A mobiltelefon, mint személyes adatok hordozója

KÖNYVES TÓTH PÁL
kotopa@freemail.hu

Kulcsszavak: mobiltelefon, elektronikus személyazonosítás (eID), adatvédelem, biztonságos elektronikus aláírást előállító eszköz (BALE)

A statisztika szerint Magyarországon a használatban lévő mobiltelefonok száma meghaladja az ország lakosainak a számát, s ha tekintetbe vesszük, hogy az idős- vagy az óvodáskorúaknak, továbbá a mobiltelefon használatára nem képes személyeknek – nyilvánvaló okokból – nincs mobiltelefonjuk, jónéhányunknak több is van belőle. A cikkben áttekintjük a mobiltelefon használatával kapcsolatos személyes adatok körét, különös tekintettel e kör bővítésének lehetőségeire és jogi kérdéseire.

1. Bevezetés

A telefonszolgáltatást vagy helyhez kötött előfizetői végpontra, azaz vezetékes hálózatra csatlakozó készülék, vagy nagy térben mozgó, mobil rádiótelefon hálózat hálózati végpontján csatlakoztatott, nem helyhez kötött berendezés, a mobiltelefon használatával vesszük igénybe. Ennek feltétele a szolgáltatóval megkötött előfizetői szerződés, amely rögzíti az előfizető személy azonosító adatait. Hangsúlyozni kell, hogy ezek az adatok az *előfizetőt* azonosítják, mindenekelőtt a szolgáltatás igénybevételi díjának számlázása céljából és nem azt a személyt, aki a szolgáltatást igénybe veszi, vagyis a *felhasználót*.

A mobiltelefon *tehát nem mindig azonosítja* használóját, aki azt rendszerint magánál is tartja, a világ bármely táján is tartózkodik. Amint bekapcsolja és jelzést fogad, a használója földrajzi helyét meglehetősen pontosan – gyakran 50 méteres pontossággal – meg lehet határozni, hiszen a mobiltelefon-hálózat globális, az országhatárokon átnyúlik, a fizikai távolságnak nincs jelentősége. A hálózat üzemeltetője rögzíti, és – legalábbis az Unió tagállamaiban kötelező módon[1] – hosszabb ideig meg is őrzi, hol tartózkodik vagy tartózkodott a használat időpontjában a mobiltelefon birtokosa, továbbá azt is, milyen számot hívott, s milyen számról hívták.

Az is kérdéses azonban, hogy a felhasználó, pontosabban a mobiltelefont birtokló személy kicsoda. Mindazonáltal a hálózat üzemeltetője által tárolt adatokból – s ezt teszik a titkosszolgálatok és a bűnöldöző szervek – következtetni lehet, ő-e az, akire az adatok mutatnak.

2. Személyazonosító adatok

A mobiltelefon, pontosabban a SIM kártya vásárlásakor egyébként egyrészt meg kell adnunk személyazonosító adatokat, másrészt hitelesen igazolnunk is kell azokat. Az adatokat – önkéntes és tájékozott beleegyezésünk alapján – a mobilszolgáltató az adatvédelmi jogszabályok és rendelkezések szerint kezelheti, sajátos szabályait üzletszabályzatában (ÁSZF) rögzíti.

Ha az információs társadalomra jellemző szolgáltatások (elektronikus kereskedelem, bankolás, hatósági ügyintézés, magánjogi ügyletek lebonyolítása, a hűségkedvezmények gyűjtése, beléptető rendszerek stb.) általánosan elterjednek, – márpedig eddigi bővülésük erre enged következtetni –, a több intelligens kártya helyett, melyek tárkapacitása egyébként is jóval kisebb, mint amennyit a mobiltelefon befogadhat, egyetlen készüléket kell csak magunknál tartani.

Hangsúlyoznunk kell, hogy a mobilhálózat üzemeltetője által rögzített adatok a mobilállomásra vonatkoznak, s nem az azt használó személyre, hiszen azok csupán a használat földrajzi helyét bizonyítják. A személy, az ember azonban nem mobiltelefon. Azt a készüléket és az általa elérhető szolgáltatásokat, melyet és melyeket a szolgáltató az általa nyilvántartott személlyel azonosít, használhatja bárki, például családtagja vagy akit erre feljogosít, esetleg aki azt tőle ellopta, vagy az elveszett készüléket megtalálta. Gyakori ugyanakkor az is, hogy egy alkalmazott a munkáltató adataival regisztrált mobiltelefont használ. Az előfizető és a felhasználó személye következésképpen elkülönül.

