HADMÉRNÖK

XII. Évfolyam „KÖFOP" szám – 2017. október

ADATVÉDELEM ÉS ADATBIZTONSÁG AZ ELEKTRONIKUS OKMÁNYOKNÁL

DATA PROTECTION AND DATA SECURITY OF ELECTRONIC IDENTIFICATION DOCUMENTS

SZÁDECZKY Tamás

(ORCID: 0000-0001-7191-4924)

szadeczky.tamas@uni-nke.hu

Absztrakt

Hazánkban a biometrikus útlevél 2006-os megjelenését követően egy évtizeddel később bevezetésre került az elektronikus személyazonosító igazolvány. Az új típusú okmányok megjelenésének oka a biztonsági paraméterek megerősítése mellett új funkciók bevezetése.

Tanulmányomban elemzem az adatok tárolására alkalmas kártyák generációit és főbb jellemzőit, a passzív tárolástól a chipkártyákig, beleértve a biometrikus útlevelet is. Részletesen elemzem továbbá az elektronikus személyazonosító igazolvány adattartalmát, személyesadat-védelmét, és funkcióit (ePASS, eID, eSIGN), valamint az eID típusú okmányok biztonsági veszélyeit és védelmi lehetőségeit.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Zrínyi Miklós Habilitációs Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *elektronikus személyazonosító okmány, biometrikus útlevél, okmányvédelem*

Abstract

The biometric passport has been introduced in Hungary in 2006. A decade later the electronic identity card (eID) was implemented. The reason of the improvement of such document is twofold: enhancing security features and implementing new functions.

The paper analyses the generations and properties of data storage cards from the passive elements to the chipcards, including the biometric passport. Furthermore, the data elements, data protection and the functions (ePASS, eID, eSIGN) of the new Hungarian identity card, as well as the security risks and protection properties of the eID-type documents are being analyzed.

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Miklós Zrínyi Habilitation Program.

Keywords: *e-ID, e-Passport, protection of Government Issued Documents*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.24.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.10.27.

BEVEZETÉS

A beléptetés, személyazonosítás alapvető eszköze a kártya, amelyet a birtoklás alapú azonosítás eszközeként az objektumbeléptetéstől a hatósági személyazonosításig széles körben használunk.

Az elektronikus adatkártyák célja az adatok tárolása általános, azonosítási vagy hozzáférési célból. Ezeket az eszközöket tárolási módszer és az eszköz fajtája alapján tipizáljuk. Mind a tároló kapacitás, a biztonság és a felhasználhatóság is ezen eszközök fajtájától függ.

A legegyszerűbb adattárolási lehetőséget a passzív megoldások, mint a lyukkártyák, a vonalkódok, és a bankkártyáknál is alkalmazott mágneskártyák jelentik. Ezeket a megoldásokat régóta használják a hatósági okmányok esetében, elsősorban a hatékony gépi adatfeldolgozás biztosítása végett.

ADATTÁROLÁS A KÁRTYÁN

A legrégebbi adatkártya a lyukkártya, amely egy papír alapú hordozón lyukakban illetve a lyukak hiányában hordozta az adatot. A kártya leolvasása kontakt elektronikus (a két egymással szemben lévő érintkező összeér-e vagy sem) illetve optikai (a fény átvilágít-e a lyukon vagy sem) lehet. A kártyán igen kevés adat tárolható, 80-90 bájt, valamint használata is igen lassú és nehézkes. Alapvetően adattárolási eszközként használták a számítástechnika hajnalán, ma már gyakorlati jelentősége nincs. Az elv használható azonosítási célra is, például menzán az étkezési jegy egy műanyag kártya, amelyen az elhelyezett furatok jelölik a sorszámot. A kártyát optikai úton leolvasva, a kártya jogosultsága az adott napszakban való étkezésre megállapítható a pénztári számítógépen lévő adatbázissal való összehasonlítás után. A kártya eredetiségének megállapítása szemrevételezéssel történhet, egyszerűsége miatt felügyelet nélkül nem alkalmas az azonosításra.

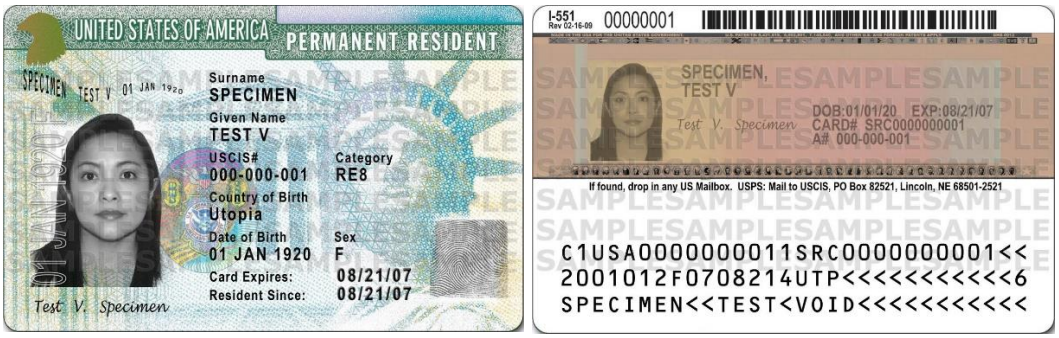
A hagyományos, mindenki által jól ismert adatkártya típus a mágneskártya. Itt az adathordozó egy plasztik lapra épített mágnesezhető fémcsík. Ennek leolvasása a szalagos magnóból ismert mágneses olvasófejek segítségével történik, tehát megköveteli a kontaktust a kártya és az olvasó között. A technológiát több szabvány, például az ISO 7811, ISO 7812, ISO 7813, ISO 4909 határozzák meg. A tárolható adatmennyiség itt is korlátos, nagyságrendileg 100 bájt. Egy bankkártya esetén például ugyanazok az adatok kerülnek eltárolásra, mint ami a kártyán is látható, kiegészítve pár ellenőrző adattal. [1] Ennek a használata még mindig folyamatos, egyszerűsége miatt. Azonosításra felügyelet nélkül is alkalmas. PIN kód használatával biztonsága jelentős mértékben növelhető. A hamisítása a mágnes csík leolvasásával és egy üres kártya felmágnesezésével történhet, nem igényel számottevő felkészültséget. Ebből kifolyólag a szemrevételezéssel történő azonosításnak itt is jelentősége van. Emiatt (is) vannak a bankkártyákon jellemzően hologramos okmánybiztonsági elemek.

