantálni, hogy az állam (illetve tisztviselője) ne élhessen vissza az adatátkérés intézményével. Szükséges, hogy az adatkezelő ténylegesen meggyőződhesen az adatkérés jogosságáról, ehhez az ügyfél egyértelmű hozzájárulása a legmeggyőzőbb indok. Mindezek alapján az adatkérésekhez szükséges bevezetni egy adatkérési jogalap űrlapot, amivel a kérő szerv az adatszolgáltató szerv felé megjelöli az adatkérés adatait és okát. (Ez nyilván elmaradhat a törvényben nevesített adatkapcsolatnál. Tehát ha például egy törvény egy rendszer számára ellenőrzési kötelezettséget ír elő a személyiadat-nyilvántartásban, akkor nem kell ilyen nyilatkozat az e törvény alapján működő rendszerből jövő kérésre, például okmányirodából a KEK KH felé).

Az ügyféltől ügyindításkor űrlapon hivatalból bekérik a hozzájárulást valamely külső adatkéréshez (innen tudja meg ügyfél, mely adatát fogják kezelni), az űrlapot az ügyfél választása szerint hitelesíti, vagy hitelesíteti az állami rendszerrel. Az adatszolgáltató a központi regisztrációtól lekérheti, hogy az ügyféltől milyen hitelesítést fogadjon el. (A vonatkozó ügyfél-meghatalmazást a regisztrációnál papíron adott nyilatkozat szkennelt változatának bemutatásával igazolják annál, akinek nincs elektronikus aláírása.) Az ügyfél

<sup>7</sup> a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény

beleegyezését az adatkéréssel együtt továbbítják az adatszolgáltató szerv felé, amely így képes a kérés jogosságának ellenőrzésére.

Egyszerűbb a helyzet, ha egy rendszeres értesítőben vagy a lekéréskor az ügyfél azonnal értesítést kaphat az adatszolgáltatásról. Ha az ügyfél mindig értesül az adatai megismeréséről, elegendő lehet csak a különleges (érzékeny) adatok esetében az eseti hozzájárulás megkövetelése, a többinél vélelmezhető a hozzájárulás, de utólagosan értesítést kell kapnia az ügyfélnek. Az értesítés alapján az ügyfél már panaszt tud tenni, ha indokolatlanul kérték az adatát, de azt a tájékoztatást, hogy kitől fognak kérni, ekkor is meg kell előre adni, mert annak alapján bizonyítható, ha egy adatkérés illegális, és ez arra is biztosíték, hogy utólag ne legyen beleérthető, belemagyarázható az ügyintézésbe bármi.

### c) **Az ügyfél tájékoztatása az adatokról történő adatszolgáltatásról rendszeres összesítőben**

A szolgáltatás a bankok havi értesítőjéhez hasonló szerepet tölt be. Az adatkezelők a saját adatkezelésükről és a társszervi adatigénylésekről – azon ügyfelek esetében, akik ezt kérték – adatot szolgáltatnak egy központi összesítő készítője részére (kinek kiről adtak adatot s milyen jogcímen), amit az feltüntet az adatszolgáltatásokról készült összesítőben, és az összesítőt megküldi vagy elérhetővé teszi az ügyfél számára (értelemszerűen minden ügyfél csak a saját adatait tekintheti meg). Ez lehetővé teszi, hogy az ügyfél az esetleges illegális adatkérést észrevegye, és panasszal éljen. Elvben szakrendszerenként kellene készíteni a rendszeres összesítőt, de az ügyfél számára előnytelen lenne, ha nagyszámú jelentést kellene rendszeresen végignéznie. Ebben az esetben az arányosság érdekében a központi publikálás előnyösebb (még a csak hivatkozásszerű kialakítás esetén is) azzal, hogy a jelentéseket, ill. az azokból készült összesítőt a központ csak egy adott reklamálási időszak végéig őrizheti meg, nem építhet adatbázist, még naplózási jelleggel sem tárolhatja az összesítő tartalmát hosszabb időtávra. A tájékoztatás csak az adatkérések tényére vonatkozik, konkrét tartalomra nem (arról az ügyfél a szakrendszerrel érdeklődhet az összesítőben szereplő hivatkozás alapján).