A hazai mobiltelefon-szolgáltatók üzletszabályzatai (Általános Szerződési Feltételek – ÁSZF) szerint az előfizető személye azonosítására alkalmas adatokat, hívószámával együtt az előfizető kártya, szaknyelven SIM kártya (Subscriber Identification Module – az előfizetőt azonosító modul) is tartalmazza. A SIM kártya a szolgáltató kizárólagos tulajdonát képezi, s e tulajdonjog nem ruházható át. Ugyanakkor azonban a felhasználó és az előfizető nem feltétlenül ugyanaz a személy. A felhasz-

1 *Adatmegőrzési irányelv: Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról.*
Az Irányelv rendelkezéseinek megfelelő rendelkezéseket az elektronikus hírközlésről szóló 2003. évi C. törvény tartalmazza.

náló az a természetes vagy jogi személy, jogi személyiség nélküli gazdasági társaság, vagy nyilvántartásba vett más szervezet (nem természetes személy), aki az előfizetői szerződés megkötését követően az előfizetői kártyát üzemben tartja.

Az előbbieken túlmenően a mobilhálózat üzemeltetői további négy nyilvántartást vezetnek:

- *honos helyzetregiszter* – HLR (Home Location Register), a mobil előfizetők adatbázisa, amely többek között tartalmazza az előfizető (pontosabban készüléke) IMEI kódját;
- *látogató helyzetregiszter* – VLR (Visitor Location Register), azon mobilkészülékek listája, amelyeket a HLR-jükön kívül használnak;
- *készüléket azonosító regiszter* – EIR (Equipment Identity Register), a mobilkészülék adatait tartalmazza, számlázási célokat szolgál, és lehetővé teszi a lopott vagy talált készülékek blokkolását;
- *azonosító központ* – AuC (Authentication Centre), az előfizetőt adatai alapján feljogosítja a hálózat használatára.

3. Az elektronikus személyazonosítás eszközei

Az *elektronikus személyazonosítás* (eID – electronic IDentification) eszközeként az utóbbi évtizedben az intelligens kártya (smart card) és egyéb IT-eszközök (pl. személyi számítógép, PDA) terjedtek el, holott a mobiltelefonnak mint eID eszköznek az intelligens kártyával összehasonlítva számos előnye van.

Kezdetben és mindmáig az elektronikus személyazonosítás hatékony kezelésére irányuló törekvések elsősorban az intelligens kártyára koncentrálódtak és korlátozódtak. Ilyen kártyák széles körű használata terjedt el a telefóniában, a bankolásban, az egészségügyben (e-health), a közforgalmú személyszállításban, hogy csak a közismert alkalmazásokat említsük. Használatuk biztonságos, ellenálló a csalásokkal szemben, az elektronikus ügyletek lebonyolításához biztonságos környezetet teremt. Alkalmazásukkal lehetővé válik mind online, mint offline szolgáltatásokhoz való hozzáférés, miközben a felhasználó meggyőződhet arról, hogy az elektronikus hírközlési csatornán továbbított adatai felett teljeskörű ellenőrzést gyakorol.

Mindez azonban korántsem jelentheti és nem is jelenti azt, hogy az elektronikus azonosság csupán az intelligens kártyával valósítható meg. Az eID sokkal inkább egy koncepció (lásd később az osztrák polgárkártya-koncepciót), amely különféle eszközökön testesülhet meg. Jelen elemzésünk tárgyát tekintve a mobiltelefonok SIM kártyájának és a mobiltelefonba vagy mobiltelefonra telepíthető egyéb intelligens moduloknak (chipeknek) van jelentősége.

Bármilyen eszközt – adat és szoftverhordozót – választunk is, az eID sémának alkalmasnak kell lennie nemcsak a felhasználó azonosítására, hanem adott szolgáltatás igénybevételére való feljogosítására is, esetleg az elektronikus aláírás támogatására stb. Az eszköz tartalmazhat fejlett biztonsági megoldásokat a személy egyértelmű és kizárólagos azonosságának hitelesítésére (pl. biometrikus azonosítókat).

Megjegyzendő, hogy a biometrikus adatok nem nyújtanak lehetőséget az abszolút hiteles személyazonosításra. A vonatkozó statisztikai adatok arról tanúskodnak, hogy az emberek 19%-a nem azonosítható ujjlenyomat, 31%-a arcgeometriája alapján, nem is beszélve arról a 10%-ról, akiknek az írisze (szivárványhártyája) azonosítás céljára nem is alkalmas, vagy nem rögzíthető.