Szintén használatos a vonalkódos kártya, amely egy vagy kétdimenziós vonalkódban tárolja az adatot. Az így tárolható adatok mennyisége kisebb, mint a mágneskártyán tárolható, egydimenziós (lineáris) vonalkód esetén pár bájt. Az adat kódolása nemzetközi szabványok alapján történik, széleskörűen az 1978-ban bevezetett EAN 8 vagy EAN 13 kód használatos. A Magyar Köztársaságban az adóigazolványon és a társadalombiztosítási igazolványon is az Adóazonosító jelet illetve Társadalombiztosítási azonosító jelet is egydimenziós vonalkódban tüntették fel a kártyán. A lineáris vonalkód továbbfejlesztéseként jelent meg a négyzetes adatmátrixkód a ’90-es évek elején. A fekete-fehér adatmátrixnak az adattároló-kapacitása elérheti a 2335 alfanumerikus karakterszámot. [2] Legismertebb változata a nyomdatechnikailag könnyen előállítható PDF417 kódrendszer, amelyet a belügyi és rendvédelmi szervek szolgálati igazolványain is alkalmaznak. Az igazolvány teljes adattartalmát kétdimenziós vonalkódban is feltüntetik.Az ABEV program a számítógéppel

kitöltött adóbevallásokon is használja ezt a kódrendszert. Ehhez hasonló a manapság divatos, az 1. ábrán látható QR kód is, amely a kialakításának köszönhetően könnyen leolvasható mobil eszközökkel is.

1. ábra QR kód [3]

Ezen módszerek hátránya, hogy a vonalkód fénymásolható, leolvasható, hamisítható. Ennek megelőzésére egy speciális fedőréteggel lehet ellátni a vonalkódot, amelyet így például csak infravörös fény segítségével lehet megjeleníteni. Ezzel a módszerrel nagymértékben nehezíthető a hamisítás.



2. ábra USA Letelepedési engedély korábbi változata [4]

Költségessége miatt kevéssé elterjedt módszer a lézerkártya. Ennél a kemény műanyag hordozón a kompakt lemezhez hasonló technikai megoldással 1,6-3,5 cm szélességben lézersugárral kiolvasható adathordozó csík található. Ilyet Magyarországon nem használnak, de a Kanadában, az Amerikai Egyesült Államokban, Costa Ricán és Olaszországban különböző állampolgárságot és Indiában gépjármű-regisztrációt igazoló okmányokon így oldották meg a digitális adat tárolását. A tárolható adat mennyisége az eddigi módszereknél jóval nagyobb, 1,1MB, 1,8 MB vagy 2,8MB. A 2. ábra felső sorában egydimenziós vonalkód, alatta optikai (lézeres) tároló, legalul MRZ kód (Machine Readible Zone) látható, ami gépi adatbeolvasást egyszerűsíti.

Az eddig ismertetett kártyák közös jellemzője, hogy adattartalmukat nem, vagy igen nehezen lehet megváltoztatni és nem tartalmaznak aktív elemet, amely lehetővé tenné biztonságosabb felhasználásukat. Amennyiben szükséges a tárolt adatok megváltoztatása, valamely egyéb módszert kell bevezetni. Egyszerű megoldásként említhető a kilencvenes években Olaszországban használt telefonkártyák módszere, ahol a kártyán lévő fehér csíkra (a biztonság miatt szükségszerűen különleges festék alkalmazásával) a letelefonált egységekkel arányosan a telefon fekete téglalapokat nyomtatott. A telefonkártya addig volt használható, amíg volt rajta szabad fehér felület. Ennek ellenőrzése optikai úton történt. A mágneskártyák adattartalma is változtatható, amennyiben elhelyezünk a leolvasóban egy törlőfejet is.

Ezeknél komplikáltabb és biztonságosabb megoldás a memória-áramkörök alkalmazása, ahol is a plasztik kártyába egy elektronikus úton újraprogramozható, nem felejtő memória-áramkört (EEPROM) ültetve azon adatot lehet tárolni illetve módosítani lehet azt. Ilyet alkalmaznak például a magyar telefonkártyákban. A hamisítás kommersz memória-áramkörök használata esetén nem túlzottan nehéz, valamint a csatlakozópontok kivezetésével és számítógéphez való illesztésével a működés emulálására program írható, megtévesztve az olvasó eszközt. [5]

A kártyák felhasználását forradalmasította az aktív kártyák bevezetése, amelyeken nem csak írni-olvasni lehet az adatokat, hanem a kártya képes adatfeldolgozási és más matematikai műveleteket végezni. Az aktív kártyák központi eleme a mikrokontroller. A mikrokontroller gyakorlatilag egy darab áramköri lapkán (chip) megvalósított kvázi komplett számítógép. Egy tokban megtalálható benne a processzor, a nem felejtő memória (ROM, FLASH) és a tetszőleges hozzáférésű memória (RAM), a ki- és bemeneti egységek (I/O) valamint egyéb kiegészítő elemek (például óra, komparátor stb.). Ez, mint aktív elem, lehetővé teszi a negyedik generációs kriptorendszerek implementálását, aktív védelmet biztosítva a tárolt adatoknak illetve a hozzáférésnek. A tárolókapacitása a típustól függően 1-256 kilobájtos nagyságrendű lehet. Mikrokontroller alkalmazásával kialakíthatunk kontakt és nem kontakt (érintés nélküli) adatkártyákat is. Ilyen kontakt adatkártya a smart card (intelligens kártya, chipkártya). Ilyet alkalmaztak Magyarországon a régi típusú felsőoktatási diákigazolványban valamint a bankkártyákon (EMV chip) is. Ez az elsődleges eszköze az elektronikus aláírás magánkulcsa tárolásának is (ez BALE-n, biztonságos elektronikus aláírás létrehozó eszközön történik). Több féle nemzetközi szabvány foglalkozik a chipkártyákkal, mind funkcionális, mind biztonsági szempontból. [6] Ilyen funkcionális szabvány például az ISO/IEC 7816. Az adatkártya kiolvasásához közvetlen érintkezés kell a leolvasóval, amely így közvetlen villamos kapcsolatot létesít a mikrokontroller kivezetéseivel. Értelemszerűen ez a leggyorsabb és legbiztonságosabb módja az adatátvitelnek.