## 3. **Az értesítés hitelessége**

A jogbiztonsági követelményekhez hozzá tartozik az, hogy az ügyfél nevében tett jognyilatkozatot az állam ne manipulálhassa, azt jogvita esetén ne tagadhassa le, helyette ne kreálhasson nyilatkozatot. Ez az elv a köztisztviselőkre is igaz, azaz egy ügy jóváhagyója csak meghatározott személy lehessen (az, aki papíron is aláír), és így az állam ne moshassa el a felelősséget egy esetleges korrupciós ügyben, ne terelhesse a gyanút másokra. Márpedig a jelenleg alkalmazott megoldás, hogy a központi rendszeren keresztül benyújtott iratokat a központi rendszer hitelesíti, illetve, hogy e technikát kívánják a hivatalok felől jövő értesítéseknél is alkalmazni, jelentősen sérti a jogbiztonságot, mivel a központi rendszer – informatikai fejlesztői segítségével – mások nevében képes jognyilatkozatok létrehozására.

A jelenlegi megoldás további problémája, hogy az adatok megismerés elleni védelme és a központi hitelesítés súlyosan ellentmond egymásnak. Ha a küldő (akár ügyfél, akár hivatal) titkosítja az iratot, a hitelesítés egy titkosított iratra vonatkozik (ráadásul a jelenlegi rendszerben egy űrlap összetett adatszerkezetére). Ez azonban egyetlen piaci eszközzel sem tekinthető meg, azaz akár külföldön, akár húsz év múlva egy bírósági eljárásban ezen iratok komoly probléma elé állítják a felhasználójukat. A visszafejtett dokumentumon nincs semmilyen szabványos hitelesítés, mivel nem az eredeti dokumentum nem lett hitelesítve, hanem csak a titkosított. Emiatt a küldés idejére alkalmazott titkosított példányt kell megőrizni az eredeti irat helyett, mint hiteles példányt, de hogy az annak visszafejtésére képes szoftver működik-e 20 év múlva, vagy hogy mi igazolja, hogy a szoftver valóban az eredeti üzenetet állítja elő (nem manipulált-e a visszafejtő program), az igazságügyi szakértő

bevonását fogja igényelni minden egyes dokumentum felhasználásánál, ami kezelhetetlen helyzet. Emellett az ilyen dokumentum nem alkalmas továbbküldésre sem, mivel a visszafejtéséhez a címzett titkos kulcsára van szükség (amit nyilván nem tehet közzé), az eredeti címzett jelenléte nélkül tehát a dokumentum nem ismerhető meg. Ez például kizárja, hogy valaki pl. bankjánál vagy munkáltatójánál olyan ügyet intézzon elektronikusan, amihez elektronikus közokiratot kell csatolnia, hisz nem tud hiteles, a bank vagy munkáltatója által is olvasható iratot csatolni, vagyis ez a hitelesítési mechanizmus gyakorlatilag felhasználhatatlanná teszi az elektronikus formájú közléseket. Ha viszont a központi hitelesítés nem a titkosított dokumentumra vonatkozik, akkor az adatvédelem sérülhet.

További probléma, hogy a jelenleg alkalmazott ügyfélkapus megoldás közismerten egyszerűen kijátszható (rosszindulatú programokkal, illetve technikai vagy vizuális megfigyeléssel a jelszó megszerezhető), így a felhasználó kiszolgáltatottsága nagyon nagy.

A fenti gondok kiküszöbölésére alkalmazhatók a következők:

**a) Választható biztonsági szint**

Az ügyfél dönthet saját kockázatvállalásáról, s nem az állam írja elő azt. Ha úgy rendelkezik regisztrációnál, akkor tőle csak elektronikus aláírást fogadhatnak el, és az állam nem képes az ő nevében nyilatkozat kreálásra. Persze az önkéntesség a másik irányban is igaz: akár egy megadott e-mail címről jövő levelét is el kell fogadni az ügyfél nyilatkozatának – a benyújtó egyszerűsített azonosításával megerősítve –, ha az ügyfél így rendelkezett (és ha törvény ezt nem zárja ki). Ezt a rendelkező nyilatkozatát viszont minden esetben az állami hitelesítéshez mellékelik (mint egy szokásos meghatalmazást).

