DOI:10.38146/bsz-ajia.2013.v61.i5.pp101-112

HAZAI LÁSZLÓNÉ

A biometrikus azonosítás feladatai

Az okmányvédelem jövője, helyünk és feladataink az unióban, a fejlesztések hatása a szakértői tevékenységre

Napjainkban a biztonsági okmányok védelmével kapcsolatos, korábban nemzeti hatáskörben lévő feladat, szabályozási tevékenység megoszlik az Európai Unió és a tagállamok nemzeti hatóságai között. Az Európai Unió biztonsági okokból, az ellenőrzés hatékonyságának növelése érdekében kiemelt figyelemmel kezeli az Európai Unión belüli, a tartózkodás jogszerűségét igazoló, illetve a harmadik országokból történő beutazást lehetővé tevő dokumentumok biztonságának kérdését, a hamisítások megakadályozását, illetve megnehezítését. Ezért egyes okmányoknál előírja az *egységes védelmet és a technikailag magas szintű biztonsági elemek kötelező alkalmazását* (ezeket hívjuk egységes formátumú EU-okmányoknak), *illetve* más okmányok esetén *az úgynevezett minimum biztonsági követelmények bevezetéséről döntött*.

A tagállamok szakembereiből álló, az EU Tanácsa mellett működő, *a vízumok egységes formátumáért felelős szakértői, technikai bizottság,* vagyis a 1683/95/EK tanácsi rendelet 6. cikke alapján felállított bizottság *(a továbbiakban: 6. cikk bizottság)* az a szervezet, amely okmánytechnikai és okmánybiztonsági kérdésekben véleményt alkot és ajánlásokat, javaslatokat fogalmaz meg.

Ennek a szakértői, technikai kérdésekkel foglalkozó bizottságnak a feladata az egységes formátumú európai uniós okmányok technikai, biztonsági fejlesztése kérdéseinek tagállamok közötti egyeztetése, javaslatok felterjesztése az EU Bizottsága (a szabadság, jog és biztonság főigazgatósága) részére.

A 6. cikk bizottság feladatkörébe utalt biztonsági okmányok köre az elmúlt időszakban folyamatosan bővült, és az egységes európai ellenőrzési rendszerek bevezetésével a biztonság mint közös érdek érvényesülésével ez várhatóan a jövőben is folytatódik.

Az EU-okmányok és a kiemelt védelmet igénylő, nemzeti fejlesztésű biztonsági okmányok védelmének garantálása, az e kérdéskörben meghozott uniós intézkedéseknek, technikai specifikációknak, állásfoglalásoknak való megfelelés a tagállamok felelőssége.

Valamennyi tagállamban kijelölt kormányzati szervek, hatósági jogkörrel felruházott, felelős szervezetek feladata az erről való gondoskodás.

Az uniós normák az úgynevezett egységes formátumú EU-okmányok (vízum, tartózkodási engedély) vonatkozásában megkövetelik, hogy minden tagállam a gyártás biztonsága érdekében egy nemzeti hatóságot jelöljön ki az okmánygyártáshoz szükséges specifikációk átvételére és kezelésére, az előírások betartásának ellenőrzésére.

Erre a feladatra a kormány a Nemzetbiztonsági Szakszolgálat Szakértői Intézetét jelölte ki a *Nemzeti Vízum- és Okmánybizottság létrehozásáról* és a biztonsági okmányokkal kapcsolatos kormányzati feladatokról szóló kormányhatározattal.

A biztonsági okmányok védelmének, az előállítás hatósági felügyeletének szabályait a *86/1996. (VI. 14.) kormányrendelet írja* elő. A kormányrendelet hatósági jogkörrel ruházza fel a Nemzetbiztonsági Szakszolgálatot. Ezt a jogkört a szakszolgálaton belül első fokon a Szakértői Intézet gyakorolja.

Ez a jogszabály határozza meg a biztonsági okmányok fogalmát és körét, külön kategóriába sorolva az Európai Unió által kiemelten kezelt biztonsági okmányokat.

A *biztonsági okmányok* olyan védelmet igénylő okmányok, amelyek a használó (birtokos) személyét, jogosultságát hitelesen igazolják, és a velük való visszaélés, jogszerűtlen használat súlyosan sérti az Európai Unió, illetve hazánk biztonsági érdekeit.