A mikrokontrolleres aktív adatkártya nem kontakt megvalósítása a proximity kártya (RFID, rádiós kártya). Az ebben alkalmazott aktív eszköz alapvetően megegyezik a intelligens kártyában alkalmazottal, lényegi különbség az, hogy a leolvasóval való kapcsolata rádiófrekvencián történik. A működési elve az, hogy az adatkártyán egy nagy tekercsantenna található, amely össze van kötve a mikrokontrollerrel. Alap kiépítés szerint a kártya áramforrást nem tartalmaz, a működéséhez szükséges energiát a leolvasó által gerjesztett elektromágneses térből veszi fel. Tehát a leolvasóhoz közelítve a kártyát, az automatikusan bekapcsol és meghatározott modulált jelet sugároz ki, például elküldi a kártya azonosítószámát. A leolvasó ellenőrzi, hogy az adatbázisában szerepel-e ez az azonosítószám és ennek függvényében például engedélyezi a belépést. Könnyen felismerhető ennek a rendszernek a hibája, ugyanis az adat kinyeréséhez csak az adott frekvenciájú elektromágneses térre van szükség. Tehát bármilyen leolvasónak „elárulja” a kártya az azonosítószámát, így a rosszindulatú személy által üzemeltetett leolvasónak is. Ő ezt az azonosítót csak lemásolja egy üres kártyára és máris megtörtént a kártya másolása. Ennek megakadályozására a rendszer kombinálható az olvasó azonosításával is. A kártya ekkor az elektromágneses térbe kerülésekor csak jelzést ad a jelenlétéről, ezután az olvasó küldi el az azonosító kódját. Amennyiben ez a kód szerepel a kártya memóriájában tárolt engedélyezett olvasók listáján, akkor fogja csak kiadni a kártya a saját azonosítószámát. Az adatátvitel komplikálható még az adatátvitel titkosításával, például elektronikus aláírás alkalmazásával. A rádiófrekvenciás adatátvitel miatt az átvitel sebessége és ebből kifolyólag a tárolt adat mennyisége is több nagyságrenddel kisebb az intelligens kártyákénál, általában 26-37 bit hosszúságú adatot használnak. Kártyába épített akkumulátor segítségével az alapesetben az olvasótól való néhányszor 10 cm-es legnagyobb távolság akár 10 m-es nagyságrendűvé növelhető (long range proximity). A technológiát az ISO/IEC 14443 szabvány írja le.

Ezek az aktív kártyák már elég biztonságosnak alakíthatóak ki arra, hogy hitelesen alkalmazhatóak legyenek közokiratokban egyedüli vagy kiegészítő azonosítási funkciókra.

BIOMETRIKUS AZONOSÍTÁS A KÁRTYATECHNIKÁBAN

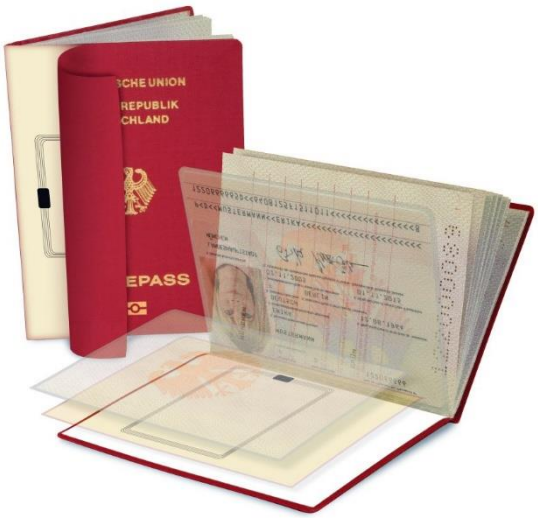
Az aktív kártyák következő generációja a biometriai biztonsági elemekkel kombinált kártyák alkalmazása. Az emberi kültakaró legjellegzetesebb eleme az arc, mely a Homo Sapiens egyéb érzékeinek (pl. szaglás) fejletlensége miatt a látás útján a szociokommunikációs funkciói mellett a személyek azonosításának elsődleges eszköze. Ennek alkalmazása ösztönös és az emberi faj kezdetektől alkalmazza. Az első nyoma más biometrikus jellemzők alkalmazásának a XIV. századi Kínában ujjlenyomat használata volt a gyermekek azonosítására, amit Joao de Barros felfedező jegyzett le. [7] Európában 1890-ben Alphonse Bertillon párizsi rendőr vezetett be testrész-méret alapú azonosítási rendszert bűnözők azonosítására. Módszerét a téves azonosítások tömeges előfordulásáig használták. Az ujjnyomat alapú azonosítást Bertillon munkája alapján Richard Edward Henry vezette be a Scotland Yard-nál. A XX. században Karl Pearson a University College of London alkalmazott matematikusa tett komoly felfedezéseket a biometria területén. Az 1960-as években az aláírás-dinamika elemzés terén történt komoly fejlődés, amely viszont megmaradt a katonai és nemzetbiztonsági alkalmazásban. A terrorveszély fokozódásával az Amerikai Egyesült Államokban és Nyugat-Európa területén a biometrikus azonosítás állami alkalmazása ugrásszerűen megnőtt.

Jelenleg az alábbi biometrikus jellemzőkön alapuló azonosítási rendszerek jellemzőek:

- ujjlenyomat
- kézfej geometria
- tenyérlenyomat
- vénamintázat
- markolás-dinamika felismerés
- koponya hőkép
- 2D arcvonások
- 3D arcvonások
- írisz (szivárványhártya) felismerés
- retina (ideghártya erezete) felismerés
- hangfelismerés
- aláírás dinamikája
- billentyűleütés dinamikája
- DNS
- testtartás felismerése

Ezek többé-kevésbé alkalmazottak a személyek azonosítására. A biometrikus jellemzők matematikai leírásával és annak tárolásával lehetőség van az egyedre jellemző adatok alapján pontosabb azonosítást végezni.

Az úti okmányok történetében az adatkártyák, mint kiegészítő elem és a biometria, mint a személyhez kötöttség magasabb foka együttes integrálásával új generáció került megalkotásra, amely az eddiginél szignifikánsan magasabb megbízhatóságot jelent az okmánybiztonság területén.



3. ábra ePassport [8]

