Kiss Tibor
szakértő
Nemzeti Hírközlési és Informatikai Tanács

Szegő Tamás
szakértő
Nemzeti Hírközlési és Informatikai Tanács

A személyazonosítás múltja, jelene és jövője – e-Személyazonosító igazolványra épített szolgáltatási lehetőségek

Jelen tanulmány célja rávilágítani az elektronikus személyazonosító igazolványon (eSzemélyi, eSZIG, eSzemélyiazonosító igazolvány) alapuló szolgáltatási lehetőségekre, felhívva az érintett közigazgatási szereplők figyelmét a várható igényekre, illetve azok közigazgatásra gyakorolt hatására.

1. Személyazonosítás története

Ahhoz, hogy megértsük és értékelni tudjuk a jelenkor személyazonosítási rendszerét, a kapcsolódó szolgáltatásokat, illetve lehetőségeket érdemes áttekinteni a személyek azonosításának történetét, továbbá azt a folyamatosan épülő állami (illetve önkormányzati) és állampolgári igényrendszert, amely követelményt támaszt az újabb és újabb módszerek és technológiai megoldások kidolgozására.

1.1 Az egyének egyértelmű azonosításának igénye és eszközei

A személyek egyértelmű beazonosításának igénye már az ókori civilizációs folyamatok során megjelent. Tekintettel arra, hogy az ujjlécrajzolatok egyediségét már nagyon régóta ismeri az emberiség, ezért már az ókorban is erre építették a személyazonosítást, például ujjlenyomatos agyagpecsétek használatával. Az asszírok és a babilóniaiak például fontos okmányaikra agyagból készített pecsétet tettek, amelybe belenyomták a hüvelykujjuk végét. Kínában számos hivatalos ügylet csak akkor volt érvényes, ha azt agyagpecséttel hitelesítették, és ujjlenyomattal igazolták a szerződéseket, üzletkötéseket, zsoldfizetést vagy akár büntetőügyeket is.

Az írástudatlan indiaiak az ujjlenyomatot egyfajta aláírásként használták, ezért például a nyugdíjak kiosztásakor a fizetési listákon az ujjakról vett lenyomattal igazolták a pénz átvételét. Japánban az ujjlenyomatokat aláírásként használták a kerámiákon, illetve bűnügyek felderítésénél is összevetették a helyszínen talált, illetve a feltételezett elkövető ujjlenyomatait.

A modernkori társadalmi szükségletek – történelmi léptékkel nézve nem is olyan régen, néhány évszázada – hozták létre a személyazonosító okmányokat, amelyek a pecsétek és ujjlenyomatok vizsgálatánál gyorsabb személyazonosítást tettek lehetővé.

Magyarországon a kezdeti okmányok csak másodlagosan szolgálták az egyén azonosítását, ám az állami és társadalmi igények megalapozták a közhiteles személyazonosító okmány bevezetését, amelynek szerepét kezdetben a születési anyakönyvi kivonat töltötte be. Mindezek mellett használatban voltak még államigazgatási- és település-elöljárósági iratok is (pl.: katonai sorozásra vonatkozó, vagy vagyoni igazolás, esetleg születési bizonyítvány), amelyek az egyházi anyakönyvi okiratokkal együttesen, vagy akár külön is személyazonosítási funkciókat betöltöttek.

A személyazonosságot bizonyító hivatalos iratok az 1800-as években a társadalmi mobilizálódás következtében jelentek meg. Kezdetben *„Igazoló jegy”* néven, majd a 20. század elejétől fényképes igazolványok formájában. Az arcképes iga-

zolványok sorában használatban voltak foglalkozás szerinti igazolványok (pl.: MÁV-, vagy hivatali alkalmazotti, ügyvédi, üzletkötői, cégképviselői).

Bár különböző érdekek mentén, de az egyértelmű személyazonosítás a történelem során mind az állampolgárok, mind a „vállalkozások", illetve az állam számára egyaránt fontos társadalmi elvárásként jelentkezett. Az egyértelmű azonosítás teremtett több szolgáltatás tekintetében bizonyosságot, illetve csökkentette a kockázatokat kiemelt szolgáltatások tekintetében (pl.: banki, ügyvédi szolgáltatások). A bemutatott érdekek rendszere vezetett a 20. század második felére oda, hogy a személyiségi jegyeket tartalmazó ujjlenyomat mellett (tekintettel azok erőforrásigényes ellenőrzésére) megjelenjenek a személyeket egyértelműen azonosítani képes központilag kiadott személyt azonosító okmányok.

1.2 A személyi igazolvány megjelenése Magyarországon

A személyi igazolvány Magyarországon 1954–2000 között kiadott hatósági igazolvány volt, amely ebben az időszakban az *„egyetlen hitelt érdemlően igazoló okmány, amelyet mindenki köteles gondosan megőrizni, és állandóan magánál tartani"*. 1992-től a személyi igazolvány adattartalma lényegesen megváltozott, 2000-től pedig a személyi igazolvány kifejezést a személyazonosító igazolvány, és külön a személyi azonosítót és lakcímet igazoló hatósági igazolvány váltotta fel. Ugyanekkortól a személyazonosításra alkalmas okmányok köre az útlevéllel, majd 2001-től a kártyatípusú vezetői engedéllyel bővült – aki ezek bármelyikével rendelkezik, annak a személyazonosító igazolvány kiváltása nem kötelező. Az 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról (továbbiakban Nytv.) 29. § (6) bekezdésének rendelkezése alapján a 14 éven aluliak személyazonosságának igazolására 2009. június 27-ig alkalmas volt a tanulói jogviszonyt igazoló diákigazolvány is. A 2016. január 1-jével megjelent új, elektronikus személyazonosító igazolványba épített magas biztonságú tárolóelem (chip) pedig minden esetben tartalmazza a személyazonosító adatokat, illetve a társadalombiztosítási és adóazonosító jelet, amennyiben azokkal az állampolgár rendelkezik. Továbbá az állampolgárok döntésétől függően az elektronikus elem tartalmazhatja az állampolgár ujjnyomatát, és az elektronikus aláírás létrehozásához szükséges adataikat is.

A magyar állampolgárok teljes körére kötelező személyi igazolványt a Minisztertanács az 1/1954. (I. 9.) MT rendelete vezette be. A rendelet végrehajtását az 1/1954. (I. 9.) BM rendelet szabályozta, amely alapján az országban lakó 16éven felüli minden magyar állampolgár számára kötelező volt a személyi igazolvány.

Az igazolvány formai és kisebb jelentőségű tartalmi változásain túl, lényeges újdonság volt a személyi szám (később: személyazonosító jel) megjelenése, illetve az, hogy 2000-től az összevont tartalmú *„személyi igazolvány"* helyett belépett a *„személyazonosító igazolvány"*, és külön a „személyi azonosítót és lakcímet igazoló hatósági igazolvány". A személyi igazolvány kifejezést 2000-től a személyazonosító igazolvány, és külön a személyi azonosítót és lakcímet igazoló hatósági igazolvány váltotta fel. Az Nytv. 2000. január 1. napján hatályos 29. § (3) bekezdése szerint, a személyazonosító igazolvány tartalmazza a polgár

a) nevét;
b) születési helyét;
c) születési idejét;
d) állampolgárságát;
e) anyja nevét;
f) nemét;
g) arcképét;
h) saját kezű aláírását, illetőleg a cselekvőképességet kizáró gondnokság alá helyezett személy törvényes képviselőjének aláírását;
i) a személyazonosító igazolvány okmányazonosítóját és érvényességi idejét.

A személyazonosító igazolvány kiadásáról és nyilvántartásáról szóló 168/1999. (XI. 24.) Korm. rendelet 7. § (1) bekezdése szerint az állandó személyazonosító igazolvány az Nytv. 29. § (3) bekezdésében meghatározott személy- és okmányazonosító adatokon kívül tartalmazza a személyazonosító igazolvány kiállításának keltét, a kiadó magyar állam kódját és a kiállító hatóság nevét.

A másfél évtizede alkalmazott gépi olvasási eljárások támogatására az igazolvány az adatokat gépi olvasására alkalmas adatsor formájában (MRZ) is tartalmazza nemzetközileg szabványos tartalommal, amely például a határátlépések alkalmával történő ellenőrzéseket nagymértékben felgyorsította. Az ezredfordulót követő *„Internet forradalom"* megfogalmazta az elektronikus ügyintézés lehetőségét, mint társadalmi elvárást, amelynek előfeltétele a megfelelő biztonságú elektronikus személyazonosítás.