Okmányvédelem és okmányellenőrzés

Az okmányvédelemre – a sok száz éves fejlődés alatt – a technikai fejlődésnek megfelelő folyamatos megújulás, az új technológiák, anyagok, módszerek beépítése, alkalmazása volt a jellemző, és így van ez napjainkban is.

Az okmányvédelem tervezésénél az okmányvédelmi rendszerek felépítésének kiindulópontja az *okmányvédelem és okmányellenőrzés klasszikus háromszintű felépítése.*

1. Általános vagy alap okmányvédelmi és ellenőrzési szint: az alapszintű biztonsági elemek jól látható, gyorsan megtanulható, alapvetően vizuális ellenőrzéssel azonosítható jellegzetességek az okmányokban. Ilyenek lehetnek például az okmányok, biztonsági termékek szöveges, grafikai elemei.
2. Hivatalos ellenőrzéseket segítő okmányvédelmi és ellenőrzési szint: az adott okmánnyal hivatalból foglalkozók, az ellenőrzést végző szakterületek munkáját segítő, összetett azonosító jellegzetességek tartoznak ide. Ilyenek az alapszintű, vizuálisan ellenőrizhető biztonsági elemeken túl az egyszerű eszközök-

kel ellenőrizhető okmányvédelmi megoldások, okmánytechnikai jellegzetességek, a különböző elektronikus azonosítást támogató megoldások (MRZ, vonalkód, 2D barkód, kontakt, illetve kontaktmentes chipadatok stb.).
Az ellenőrzés helyétől függően különböző környezeti, technikai feltételek és szituációk lehetnek, és ez a szinten belül további ellenőrzési fokozatok létrehozását indokolhatja.

3) Szakértői vizsgálatokkal vizsgálható okmányvédelmi, ellenőrzési szint: a szakértők, speciális szakmai ismeretekkel felvértezettek munkáját segítő azonosítási, okmányvédelmi jellegzetességek, anyagok, speciális okmánytechnikai ismérvek és vizsgálati módszerek. (Ezek a jellegzetességek már többnyire különböző szinten minősített információk, okmányvédelmi elemek.)

Új módszerek, új elemek az okmányvédelemben, a biometrikus azonosítás

Az *okmánybiztonság* iránti fokozott igény miatt, valamint az Egyesült Államok vízummentességi programja nyomán az Európa Tanács 2003. júniusi theszaloníki, majd brüsszeli ülésén felszólította az EU Bizottságát, hogy a *biometrikus személyazonosító elemek alkalmazása* érdekében dolgozza ki a szükséges javaslatokat, és kezdjen neki a technikai részletek megtervezésének.

Az EU-n belül, az e célból létrehozott szakmai munkacsoportokban, így a 6. cikk bizottságban is széles platformú együttműködésben folyik jelenleg is az a munka, amelynek kiemelt területe az okmányvédelem folyamatos fejlesztése, a biztonsági kérdések új dimenzióinak vizsgálata, véleményezése.

A fejlesztések célja az *okmányok védelmének magasabb színvonalra emelése* mellett az *ellenőrzés és a személyazonosítás biztonságának növelése.*

Mi is a biometria? Az emberek egyedi biológiai jellegzetességein alapuló, tudományos módszerekkel mérhető, az egyéni azonosítást lehetővé tevő módszereket nevezzük biometriának. Ilyen viszonylag hozzáférhető (nem minden esetben mondható az, hogy egyszerű) módszerekkel, eszközökkel mérhető belső, illetve külső biológiai jellegzetessége az embernek az ujjlenyomata, a tenyérlenyomata, illetve a szem íriszének mintázata, az erek mintázata a retinán, az ujjon, a tenyéren, illetve a testrészek – arc, kéz – geometriája, de idesorolhatók a hangképzés jellegzetességei is. A felsorolás természetesen nem teljes.

Néhány tanult, szerzett képesség is karakterisztikus, egyedi azonosításra alkalmas sajátossággal bír. Ilyen például az írás.

Ezek a meglévő vagy tanult, szerzett jellemzők azonban az ember élete folyamán különféle tényezők hatására kisebb vagy nagyobb mértékben változnak.