Az Egyesült Államok után az Európai Unióban is elkezdték az elektronikus azonosítással is rendelkező útlevelek (ePassport vagy e-Passport) bevezetését. Ennek főbb okai az úti okmányok biztonságának növelése, ezzel az EU határbiztonság növelése, valamint az US Visa Waiver programban való bennmaradás, amely az EU államok vízummentességét jelenti. A német okmány a 3. ábrán látható. Magyarország szempontjából az ePassport bevezetése a programba való bekerülést célozta meg akkoriban. Az ePassport az előbbiekben ismertetett proximity kártya beépítése az útlevélbe. Először csak az adatok, majd ujjlenyomat tárolásával. A Tanács 2252/2004/EK rendelete alapján az ePassport első bevezetése az Európai Unióban 2005 októberében történt Svédországban. Magyarországon 2006. augusztus 29-e óta az adatoldal teljes tartalma megtalálható volt a tárolóelemben, a fényképpel és az aláírással egyetemben. Az ujjlenyomat 2008 óta kerül tárolásra. A Tanács döntése értelmében 2009. június 28-áig az Unió minden államának át kellett térnie az ujjlenyomatot is tároló ePassport alkalmazására. Ez természetesen az Unió több államában elismert adatvédelmi szakemberek ellenállásába ütközik, így Péterfalvi Attila és Majtényi László is ellenezték ezt. Az ePassport első oldalába került integrálásra egy tároló elem, amely tárolja a szóban forgó adatokat. Az adatok védelmére több biztonsági intézkedést implementáltak. A hagyományos okmánybiztonsági védelmi eljárásokon (alapanyagba integrált fénykép és aláírás, egyedi mintázatok, különleges festékek) kívül az elektronikus tároló egység a fizikai támadás hatására megsemmisíti a tárolt tartalmat. [9] Másrészről a chip aktív hitelesítésre képes, ami az abba integrált PKI magánkulcs segítségével történik, passzív hitelesítésként pedig belekerült az útlevél kiadójának tanúsítványa. A proximity kártyánál ismertetetett módon megtörténik az olvasó hitelesítése is egy ún. Basic Access Control (BAC) módszer segítségével. Ennek működése a következő: az útlevelek adat oldalának alsó részén hasonlóan a személyazonosító igazolványhoz, az MRZ kód található, amely az okmány és tulajdonosa legfontosabb adatait tartalmazza. Ez az adatok gépi leolvasásának egyszerűsítését szolgálja. Ebből kinyerve az útlevélszámot, a születési időt és az érvényességi időt generál a leolvasó egy hozzáférési kulcsot. Az ePassport ezen hozzáférési kulcs után fogja csak a tárolt adatokat rádiófrekvencián elküldeni a leolvasónak. Ezzel a módszerrel a leolvasó bizonyítja azt az útlevél felé, hogy ténylegesen hozzáfér ahhoz (nem távolról próbálja egy adatkalóz kihalászni a tartalmat). Ez a módszer korlátozott mértékben biztonságos. A kulcs megfejtése bruteforce módszerrel a kb. 50 bites entrópia miatt több mint 35 év, míg az adatok elemzésével (születési idő intervallum megválasztása, útlevélszám kiosztásának követése) 35 bitre csökkenti az entrópiát, így akár 3 óra alatt feltörhető a kód. [10]

A kód törése történhet a titkosított adatforgalom lehallgatásával, rögzítésével, majd bruteforce módszerrel való törésével, esetleg közvetlen támadással, amelyhez viszont háttérismeretek szükségesek. Az alapszintű (BAC) védelemmel ellátott kommunikáció több esetben bizonyítottan törésre, az adattartalom másolásra került. [11] Ez a kódolás nem igazán alkalmas az ujjlenyomat titkosítására, erre egy biztonságosabb eljárás került kifejlesztésre, amelyet Extended Access Control-nak (EAC) hívnak. [12] Az EAC nem egységes szabvány alapján történik, alapját az ICAO Doc 9303 fekteti le. Megfontolandó továbbá a tagállamok részére a sorszámozás megváltoztatása nagyobb tartományra, illetve a tartományon belüli véletlenszerű kiosztásra. Minden tagállamban az eddig kiadott úti okmányok érvényben maradnak, viszont az újonnan kiadottak minden esetben már az új módszerrel készülnek.

E-ID VÉDELMI LEHETŐSÉGEK

Hasonlóképpen az elektronikus útlevelekhez, az eID okmányokban is egy chip tárolja az adatokat, amihez kontakt vagy rádiós interfészen keresztül lehet hozzáférni. Tekintettel arra, hogy az okmány személyes adatokat tartalmaz, amikkel potenciálisan vissza lehet élni, ezeket az adatokat védeni kell. Mivel a távoli leolvasás is lehetséges, – irányított antennával akár több méterről – így nem elegendő a biztonságot csak a fizikai védelemmel megoldani. Fizikai védelem alatt jelen esetben azt értve, hogy a kártyára vigyázunk és csak annak adjuk oda, akivel szeretnénk a teljes adattartalmát megosztani. A potenciális támadások magukban foglalják a lementett adatok megszerzését, a kártyán lévő adatok megismerését például lehallgatással, skimming eljárással,[1] valamint a követést. A követésnél a támadó a kártya földrajzi mozgását követve készít profilt a célpontról. Sajnos ez utóbbit lehetővé teszi az ISO 14443 szabvány, ami előírja a kártya egyedi azonosítását a kommunikációt megelőzően. [13]

A védelem egyik legnyilvánvalóbb módja a titkosítás, ahol a titkosítási algoritmust minden kompatibilis kártyaolvasó ismeri, de a (szimmetrikus) titkosítás kulcsával és így a megfejtés lehetőségével csak azok az olvasók rendelkeznek, amelyekkel meg kívánjuk osztani az adatokat. Ebben az esetben a kulcselosztás problémájával találkozunk, tehát ha van százezer olvasónk, akkor vagy egy jelszót használ mindegyik és akkor nem lehet visszavonni a kompromittálódott kulcsokat, vagy minden olvasó külön jelszót használ, de akkor a jelszavak menedzsmentje igen nehéz, a kiadott kártyákon az olvasók jelszavainak a kezelése pedig szervezési szempontból egyenes lehetetlen. Ez a módszer önmagában csak egy zárt rendszer esetében alkalmazható, például egy vállalati rendszer esetén.

Hitelesítés alkalmazása esetén alapvetően nem a kommunikáció bizalmasságának eléréséről beszélünk, mint az előző esetben, hanem az adatokhoz való hozzáférést akarjuk korlátozni. Ebben az esetben az olvasó oldaláról meg kell adni egy rövid azonosító kódot, amit hívhatunk PIN-nek (Personal Identification Number, személyazonosító szám), CAN-nek (Card Access Number, kártyaazonosító szám) vagy jelszónak. Az olvasó ezzel a kóddal azonosítja magát a kártya felé. A kártya az így azonosított olvasónak kiadja a tárolt adatokat. A kommunikáció opcionálisan titkosítható, ami történhet egy, csak az adott kommunikáció során használt viszonykulccsal (session key), előre meghatározott szimmetrikus kulccsal vagy az aszimmetrikus titkosításban használt nyilvános kulcs-titkos kulcs párossal. Ez utóbbi lehet például a kártyát kibocsátó hatóság által üzemeltetett hitelesítés-szolgáltató tanúsítványával is ellátva. A kártya memóriája több részre osztható az adatok bizalmassága szerint.

[1] magyarra lefölözésként fordítható, ekkor nem a megnyitott adatkapcsolaton keresztül történik a hozzáférés – mint a lehallgatásnál – hanem egy új kapcsolatot kezdeményez a támadó

A spanyol elektronikus személyi igazolvány memóriája például három részre van osztva: a nyilvános részhez való hozzáférés nem korlátozott, a bizalmas területhez való hozzáféréshez kell a kártya PIN-kódja, míg a védett területhez csak a közigazgatási szervek férhetnek hozzá. [13]

Érdekes hitelesítési lehetőséget kínál az európai egészségbiztosítási kártyákra vonatkozó tervezet, amely két okoskártya közötti azonosítást határoz meg. Ennek során a beteg egészségbiztosítási kártyáján (health insurance card, HIC) lévő egészségügyi adatokhoz csak az orvos kártyájával (health professional card, HPC) lehet hozzáférni, így biztosítva az egészségügyi különleges adatok védelmét.