2. Azonosítási rendszerek

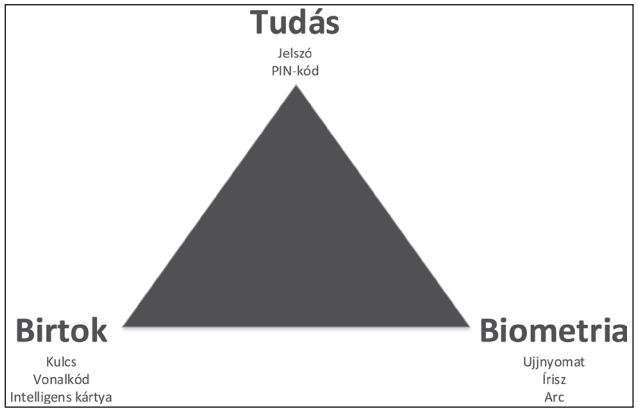
Az informatikai megoldások terjedésével, illetve az azokra épülő módszerek és szolgáltatások kialakításával az elektronikus térben is egyre fontosabb kérdéssé vált az igénybe vevők személyének biztonságos és hatékony azonosítása, illetve hitelesítése.

Az elmúlt évtizedekben kialakult megoldások igazolták, hogy a digitális térben nagyobb rendelkezésre állással és hatékonyabban kezelhetőek az ügyek, tranzakciók a személyes megjelenést igénylő papír alapú csatornákhoz képest. Gyakorlati oldalról erre szemléletes példa a banki tranzakciók kezelése, amelyeket az ókori Kínában agyagpecséttel, majd egészen a 1990-es évekig személyes okmányra épülő azonosítással, és papír alapú aláírással hitelesítettek, azonban napjainkban már az online rendszereken keresztül kezdeményezett banki átutalások tekinthetőek általánosnak. Tehát az egyik legérzékenyebb területen sikeresen megtörtént a digitális transzformáció, amelynek kulcseleme a digitális térben történő személyes azonosítás lehetőségének kialakulása. Az alábbiakban – építve a BME Searchlab által publikált kutatási eredményekre – összefoglaljuk a hatékony és hiteles személyazonosítás általános módszertani keretrendszerét, és az egyes megoldások sajátosságait.

2.1 Azonosítási rendszerek, módszertani keretek

Az informatikai rendszerek, kiváltképpen a közigazgatási vagy pénzügyi tranzakciókat is magukban foglaló szolgáltatások használatának egyik alapvető kihívása a felhasználó megfelelő biztonságú és hatékonyságú azonosítása. Sok esetben azonban épp ez a funkció az, amelyet kellő biztonsággal megvalósítani nehéz, így a legtöbb esetben ez jelenti egy rendszer leggyengébb pontját.

Egy személyt több jellemzője alapján azonosíthatunk egy informatikai rendszerben, a különböző lehetséges azonosítási elvek közül három alapmódszer alkalmazott: a tudás, a birtok és a biometria alapú azonosítási eljárás.



1. számú ábra. Azonosítási megoldások

Mindegyik módszernek megvan az erőssége és gyengesége, ezért a kellő biztonsági szint eléréséhez együttesen (egy időben, egyszerre) javasolt legalább két eltérő elven alapuló módszert egymástól függetlenül ötvözni. A függetlenség kihangsúlyozása azért fontos, mert az egymástól függő megoldások nemhogy erősítik, de akár gyengíthetik is egymást.

2.2 Tudás alapú azonosítás

A felhasználóazonosítás legegyszerűbb, és bárhol használható megoldása, ha egy személyt olyan információ ismerete révén azonosítunk, amelyről másnak nincs információja. A tudás alapú azonosítás különféle jelszavak, illetve kérdésekre adott válaszok formájában történik. A teljesség igénye nélkül az alkalmazott megoldások a következők lehetnek:

- felhasználók által kitalált jelszavak;
- számítógép által kitalált jelszavak;
- PIN-kódok;
- kérdés és válasz kódok;
- kombinációs jelszavak;
- jelmondatok.

A jelszavak használata során számos veszély, támadási, visszaélési lehetőség fenyegeti az alkalmazott megoldás biztonságát. Ezen lehetőségekre fel kell készülni, és amennyire lehet, ki kell védeni azokat. A megfigyelés jellegű visszaélések ellen a billentyűzet megfelelően takart elhelyezésével lehet valamelyest védekezni, de végső soron a felhasználón múlik, hogy mennyire ügyel a jelszavának titokban tartására. További támadási felület, hogy a megfelelő vírusvédelemmel nem rendelkező klienseket gyakorlatilag észrevétlenül megfertőzhetik a kártékony kódokat tartalmazó szoftverek, így az úgynevezett *„key logger”* módszerrel minden leütött karaktert – így a jelszavakat is – megszerezhetik a támadók.

A jelszavak dekódolhatóságának elkerülése érdekében ma már általános előírás, hogy azokat titkosított formában tárolják a szolgáltatói rendszerek adatbázisai. Ilyen esetekben az azonosítás során az ellenőrzés úgy zajlik, hogy a megadott jelszóból is lenyomatot számít a rendszer, és azt hasonlítja össze az eltárolt lenyomat értékkel. Tekintettel arra, hogy ma még azért nem minden szolgáltatói rendszer tárolja titkos formában a jelszavakat, így a felhasználói oldalon javasolt arra törekednünk, hogy minden rendszer esetén eltérő jelszavunk legyen. Ezen elővigyázatos magatartás szükségességét erősíti, hogy évről-évre jelennek meg olyan hírek, hogy egy-egy szolgáltató felhasználó adatbázisát feltörték, és több 100.000, eseténként több millió felhasználó adott rendszerben tárolt felhasználó neve, e-mail címe és jelszava szivárgott ki. A kompromittálódott adatokat a cyber bűnözők egymás között kicserélik, és azok felhasználásával újabb támadásokat hajtanak végre. Ebből adódóan, ha egy felhasználó minden általa használt rendszerben megegyező jelszót használ, akkor rendkívüli módon megkönnyíti a bűnözők dolgát.

További támadási felület a jelszavak úgynevezett *„brute force”* alapú feltörése, amely minden lehetséges jelszó kombináció kipróbálásának módszerére épül. A jelenlegi online rendszerek már jó védelmi mechanizmusokat építettek ki ez ellen, azonban a hackerek (nem gépi generált) értelmes szavakból álló jelszavak esetén az úgynevezett szótárazási technikával még napjainkban is tudnak *„eredményeket”* elérni.

A tudás alapú azonosítás jellemzői:

- használata egyszerű és olcsó;
- hátránya, hogy észrevétlenül kompromittálható (a tudás észrevétlenül másolható és tulajdonítható el, nincs visszajelzés arról, hogy valaki más is a jelszó birtokába jutott);
- erős védelmet jelentő jelszavak megjegyzése az ember számára nehéz.

Összességében megállapítható, hogy a tudás alapú azonosítást kritikus rendszereknél önállóan alkalmazni nem tekinthető biztonságos megoldásnak, azonban ez jó kiegészítője lehet egy birtok alapú azonosítási eljárásnak. A banki tranzakciós példához kapcsolódva; az online rendszerek jellemzően két lépcsős azonosítást alkalmaznak, amelyek során a felhasználónév és jelszó megadását követően egy a felhasználó által birtokolt mobiltelefonra küldött hitelesítő jelszó segítségével végezhető el a tranzakció.

2.3 Birtok alapú azonosítás

A birtok alapú azonosítás a felhasználó birtokában lévő tárgyra épül, amely azonosítási mód már lényegesen biztonságosabbá tehető, mint a tudás alapú, de a módszer eredendő gyengesége, hogy a kulcs eltulajdonítható. A biztonsági fak-

tort két tényező befolyásolja: a másolhatóság, és az elvesztés után történő illetéktelen felhasználás lehetősége.

A passzív felhasználó-azonosító eszközök (úgymint a vonalkód és a mágneskártya) használata főleg olcsóságuk és könnyű kezelhetőségük miatt terjedt el. Az aktív (írható-olvasható) eszközök nagyobb megbízhatóságot tesznek lehetővé passzív társaiknál, bonyolultabb műveletek elvégzésére képesek, és nehezebben másolhatóak. Az intelligens eszközök nyilvános kulcsú és/vagy többfaktoros kriptográfiai eljárásokat alkalmaznak az azonosítási folyamat során. A bennük tárolt titkos kulcsot szakszerű kiépítés esetén gyakorlatilag semmilyen módszerrel nem lehet kinyerni belőlük, ezért ezek garantálják a legmagasabb fokú biztonságot.