A *biztonságos elektronikus aláírást előállító eszközzel* (BALE) szemben támasztott követelményeket az elektronikus aláírásról szóló 2001. évi XXXV. törvény (Eat) 1. sz. melléklete rögzíti, teljes összhangban az EU vonatkozó irányelvével[2], mégpedig a következőképpen:

„1. A biztonságos aláírás-létrehozó eszközöknek megfelelő technikai és eljárási eszközökkel biztosítaniuk kell legalább a következőket:
   a) az aláírás készítéséhez használt aláírás-létrehozó adat aláírónként biztosan mindig különbözik, s titkossága kellően biztosított,
   b) az aktuálisan elérhető technológiával kellő bizonyossággal garantálható, hogy az aláírás készítéséhez használt aláírás-létrehozó adat nem rekonstruálható, megvalósítható annak a jogosulatlan felhasználókkal szembeni védelme, illetve az aláírás nem hamisítható.
2. A biztonságos aláírás-létrehozó eszközöknek nem szabad az aláírandó elektronikus dokumentumot az aláírás elhelyezéséhez szükséges mértéken felül módosítaniuk, illetőleg nem akadályozhatják meg azt, hogy az aláíró a dokumentumot az aláírási eljárás előtt megjelenítse."

Sem e követelményekben, sem a törvény teljes szövegében nem lelhető fel a mobiltelefon vagy más IT-technológiai eszköz, vagy ilyenre való utalás. Ennek ellenére a BALE leginkább az intelligens kártya formájában jelenik meg, s a személyazonosítási kártyára vonatkozó ISO szabványok is e formára vonatkoznak. Ausztriában azonban e formát nem tekintik kizárólagosnak és a mobiltelefon SIM kártyáját is törvényes eID-hordozónak tekintik.

Az Eat szerint /7.§ (5)/ minősített elektronikus aláírás létrehozásához kizárólag olyan aláíró eszköz és egyéb elektronikus aláírási termék használható, amely rendelkezik a Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiadott igazolással. A BALE tehát nem korlátozódik az intelligens chipkártyára. Ugyancsak ezt olvashatjuk az NHH honlapján a gyakori kérdésekre adott válaszok között[3]:

2 Az Európai Parlament és Tanács 1999. december 13-i 1999/93/EK Irányelve az elektronikus aláírásra vonatkozó közösségi keretfeltételekről
3 http://www.nhh.hu/index.php?id=kerdes&cid=53&page=2

„Mi a biztonságos aláírás-létrehozó eszköz (BALE)? Ez egy olyan hardvereszköz (pl. intelligens kártya, USB eszköz stb.) amelyet egy erre kijelölt és megfelelő felkészültséggel rendelkező, az EU bármelyik tagállamában működő tanúsító szervezet megvizsgált és a biztonsági és működési követelményeknek megfelelőnek talált. Erről a tanúsító szervezet tanúsítványt állít ki."

Az NHH nyilvántartása szerint hazánkban mindössze két tanúsító szervezet létezik (a Mátrix és Hunguard), kijelölési okiratuk tartalmazza a tevékenységükre vonatkozó jogszabályokat, szabványokat és MIBÉTS[4] módszertanokat. Honlapjaikat felkeresve azonban nem találtunk olyan tanúsítványt, amely BALE-ként mobiltelefont alkalmazna.

Arra a kérdésre, telepítenek-e elektronikus aláírást, s az ehhez szükséges adatokat és szoftvereket mobiltelefonba, a két tanúsító szervezet egyike, továbbá a hitelesítés-szolgáltatók egyike az alábbi válaszokat adta.

MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft.:

„Mivel a mobiltelefonok gyakorlatilag 100%-ban lefedték napjainkra a fejlettebb országok lakosságát, jogos az igény, hogy a telefonkészülékeket és a mobil hálózatokat egyre több szolgáltatás nyújtásába tudják bevonni. Ezeknél az extra szolgáltatásoknál általános igény a felhasználó hiteles azonosítása a telefonhálózatokban jelenleg alkalmazott mostani megoldásoknál magasabb megbízhatósági szinten.

Az egyik lehetséges megoldás a PKI-rendszerek használata, amihez az előírások szerint szükség van többek között egy biztonságos aláíró eszközre is (magyarul BALE, angolul SSCD). A megfelelően biztonságos elektronikus aláírás létrehozásának egy szükséges, de nem elégséges feltétele a BALE használata, az egész aláíró alkalmazásnak és környezetnek megfelelően biztonságosnak kell lennie.

Az Elektronikus Aláírási Törvényből idézett követelmény szükséges feltétele egy BALE-eszköznek, de nem elégséges. A részletes műszaki követelmények megtalálhatók például a CWA 1469 CEN Workshop Agreement anyagban, amely általánosan elfogadott követelményeket fogalmaz meg. A jelen cikk szerzője nem ismer olyan mobiltelefont, amely kielégítené ezeket a követelményeket és Common Criteria minősítéssel rendelkezne.