Az adatokhoz való hozzáférés korlátozása történhet valamilyen azonosító használatával is. Ebben az esetben az eID csak egy felhasználói azonosítót (User ID, UID) oszt meg a szolgáltatóval, aki egy központi adatbázisba bejelentkezve tudja lekérdezni a számára hozzáférhető adatokat az UID alapján. A közigazgatási szervek ettől függetlenül közvetlen hozzáféréssel rendelkezhetnek a kártyán tárolt adatokhoz. Ez a megoldás is több kérdést vethet fel, így az egységes azonosító használatát érintő adatvédelmi kérdések, a piaci szereplők által hozzáférhető központi adatbázis és hasonló problémák.

A magánszféra védelmét hatékonyabban valósítja meg az előző azonosító-képzési módszernek egy módosítása, amelyben hash-függvényeket alkalmazunk. Ekkor egy bemeneti adatból egy úgynevezett hash függvénnyel ujjlenyomatot képezünk. Ez a függvény egy csapóajtó függvény, amely azt jelenti, hogy a függvény elvégzése az egyik irányba egyszerű, a másik irányba pedig bonyolult matematikai feladat. Ez a függvény tetszőleges mennyiségű adatból egy állandó méretű (128-512 bit) adathalmazt generál. A bemeneti adathalmazban egyetlen bit megváltozása legalább a kimeneti bitek 50 százalékát meg fogja változtatni (ez a lavinahatás). A kimenetként kapott adathalmazt ujjlenyomatnak nevezzük, mivel közel egyedi módon jellemzi a bemeneti adathalmazt. A kimenetből a bemenetet előállítani nem lehet. A gyakorlatban jellemzően az SHA-256, SHA-512, esetleg a Whirlpool illetve az SHA-3 algoritmusokkal találkozhatunk. Az elavult MD5, SHA-1, RIPEMD-160 algoritmusok használata többé elektronikus aláírási vagy hasonló célra nem biztonságos. [14] Ha az előzőekben alkalmazott UID-ből egy felhasználástól függő azonosítóval együtt képezzük a hash értéket, akkor megnehezítjük azoknak a rosszindulatú szolgáltatóknak a dolgát, akik a különböző adatbázisokban tárolt személyes adatokat összevonni próbálják, hiszen az adatbázisokban tárolt UID-k a felhasználástól függően különböznek egymástól és azokból az eredeti (egységes) UID visszafejtése matematikailag kivitelezhetetlen feladat.

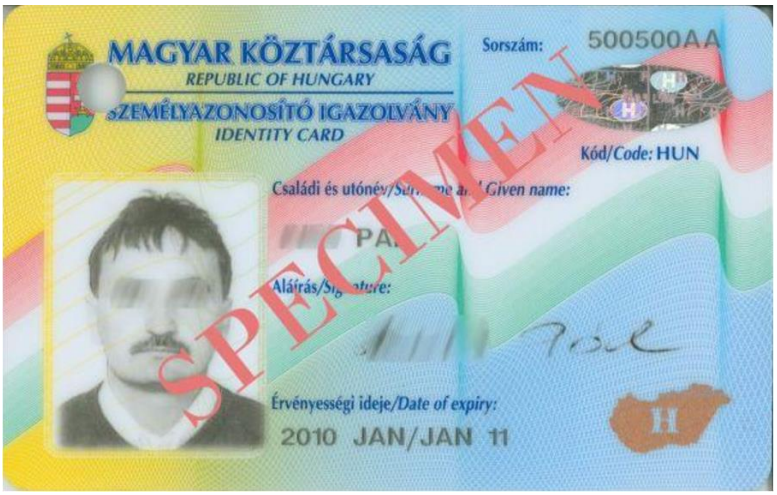
A személyes adatok védelmének egy további módja az, ha a kártya nem adja ki a benne tárolt személyes adatokat, csak ellenőrzési lehetőséget biztosít. Tehát az olvasó által ismert – például vizuálisan vagy optikai úton leolvasott – adatokat a chipnek megküldve csak egy válaszüzenetet kapunk, hogy a megadott adat megegyezik-e a biztonságos tárolóeszközben tárolt adattal. Ennek a megoldásnak példája az ujjnyomat-minta ellenőrzése. Az olvasó eszközön leolvassák a személyazonosító okmányt bemutató személy ujjnyomatát, amiből előállítanak egy, a kártya számára értelmezhető adatsort. A kártya az adatsort megkapva összehasonlítja azt a saját tárolójában lévő ujjnyomat-adatokkal és egy százalékos valószínűség-értéket ad meg az olvasó felé, arra vonatkozóan, hogy mekkora az egyezés valószínűsége. Ebben az esetben fontos a kártya megbízhatósága, tehát hogy valóban a kártya válaszoljon az olvasó által feltett kérdésre, ne a támadó.

Lehetőség van a felhasználó azonosítására abban az esetben is, ha kártya képes elektronikus aláírásra. Az egyik lehetőség, ha az azonosítást kérő rendszerrel védett csatornát épít ki a kártya valamely kulcscsere-protokoll segítségével (pl. Diffie-Hellman Key Exchange). Másik lehetőség, ha az azonosítást kérő rendszer küld egy generált (pszeudo)véletlen adatsort és a kártya segítségével az azonosítandó személy aláírja és visszaküldi azt.

Bár technikailag mind a két megoldás megfelelő, az adatokkal való visszaélésnek nagyobb az esélye az utóbbi esetben, ha az aláírandó adatcsomag nem véletlen, hanem célzottan generált adat.

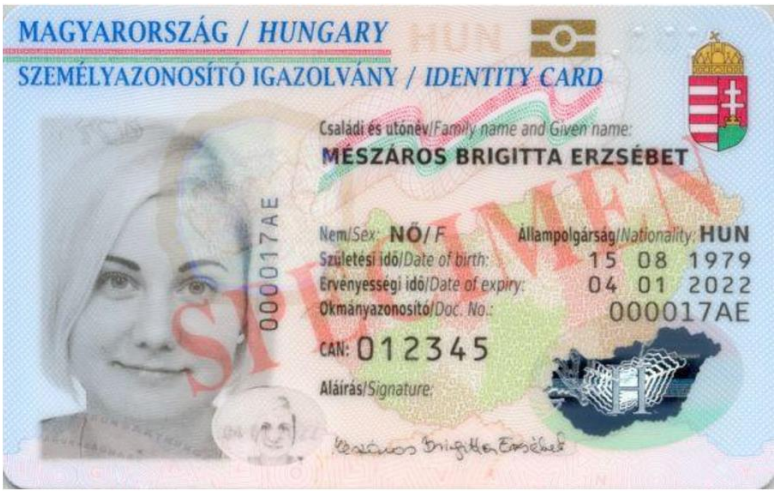
ÚJ SZEMÉLYAZONOSÍTÓ IGAZOLVÁNY MAGYARORSZÁGON

A korábbi papíralapú személyi igazolvány helyett a 168/1999. (XI. 24.) Korm. rendelet 2000. január 1-jétől bevezette a 4. ábrán látható plasztikkártya-alapú személyazonosító igazolványt. Az okmány biztonsági elemei mellett az ISO/IEC 7810 szabványban meghatározott ID1-es (85,6 mm * 53,98 mm) szabvány kártyamérete és vízállósága miatt az állampolgárok is kedvelték a kártyát. Hátránya vagy szimplán tulajdonsága, hogy a lakcímet nem tartalmazta, hanem azt külön (azonos méretű) kártyán, a lakcímet igazoló hatósági igazolványon bocsátották a jogosult rendelkezésére. Ez az okmány több, kisebb frissítésen is átesett.