Az intelligens kártya sikerét a bankkártyákkal való hasonlósága, és az azonosítás funkcióján jelentősen túlmutató egyéb szolgáltatásainak köszönheti (memória kapacitás, rejtjelkulcsok védett tárolása, digitális aláírás). Biztonságtechnikai szempontból fontos, hogy a chip-kártyáknak két nagy osztálya létezik annak ellenére, hogy fizikai kialakításban nincs közöttük különbség, mindkét esetben a kártyák fizikai felépítését és elektronikai kommunikációját az ISO 7816-os szabványcsalád írja le. Az egyszerűbb chip-kártyákat, amelyek nem rendelkeznek érdemi számítási kapacitással memória-kártyáknak, míg a komoly számítási műveletek (tipikusan rejtjelezés elvégzésére is) alkalmas kártyákat intelligens kártyáknak, angolul smartcard-nak szokás nevezni. A felhasználó-azonosítás szempontjából a lényegi különbség a két osztály között, hogy a memória-kártyák természetüknél fogva másolhatóak, míg az intelligens kártyáknál nyilvános kulcsú kriptográfiával megoldható, hogy az azonosítás során is titokban tartsák a bennük elhelyezett rejtjelkulcsot, így gyakorlatilag másolhatatlannak tekinthetőek.

Az intelligens kártya tulajdonképpen egy kisméretű számítógép: processzorral, operatív- és tároló-memóriával, esetleges kiegészítőkkel (I/O, kripto-processzor). A memória-kártyákhoz képest megnövekedett tárterület és számítási kapacitás jóval bonyolultabb, akár többfunkciós alkalmazások futtatását is lehetővé teszi magán a kártyán. Sok esetben ezek a kártyák saját operációs rendszerrel is rendelkeznek.

További különbséget tesz a chip-kártyák között az alkalmazott kommunikációs interfész. Ez alapján felszíni érintkezős teljes (bankkártya nagyságú), illetve mini (GSM SIM kártya nagyságú) kivitelezésről, vagy rádiófrekvenciás (contactless) kártyákról beszélhetünk. Létezik továbbá mindkét interfészt használó úgynevezett kombi-kártya is, amely mindkét típusú olvasóval képes kommunikálni.

Ezen technikai adottságok lehetőséget adnak kriptográfiai eljárások futtatására is, így intelligens kártyával gyakran találkozhatunk különböző biztonságtechnikai rendszerekben is. A chip-es kivitelezésnek köszönhetően a gyártók azt állítják, hogy a chip-ben tárolt információk fizikai úton (a chip megbontásával) nem, vagy csak nagyon költséges eljárással (elektronmikroszkóp használatával) olvashatóak ki, kellően erős védelmet nyújtva így a tárolandó információknak, tipikusan a rejtjelkulcsoknak. Nyilvános kulcsú kriptográfia alkalmazásával megoldható, hogy ezen adatoknak a birtoklását a kártya úgy bizonyítsa, hogy közben magát a kulcsot ne árulja el. Az ilyen azonosítási módszereket nevezzük zero-knowledge azonosítási módszernek.

A birtok alapú azonosítás jellemzői:
- használata általában egyszerű;
- költsége széles spektrumon mozog;
- eltulajdonítható (az eltulajdonítás ténye észlelhető, a kulcs letiltható);
- másolás ellen védhető (lehetőség szerint ne lehessen titokban másolni a kulcsot).

2.4 Biometrián alapuló azonosítás

A biometria alapú azonosítás a felhasználó valamilyen tulajdonságára épít, közvetlenül azt vizsgálja, hogy a felhasználó fizikai-biológiai voltában hogyan azonosítható. Napjainkban a biometrián alapuló módszerekkel tudunk a legnagyobb pontossággal személyeket azonosítani.

A biometrikus azonosítás előnyei:
- A módszer ténylegesen magát a személyt azonosítja, nem olyan közvetett jellemzőket ellenőriz, mint jelszó vagy kulcs, amelyek eltulajdoníthatóak vagy megfejthetőek.
- Megfelelő eszköz, illetve technológia alkalmazásával meg lehet győződni arról, hogy a mintavételezés valós élő személytől származik, ezzel jelentősen csökkentve a megtévesztés lehetőségét.
- Lehetőség lehet csendes riasztásra, ha például ujjnyomat leolvasásnál másik ujját, vagy hangazonosításnál más jelszót használ a kényszerített személy.
- A biometrikus azonosítás hátrányai:
- A legtöbb módszer speciális hardvert igényel.
- Fogyatékos emberek esetén a módszer esetleg nem alkalmazható.
- Higiéniai szempontból a fizikai kontaktust igénylő megoldások problémásak lehetnek.
- A vizsgált jellemzők az idő múlásával, betegség illetve sérülés következményeként változhatnak.
- A leolvasások eredménye soha nem egyezik meg teljesen, így érzékeny pontja ezeknek a rendszereknek a hibatűrés mértéke, hiszen ez ronthatja az azonosítás megbízhatóságát mind a téves elfogadás, mind a téves elutasítás szempontjából.
- A számítógép nem biztos, hogy le tudja ellenőrizni a leolvasó hardver hitelességét, így az is támadások célpontja lehet.
- Jogi, adatvédelmi kérdéseket vethet fel, ha a leolvasás akár távolról, az adott személy beleegyezése nélkül is megtörténhet (például arc-azonosítás).
- Általánosságban elmondható, hogy az emberek idegenkednek ezen módszerek hétköznapi használatától (például az ujjnyomatnál Európában egyből a rendőrségi nyilvántartásra asszociálnak az állampolgárok).

Ujjlenyomat

Ujjlenyomat-azonosításra sokféle megoldást lehet alkalmazni a klasszikus rendőrségi módszeren alapulótól egészen az ult-

rahangos letapogatásig, amelyek közül néhány megoldás még azt is felismeri, ha nem élő ujjat tesznek a szenzorra.

Az ujjlenyomat az ujjak felületén képződött bőrredőzet, amely egyedi. Ez abból adódik, hogy az ujjakon lévő fodorszálak végződései, elágazásainak helye és iránya személyre jellemző sajátosság. Mindegyik megoldás ezek képét rögzíti, vagy az ebből származtatott adatokat. Abban különböznek a módszerek, hogy milyen módon tudjuk a kívánt adatot begyűjteni. Elektronikus letapogatásnál a felhasználónak az aktív felületre kell tenni az ujját. A bőr felülete ilyenkor úgy viselkedik, mint a kondenzátor, a redőzésnél a felület nem mindenütt egyforma távolságba van az ujjtól, ezért itt más kapacitás az érték. Ezek a változások alapján határozza meg a lenyomatot a berendezés. Egyszerű szkennelésnél alakzat-felismerési módszert használva azonosítják az ujjnyomatot, de az ultrahangos letapogatás is alkalmazható.

Bármilyen eljárást használunk vannak problémák, amelyek mindig fennállnak. Az egyik, hogy a felhasználó hogyan helyezi el ujját a vizsgáló eszközön, mert egyszerűbb berendezés nem ismeri fel, ha nem ugyanolyan pozícióban van, mint ahogy az adatot eredetileg megkapták. Ennek megoldása történhet szoftveres úton, vagy elő kell írni az eszköz használatában ezt a részt is.

Másik probléma az azonosítás pontossága, mert el kell dönteni, hogy milyen helyes azonosítási értéket akarunk. Ennek beállítása általában úgy történik, hogy az ujjlenyomat-azonosítón megadjuk hány jellegzetes pontot vizsgáljon. Ennek értéke akár 60 jellemző hely felismerése is lehet.

Hangazonosítás

Mivel a mindennapi életben az emberek többsége nagy biztonsággal képes egymást hangról is felismerni, felmerül a lehetőség, hogy ezt a tényezőt biometrikus paraméterként számítógépes azonosításra használják fel. A hangazonosító rendszerek általában eltárolják az azonosítandó személyek egy-egy rövid hangmintáját, amely lehet például egy jelszó, vagy egy rövidebb mondat, szókapcsolat is. A személyek ezután úgy azonosíthatják magukat, ha az eltárolt, vagy mindig változó szöveget ismét elmondják, hiszen a visszajátszás-elleni védelem az lehet, hogy a felolvasandó szöveg változik. Mivel a hangszálak sérülékenyek, ezért elég egy megfázás vagy rekedtség, és a rendszer használata pontatlanná válik.