**b) Azonosítás biztonságának erősítése**

Jelszó mellett (helyett) választható kódtáblázatos azonosítás. A kódtáblázatot akár az ügyfél maga is generálhatja, és feltöltheti a regisztrációs rendszerbe, de kérheti a regisztrációs szervtől is. Előnye, hogy telefonos ügyintézésnél is alkalmazható. Az azonosításhoz a rendszer véletlenszerűen kérdez néhány számot a kódtáblázatból. A gépi támadások (robot bejelentkező) ellen képi formában megadott számok, betűk, és szövegesen megadott műveletek eredményének bekérése, egyszerű kérdésekre adható egy- vagy többszavas válaszok megadása is alkalmas, és ha ennek során ismételt tévedés fordul elő, akkor kitiltható az ügyfél (az újbóli aktiváláshoz ügyfélszolgálat vagy regisztrációs szerv segítsége kell). E megoldás az egyszerű jelszavas védelemnél jóval kevésbé lehallgatható, illetve megfigyelhető (különösen, ha a számmátrix generálása a regisztrációs hatóságnál vagy más biztonságos környezetben történik).

**c) A benyújtó egyszerűsített azonosítása**

A benyújtó (ügyfél) azonosításához nem kell mindenkor az ügyfélkaput alkalmazni, ez is jelentősen csökkenti a megfigyelhetőséget. Az ügyfél választhat közvetlenebb kapcsolati formát is a hivatalokkal. Ehhez a normál internetes kapcsolat mellett (e-mail vagy ügyfélkapus tárhely) külön – független – csatorna megléte szükséges, ezért az ügyfél a regisztrációjánál megadja annak adatait. Megadhatja mobil telefonszámát SMS-hez – ha vállalja a küldési költséget, vagy az ügy olyan, hogy a díjból fedezhető –, vagy megadhat további e-mail címeket. (Legjobb az SMS, ahol feladó telefonszáma is ellenőrizhető adat.) Ha az ügyfél iratot kíván beküldeni, bejelentkezik az elsődleges csatornáján, és jelzi szándékát. Ha e-mailt választott független csatornaként, célszerű egy segédprogrammal

egy kulcspárt generálnia, és a kezdeményezéskor beküldenie a nyílt kulcsot. Ha mobiltelefonos kapcsolatot vállalt, erre nincs szükség. A rendszer az ügyfél által a regisztrációnál megadott független csatornán keresztül válaszol: küld egy értesítést, abban egy egyszer használatos kódot, és egy időt, ameddig a kód érvényes. Ha az ügyfél e-mail csatornát választott, és adott titkosító (nyilvános) kulcsot, akkor titkosítottan kapja a kódot, amit a kulcspár nála lévő (titkos) részével visszafejthet. Mód van a kód részekre szedett módon több e-mail címre küldésére is. Az ügyfélnek nyilván ellenőriznie kell, hogy a feladó a hivatal-e (ez telefonos kapcsolatnál a szám alapján elég megbízhatóan elvégezhető, e-mailnél kevésbé), majd ezt követően a megadott időn belül benyújthat iratot a kapott kódnak a beadvány meghatározott helyén történő feltüntetésével (vagy interaktív bejelentkezés esetén egy meghatározott helyen történő megadásával). A hivatal a megadott időn belül a megküldött kóddal a megadott címről érkező iratot a személy nyilatkozatának tekinti (feltéve, hogy nem kap nagyszámú beadványt az adott címről, mert ott programozott támadás vélelmezhető, s a kapcsolat letiltódik). Lényeges azonban, hogy a benyújtásról hivatalos megerősítést kapjon az ügyfél a nyilatkozat tartalmának hivatal által hitelesített visszaküldésével (lásd külön). Ez a technika információlekérésnél is alkalmazható (az APEH, ha nem is minden elemét, de már használja az általa „előkitöltött” nyomtatványok elektronikus megküldésénél).

#### **d) Jognyilatkozat hivatal általi visszaigazolása**

Minden olyan egyszerű hitelesítésnél, amelynél a nyilatkozathoz nem maga az ügyfél rendel valamilyen hitelesítést (elektronikusa aláírást), nem elegendő, hogy az állam jogszabályban kimondja, hogy az ügyfél nyilatkozatának állami hitelesítése elfogadható, ill. hogy azt el kell fogadni. Ez teljes kiszolgáltatottságot eredményez. A hivatalnak a beadványt a saját hitelesítésével (elektronikus aláírással, ami lehet gépi is) ellátva, olvasható formában kell visszaküldenie (vagy megtekinthetővé és letölthetővé tennie), a nyugta nem elegendő az ügyfél számára, hisz nehezen tudja bizonyítani, hogy mire is vonatkozik. A szerv által átvett elektronikus irat kérésre történő megküldését a Ket. már korábban is lehetővé tette, azonban erre egyetlen hivatal sincs felkészülve. Az informatikai rendszerekben nem jelentene érdemi bonyolítást, hogy – ha csak kifejezetten nem tiltja az ügyfél – kérés nélkül, automatikusan megküldjék olvasható (s így az átlagos ügyfél számára is egyszerűen ellenőrizhető) formában a befogadott elektronikus iratot. Fontos, hogy olvasható formájú legyen a visszaküldött irat (például PDF vagy megfelelő megjelenítési sémát is tartalmazó nyílt formátumú), és elektronikusan alá legyen írva, mert standard eszközökkel ez ellenőrizhető könnyen az ügyfél számára, s ezzel tud egyszerűen bizonyítani is (például külföldön vagy polgári kapcsolatrendszerében).