4. ábra Személyazonosító igazolvány 2000-2015 között [15]

Jelentős változást a 414/2015. (XII. 23.) Korm. rendelet alapján 2016 január 1-jétől bevezetésre került elektronikus személyazonosító igazolvány (eID, eSZIG vagy eSzemélyi) hozott. Az általában alkalmazott okmányminta az 5. ábrán látható. Az eID a megváltozott dizájn és az új típusú biztonsági elemek mellett bevezette az elektronikus útleveleknél már egy évtizede alkalmazottakhoz hasonló, rádiós interfészen keresztül hozzáférhető (contactless) aktív tárolóelemet.



5. ábra Személyazonosító igazolvány 2016-tól [16]

Az új típusú személyazonosító igazolvány a vizuális és elektronikus adattartalmát a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény 29. §-a tartalmazza, ez az 1. számú táblázatban kerül összefoglalásra.

Tartalmazza az alábbiakat:	Vizuálisan [17; 29. § (2)]	Gépi (MRZ) kódban	Tárolóelemben[2]
a polgár nevét,	Igen	Igen	Igen
a polgár nevét nemzetiségi nyelven,	A nemzetiséghez tartozó polgár kérelmére [18; 33. § (1)]		
a polgár születési helyét,	Igen		Igen
a polgár születési idejét,	Igen	Igen	Igen
a polgár állampolgárságát,	Igen	Igen	Igen
a polgár anyja nevét,	Igen		Igen
a polgár nemét,	Igen	Igen	Igen
a polgár arcképmását,	Igen		Igen
a polgár aláírását,	12 év feletti írástudó esetében		12 év feletti írástudó esetében
a polgár személyazonosító igazolványa érvényességi idejét,	Igen	Igen	Igen
a polgár személyazonosító igazolványa okmányazonosítóját,	Igen	Igen	Igen
a polgár személyazonosító igazolványa kiállításának idejét,	Igen		Igen
a polgár személyazonosító igazolványát kiállító hatóság nevét,	Igen		Igen
a külföldre utazási korlátozás tényét,	Meghatározott esetekben és módon		Meghatározott esetekben és módon
a tároló elemben rögzített adatokhoz történő jogszerű hozzáférést biztosító protokoll elindításához szükséges kódszámot (CAN),	Ha van tárolóelem		
a polgár ujjnyomatát,			12 év felett, ha nem utasította vissza és fizikailag nem alkalmatlan
az elektronikus aláírás létrehozásához szükséges adatot,			Polgár kérelmére
a polgár társadalombiztosítási azonosító jelét,			Igen
a polgár adóazonosító jelét,			Igen
személyazonosító igazolvány elektronikus egyedi azonosítóját,			Igen
legfeljebb kettő, vészhelyzet esetén értesítendő telefonszámot.			Polgár kérelmére

1. táblázat Az új típusú személyazonosító igazolvány adattartalma (saját szerkesztés)

[2] A 65 éves kor felett igényelhető „határidő nélküli”, valójában 60 év érvényességi idejű okmány nem tartalmaz tároló elemet ld. [17] 29/E. § (2)

Az állandó személyazonosító igazolvány érvényességének időtartama 18 éves kor alatt 3 év, a felett 6 év. 65 év felett tároló elemet nem tartalmazó „határidő nélküli" (valójában 60 év) érvényességi idejű személyazonosító igazolvány kerülhet kiállításra. A személyazonosító igazolvány érvényességének időtartama alapestben a jogosult születési idejének napjához illeszkedik. [17; 29/E. §]

A személyazonosító igazolvány a biztonsági okmányok védelmének rendjéről szóló 86/1996. (VI. 14.) Korm. rendelet szerint a nemzeti fejlesztési hatáskörbe tartozó biztonsági okmányok körébe tartozik, amelyekre vonatkozóan az Európai Unió valamely követelményt határoz meg, valamint mint a személyazonosság igazolására alkalmas okmány az „A" okmányvédelmi kategóriába tartozik. [18; 5/A. § (5)] A követelmények szerint a „A" okmányvédelmi kategóriába tartozó biztonsági okmányok minden alkatrészét védeni kell a teljes vagy részleges hamisítás ellen. A védelmi módszereknél a kémiai, fizikai, technikai, technológiai és adminisztratív eljárásokat, valamint elektronikus biztonsági okmány esetében a digitális védelmi módszereket, eljárásokat együtt kell alkalmazni. [19] A konkrét védelmi megoldások az okmányvédelmi tervben kerültek meghatározásra, azok nem nyilvánosan hozzáférhetők. Az okmány képe és egyes biztonsági elemei viszont nyilvánosan hozzáférhető az Európai Unió Public Register of Authentic Travel and Identity Documents Online (PRADO) rendszerben.

A biztonsági okmányok védelmének rendjéről szóló rendelet szerint az elektronikus biztonsági okmány informatikai adathordozót tartalmazó biztonsági okmány, ahol az informatikai adathordozó az okmányba integrált vagy az okmányon megjelenő adat tárolására alkalmas elem, amely lehet chip, vonalkód, optikai adattároló elem, mágneses adattároló elem. A személyazonosító igazolványban ezek közül az egyetlen aktív eszköz, a chip található meg, a korábban ismertetett MRZ kód mellett.

Az okmányvédelmi kategóriák mellett a jogszabály nevesíti az okmányinformatikai védelmi kategóriákat is. [19; 2. sz. mell. II.] Az A okmányvédelmi kategória esetén „Kiemelt", „Fokozott" és „Alap" okmányinformatikai védelmi kategória is használható. A kategóriák tartalma a 2. táblázatban található.