Retina azonosítás

A szem sajátosságai alapján történő azonosítás lehetőségének bemutatása a New York State Journal of Medicine folyóiratban jelent meg 1935-ben, amely először vetette fel, hogy a vérerek mintázata a retinahártyán felhasználható egyének azonosítására. Ezt követően további jelentős kutatási és fejlesztési munkák foglalkoztak mind az írisz, mind pedig a retina mintázatok feltérképezésével, illetve ezek egyediségével. A retina azonosítás tehát az emberi szem hátsó falán található vérerek mintázatán alapul. A retina-azonosítás során alacsony intenzitású infravörös fénnyel világítják be a szemfenéken található retinát. Az infravörös fény használatát az indokolja, hogy a retinán található vérerek gyorsabban nyelik el az ilyen fényt, mint a környező szövetek. A retina mintázatot formázó fényt ezután visszatükrözik egy videokamerára, amely rögzíti a mintát. Mivel a retina azonosítás rendkívül nagy pontossággal működő biometrikus technológia, így elsősorban magas biztonsági fokot igénylő alkalmazásokban használják (hadi ipar). A módszer legnagyobb hátránya, hogy a felhasználók által nehezen elfogadható a mintavételi eljárás. Használata betanítást igényel, a felhasználók számára sokszor kellemetlen, illetve a *„letapogató"* technikával szemben vannak félelmek.

Mindezek ellenére a retinaazonosítás a biometrikus módszerek közül az egyik legjobb teljesítményt nyújtja, kis méretű adatsablonokkal, valamint gyors azonosítási eredményekkel. A jövőre nézve azonban nincs sok esély a nagyfokú elterjedésére, mivel az írisz-azonosítás még komplexebb és pontosabb eredményt ad.

Írisz azonosítás

Az írisz a szem szivárványhártyáján alapuló biometrikus azonosítás, a legjobb gyakorlati jellemzőkkel bíró azonosítási módszer. A szem szivárványhártyájának vizsgálata a látható, valamint a láthatatlan (infravörös) tulajdonságokon alapul. Az elsődleges látható paraméter a trabekuláris hálózat, amely az írisz sugaras mintázatát adja, amely rajzolat az embrionális fejlődés 8. hónapjában alakul ki, és többet nem változik az ember élete során. További jellegzetességek a körök, az árkok, vagy a korona. Az infravörös leolvasás során pedig a retinahártya láthatatlan erezetéről készíthető felvétel.

Előnye a rendszernek, hogy az írisz mintázata az idővel sem, sőt baleset, betegség vagy műtét következtében is csak extrém esetben, illetve jelentős mennyiségű alkoholfogyasztásnál változhat. Szintén az előnyök között lehet felsorolni, hogy amíg az íriszről készült, kellően részletes kép tárigénye nagy lehet, addig az azonosításhoz szükséges összes információ akár 256-512 bájtban is kódolható.

Az írisz alapú azonosítás jelentős hátránya az, hogy a leolvasó berendezések még napjainkban is költségesek. Az írisz alapú azonosítás az imént felsorolt hátrányai ellenére nagy jövő előtt áll, hiszen a retina-azonosításhoz hasonlóan rendkívül kedvező hibaparaméterekkel rendelkezik. Ezen felül a szükséges információ jól tömöríthető, így könnyen tárolható, valamint az adatbázisokban való keresés is gyorsan valósítható meg: egy átlagos személyi számítógép másodpercenként akár 100.000 rekordot is átvizsgálhat. Ezen azonosítási módszer azonban belátható időn belül biztosan nem terjed el széles körben a magas költségek miatt.

Arc felismerés

Mióta a kamerák ára kellően alacsony lett ahhoz, hogy kézi eszközökbe (például mobiltelefonokba) is jó minőségű képfelvételezésre alkalmas megoldások kerültek, megnőtt az igény az arc alapján történő azonosításra, hiszen a leolvasó berendezések minden személy esetén rendelkezésre állnak. Szintén az ilyen azonosítási módszerek mellett szól, hogy a legtöbb személyi adatbázisban is régóta tartanak fényképfelvételeket a nyilvántartásba vett személyek arcáról, amelyeket

így fel lehet dolgozni, és adatbázist lehet készíteni az automatizált azonosításhoz.

Az azonosítás során a leolvasás két lépésben történik. Az első lépés során a képen meg kell keresni az arc körvonalát, majd eltávolítani a nem kívánt hátteret. A második lépés az arc összevetése az adatbázisban tárolt adatokkal. Erre két matematikai transzformációkon és analízisen alapuló eljárást használnak. Az egyik módszer magát az arcról készült képet, mint különböző árnyalatú foltok halmazát vizsgálja, míg a másik módszer az arc különböző elemeit keresi meg (orr, szemek, csontozat, szemöldök, száj, stb.), és azok egymáshoz viszonyított helyzetét, távolságát vizsgálja. Az összehasonlításra léteznek egyéb, neurális hálókat használó módszerek is, valamint egyes rendszerek több irányból készített felvételek segítségével az arc háromdimenziós modelljét állítják elő és vizsgálják.

A módszer a jövőben a hétköznapi életben is könnyen elterjedhet, a számítógépek mellett egyre sűrűbben előforduló, egyre olcsóbb kameráknak köszönhetően. A felhasznált szoftverekben a megfelelő hibaarány elérése egyes esetekben még jelenleg is kihívás, de ha ezt sikerül elérni akkor is megtéveszthető lehet a rendszer egy jól elkészített maszkkal.

2.5 Módszerek független kombinációja

Tekintve, hogy mindegyik felhasználó azonosítási módszernek vannak kiküszöbölhetetlen, eredendő hiányosságai a kellő biztonság szavatolásához legalább két különböző módszer egyidejű, de mégis független kombinációjának alkalmazása javasolt.

A megvalósítás során komoly hibalehetőség a kombinációk függetlenségének figyelmen kívül hagyása. Rossz megoldásra példa, amikor mágneskártyát és PIN-kódot úgy használnak egyszerre, hogy a PIN-kódot a mágneskártyán tárolják. A mágneskártya tartalma eltulajdonítás után könnyen kiolvasható, a rajta tárolt PIN-kód megismerhető, így az nem jelent külön védelmet. Sőt, ha a PIN-kódot máshol is használják, akkor megszerezve a mágneskártyát még más rendszerekhez is hozzáférés nyerhető. Ekkor a két módszer nemhogy erősítené, de még gyengíti is egymást.

A hazai eSZIG módszertani szempontból minden fentebb említett elvárásnak megfelel, tekintettel arra, hogy az elektronikusan adatokat intelligens chip tárolja, amelyek kiolvasásához PIN-kód szükséges. Továbbá a legkritikusabb folyamatok (mint például határátlépés ellenőrzése) megfelelő adatfelvételezés kialakításával még a biometrikus azonosítási módszerekkel is kiegészíthetőek a letárolt ujjlenyomat, illetve arckép révén.

3. Személyazonosító igazolvány elektronikus megközelítésben

3.1 Nemzetközi kitekintés

A Képviselői Információs Szolgálat által kibocsátott összegzés szerint Európa 17 tagországa már elektronikus személyazonosító kártyát bocsát ki, amely a benne található chip révén nemcsak a hagyományos, személyazonosításhoz szükséges adatokat tartalmazza, hanem számtalan elektronikus szolgáltatás is igénybe vehető a segítségével. A kártyák online használatához kártyaolvasó készülékre, egy letölthető programra, valamint egy nyilvános és egy titkos kódra van szükség. Az e-személyazonosító igazolványok révén hivatalos dokumentumokat, például adásvételi szerződést is *„aláírhatunk"* nyomtatás nélkül, elektronikus környezetben. Az *„aláírást"* ez esetben szintén egy nyilvános és egy, külön erre a célra kapott titkos kód megadása jelenti, amely jogilag egyenértékű a kézzel írt aláírással.

A Svájci Államszövetségben 2010 májusában kezdte meg a SuisseID országos szintű terjesztését a Svájci Posta. A SuisseID az első olyan standardizált termék Svájcban, amely a személyazonosság elektronikus igazolását biztosítja. A SuisseID-val közigazgatási szervek, vállalatok és magánszemélyek egyszerű és biztonságos módon vehetnek igénybe online szolgáltatásokat, és bonyolíthatnak le egymással tranzakciókat. Tekintettel arra, hogy a SuisseID chip kártya formájában kerül forgalomba, könnyedén beilleszthető lesz a SwissStick-be. A két eszköz együttes használatával így jogilag kötelező erejű aláírással ellátott hivatalos dokumentumok elektronikus továbbítására (ajánlott küldeményként) nyílik lehetőség, amelyhez természetesen kérhető a feladás és átvétel tényét bizonyító visszaigazolás is.