Annak az eldöntése, hogy melyik az ideális, legjobb biometrikus azonosító, számos tényező függvénye. Mindenekelőtt fontos meghatározni, hogy milyen célból, miért van szükség a biometrikus azonosításra, ez után vizsgálni kell a *biztonság kérdését, amely magában foglalja* a szükségességi és az arányossági szempontok mérlegelését, a biometrikus azonosító hamisíthatóságának, a mérések pontosságának és megbízhatóságának, az ebből eredő hibák nagyságának az elemzését. Fontos továbbá vizsgálni az alkalmasság, illetve alkalmazhatóság szempontjából a használhatóságot, amely olyan, a gyakorlatban fontos kérdések elemzését takarja, mint a mérések gyorsasága, hitelessége, a mérés bonyolultsága, a mérőeszközök nagysága, költsége, a mérést befolyásoló tényezők, kockázatok ismerete, a módszer elfogadottsága stb.

A biometrikus azonosítók biztonsági okmányokba történő integrálására irányuló fejlesztések az Európai Unióban két irányban indultak el: a *harmadik országok állampolgárai részére kiadott vízumok és tartózkodási engedélyek, illetve az uniós tagállamok által kiadott útlevelek és úti okmányok biometrikus azonosítókkal történő ellátása irányába.*

A vízum és a tartózkodási engedély egységes uniós okmány, ezek vonatkozásában az Európai Unió rendeletben szabályozott módon egységesen, kötelezően és részleteiben meghatározott formai és biztonsági jellemzőket ír elő a tagállamok részére.

Az útlevelek és úti okmányok ezzel szemben nemzeti fejlesztési hatáskörbe tartozó okmányok, e tekintetben az uniós rendelkezések formai és tartalmi előírásokat, valamint az okmánybiztonsági követelmények minimálisan teljesítendő szintjét határozzák meg, ezek mellett azonban az okmányok további biztonsági, okmánytechnikai fejlesztése, kialakítása a tagállamok hatáskörébe tartozik.

A feladatokat, a vonatkozó rendeleteket, határidőket a *1. számú táblázat* foglalja össze.

A táblázatban is feltüntetett fontos különbség, hogy egyes okmányoknál a biometrikus adatok elhelyezése, tárolása az adatbázisban (vízum), míg más biztonsági okmányoknál (útlevél, személyazonosító igazolvány, tartózkodási engedély) az okmányokba integrált (megfelelő biztonságot nyújtó technológiával beépített) adathordozón történik.

Az EU a biometrikus adatok *ellenőrzéséhez elsődleges biometrikus azonosítóként az arcképet, másodlagos biometrikus azonosítóként az ujjlenyomatot* jelölte meg. Ezek rögzítése az EU-tagállamok által kiadott útlevelekben és az egy évnél hosszabb érvényességi idővel, utazási célra kibocsátott okmányok-

1. számú táblázat

Néhány, az unió által kiemelten kezelt biztonsági okmány fejlesztésének helyzete

Okmány	Célok, feladatok	Jogalap	Határidő	Biometrikus adatok tárolása
Útlevél	biometria bevezetése	2252/2004/EK rendelet; B (2006) 2909 határozat	2006. 08. 29. (fénykép) 2009. 06. 29. (ujjlenyomat)	az okmányba integrált adathordozóban
Személyazonosító igazolvány	biometria bevezetése (ajánlás jellegű)	2006. 12. 4–5-i tanácsi következtetések	tagállami hatáskör	az okmányba integrált adathordozóban
Vízumbélyeg	Vízuminformációs rendszer bevezetése (biometria)	767/2008/EK rendelet	2011. 10. 11.	központi adatbázisban (VIS)
	okmánybiztonsági fejlesztés	1683/95/EK rendelet; 856/2008/EK rendelet; C (2010) 0319 határozat	2012. 01. 27.	
Tartózkodási engedély	a megújult kártyaformátumú okmány bevezetése	1030/2002/EK rendelet; 380/2008/EK rendelet; C (2009) 3770 határozat	2011. 05. 21.	okmányba integrált adathordozóban
	biometria bevezetése		2011. 05. 21. (fénykép) 2012. 05. 21. (ujjlenyomat)	

ban az elsődleges azonosító esetén 2006, a másodlagos azonosító vonatkozásában pedig 2009 óta kötelező.