#### **e) Rendszeres összesítő**

Ha az állampolgár nyilatkozata nincs a saját elektronikus aláírásával hitelesítve, s az állam (központi) rendszere hitelesíti, nagy a kockázata annak, hogy az állampolgár nevében és tudta nélkül létrehoznak jognyilatkozatot. Ez küszöbölhető ki egy rendszeres (pl. havi) összesítő kivonattal (a bankok havi elszámolásaival analóg módon). Ennek lényege, hogy központilag rendszeres időnként (pl. havonta) összesítés készül az ügyfél beadványairól, amely beadványok kivonatait saját elektronikus aláírásukkal hitelesítik az érintett szervek, és az összesítést a készítő olvasható formátumban (pl. PDF) megküldi vagy elérhetővé teszi. Az összesítőt kérheti az ügyfél e-mailben vagy tárhelyére is. Az összesítóből az ügyfél ellenőrizheti ügyeinek tényét (a részleteket nem), és reklamálhat, ha például nem a saját nyilatkozata szerepel benne. (Ismernie kell, hogy milyen rendszerességgel küldik az

összesítőt, így ha nem kapja meg, új kivonatot kérhet, mint a bankoknál. A küldő második sikertelen küldés esetén az ügyfélkapus tárhelyet ajánlhatja fel az ügyfél számára, lásd korábban). Akkor ügyfélbarát ez a szolgáltatás, ha pontos menetrend szerint olyan gyakorisággal küldik az összesítőt, hogy az ügyek fellebbezési határidejébe beleférjen, mivel ekkor még a reklamáció intézéséhez sem kell új jogszabályi háttér. A rendszeres összesítőt a készítője nem tárolhatja tartósan, csak a reklamáláshoz biztosított ideig, hogy ebből se képezhessenek profilt. A megküldött vagy hozzáférhetővé tett összesítés közös lehet az ügyfélről tárolt adatok felhasználásáról szóló, korábban említett összesítéssel, de mivel logikailag más, az ügyfél külön is rendelkezhet róluk, ezért külön lehetőségként szerepeltettük.

#### **d) Központi hitelesítésszolgáltatás**

A jelenlegi megoldás alap gondolata, hogy mivel az emberek jelentős részének nincs elektronikus aláírása, és az ehhez szükséges eszközök költséget jelentenek, legyen olcsó tömeges megoldásra lehetőség. Ez önkéntes, választható megoldásként fenntartható, de csak a dokumentum küldésétől elkülönült, önállóan igénybe vehető szolgáltatásként. A dokumentumot az ügyfél készíti el, azt külön, ha akarja, azonosításon alapuló szolgáltatással hitelesítetteti, amelynek során az ügyfél személyazonosságának ellenőrzését követően (az ellenőrzés történhet jelszó, kódtábla használatával vagy egyéb, a lehetőségek közül az ügyfél által választott módon) a hivatal elektronikus – gépi – aláírással és időbélyeggel hitelesíti a dokumentumot. A hitelesítéshez igénybe vett szolgáltató lehet állami szolgáltató is (némi átalakítással a jelenlegi megoldás). Fontos azonban, hogy a hitelesítés nem kapcsolódik a küldéshez, feltöltéshez, az így hitelesített dokumentumot akár e-mailben vagy adathordozón is elküldheti az ügyfél, a hitelesített dokumentumot titkosíthatja stb., mindez a dokumentum hitelesítését már nem érinti. A hitelesítés során – mivel a jelenlegi hitelesítési technikák ténylegesen egy „lenyomatra” s nem az egész dokumentumra vonatkoznak – a lenyomatkészítő program az ügyfél gépén futhat, hitelesítésre felküldeni pedig csak a lenyomatot kell, azaz kizárható az adatok megismerhetősége. Hasonló út járható akkor is, amikor egy hivatal tisztviselőjének van szüksége egy dokumentum hitelesítésére.