A svájciak egy összetett rendszert alakítottak ki, amelyben az eszköz nem ad ki személyes adatokat, sőt az fizikailag is csak a név, az e-mail cím és a SuisseID azonosító számot tartalmazza. Amennyiben az adott ügyintézéshez kapcsolódóan további felhasználói adatok is szükségesek (pl.: állampolgárság, születési idő) akkor azokat a megfelelő felhatalmazások és jogosultságok birtokában a központi szerverről érheti el az érintett alkalmazás a Claim Assertion Infrastructure (CAI) rendszeren keresztül. Tehát a CAI segítségével válhatnak a személyes adatok hozzáférhetővé az alkalmazások számára, amelynek részletes leírását a SuisseID specifikációk tartalmazzák a protokoll- és interfész- definíciók mellett. A felhasználási területet kiszélesítheti, hogy a kártyához kapcsolhatóak különféle addicionális adatok, amelyekkel akár az egyes alkalmazásokhoz kapcsolódó jogosultsági szintek is elkülöníthetővé válnak (pl.: ügyvéd, közjegyző, orvos). Az okmány hatékony és gyors bevezetését közvetlen állami támogatással segítik. Ennek eredményeként a piaci ár feléért, hozzávetőlegesen 12.000 forintnak megfelelő összegért juthatnak a svájciak az innovatív eszközhöz. Az induló szolgáltatások között gyakran említik az adóbevallási szolgáltatásokat és az erkölcsi bizonyítvány igényléseket, de a SuisseID természetesen beválhat elektronikus aláírásként is, amellyel online szerződéseket, dokumentumokat, vagy e-maileket írhat alá a felhasználó. A szolgáltatás terjesztésébe a svájci postát is bevonta a gazdasági tárca, azaz a technológiához rögtön kapcsoltak egy állampolgárokhoz közel álló front-office szolgáltatást.

Szlovákiában 2013 decemberétől igényelhető e-személyi kártya, és az igénylők a kártya mellé ingyen kártyaolvasót, és elektronikus aláíráshoz szükséges kódot is kaphatnak. Elektronikusan is intézhető többek között a lakcímbejelentés, az iparengedély kiváltása, és egyre több bank teszi lehetővé az online számlanyitást.

Észtországban az e-személyi igazolvánnyal okmányirodai, földhivatali, közjegyzői ügyek mellett például az iskolai beíratás is intézhető elektronikusan, de használható tömegközlekedési bérletként is. A helyhatósági, parlamenti választásokon voksolni lehetett vele, és a népszámlálást is ennek segítségével bonyolították le. Az állampolgárok a közigazgatásban róluk tárolt összes adathoz automatikusan hozzáférhetnek, orvosi leleteiket is ily módon láthatják.

Belgiumban a közigazgatási állásokra jelentkezőkkel akár a munkaszerződést is e-személyazonosító kártya segítségével kötik meg. Szociális támogatások is igényelhetők vele az interneten keresztül, és akár vonatjegyként is használható.

Az elektronikus személyi igazolvány nyújtotta szolgáltatások igénybe vétele sehol sem kötelező, a fogadtatása pedig vegyes képet mutat. Finnországban ugyan már 1999-től lehet ekártyát igényelni, ám 2011-ben az 5,4 milliós népességből mindössze 300 ezren éltek a lehetőséggel; igaz, a kártya kiállításának költségei itt minden esetben a kérvényezőt terhelik. Olaszországban is mérsékelt maradt a 14 éve bevezetett kártya népszerűsége, elsősorban azért, mert viszonylag kevés helyhatóság fogadja el az ügyintézés során. Szlovákiában 2014 júniusáig csak az elektronikus személyazonosítót kapó állampolgárok fele kérte, hogy az új kártyában levő chipet aktiválják. Észtországban ugyanakkor teljesen általánossá vált az elektronikus kártyahasználat, 2012-ben már a lakosság 90 százaléka rendelkezett vele. Az 5,65 milliós lakosú Dániában 2014-ben 4,18 millió állampolgárnak volt e-kártyája, közülük 3,2 millióan használják is az elektronikus szolgáltatásokat.

Ausztria 2009-ben tovább lépett az elektronikus közszolgáltatások terén, amikor bevezette a mobil telefonon keresztüli személyazonosítás és elektronikus aláírás lehetőségét. Az ügyintézés ettől kezdve már számítógépet, szoftvert és kártyaolvasót sem igényel, elegendő egy mobiltelefon és az SMS szolgáltatás. 2014 novemberében már 420 ezren rendelkeztek mobiltelefonos elektronikus aláírással, és havonta további 20-25 ezren kérik az ingyenes szolgáltatás aktiválását. Hasonló mobiltelefonos személyazonosítás létezik már Észtországban és Dániában is.

3.2 Jogi háttér

Az intelligens kártyára épülő személyazonosítás fogalmát a kettős felhasználású termékek kivitelére, transzferjére, brókertevékenységére és tranzitjára vonatkozó uniós ellenőrzési rendszer kialakításáról szóló 428/2009/EKrendelet rögzíti, amely szerint elektronikusan leolvasható személyes okmánynak az tekinthető, amely alábbi jellemzők bármelyikével rendelkezik:

– A rejtjelezési képesség csak a jogszabályban meghatározott berendezésben vagy rendszerben történő felhasználásra korlátozódik, és az más célú felhasználásra nem programozható át; vagy
– Rendelkeznek az összes alábbi jellemzővel:
  – kifejezetten úgy tervezték és korlátozták, hogy biztosítsa a benne tárolt személyes adatok védelmét;
  – kizárólag nyilvános vagy kereskedelmi ügyletek, illetve személyazonosítás céljára lett személyre szabva, vagy csak ilyen célra szabható személyre;
  – a rejtjelezési képesség a felhasználó számára nem hozzáférhető.

A polgárok az egyes gazdasági, állami, önkormányzati szolgáltatásokat elektronikus kártyával történő azonosítással, elektronikus kártyák segítségével, informatikai rendszerek útján veszik igénybe. A szolgáltatások számának növekedésével azonban a különböző platformon működő elektronikus kártyák száma is növekszik, hiszen az egyes rendszerek közötti koordinációt és technológiai egységesítést senki sem valósítja meg. A kártyakibocsátók száma folyamatosan nő, viszont jellemző, hogy a szigetszerűen megvalósított fejlesztések egymással nem kompatibilisek, nem átjárhatóak.

Központi rendszer hiányában korábban nem állt rendelkezésre egy olyan megoldás, amely egységesen és hitelesen, az állam által garantált módon, elektronikus úton tudná biztosítani a felhasználók azonosítását; és ezzel személyhez kötött – akár az állam, akár piaci szereplők által garantált – szolgáltatások nyújtását, jogosultságok, kedvezmények igénybevételét.

A fentiekben meghatározott felvetésekre adott választ az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény (NEK tv.), amely alapján az állam az egyes költségvetési szervek és közfeladatot ellátó más szervek, valamint gazdálkodó és civil szervezetek által kibocsátásra kerülő, jogosultságot vagy tényt igazoló, vagy szolgáltatások igénybevételére jogosító kártyák előállítása, kibocsátása, felhasználása és nyilvántartása egységes keretfeltételeinek biztosítása érdekében a Kormány által rendeletben kijelölt államigazgatási szerv (a továbbiakban: működtető) útján egységes elektronikuskártya-kibocsátási keretrendszert (a továbbiakban: NEK) működtet.

A keretrendszer kiépítésével a rendszerben garantált hitelességi, azonosítási funkciók segítségével az eddig szigetszerűen megvalósuló fejlesztések - erre irányuló szándék esetén - sokkal olcsóbban valósíthatóak meg, vagy válthatóak ki. Ebben az esetben ugyanis az egyes szakrendszereknek már nem kell a kártyakibocsátás folyamatának valamennyi aspektusát (azonosítás, arckép-készítés, rendszerfejlesztés, gyártás stb.) megszervezniük; piaci felhasználás esetén elegendő csupán az egységes kártyarendszerhez történő csatlakozást biztosító, jogszabályban meghatározott csatolófelület technikai előírásainak való megfelelést biztosítani, állami felhasználás esetén pedig az ágazati jogszabályok szintjén elrendelni a csatlakozás kötelezőségét, és meghatározni a kapcsolódó ágazati adatkezelés szabályait.

Az egységes elektronikuskártya-kibocsátási keretrendszer tehát nem közvetlen kártya-kibocsátást és -felhasználást jelent, hanem egy olyan jogi-műszaki keretrendszert takar, amely

– megteremti az elektronikus kártyakibocsátás egységesítésének legfontosabb, alapvető technológiai, eljárási, szervezeti és egyéb keretfeltételeit, és
– az állam által biztosított azonosítási szolgáltatással, valamint háttér-adatbázissal (a törvény értelmében: a személyi adat-, és lakcímnyilvántartás segítségével) megszünteti az azonosításhoz kapcsolódó hitelességi hiányosságot, így a nyilvántartás tartalmazza az egyes személyekhez tartozó kártyák adatait, biztosítja az ágazati vagy kereskedelmi rendszerekkel való kapcsolatot, ezzel garantálva azt, hogy az egyes jogosultságok nem a kártyákhoz kapcsolódnak, hanem a ténylegesen arra jogosult személyhez.