A biometrikus azonosításra alkalmas biztonsági okmányok bevezetése ennek megfelelően az arckép elektronikus formátumban történő tárolásával és a biometrikus adatnak az úgynevezett egy az egyben ellenőrzésével kezdődött. Azért az arcképpel, mert az okmányokban az arckép elektronikus formában történő tárolása, illetve visszaellenőrzése igényli a legkevesebb állampolgári együttműködést, egyben az ellenőrző személy számára a legegyszerűbben összehasonlítható biometrikus jellemző.

Az e-útlevelek a jelenlegi szabályozás szerint minimum 64K tárolókapacitású, kontaktmentes RF-chipet kell hogy tartalmazzanak. Általában az e-útlevelekben a chip 72 K-s.

A chipen tárolni kell a személyes adatokat, az arcképet és az ujjlenyomat képét, továbbá egyéb, a chip működéséhez, működtetéséhez, az adatok biztonságának megőrzéséhez szükséges adatokat.

A chipkapacitás minimumának kiszámításakor és az alkalmazandó biometrikus azonosítók kiválasztásakor a fejlesztésekben közreműködő szakemberek kutatásokat végeztek az arckép, az ujjlenyomat és az íriszkép mint további biometrikus azonosító tömöríthetősége tárgyában (addig tömöríthető, amíg az a visszaolvasás utáni állapotban nagy biztonsággal azonosítható). Megállapították, hogy a szabvány arckép JPEG2000 formátumban 12K méretre, az ujjlenyomat WSQ algoritmussal ujjanként 10K-ra, míg az íriszkép szemenként 30K-ra tömöríthető a minőség jelentős romlása nélkül.

Az unió meghatározta ehhez a megfelelő, PKI-alapú hitelesítési rendet (előírta a hatóságok kijelölését és a kötelező protokollszabályokat).

A biometrikus azonosítót is tartalmazó okmányok fejlesztése gyors ütemben történik.

A Nemzetközi Polgári Repülési Szervezet *(International Civil Aviation Organization; ICAO)* által gyűjtött statisztikai adatok szerint szerte a világon *2010 elején már több mint százmillió úgynevezett e-útlevél, illetve úti okmány kibocsátására került sor, több mint ötven ország részéről,* és ezekben is az elsődleges biometrikus adat a tulajdonos elektronikus formában tárolt arcképe. *2011-re* a biometrikus okmányt kibocsátó országok száma meghaladta a *nyolcvanat.*

Nincs adat arról, hogy ebből mennyi és melyik tartalmaz egy (arckép) és mennyi több (arckép és ujjlenyomat) biometrikus adatot.

A *személyazonosító igazolványokra* vonatkozó minimum biztonsági követelmények elfogadására és a biometrikus azonosítók integrációjának kötelezettségére vonatkozóan a tagállamok között politikai egyezség született, az erre vonatkozó jogi normák kidolgozása azonban még folyamatban van.

A fejlesztések tehát nemcsak az útleveleket, úti okmányokat érintik, hanem egyre több ország vezeti be az *elektronikus, az előzőekben részletezett paraméterekkel jellemzett ID-kártyákat, tartózkodási kártyákat, vezetői engedélyeket* stb. (Németország: ID 2010-ben, vezetői engedély 2011-ben; Egyesült Államok: zöldkártya 2010-ben; EU-tagállamok: tartózkodási engedélyek.)

Komplex okmányvédelem és -ellenőrzés versus digitális ellenőrzés

A klasszikus okmányvédelmi megoldások és a digitális adatok tárolására alkalmas eszközök integrálása, beépítése a biztonsági okmányokba kiszélesítette a védelem és az ellenőrzés lehetőségeit, növelte a védelmi szintek komplexitását. Az új adathordozót[1] úgy kell tekinteni, mint egy új biztonsági elemet, amely

– *növeli az okmány és az ellenőrzés biztonságát,* mert elektronikus formában ellenőrizhetővé teszi az okmány és a tulajdonosának az összetartozását, és így segíti az ellenőrzőt;
– *technikailag megnehezíti a hamisítást.*

Az informatikai adatot tároló adathordozót – amely fizikailag beépül az okmányokba – az okmányvédelem részeként kell kezelni. Az új fejlesztésnél meg kell hogy valósuljon az okmánytechnikai biztonság és az informatikai biztonság magas szintű integrációja.