Járhatóbb útnak tűnik olyan SIM kártyák használata, amelyek támogatják a PKI rendszerekhez használatos kriptográfiai funkciókat és kielégítik a BALE-eszközökkel szemben támasztott követelményeket.

Ez megoldja a BALE kérdést, de ettől még nem lesz az elektronikus aláírás a törvény által elfogadott, ehhez a telefon egészét megfelelően biztonságosra kell kialakítani. Ez műszakilag lehetséges, és nagy valószínűséggel előbb vagy utóbb meg is fog valósulni, de jelenleg a szerző nem ismer ilyen megoldást (ettől még nem lehetetlen, hogy már van ilyen)."

MÁV Informatika Zrt.:

„Társaságunk még nem telepített mobiltelefonba elektronikus aláírást hitelesítő tanúsítványt, illetve ehhez szükséges aláíró kulcsot, ez irányú igénnyel még nem jelentkeztek ügyfelek, és az elmúlt 8 év folyamán a mindennapi gyakorlatban sem láttunk-végeztünk még ilyet.

A törvény sem kötelezi a szolgáltatókat arra, hogy bármilyen aláírás-létrehozó eszközre telepítsenek tanúsítványokat, sokkal inkább saját jól felfogott üzleti érdekből teszik ezt meg, ha a műszakilag erre felkészültek és ha jogszabályi feltételek ezt lehetővé teszik. Ez utóbbit kiemelném, ugyanis a hazai gyakorlatban használható aláírás létrehozó eszközökről az illetékes hatóság (NHH) nyilvántartást vezet, és ezek között nem található „mobiltelefon".

Így ha kiadnánk tanúsítványt mobiltelefonra, akkor nem kellő körültekintéssel járnánk el (ti. az ügyfél azt hinné, hogy minden rendben van, holott a mobilja nem nyilvántartott aláírás-létrehozó eszköz, következtetésképpen az aláírása valószínűleg nem lenne érvényes).

Ettől függetlenül biztos, hogy vannak olyan mobilok, illetve SIM-kártyák, amelyeket ha a törvényben megjelölt bevizsgáló cég megvizsgálná, akkor aláírás-létrehozó eszköznek minősülnének és az NHH nyilvántartásba venné, de hazai viszonylatban nincs tudomásunk ilyenről."

4. Az intelligens kártya vagy mobiltelefon

Az intelligens kártya sok tekintetben nem több, mint egy szokatlanul kis méretű számítógép. Tartalmaz CPU-t, különféle memóriákat (ROM, EEPROM, RAM), továbbá más sajátos elemeket, például kriptográfiai koprocesszorokat. Mindez a mobiltelefonba is, magába a SIM kártyába vagy a készülékbe telepített újabb csipmodulba is beépíthető.

Elemzésünk tárgyát illetően hatalmas mennyiségű információt tartalmaznak a kormányzati vagy közigazgatási informatikai bizottságok dokumentumai. E bizottságokat – különféle megnevezéssel – kormányhatározatok[5] hozták létre, egyúttal meghatározva feladataikat is. A jelenleg működő bizottság elnevezése: Közigazgatási Informatikai Bizottság, amely a korábban létrehozott bizottságok feladatainak ellátását folytatja, elnöke az infokommunikációért felelős kormánybiztos. Dokumentumai letölthetők az Elektronikus kormányzat-központ honlapjáról[6].

4 Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma

5 Lásd: 1054/2004. (VI. 3.) Korm. határozat a kormányzati informatika fejlesztésének koordinálásával kapcsolatos egyes feladatokról, 2124/2003. (VI. 6.) Korm. határozat a közigazgatási szolgáltatások korszerűsítési programjának kormányzati koordinálásáról, 1026/2007. (IV. 11.) Korm. határozat a közigazgatási informatikai feladatok kormányzati koordinációjáról (jelenleg már csak ez hatályos)

6 http://www.ekk.gov.hu/hu/ekk

Számunkra jelentős a Bizottság 26. számú Ajánlása „A Magyarországon elektronikus azonosításra, hitelesítésre, aláírásra és elektronikus azonosítók hordozására alkalmas eszközök követelményei”-ről. A 2008. júniusában kelt ajánlás a HUNEID (Hungarian Electronic Identification) specifikációt részletezi. Célja (idézzük): „olyan egységes követelményrendszer megfogalmazása, mely egyértelművé teszi a Magyarországon biztonságos elektronikus azonosításra-hitelesítésre, aláírásra, valamint az egyéb azonosító adatok tárolására alkalmas intelligens kártyák kibocsátását és alkalmazását a közigazgatás egészére. Mindezekkel gyártófüggetlen, platformfüggetlen és alkalmazásfüggetlen módon kívánja elősegíteni az intelligens kártyák elterjedését kibocsátótól függetlenül a magyar információs társadalmi törekvések megvalósításához”.