Az egyes konkrét felhasználói alkalmazások így a keretrendszernek nem részei, hanem annak megfelelően létrehozott önálló fejlesztések eredményei. A törvény alapján a NEK rendszerében kibocsátott kártya betölthet:

– piaci funkciókat (ez esetben kártyakibocsátó az lehet, akit a kijelölt állami szerv - alapos műszaki és nemzetbiztonsági vizsgálatot követően - hatósági eljárásban kártyakibocsátásra feljogosít);
– állami funkciókat (ebben az esetben a kártyakibocsátó kijelölése ágazati törvényben történik meg, kibocsátó pedig csak költségvetési szerv és közfeladatot ellátó más szerv lehet).

A személyazonosító igazolványra vonatkozó alapvető rendelkezéseket az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról szóló 2015. évi CXXX. törvény állapította meg. Továbbá a – már korábban – 2014. év végén elfogadott az elektronikus közigazgatás kiterjesztésével kapcsolatos feladatokról szóló 1743/2014. (XII. 15.) Korm. határozat 9. pontja előírta, hogy létre kell hozni az elektronikus tároló elemet tartalmazó (vizuális és elektronikus) személyazonosításra és elektronikus aláírásra alkalmas okmányt (e-kártya), amely biztosítja az állampolgárok számára, hogy egyetlen okmány használatával intézhessék hivatalos ügyeiket, kiemelten az adóigazgatási eljárásokat és a társadalombiztosítási ellátások igénybevételét, ezáltal alkalmas a TAJ-kártya és az adóigazolvány kiváltására, és legyen alkalmas egyes közlekedési szolgáltatások igénybevételére is.

Az e-kártyától elvárt funkcionalitást az e-személyazonosító igazolvány testesíti meg, amely 2016. január 1-ei bevezetésének alapvetően két fő célja volt:

– egyrészt az okmány biztonságának növelése;
– másrészt az elektronikus kormányzás és az elektronikus ügyintézés egy új, interoperábilis elérést biztosító hordozó eszköz megteremtése, amely EIDAS rendelet követelményeit teljesíti.

Az e-kártya olyan okmány, amely a funkciók lépcsőzetes bővítését követően, biztonságos módon egyesít különböző vizuális és elektronikus személyazonosításhoz kapcsolódó elemeket. Az új e-kártyához a bevezetéskor első szakaszban három közvetlen szolgáltatás kapcsolódik, amely azóta kiegészült a közlekedési szolgáltatások támogatásával is:

– Az eSIGN (e-aláírás) által lehetővé válik elektronikus dokumentum – elsősorban – magánszemély általi, minősített elektronikus aláírása, teljes bizonyító erejű magánokirat elektronikus elkészítése. A törvény szerint a polgár kérésére a kártya tartalmazza az elektronikus aláírás szolgáltatást is. Az e-aláírást (vagy eSigniture) a Nemzeti Infokommunikációs Szolgáltató Zrt. biztosítja. Használatához szükséges maga a személyigazolvány, egy email cím, egy kártyaolvasó és egy számítógép. Az e-aláírás 2016-ban biztonságos aláírás-létrehozó eszközként (BALE) lett tanúsítva, így minősített biztonságú aláírás hozható létre vele, valamint igénybe vehető szintén a NISZ által biztosított időpecsét szolgáltatás is.
– Az eID (elektronikus azonosítás, illetve hitelesítés) kártyafunkció más azonosítási rendszernél magasabb hatásfokkal és biztonsági szinten képes biztosítani az elektronikus kormányzati és e-közigazgatási rendszerek igénybevételéhez szükséges elektronikus azonosítás funkciókat. Az e-azonosítás funkció egyrészt biztosítja a személyes azonosítást, másrészt elektronikus ügyintézés során hitelesítést biztosít a távoli eléréshez, például az ügyfélkapu használatához. Utóbbi szolgáltatáshoz kártyaolvasóra van szükség.
– Az ePASS (úti okmány) kártyafunkció az európai utazások során teszi lehetővé az elektronikus úti okmány funkciók használatát, ugyanis az elektronikus úti okmány minden olyan határátlépésnél felhasználható, ahol a schengeni, vagy más államközi egyezmények által szabályozott hozzáférési jogosultsággal rendelkező rendszerek, tehát pl.: zsilipkapus beléptető rendszerek üzemelnek. Az útlevéllel azonos biztonságos utazást jelentő ePASS szolgáltatás eléréséhez az állampolgárok ujjlenyomatát is elektronikusan rögzíteni szükséges a kártyában.
– eNEK funkció – 2016. november 14-étől egyes közlekedési szolgáltatások igénybevételét támogató alkalmazás kártyán való elhelyezése is megvalósult. A korábban kibocsátott kártyákra utólagosan feltölthető az alkalmazás (kormányablakokban, bérletpénztárakban (MÁV), interneten keresztül otthon).

3.3 e-Személyazonosító igazolvány

A személyazonosító igazolvány a polgár írásbeli nyilatkozata, valamint az anyakönyv és a nyilvántartás – nem magyar állampolgár esetén ezeken túlmenően a polgár útlevele és a magyarországi tartózkodásának jogcímét igazoló közokirat – alapján kiállított olyan hatósági igazolvány, amely a polgár személyazonosságát és a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvényben (a továbbiakban: Nytv.) meghatározott adatait közhitelűen igazolja.

A személyazonosító igazolvány fajtái:

– az állandó személyazonosító igazolvány;
– az ideiglenes személyazonosító igazolvány.

A személyazonosító igazolvány adattartalma

Az Nytv. 29. § (2) bekezdése szerint az állandó személyazonosító igazolvány vizuálisan észlelhető módon tartalmazza

a) a polgár nevét,
b) a polgár születési helyét,
c) a polgár születési idejét,
d) a polgár állampolgárságát,
e) a polgár anyja nevét,
f) a polgár nemét,
g) a polgár arcképmását,
h) a polgár aláírását, ha 12. életévét betöltötte, valamint nem írásképtelen vagy írástudatlan,
i) a polgár személyazonosító igazolványa érvényességi idejét,
j) a polgár személyazonosító igazolványa okmányazonosítóját,
k) a polgár személyazonosító igazolványa kiállításának idejét,

A minta személyazonosító igazolvány előlapja

A minta személyazonosító igazolvány hátoldala

3. ábra. Vizuális megjelenés előlap és hátoldal
Forrás: https://eszemelyi.hu/uj_eszemelyi/altalanos_informaciok

l) a polgár személyazonosító igazolványát kiállító hatóság nevét,

m) az Nytv. 29. § (4) bekezdés szerinti tényt vagy a 29/G. § (1) bekezdésében foglalt esetekben – jogszabályban meghatározott nem olvasható formában – a külföldre utazási korlátozás tényét.

A fentiek mellett kiemeljük, hogy az okmány jogszabály által meghatározott vizuális adattartalma nem azonos az okmányon elhelyezett biztonsági elemekkel.

A személyazonosító igazolvány előlapján és hátlapján látható elemek nem egyenlőek annak adattartalmával. A személyazonosító igazolvány vizuálisan észlelhető módon tartalmazza az Nytv. 29. § (2) bekezdésében meghatározott adatokat, továbbá gépi olvasásra alkalmas adatsort [Nytv. 29. § (3) bek.], külföldi állampolgárságú vagy hontalan polgár részére kiállított állandó személyazonosító igazolvány tartalmazza annak tényét, hogy az állandó személyazonosító igazolvány külföldre történő utazásra nem jogosít [Nytv. 29. § (4) bek.], tároló elemben rögzített adatokhoz történő jogszerű hozzáférést biztosító protokoll elindításához szükséges kódszámot [Nytv. 29. § (5) bek.], adattároló kódot [Nytv. 29. § (6) bek.], tároló elemet [Nytv. 29. § (7) bek.].

A chip adattartalma

Az állandó személyazonosító igazolvány 2016. január 1-jétől elektronikus adathordozó egységet, tároló elemet (chip) tartalmaz. A tároló elem elektronikus formában tartalmazza valamennyi személyes adatot és okmányadatot, amely az állandó személyazonosító igazolványon vizuálisan is megjelenik. A tároló elem ezen adatokon kívül az alábbi adatokat tartalmazza:

– a polgár ujjnyomatát, kivéve, ha
– a személyazonosító igazolvány kiállításakor a 12. életévét még nem tölti be,
– az ujjnyomat rögzítését visszautasította, vagy

– ujjnyomat adására fizikailag képtelen;
– (az állampolgár kérelmére) az elektronikus aláírás létrehozásához szükséges adatot és az állampolgár aláíró tanúsítványát,
– a polgár társadalombiztosítási azonosító jelét,
– a polgár adóazonosító jelét,
– a személyazonosító igazolvány elektronikus egyedi azonosítóját és
– a polgár kérelmére legfeljebb kettő, vészhelyzet esetén értesítendő telefonszámot.