Fontos hangsúlyozni azonban azt, hogy *az elektronikus azonosítás önmagában nem elégséges* a személyazonosításhoz.

Egyes szakemberek szerint az elektronikus adattárolás lehetőségének megteremtésével módosult a klasszikus háromszintű okmányvédelem és -ellenőrzés.

Hesse amerikai és *Stevens* angol szakértők[2] *már a biztonság hat szintjéről beszélnek az okmány eredetiségének ellenőrzése, illetve a tulajdonosának azonosítása szempontjából.* Ezek a következők:

– Folyamatosan fejlesztett, vizuálisan ellenőrizhető, az okmányt és a tulajdonosát egyértelmű, de egyedi elemekkel, okmányvédelmi megoldásokkal azonosító jellegzetességek (lásd klasszikus okmányvédelem *első szint*).
– Egyszerű okmányvizsgáló eszközökkel ellenőrizhető okmányvédelmi elemek (lásd klasszikus okmányvédelem *második szint*).
– A megszemélyesítéssel felvitt speciális biztonsági, azonosító elemek a gépi olvasással olvasható zónában (lásd klasszikus okmányvédelem *második szint*).
– Az okmányban biztonságos feltételek mellett tárolt biometrikus azonosítók, amelyek az okmány használójának (birtokosának) *egy az egyben (kép/kép)* azonosítását teszik lehetővé (lásd klasszikus okmányvédelem *második szint*).
– Az adatbázisokhoz való engedélyezett hozzáféréseket nyújtó technológiák, megoldások, amelyek lehetővé teszik az *1 : n (kép/adatbázis)* típusú ellenőrzéseket (lásd klasszikus okmányvédelem *második szint*).

1 A biztonsági okmányokban az elsődleges adathordozó a papír- vagy polimeralapú, vagy ezek kombinációjával létrehozott, megfelelő védelemmel ellátott lap vagy oldal.

2 James R. Hesse – Charlie Stevens: Biometrics in travel and identity documents. A compelling case for physical security features. Keesing Journal of Document & Identity, iss. 33, 2010, pp. 21–24. http://www.hidglobal.com/sites/hidglobal.com/files/gov-id-biometrics-travel-and-identity-wp-en.pdf

– Olyan biztonsági elemek és kódok, amelyek csak kriminalisztikai eszközökkel, módszerekkel ellenőrizhetők és magas, úgynevezett szakértői szinten ismertek csak (lásd klasszikus okmányvédelem *harmadik szint*).

A személyes és a biometrikus adatoknak az okmányokban történő elektronikus tárolásával az ellenőrzési módszerek és lehetőségek köre bővül, különösképpen a második szintű védelem és ellenőrzés területén. A fejlesztéseknél hangsúlyozott cél a hivatalos szervek ellenőrzési tevékenységének támogatása, segítése és ezzel együtt a biztonság növelése.

Világszerte nagy erőkkel folyik az automatikus okmány- és személyazonosító ellenőrzési rendszerek fejlesztése, tesztelése. A feladatok összetettsége miatt azonban egyelőre még továbbra sem nélkülözhető az ellenőrzések során az ember részvétele a végső döntések meghozatalában.

Miként változik a klasszikus okmányvédelem az informatikai eszköz kombinációjának hatására?

Az okmányvédelmi fejlesztéseknél alapelv, hogy *minden okmányvédelmi rendszernek* támogatnia kell az okmány eredetiségének és sértetlenségének ellenőrzését.

Az okmányvédelem új elemekkel való bővítése ezért szükségessé teszi az okmánybiztonsági és informatikai védelmi funkciók logikai összerendelését. Ennek egyik lehetséges kombinációját szemlélteti a *2. számú táblázat.*

2. számú táblázat

Az okmánybiztonsági és informatikai védelem logikai összerendelése

Okmányvédelmi kategória	A	B	C
Informatikai védelmi kategória	I.		
	II.	II.	
	III.	III.	III.