Paraméter	„Kiemelt"	„Fokozott"	„Alap"
Tárolt adat kriptográfiai védelme	a tárolt adat titkosított, a titkosítás algoritmusa legalább RSA 2048	a tárolt adat titkosított, a titkosítás algoritmusa legalább AES 128	a tárolt adat nem titkosított
Integritásvédelem	az adatok rögzítésének, írásának és felülírásának korlátozása	az adatok rögzítésének, írásának és felülírásának korlátozása	az adatok rögzítésének, írásának és felülírásának korlátozása
Hozzáférés-szabályozás	kiterjesztett hozzáférési protokoll alkalmazása	az adatokhoz való hozzáférés korlátozása	
Kommunikációvédelem	védett kommunikációs csatorna az informatikai adathordozó és az olvasó között (ha értelmezhető)		
Tanúsítás	az informatikai adathordozó gyártói tanúsítása (ha értelmezhető)	az informatikai adathordozó gyártói tanúsítása (ha értelmezhető)	

2. táblázat Az okmányinformatikai védelmi kategóriák műszaki tartalma (saját szerkesztés)

Az előírásban nehezen értelmezhetők a konkrét megnevezett algoritmusok, ugyanis a 2048 bites modulusméretű RSA kriptográfiai algoritmus jósága nehezen hasonlítható össze a 128 bites AES algoritmussal, hiszen más technológiát képviselnek: az előbbi aszimmetrikus, az utóbbi szimmetrikus kulcsú titkosítást tesz lehetővé.

A személyazonosító igazolvány vizuális adattartalma gyakorlatilag megegyezik a korábbi személyazonosító igazolvány adattartalmával. A címben felvetett kérdések tehát alapvetően az elektronikus tárolóelemben tárolt adatok körére és biztonságára vonatkoznak.

A tároló elem egy elektronikus adathordozó egység [17; 5. § (19)], amely a Common Criteria for Information Technology Security Evaluation szerinti (CC EAL5+, ill. CC EAL 4+) tanúsítvánnyal rendelkezik, valamint biztonságos aláírás-létrehozó eszköznek (BALE) minősül.

FUNKCIÓK

Az elektronikus személyazonosító igazolvány három fő funkcióval rendelkezik:

1. Elektronikus úti okmány (ePASS) funkció
2. Elektronikus azonosítási (eID) funkció
3. Elektronikus aláírási (eSIGN) funkció

Az elektronikus úti okmány (ePASS) funkció célja a különböző államközi egyezményekben – elsősorban a Schengeni Egyezményben – szabályozott határátlépési lehetőség biztosítása. Ilyen tekintetben tehát csak meghatározott esetekben helyettesítheti az útlevelet.

Az elektronikus azonosítási funkció célja az elektronikus közigazgatási funkciók hatékonyabb igénybevétele. A tervek szerint határon átnyúló szolgáltatások igénybevételére is lesz lehetőség később, a terület az Európai Unió Common List of Basic Public Services követelményjegyzék (EU CLBPS, alapvető közszolgáltatások közös listája), vagy másként 12+8-as lista elemeként is megjelenik. [20] Ettől függetlenül a tagállami implementáció lassú, egyelőre mind a bevezetés mértékében, mind tartalmi tekintetben elmarad az elvárttól. [21]

Az elektronikus aláírási (eSIGN) funkció az előző kettő funkcióval szemben teljes mértékben csak a felhasználó érdekeit szolgálja, tetszőleges dokumentumon tudunk vele elektronikus aláírást létrehozni. Az elektronikus aláírás készítésének folyamata a következő: az adatból hash függvénnyel lenyomatot képezünk. Ezt a kriptográfiai magánkulccsal titkosítjuk. Így megkapjuk az elektronikus aláírást, amely a bemeneti dokumentumtól független adatcsomag lesz. Az aláírt dokumentumot és az aláírást együtt, egy nyilvános csatornán, például e-mailben elküldhetjük a címzettnek. A címzett az elektronikus aláírást a mi nyilvános kulcsunkkal megfejti, így megkapja azt az ujjlenyomatot, amelyet mi készítettünk. Ezalatt az átküldött dokumentumból ő is elkészíti az ujjlenyomatot, és ezt a kettőt összehasonlítja. Amennyiben ezek megegyeznek, biztosan állíthatjuk, hogy az aláírt dokumentumban nem történt változtatás, valamint, hogy egy meghatározott kulccsal történt a dokumentum aláírása. Nem bizonyítja viszont azt, hogy ez ténylegesen a feladónak a magánkulcsa volt, azt, hogy ezt nem vonták vissza, és nem állapítható meg belőle a feladás ideje sem. Ezek bizonyítására más, kiegészítő funkciókat kell alkalmazni. A kulcsok személyhez kötését, a hitelességi problémát kétféle módon oldhatjuk meg: egyrészről a bizalmi háló (*web of trust*) módszerével, amelyet a PGP használ. [22] Ezen módszer szerint az egymásban megbízó személyek egymás kulcsait aláírják, így ha a címzett megbízik a feladó kulcsát aláíró bármelyik személyben, vagy vissza tudja vezetni az aláírásokat egy megbízható személyig, akkor ez biztosítékot jelent számára a feladó megbízhatóságára is. Ennek a módszernek a hátránya, hogy igen nagy bizalmi hálókat követel meg az, hogy két ismeretlen ember közös ismerőssel rendelkezzen. Másik módszerként aaz S/MIME rendszer használatos. Itt a felek megbízhatóságát egy mindenki által megbízható harmadik személy tanúsítja. Ez

tanúsítvány segítségével történik, amely egy elektronikus adathalmaz és általában tartalmazza a nyilvános kulcsot is. A harmadik személy az állam által megbízhatónak tartott tanúsítás szolgáltató (*Certificate Service Provider*, CSP), aki a tanúsítvány kiadása előtt ellenőrzi a kulcsbirtokos és a kulcs összetartozását (például személyigazolvány kérésével). Ezek a tanúsítás szolgáltatók tanúsítási láncot alkotnak, amelynek a tetején a legmagasabb szintű tanúsítás szolgáltató (*Certificate Authority*, CA) áll. Ezek a CA-k mindenki által elfogadottak és ebből kifolyólag a tanúsítási lánc többi eleme is megbízhatóvá válik. Az aláírás idejének hiteles megállapítása időbélyeg szolgáltató (*Timestamping Authority*, TSA) segítségével történik, aki a pontos időt látja el saját elektronikus aláírásával, amit a feladó beépít a dokumentum elektronikus aláírásába. Az időbélyeg igénylése alapvetően Interneten keresztül, on-line történik. A TSA megbízhatóságát a tanúsítványa biztosítja, amely a tanúsítási lánc mentén visszavezethető egy CA-hoz. Az elektronikus aláírások, illetve tanúsítványok használati köre általában korlátozott. Egy kulcspárt jellemzően csak elektronikus aláírásra, vagy titkosításra, vagy biztonságos kapcsolat kiépítésére (SSL) lehet használni. Amennyiben ezek közül több funkciót is használni kívánunk, több kulcspárra, illetve tanúsítványra lehet szükségünk. [23]

Az új típusú személyazonosító igazolványhoz kapcsolódó e-aláírás és időbélyegzés szolgáltatást a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., mint kormányzati hitelesítés-szolgáltató nyújtja. A eSzemélyiben alkalmazott tanúsítvány megfelel az eIDAS rendelet (Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről) követelményeinek.