Az eSzemélyi kártyaokmány jelenleg elérhető funkciói

– ePASS (elektronikus úti okmány) funkció;
– eID (e-azonosítás) funkció;
– e-SIGN (e-aláírás) funkció;
– eNek (közlekedés támogatás) funkció.

A hazánkban 2016. január 1-jétől rendszeresített elektronikus személyi igazolvány – illetve a kapcsolódó technológia fejlettségi szintje – lehetővé teszi azt a korábban elképzelhetetlen megoldást, hogy az állampolgárok azonosítása, illetve hitelesítése az elektronikus térben közhiteles adatokra építve nagybiztonsággal (azaz több azonosítási módszert is ötvöző megoldással) elvégezhető legyen. Az eSZIG olyan szolgáltatási lehetőségeket és fejlődési perspektívát hordoz magában mind az állampolgárok (távoli ügyintézés), mind a vállalkozások (azonosításon alapuló online szolgáltatások), valamint a gazdasági élet szereplői, illetve az állam (további e-közigazgatási szolgáltatások) számára, amelyre érdemes odafigyelni, és a várható igényekre a közigazgatás oldaláról is szükséges felkészülni.

4. Szolgáltatások

4.1 Elektronikus aláírás

Az elektronikus aláírás gyakorlatilag az e-Személyiazonosító igazolványhoz kapcsolódó horizontális (ágazat független) szolgáltatásnak tekinthető.

Az elektronikus aláírás szolgáltatás által lehetővé válik elektronikus dokumentumok magánszemély általi elektronikus aláírása, illetve időbélyegzése. Így az elektronikus személyi igazolvány felhasználható különböző ügyek elintézésére, például az e-közigazgatási folyamatokban például eHR rendszer.

Az e-aláírás és az időbélyegzés szolgáltatás összefügg egymással: míg az elektronikus aláírás azt igazolja, hogy ki írta alá a dokumentumot, addig az időbélyegző lényegében azt igazolja, hogy mikor történt az aláírás.

*„Az **elektronikus aláírás** (e-aláírás) az elektronikus dokumentumhoz hozzárendelt adatsor. Az e-aláírás minden kétséget kizáróan bizonyítja a dokumentum eredetét, hitelességét, sértetlenségét, és azonosítja az aláíró személyét, illetve biztosítja az aláírás letagadhatatlanságát.*

A vonatkozó jogszabályok rendelkezései szerint az e-aláírást a bíróság is elfogadja bizonyítékként egy esetleges peres ügyben.

Ha valaki e-aláírás szolgáltatást igényel az eSzemélyihez, akkor az okmány tároló elemén (chip) létrehozásra kerül egy ún. kulcspár, amely egy egyedi elektronikus adat, és amely két részből áll: egy ún. magánkulcsból (aláírás-létrehozó adat), és egy ún. nyilvános kulcsból (aláírás-ellenőrző adat). Az e-aláírás az eSzemélyin levő magánkulccsal készül. Kizárólag a magánkulcs párjával, a nyilvános kulccsal lehet ellenőrizni az aláírás eredetiségét, az aláírt elektronikus dokumentum sértetlenségét. Ha az aláírt dokumentumban változtatás történik, akkor az elektronikus aláírás nem fejthető vissza. A nyilvános kulcs és az aláíró személyének összetartozását egy tanúsítvány igazolja. A tanúsítvány egy szabványos mezőkből álló elektronikus igazolás, amelyet a kulcspár előállítását követően a kormányzati hitelesítés szolgáltató bocsájt ki és helyez el a személyi igazolvány tároló elemén. Elektronikus aláíráskor a tanúsítvány hozzákapcsolódik az aláíráshoz illetve az aláírt dokumentumhoz. Mivel a tanúsítvány tartalmazza a nyilvános kulcsot és a tulajdonos nevét, a dokumentum olvasója (a fogadó fél) meg tudja állapítani, ki írta alá a dokumentumot, illetve ellenőrizni tudja az elektronikus aláírást.

*Az **időbélyegző** az elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyeg elhelyezésének időpontjában változatlan formában létezett."*[1]

Az elektronikus aláírás alkalmazásának lehetőségei és korlátai

A ma kibocsátott eSZIG-hez a legerősebb, legszélesebb alkalmazhatóságot biztosító aláírások kapcsolódnak. Az e-aláírás funkcióval minősített elektronikus aláírás hozható létre. Az aláírás lehetőséget ad arra, hogy az állampolgárok magánjogi vagy közigazgatási jogügyleteikben elektronikusan tehessenek teljes bizonyító erejű magánokiratnak megfelelő joghatással bíró jognyilatkozatokat, illetve az Európai Unióban a minősített elektronikus aláírás a saját kezű aláírással azonos joghatású. Érdemes megjegyezni, hogy a nemzeti és az európai uniós szabályozási elvek szerint az elektronikus aláírás, illetve dokumentum elfogadását megtagadni, jognyilatkozat tételére, illetve joghatás kiváltására való alkalmasságát kétségbe vonni – néhány jogviszonyt kivéve – nem lehet kizárólag amiatt, hogy az aláírás, illetve dokumentum elektronikus formában létezik.

Magyarországon az elektronikus aláírással rendelkező magánszemélyek néhány speciális jogügylet kivételével szinte bármilyen jogügyletben tehetnek elektronikus jognyilatkozatot. Kivételt képeznek a speciális formai elvárásokhoz kötött jogügyletek (pl.: az ingatlanforgalmi szerződések), a bírósági eljárások egyes típusai, valamint a Ptk.-ban szabályozott családjogi, élettársi kapcsolati, öröklésjogi jogviszonyok (pl.: a végrendelet, házasságkötés). A jogszabályok az elektronikus

[1] Forrás: Nemzeti Infokommunikációs Szolgáltató Zrt.: Tájékoztató a személyazonosító igazolványhoz igényelhető e-aláírással kapcsolatos szolgáltatásokról.

ügyintézés során biztosítják az elektronikus aláírás felhasználhatóságát a határon átnyúló ügyekben is.

Elektronikus aláírásra épített szolgáltatási lehetőségek

Figyelembe véve, hogy a minősített elektronikus aláírás teljes egészében kiválthatja a papíralapú ügymenetet az üzleti életben, illetve az állammal való kapcsolattartást is át tudja helyezni digitális alapokra – amennyiben ezt a terültre vonatkozó jogszabály megengedi – gyakorlatilag a lehetőségek tárháza végtelen.

A versenyszférában számtalan olyan hitelesítést igénylő szolgáltatás van, amelyet elektronikus útra terelve jelentős költségmegtakarítás lenne elérhető, illetve az átfutási idők is érdemben lerövidíthetővé válnának. Ilyen szolgáltatások lehetnek például:

- elektronikus számlázás,
- elektronikus szerződéskötés és módosítás,
- vállalkozások közötti kötelezettségvállalások, szolgáltatók és felhasználók, vagy eladók és vásárlók közötti szerződések, stb.,
- elektronikus számlanyitás (pl.: pénzintézeteknél),
- hiteles elektronikus változásbejelentés megtétele (pl.: költözésnél szolgáltató felé),
- stb.
- hivatalos levelezés,
- tanúsítványok, oklevelek hivatalos kiadása,
- stb.

A közigazgatási ügyeket figyelembe véve számos olyan eset van, ahol jelentős adminisztratív teher lenne megtakarítható az elektronikus aláírás bevezetésével (illetve kötelező használatával). (Természetesen ehhez nem csak elektronikus aláírás, hanem elektronizált ügytípusok és kapcsolódó rendszerek is szükségesek.) Ilyen szolgáltatások lehetnek például:

- különböző hatósági igazolások,
- minden olyan bejelentés/ügy, ahol ma az állampolgárnak személyesen kell bemennie, és aláírásával hitelesített módon, papír alapon beadnia igényét az állami, illetve önkormányzati igazgatás intézményrendszere irányába, és az aláíráson túl nincs érdemi jelentősége a személyes megjelenésnek (több 100 érintett ügytípus),
- hatóság, állampolgár közötti kommunikáció, vagy egészségügyi intézmény-állampolgár közötti kommunikáció (pl.: diagnózis hiteles megküldése, hiteles adatcsere),
- stb.