A, B, C az okmányok okmányvédelmi besorolása[3] (a klasszikus háromszintű okmánytechnikai fejlesztésekkel, elemekkel). Az *A* kategória a teljes körű, a *B* a részleges, a *C* az adminisztratív védelmet jelenti.

3 86/1996. (VI. 14.) kormányrendelet 2. számú melléklet.

I., II., III., az informatikai védelem szintjei. (A I. szint a legmagasabb, míg a III. a legalacsonyabb biztonságiszint-igényű kategória.)

Egy-egy okmány besorolását, okmányvédelmi szintjének meghatározását minden esetben meg kell hogy előzze a biztonsági kockázatok vizsgálata.

Csak ez a többszintű, komplex felépítés garantálhatja az előnyt az elszánt hamisítókkal szemben!

Miért szükséges tehát ez *a komplex, kiterjesztett biztonság*? Miért nem elég az elektronikus (1 : 1 vagy 1 : n ellenőrzés)?

A válasz egyszerű. Mert előfordulhat *technikai hiba, és a chip nem olvasható, és mert a hamisítók nem tétlenkednek.*

A szakértői tapasztalatok szerint a leggyakrabban előforduló hamisítás, amikor az RF-chip nem működik, vagy nem nyitható meg, illetve a vizuális és a digitálisan rögzített adatok eltérők.

Íme, néhány példa a leggyakoribb esetekre:

– Az okmány eredeti, hamisításra utaló beavatkozás nem fedhető fel, de hibás a chip, nem működik – ebben az esetben az unióban okmányt személyazonosításra el kell fogadni! Ilyen helyzetben a klasszikus módszerekkel történhet az eredetiség ellenőrzése, a hamisítás tényének kizárása.
– Az okmányban sérült vagy hibás a chip, nem működik, és hamisításra utaló beavatkozás fedhető fel általában az adatoldalon, ahol a klasszikus okmányvédelmi elemek sérülése vagy hiánya állapítható meg.
– Az okmány adatoldalán lévő arckép eltér a chipben lévőtől, ebben az esetben a hamisítás ténye általában nagy biztonsággal felfedhető az okmányba épített klasszikus okmányvédelmi elemek vizsgálatával, általában ezek hiánya vagy sérülése állapítható meg (ha azonban az okmány eredeti, nem történt változtatás, természetesen nem kizárt az adminisztratív hiba, a téves adatrögzítés sem).
– Az okmány adatoldala hamis, az okmányvédelmi elemek hiánya és az eltérő előállítási technológia egyértelműen bizonyítja a hamisítást.

Fontos megjegyezni, hogy az okmányvédelem nem véd a kiállítási folyamat hibáitól és a manipulációktól.

A biometrikus személyazonosítás a jövő?

A biometria nemcsak az okmányvédelemben tört előre, hanem széleskörűen, nagy sebességgel fejlődik és terjeszkedik más, személyazonosítást igénylő területen is.

A bemutatott fejlesztések, példák szemléltetik, hogy a biometrikus adat lehet része az okmánynak, az okmányba integrált adathordozón tárolt adat formájában, de lehet adatbázisba gyűjtve.

Az automatikus, csak a biometriára épülő biometrikus személyazonosítást illetően *holland szakemberek*[4] *szerint tíz alapelv, tézis fogalmazható meg a biometria biztonságos és megbízható használatához* az okmányokban és a biometrikus adatokat tároló adatbázisokban. Ezek a következők.

a) A biometrikus személyazonosítás önmagában nem bizonyító erejű, ennek egyik oka az, hogy valószínűség-számításon alapul, és az operátorok által beállított tolerancia-paraméterek határozzák meg a téves elfogadások és visszautasítások számát[5], a másik ok, hogy nem zárható ki a biometrikus adat hamisítása sem.

b) A biometriát tehát nem lehet megalapozott azonosításként elfogadni, csak felismerésként. A biometria összerendeli a személyt az okmánnyal, de *nem mond semmit az okmány sértetlenségéről,* hamis vagy eredeti voltáról.