Nem váratlan ugyanakkor, hogy megerősíti azt a felfogást, hogy a „kártya kifejezés absztrakció, az elektronikus azonosításra-hitelesítésre és aláírásra vonatkozó követelmények USB-token és SIM-kártya formátumban megvalósított eszközökkel is kielégíthetők (illetve a jövőben megjelenő, ma még e célra nem alkalmazott eszközökkel is, amennyiben azok, az itt szereplő követelményeket kielégítik), amely eszközöknél az okmányjellegű alkalmazás, azaz a vizuális azonosíthatóság nem követelmény és nem biztosított”.

Az Intelligens Kártya definicióját az Ajánlás rögzíti:

„Az Intelligens Kártya (Smart Card) kifejezés a dokumentumban absztrakció, az e-ID White Paper és a CEN/CWA 15264 szellemében a fizikai kártyaformátum csak ott kötelező, ahol a kapcsolódó okmány funkció a kártya formátumot előírja, mely esetben a CEN/TS 15480-1 szabvány az irányadó. Intelligens Kártya alatt tehát valamilyen intelligens – előre meghatározott funkcionalitás végrehajtására alkalmas – csip platformot (csipmodul, operációs rendszer, fájlrendszer, aláíró alkalmazás vagy applet) értünk, ami többek között USB-alapú biztonsági eszközzel, vagy mobil SIM-kártyával is kielégíthető.”

Az ajánlás tartalmi ismertetését bízvást eltekinthetünk, hiszen az bárki számára hozzáférhető, letölthető és olvasható. Mégis célszerű idézni, hogy a követelményrendszer az alábbiak vonatkozásában irányadó:

- HUNEID-kártya és alkalmazás parancs interfész (felhasználói fázisban)
- HUNEID-alkalmazás fájlstruktúra specifikáció
- HUNEID-kártya és alkalmazás biztonsági követelmények
- HUNEID-kártyán lévő tanúsítványok kibocsátására és tartalmára vonatkozó minimum követelmények
- azonosító adatok és azok elhelyezése a HUNEID-alkalmazásban
- egyéb eID-alkalmazások
- azonosító adatok és azok elhelyezése egyéb eID-alkalmazásban
- kártyával szemben támasztott elvárások a kártyamenedzsment szempontjából
- kártyával szemben támasztott elvárások a kulcsmenedzsment szempontjából
- kártya- és alkalmazáskibocsátási alternatívák

Az ajánlás továbbá felsorolja mindazokat a szabványokat, amelyek a HUNEID-kártya, s a fentiek szerinti mobileszköz esetében figyelembe kell venni, valamint a vonatkozó jogszabályokat, továbbá számos referenciát is tartalmaz.

5. Digitális igazolványok

A fentebb említett e-ID White Paper szerint a digitális igazolványokat (tanúsítványokat) hamarosan beépítik bármilyen olyan eszközbe vagy szoftverbe, amely biztonságos kommunikációra képes egyéb eszközökkel vagy személyekkel, felölelve nemcsak a bármiféle számítógépeket, hanem a televíziókészülékeket, járműveket, telefonokat, beléptető rendszereket, járművezetői engedélyeket, szavazólapokat, ajtókulcsokat, elektronikus pénzt stb.

Hivatkozunk továbbá az Európai Szabványügyi Bizottság (CEN) CWA 14169 sz. Workshop Agreement-jére[7] is, amely a BALE biztonsági követelményeit rögzíti az EU e-aláírási irányelvével összhangban. Figyelemre méltó, hogy a BALE-t megvalósító eszközt magát (kártya, mobileszköz stb.), sehol sem nevesíti. Mindazonáltal többször példaként említi (e.g. smart card).

Jogosítvány, forgalmi engedély

A gépjárművek közúti forgalomban való vezetésére a vonatkozó hatályos jogszabály[8] értelmében csak a hatóság által kiállított járművezetésre jogosító okmánnyal – vezetői engedéllyel – rendelkező személy jogosult, mely jogosultságot a jogosítvány bemutatásával igazolja. Az előbbihez hasonlóan a forgalmi engedély olyan hatósági engedély, amely a jármű közúti forgalomban történő részvételének jogszerűségét igazolja.