4.2 Kiterjesztési lehetőségek

Az eSZIG kiemelt potenciállal rendelkezik a digitális térben történő hatékony és biztonságos személyazonosításra, illetve hitelesítésre, mivel a kapcsolódó infrastruktúra relatíve olcsón kiépíthető, és a központi szolgáltatások hozzáférhetőek, továbbá olyan biztonságos megoldás, amely az azonosítás különböző típusait (tudás alapú, birtok alapú, biometrián alapuló módszereket) ötvözve biztosítja – központi azonosítási rendszerrel való tranzakció szintű kommunikáció útján – az adott személy közhiteles azonosítását. Tehát az elektronikus személyazonosító igazolvány biztosítani képes a közhiteles adatbázisokkal való biztonságos kommunikációt és a kapcsolódó hitelesítést/azonosítást, továbbá megfelelő infrastruktúra (kártyaolvasó és adatátviteli hálózat) kiépítésével bárhonnan könnyen és gyorsan használható, a kapcsolódó szolgáltatásokkal egyszerűen és költséghatékonyan integrálható.

Az eSZIG kaput nyit a digitális transzformáció továbbvitelére számos szolgáltatási elem tekintetében, mint például:

- fizetési tranzakciók támogatása, készpénz kímélő megoldások elterjedésének támogatása;
- fizikai beléptető rendszerekben és épület beléptető rendszerekben alkalmazott kártyák kiváltása;
- gyors autentikáció biztosítása tömeges beléptetéseknél;
- on-line szolgáltatások autentikációs eljárásainak magasabb szintre emelése;
- igazolások rendszerének megújítása (pl.: lakcímkártya, TAJ kártya, adókártya, egyéb kártya integráció).

Ágazati megközelítésben az eSZIG-en mint *„okos"* kártyán alapuló megoldások új alapokra helyezhetik a(z)

- közlekedést (például: eSzemélyi mint bérlet, illetve e-jegy alkalmazása);
- egészségügyet (például: recept kiváltása, e-vény integráció);
- szociális kedvezmények rendszerét (például: eSZIG-hez kötött juttatáskezelés);
- oktatást (például: felvételi rendszer hozzáférés, diákhitel igénylés);
- pénzintézeti ágazat (például: tranzakció kezelés új biztonsági szintre emelése az eSZIG révén);
- sportrendezvények szervezését (például: beléptető rendszerek támogatása).

A fent bemutatott megoldások igazgatási és technológiai szempontból belátható időn belül megvalósulhatnak, sőt pilot kezdeményezések folyamatban vannak jelenleg is például a közlekedés területén. A MÁV az eSZIG-re alapozva alakítottak ki a bérletszolgáltatást Budapest-Pusztaszabolcs viszonylatban. A vasúti bérletinformációkat az igazolvány chipje tárolja, az utasok így eSZIG-el igazolhatják az utazásra szóló jogosultságukat. A MÁV a szolgáltatás igénybevételének ösztönzésére 3 % kedvezményt is nyújt a viteldíjból, amelynek megvásárlására Budapest Déli pályaudvaron és Pusztaszabolcson, valamint Százhalombattán nyílik jelenleg is lehetőség. A tapasztalatok alapján a személyi igazolványokra elektronikusan felírt vasúti bérleteket a jegyvizsgálók offline módon is biztonságosan és gyorsan ellenőrizhetik, a vásárlás pedig egyszerűbb és gyorsabb.

Az ilyen és ehhez hasonló pilot kezdeményezések adhatnak lendületet több közlekedési társaság számára, hogy eSZIG-re alapozott fejlesztésekbe fogjanak. Fontos cél, hogy a közlekedés mellett a jövőben újabb szolgáltatások és kártyafunkciók kapcsolódjanak az eSZIG-hez, ezzel az állampolgárok oldalán egyszerűbbé, a (köz)szolgáltatók oldalán pedig biztonságosabbá és olcsóbbá téve a digitális megoldások használatát.

Az eSZIG technológiai keretek mára gyakorlatilag adottak, a jogi szabályozás is lehetőséget biztosít – sőt több esetben kötelezettséget ír elő – az alkalmazásra, így az intézményrendszeren, a rendszertervezők kreativitásán, a felhasználóbarát szempontokat figyelembe vevő kivitelezésen, és az állampolgári adaptációs készségen múlik, hogy kihasználjuk-e az állam által biztosított eSZIG-ben rejlő lehetőségeket.

Források

Budapesti Műszaki és Gazdaságtudományi Egyetem, SEARCH Laboratórium – Távoli személyazonosítási technikák

Krimináltechnika, BM Könyvkiadó 1992.

Postgate, John Nicholas: Az asszír és a babilóniai birodalom, Budapest, Helikon Kiadó, 1985.

Dawson, Raymond Dawson: A kínai civilizáció világa, Osiris, 2002.

A magyar nyelv értelmező szótára I–VII. kötet szerkesztette A Magyar Tudományos Akadémia Nyelvtudományi Intézete Akadémiai Kiadó; Első kiadás: 1959–1962

Nagy Pál – Papp József: *Személyazonosító okmányok a XIX–XX. századi Magyarországon* (In: Hajdú-Bihar Megyei Levéltár Évkönyve XXIX)

http://index.hu/belfold/2015/12/29/2016-tol_megujulnak_a_szemelyi_igazolvanyok/

Elektronikus Személyazonosító Kártya. Képviselői Információs Szolgálat. Info Jegyzet, 2015/26. Letölthető: http://www.parlament.hu/documents/10181/303867/2015_26_e-kartya/3e64ca47-7986-47d4-a43b-48822fe0b8c8 p2

E-SZIG információk: https://eszemelyi.hu/

Álló Géza – Hegedűs Gy. Csaba – Kelemen Dezső – Szabó József: *A Digitális képfeldolgozás alapproblémái,* Akadémiai Kiadó, Budapest, 1989

http://www.parlament.hu/documents/10181/303867/2015_26_e-kartya/3e64ca47-7986-47d4-a43b-48822fe0b8c8

SuisseID Specification Digital Certificates and Core Infrastructure Services (Version 1.2 b) http://www.suisseid.ch/

http://hiteles.gov.hu/cikk/50/eszig_e-alairas_informaciok

Biztostű informatikai biztonságot oktató portál az Informatikai és Hírközlési Minisztérium, az Oktatási Minisztérium és a Search-Lab Kft. támogatásával (www.biztostu.hu) Hozzáférés ideje: 2004. (Archivált webes tartalom).

Nemzeti Infokommunikációs Szolgáltató Zrt.: Tájékoztató a személyazonosító igazolványhoz igényelhető e-aláírással kapcsolatos szolgáltatásokról

Krasznay Csaba: BME Informatikai Központ: *Elektronikus aláírás használatának lehetőségei és hatásai a gazdasági életben tárgyú prezentáció*

Dósa Imre – Polyák Gábor: *Informatikai jogi kézikönyv.* KJK-Kerszöv, Budapest, 2003.

E-aláírás funkció. https://eszemelyi.hu/kartya_funkcioi/e_azonositas_kartyafunkcio

E-azonosítás funkció

http://www.kekkh.gov.hu/Eszemelyi/kartya_funkcioi/e_azonositas_kartyafunkcio

Elektronikus aláírás.

http://www.kekkh.gov.hu/Eszemelyi/gyik/gyik_elektronikus_alairas

Elektronikus Személyazonosító Kártya. Képviselői Információs Szolgálat. InfoJegyzet, 2015/26. Letölthető: http://www.parlament.hu/documents/10181/303867/2015_26_e-kartya/3e64ca47-7986-47d4-a43b-48822fe0b8c8

eGovernment Benchmark Report 2015. Country Factsheet Hungary. Letölthető: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9822

eGovernment Factsheets 2016. Hungary. Letölthető: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment%20in%20Hungary%20-%20February%202016%20-%2018_00%20-%20v3_00.pdf

Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala – 2016: Megújult a személyazonosító igazolvány

http://www.kekkh.gov.hu/Eszemelyi/kartya_funkcioi/e_uti_okmany_funkcio

The Case for E-Government: Excerpts from the OECD Report "The E-Government Imperative" by the OECD E-Government Task Force (Tim FIELD, Elizabeth MULLER and Edwin LAU) OECD Journal on budgeting– VOL. 3, NO. 1 – ISSN 1608-7143 – OECD 2003.

Uniós e-kormányzati cselekvési terv 2016–2020. A közigazgatás digitális átalakításának felgyorsítása. Letölthető: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52016DC0179&from=EN

Uniós e-kormányzati cselekvési terv 2016–2020 A közigazgatás digitális átalakításának felgyorsításáról

910/2014/EU rendelet (a továbbiakban: „eIDAS rendelet"), az egész EU területére kiterjedően határozza meg az elektronikus tranzakciók szabályait