c) Mivel nem lehet egy biometrikus paramétert azonosításként elfogadni, az okmányok ellenőrzésekor követelmény kell hogy legyen a legalább három azonosító egyezősége (ezek lehetnek *biometrikus* jellemzők, vagy *a nem biometrikus védelmi elemek és a biometrikus jellemzők kombinációja).*

d) A kontrollálatlan szervezeti és emberi tényezők miatt *biztonsági kockázatot jelenthet* a biometrikus alkalmazások *túlzóan széles körű használata.*

e) Fontos, hogy a biometrikus paramétereket ne lehessen hétköznapi célokra alkalmazni.

f) A biometrikus adatok felvételéhez és ellenőrzéséhez szükséges az állampolgárok együttműködése, ezért meg kell teremteni a biometrikus azonosítás alkalmazásának társadalmi elfogadását.

g) A biometrikus adatokat nem szabad az eredeti alkalmazáson kívül használni.

h) A biometrikus adatokat adatbázisban csak megfelelő védelem mellett, kódolt formában szabad tárolni.

i) Az adatbázishoz való kapcsolódás, hozzáférés szabályozása alapkövetelmény. Az adatbázishoz való kapcsolódást regisztrálni és folyamatosan ellenőrizni kell.

4 Jan Grijpink: Safe and reliable use of biometrics – part 2., Keesing Journal of Documents & Identity, iss. 33, 2010, pp.7–13.

5 Az egyes biometrikus azonosító rendszerek használhatóságát a találati arány, illetve a téves elfogadási és téves elutasítási arány jellemzi.

j) Kiemelt feladat a szükségtelen és nem biztonságos biometrikusadat-tárolás megakadályozása, és a biometrikus adatok lopásának és jogszerűtlen használatának rendszeres ellenőrzése.

Ez az előzőekben összefoglalt, az európai tapasztalatokra épülő követelményrendszer, a témakörben folytatott széles körű adatelemzések, kockázatelemzések összegzése minden jövőbeni alkalmazás alapja lehet.

Merre tart az okmányvédelem?

Sokan felteszik azt a kérdést, hogy van-e még jövője a papír- és műanyag-alapú okmányoknak, miért van az, hogy töretlenül nagy erőkkel folyik az okmányok védelmét, a hamisítások gyors felismerését szavatoló, az azonosítást segítő biztonsági elemek, technológiai megoldások fejlesztése. Példaként csak néhány új technológiát, biztonsági okmányokba beépíthető fejlesztést említek. A nanotechnológia, a 3D-s fejlesztések eredményeinek alkalmazása már napjainkban is új távlatokat nyitott a „klasszikus" okmányvédelem fejlesztésében és a hamisítók elleni harcban.

A feltett kérdésre adható válasz egyértelmű. Az okmányokat védeni kell a high-tech támadásoktól, hogy bárhol, bármikor lehetőség legyen az ellenőrzésre, azonosításra, hogy a beépített okmányvédelmi megoldások minden helyzetben segítsék a szakembereket abban, hogy az okmány eredetiségét és sértetlenségét gyorsan és nagy biztonsággal megállapítsák.

Az okmányokba integrált adathordozók tartalmának biztonsága, hitelessége és eredetiségének ellenőrzése új feladatok elé állítja a szakembereket. Az okmánytechnika részévé váló informatikai elem védelmét is tervezni, megfelelő biztonsági protokollal garantálni és természetesen, ahogy más okmánybiztonsági elem esetében is, folyamatosan fejleszteni kell.

Egyes okmányok és adatok esetén az Európai Unió az ellenőrzés lehetőségének és hatékonyságának érdekében előírja az interoperabilitást, ezért a nemzeti megoldások harmonizálása a cél.

A biometrikus azonosítás és a szakértők feladatai

A klasszikus okmányvizsgálat feladata, hogy megállapítsa az okmány eredeti vagy hamis voltát, felfedje, hogy fizikai, kémiai, okmánytechnikai módsze-

rekkel történt-e változtatás egy okmány eredetiségét illetően vagy az okmányon vizuálisan látható adatokban.

Nem kétséges, hogy a jövőben vizsgálni kell az elektronikusan tárolt adatokon végzett esetleges beavatkozásokat is, és ez új feladat, próbatétel a szakértők részére.