A jogszabály mindkét engedély tartalmi elemeit meghatározza. Megjegyezzük, hogy 2001. január 1-jétől bevezetésre került vezetői engedély kártyaformátumú.

Elemzésünk szempontjából nem kérdéses, hogy ezek az okmányok csak eredeti, a hatóság által kibocsátott adathordozón minősülnek hitelesnek. Közjegyző ugyan készíthet róla hiteles másolatot (és erről egyikük személyesen is tájékoztatást adott), de az csupán azt igazolhatja, hogy a másolat kiállításának időpontjában az okmány érvényes volt, így ellenőrzés során a hatósági személy, többnyire rendőr, nem köteles azt elfogadni, és esetleg arra kötelezheti a másolatot felmutató személyt, hogy az eredeti okmányt a hatóságnak bemutassa. A járművezetőt igazoltató rendőr ugyanis mindkét okmányt – a jogszabályban rögzített feltételek fennállása esetén – a helyszínen elveszi.

7 Secure signature-creation devices „EAL 4+”, CEN WORKSHOP AGREEMENT CWA 14169, March 2004

8 35/2000. (XI. 30.) BM rendelet a közúti közlekedési igazgatási feladatokról, a közúti közlekedési okmányok kiadásáról és visszavonásáról

Ha tehát ezeknek az okmányoknak elektronikus másolatát mobiltelefonunkba töltjük, az semmiképpen nem minősíthető hitelesnek. Más kérdés, hogy e másolat hitelességéről a hatósági személy meggyőződhet, ha az ehhez szükséges technikai feltételek rendelkezésre állnak. Ha saját mobiltelefonjára – például NFC-technikával – e másolatot áttölti, majd azt, vagy annak adatait a kiállító hatóságnak továbbítja, a kiállító hatóság – ugyancsak hírközlési csatornán – visszaigazolhatja annak hiteles voltát.

Ezek a technikai feltételek azonban hazánkban egyrészt még nem állanak rendelkezésünkre, s ha majd igen, akkor is kérdéses, hogyan veszi el a rendőr az okmány másolatát magát. Ettől függetlenül persze kötelezheti az érintett személyt, hogy az eredeti okmányt a hatóságnak haladéktalanul ténylegesen adja át.

6. Azonosság – digitális azonosság

A való világban hozzászoktunk, hiszen azonosságunkat vagy bizonyos tulajdonságunkat számos élethelyzetben igazolnunk kell.

Digitális azonosság: lényegében ugyanúgy jellemezhető, mint a valóságos világban, csakhogy azt ott digitális formában kell meghatároznunk és az azonosság igazolásakor megosztott hálózatokban alkalmaznunk. Eszerint: a digitális azonosság a személy azonosságának az a formája, amelyet megosztott hálózatban használunk abból a célból, hogy számítógépünkkel egyéb számítógépekkel és személyekkel kapcsolatot hozzunk létre.[9] A digitális azonosság az alábbi két részből áll:

1. személyes azonosság
   (kicsoda a szóbanforgó személy?),
2. az azonosság ismérvei
   (a személyes azonosság igazolása).

Személyes azonosság: olyan, adott személyre jellemző ismérvek összessége (halmaza), melyek meghatározott időtartamban nem, vagy csak nagyon nehezen változtathatók meg. Például: születési időpont, genetikai minta (a szem színe, a magasság stb.). Megjegyezzük: születésünk időpontját ugyan hamisan is megadhatjuk, megváltoztatni azonban nem tudjuk.

Igazoláson azokat az ismérveket értjük, amelyek a személyes azonosságot meghatározzák. Például az útlevél annak igazolására szolgál, hogy adott személy ténylegesen az útlevél birtokosa. A személy ugyan azonos önmagával, arca látványának útlevélbeli fényképével való összevetése nyújtja ennek megfelelő igazolását.

Azonosítás (identifikáció): személyes ismérv hozzárendelése egy személyhez, mely személy különféle tulajdonságokat mutat. A legegyszerűbb példa, ha a személyhez a nevét rendeljük hozzá (a névadás célja ugyanis éppen az, hogy valamely személyre a nevével hivatkozzunk, s ne kelljen újra meg újra a tulajdonságaival körülírni, kiről is van szó). „Ön Például János" – mondjuk, mikor találkozunk Például Jánossal. Ebben az esetben a hozzárendelés a „Például János" név és Például János személye között jön létre. Az azonosítás azt jelenti, hogy megjelölünk egy olyan ismérvet, melyből egy személy (vagy dolog /objektum/) azonosságára adott összefüggésben egyértelműen következtethetünk.