Az Belügyminisztérium által üzemeltetett eSzemélyi honlapról letölthető eSzemélyi Kliens az elektronikus a PIN kódok aktiválására és cseréjére, valamint az e-aláírás funkció kezelésére alkalmas a Microsoft Windows 7, 8, 8.1, 10 32 és 64 bites változatain, a Apple Mac OS X Yosemite, El Capitan, Sierra verzióin és egyes Linux disztribúciókon és verziókon (CentOS 7, Debian 8, SuSe 13.2, Ubuntu 14.04.5 LTS). [24] Feljesztője a ID&Trust Kft. (korábban HunTrust Kft.), amely a nemzetközi chipkártya-piacon is sikeres magyar kisvállalkozás.

Az elektronikus aláírási funkció lehetősége önmagában is forradalmasíthatná a magyar e-közigazgatást és az elektronikus írásbeliséget, hiszen az állam ingyen a rendelkezésére bocsátja minden új típusú személyazonosító igazolványhoz az elektronikus aláíráshoz szükséges elemeket. A feltételes mód oka a szerző szkepticizmusa: a 2000-es években az eszközök, majd az elektronikus aláírásról szóló 2001. évi XXXV. törvény megjelenésével a szakma bízott a széleskörű alkalmazásban, ami végül mégsem következett be. Mindenesetre a fejlődés lehetőségét a kormány az új típusú személyazonosító igazolvánnyal biztosította.

KÖVETKEZTETÉSEK

A kártyán történő adattárolást biztosító technológiák komplexitásával és az adattárolási és adatfeldolgozási kapacitásuk növekedésével a kártyák egyre hatékonyabb módon alkalmazhatók beléptetésre, személyek azonosítására. A komplexitás növekedésével a tárolt adatok mennyisége és minősége is növekszik, – egy azonosító számtól kezdve eljutottunk az ujjnyomat digitális tárolásáig – amely a funkciók mellett adatvédelmi kockázatot rejt magában. Az ezt kihasználó támadások ellen a hatékony kriptográfiai intézkedések mellett megfelelő szervezési intézkedésekkel tudunk védekezni.

Az új típusú személyazonosító igazolvány bevezetésével a kormány a lehetőségekhez mérten biztonságos módon tette lehetővé az állampolgárok modern személyazonosítását és megnyitotta a szélesebb körben is használható funkciókat. Így különösen az elektronikus aláírás ingyenes hozzáférhetőségével az elektronikus írásbeliség kulcselemét téve szinte költségmentesen elérhetővé.

FELHASZNÁLT IRODALOM

[1] VISDÓMINE, PADILLA, L: *Track format of magnetic stripe cards.* http://www.gae.ucm.es/~padilla/extrawork/tracks.html [2017. 09. 10.]

[2] EILER E.: *Kódnyomtatás és nyomtatott vonalkód rendszerek*, Magyar Grafika, 2008. 5. sz. p. 44.

[3] *Kaywa QR Code* https://qrcode.kaywa.com/ [2017. 08. 20.]

[4] *Department of Homeland Security U. S. Citizenship and Immigration Services* https://www.uscis.gov/i-9-central/acceptable-documents/list-documents/form-i-9-acceptable-documents [2017. 09. 15.]

[5] SZÁDECZKY T.: *Azonosító kártyák biztonsága*. In: L. KRISZTIÁN (szerk.) XXIX. Kandó Konferencia – 29th Kandó Conference (Budapest, Magyarország, 2013.11.21) Budapest: Óbudai Egyetem, 2013. ISBN 9789637158056 pp. 137-144.

[6] HASSLER, V.: *IT Security and Smart Card Standards*. Graz, Austria : Institutes for Information Processing Graz, 1995.

[7] OSBORN, A.: *Biometrics history. Looking at biometric technologies from the past to the present*. http://ezinearticles.com/?Biometrics-History----Looking-at-Biometric-Technologies-from-Past-to-Present&id=91803 [2017. 09. 02.]

[8] *Bundesamt für Sicherheit in der Informationstechnik (BSI)* https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/EPassport/epassport_node.htm [2017. 06. 20.] Quelle: Bundesministerium des Innern

[9] JÓRI A. – HEGEDŰS B. – KEREKES Zs. (szerk.) et al.: *Adatvédelem és információszabadság a gyakorlatban.* Complex, Budapest, 2010.

[10] ROBROCH, H.: *ePassport Privacy Attack. Cards Asia Singapore*, April 26. 2006. https://pdfs.semanticscholar.org/828a/70de925744617be3d2886442cd0e88058c25.pdf [2017. 10. 27.]

[11] PAPP Z.: *Az új technológiák veszélyei: RFID és az elektronikus útlevél*, Hadmérnök, 2010. V. évf. 4. sz. pp. 248-254.

[12] MOSES, T.: *Protecting Biometric Data with Extended Access Control.* https://www.entrust.com/wp-content/uploads/2010/01/WP_Entrust_ePassport-Biometrics_Aug2014.pdf [2017. 09. 04.]

[13] NAUMANN, I., HOGBEN, G.: *Privacy features of European eID card specifications*, Network Security, August 2008 doi:10.1016/S1353-4858(08)70097-7

[14] SOTIROV, A. –STEVENS, M. – APPELBAUM, J. – LENSTRA, A. – MOLNAR, D. – OSVIK, D.e – WEGER, B.: *Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate*. In: S. HALEVI (Ed.): CRYPTO 2009, LNCS 5677, pp. 55–69, 2009

[15] *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-03001* http://www.consilium.europa.eu/prado/en/HUN-BO-03001/index.html [2017.09.20.]

[16] *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-05001* http://www.consilium.europa.eu/prado/en/HUN-BO-05001/index.html [2017.09.20.]

[17] *1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról (Nytv.)*

[18] *414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól*

[19] *86/1996. (VI. 14.) Korm. rendelet a biztonsági okmányok védelmének rendjéről*

[20] SZABÓ A. B.: *Okmányvédelem és az elektronikus személyazonosító igazolvány*, Hadmérnök, 2016. XI. évf. 1. sz.

[21] SIDDHARTHA A.: *National e-ID card schemes: A European overview, Information Security Technical Report*, 13 (2008) pp. 46–53. doi:10.1016/j.istr.2008.08.002

[22] ALFAREZ A-R.: *The PGP Trust Model. EDI-Forum*, April 1997.

[23] SZÁDECZKY T.: *Az elektronikus írásbeliség és problémái, Infokommunikáció és jog*, 2009. VI. évf. 3. sz. pp. 67-72. ISSN 1786-0776

[24] *Belügyminisztérium eSzemélyi honlapja* http://www.kekkh.gov.hu/Eszemelyi/kartya_funkcioi/kartyaolvaso_alkalmazas [2017.09.24.]