Hitelesítés (autentikáció): a hitelesítés az az eljárás, melynek során egy személy (akár digitális) azonosságát megállapítjuk, azonosságáról meggyőződünk. Az azonosság puszta kinyilvánítása (pl. „János vagyok") nem elegendő, hiszen hitelesítés hiányában csupán állításról van szó (egy személy azt állítja magáról, hogy ő János). A hitelesítés folyamán egy személy azonosságát megfelelő igazolással (útlevéllel, jelszóval) bizonyítani kell, melynek során megállapítjuk, hogy ő ténylegesen az a személy, akinek állítja vagy kiadja magát. Az igazolás felülvizsgálatával az azonosság valódiságára és megbízhatóságára következtethetünk. A hitelesítés célja éppen ez, vagyis az azonosság hitelességének (valódiságának) ellenőrzése abból a célból, hogy az azonosság meghatározott eljárásokban megbízható legyen.

Hitelesítési mechanizmusok

Egy azonosság hitelesítése során megfelelő igazolásokat mutathatunk be, mégpedig az alábbi módon:

- Birtokláson alapuló hitelesítés:
  A hitelesség alapja az a tárgy, amely azonossága igazolása céljából a felhasználó birtokában van. E tárgyat gyakran egy megbízható harmadik fél bocsátja ki. A digitális világban ilyen például egy intelligens kártya és az intelligens kártya funkciót tartalmazó mobiltelefon a rajta tárolt igazolásokkal.
- Tudáson alapuló hitelesítés:
  A hitelesítés alapja valaminek a kizárólagos ismerete. Ilyen például a jelszó. A felhasználó bejelentkezéskor – miután megadta személyi azonosítóját – megadja jelszavát, melyeknek a tárolt adatokkal való összevetése során egyezés esetében a személy azonossága hitelesíthető.
- Tulajdonságon alapuló hitelesítés:
  A hitelesítés alapja valamilyen kizárólagos tulajdonság – például a mobiltelefonban tárolt ujjlenyomat, szivárványhártya stb. – igazolása.

Feljogosítás: a hitelesítést követő eljárás, melynek során a hitelesített személy meghatározott szolgáltatásokhoz vagy rendszerekhez hozzáférhet. A jogosultság megadását a szolgáltató különféle feltételekhez kötheti.

Az *egyszeri bejelentkezés* (SSO) az a folyamat, melyben egy felhasználónak csupán egyetlen hitelesítő szervezetnél kell hitelesíttetnie magát, melyet követően egyébként védett dolgokhoz férhet hozzá anélkül, hogy ismételten hitelesíttetnie kellene magát.

A hálózatok számának növekedése, mely rendszerint együtt jár a hálózatok egymáshoz kapcsolódásával, továbbá az internethasználat szakadatlan bővülésével a hitelesítési eljárás meghonosodott az online világban is. A személyeknek e világban is van azonosságuk, me-

9 Lásd még: http://www.digitalidworld.com/local.php?op=view&file=aboutdid

lyet digitális azonosságnak nevezünk. Ha valaki, vagyis egy felhasználó egyes felkínált szolgáltatásokat, vagy egy kiszolgáló (szerver) alkalmazásait igénybe akarja venni, biztonsági okokból a felhasználónál rendszerint azonosítania és hitelesítenie kell magát. Az interneten leggyakrabban alkalmazott hitelesítési mechanizmus a felhasználónév és a jelszó megadását kívánja meg, melyeket nyilvántartásában a szolgáltató bejegyzésként (account) tárol. Tekintettel viszont arra, hogy a felhasználó több szolgáltatónál is bejelentkezik, szaporodnak bejegyzései, s ezzel együtt egymástól nem feltétlenül különböző azonosítói és jelszavainak száma. Hajlamosak vagyunk arra, hogy egyszerű, könnyen megjegyezhető, sőt különféle szolgáltatások igénybe vételéhez ugyanazokat jelszavakat használjuk, esetleg azokat számítógépünk közelében fel is jegyezzük. Ezáltal viszont drasztikusan csökken a jelszó használatának biztonsága, vagyis azt mások is megismerhetik vagy megfejthetik, s jelszavunkkal visszaélhetnek.

Ezt elkerülhetjük, ha a legkülönfélébb szolgáltatásokhoz – mindenek előtt például a közigazgatásban – egyetlen, a mobiltelefonban tárolt, RFID-vel továbbított azonosítóval és jelszóval férhetünk hozzá.

7. Az osztrák polgárkártya-koncepció

Ausztriában az e-kormányzásról szóló törvény 2004-ben való hatályba lépését követően több mint 10 millió eID-t bocsátottak ki. Ez a szám ugyan – minthogy Ausztria lakosainak száma 8 millió körül van – félrevezető lehet, ami abból adódik, hogy az osztrák koncepció szerint az eID nem szükségszerűen jelent eID-kártyát. Az országban 2005 márciusát követően kibocsátott ATM kártyák például beépített BALE-t is tartalmaznak, amely megfelel az EU elektronikus aláírási irányelvében rögzített követelményeknek, továbbá polgárkártyaként is aktiválható.

Az osztrák eID, eltérően más európai megoldásoktól, nem egyetlen kártyára korlátozódik. Az eID koncepciót több fizikai eszköz támogatja:

– a polgárkártya: nemzeti eID kártya és a helyi bankok által kibocsátott bankkártyák,
– a Mobilcom Austria A1 távközlési infrastruktúrája, amely az A1 által kiadott SIM kártyákba telepített intelligens kártya funkciókra épül,
– USB.

Az eID azonosítónak tényleges személyhez való rendelésére ugyan nagyon szigorú törvényes előírások szerint csak az illetékes hatóságnak van joga, a kártyának magának a kibocsátására magánjogi szervezetek is jogosultságot kaphatnak (ilyen az A1 is).

Az EU e-aláírási irányelvének osztrák értelmezése szerint az egyedi azonosító és az elektronikus aláírás nincs feltétlenül elválaszthatatlan kapcsolatban, s ezért azokat mint két elkülönült funkciót kezeli. Ez az elkülönítés különösen hasznos, amikor más országokkal való interoperabilitásról van szó, minek eredményeképpen az „idegen” azonosság minden további nélkül elfogadható Ausztriában elektronikus aláírást igénylő funkció kiváltására.

Az osztrák polgárkártya-koncepciót úgy fogalmazták meg, hogy eleget tegyen az eID-vel szemben támasztott két alapvető követelménynek:

– az e-aláírást Ausztriában elfogadják jogszabályi kötelezettség alapján, s legyen összhangban az EU e-aláírási irányelvében foglalt rendelkezéseivel,
– abból a célból, hogy az e-aláírás feleljen meg az előző követelménynek, ha egy egyedi azonosító nem szükséges, a koncepció támogat egy sajátos azonosítási eljárást, miközben betartja az adatvédelmi jogszabályok előírásait is.

Kezdetben úgy tűnhetett fel, hogy az adatvédelmi szempontból szükséges összekapcsolhatóság tilalmának követelménye nem teljesül. Jóllehet az összekapcsolhatóságnak nincs jogi definíciója, az ISO IT biztonsági szabványa szerint az „biztosítja, hogy egy felhasználó többször is igénybe vehet javakat vagy szolgáltatásokat, anélkül hogy ezeket egymással össze lehetne kapcsolni”. E tilalom szerint felhasználók és/vagy más személyek nem tudják meghatározni, hogy ugyanaz a felhasználó váltott-e ki a rendszerben bizonyos sajátos műveleteket.

E tilalomnak a forrás-személyazonosítóval bizonyos mértékig eleget tesz a polgárkártya koncepció, amely – ismételten hangsúlyozzuk – felöleli a mobiltelefont is.

Az e-Gov törvény azonosságnak az egyedi azonosítót (eindeutige Identität) definiálja, mint az érintett egy vagy több ismérv szerinti megjelölését, miáltal mindenki mástól felcserélhetetlenül és összetéveszthetetlenül megkülönböztethető.

8. Összefoglalás

E cikkben nem foglalkozhattunk a mobiltelefonban tárolt vagy tárolható adatok és lehetséges felhasználásuk teljeskörű bemutatásával. Csupán arra kívántuk felhívni olvasóink és főleg a mobiltávközlés műszaki fejlesztésével foglalkozó szakemberek figyelmét, hogy a hatályos jogszabályok lehetőséget nyújtanak újabb funkcióknak a mobiltelefonba való telepítésére.

A szerzőről

KÖNYVES TÓTH PÁL villamosmérnök, 1974 óta foglalkozik a személyes adatok védelmének és a közérdekű adatok nyilvánosságának jogi kérdéseivel. Ő készítette az e kérdéseket szabályozó 1992. évi LXIII. törvény tervezetét. Elsőként képviselte hazánkat az Európa Tanács adatvédelmi bizottságában és munkacsoportjaiban (1989-1993). 1989 óta tagja a Távközlési Adatok Védelmével foglalkozó Nemzetközi Munkacsoportnak (IWGDPT). Szellemi szabadfoglalkozásúként kutatja a hálózatos szolgáltatások – így a távközlés – gazdasági szabályozási kérdéseit is. Kezdeményzésére jött létre a „Tisztességes adatkezelésért” elnevezésű informális szakértői kör.