KISS PÉTER JÓZSEF

HITELESÍTÉSI TECHNOLÓGIAVÁLASZTÁS ÜGYFÉLSZOLGÁLATON KIALAKÍTOTT ELEKTRONIKUS KAPCSOLATTARTÁSHOZ

A jelenlegi ügyintézési gyakorlat továbbfejlesztésének kulcseleme az ügyfelek azonosítása, nyilatkozataikat tartalmazó dokumentumok elektronikus hitelesítése, letagadhatatlanságának garantálása. Ahhoz, hogy a személyes ügyfélszolgálatokon is tisztán elektronikus kapcsolattartás megvalósuljon, az elektronikus hitelesítési lehetőségek bevezetése szükséges. E feladatra alkalmazott elméleti modellek feltételezései azonban nem mindenben illeszkednek a tényleges gyakorlathoz. Az azonosításhoz felhasználható faktorok (tudás, birtoklás, tulajdonság) a gyakorlat oldaláról nézve az eltérő felhasználási környezetekben eltérő védelmet eredményeznek. Az elektronikus hitelesítéshez külön eszköz az ügyfélnél általános megoldásként nem tételezhető fel. A lehetőségeket áttekintve egy széles körben alkalmazható megoldást jelenthet a biometrikus adatok, azon belül a kézírás, illetve kézi aláírás elektronikus megfelelőjének alkalmazása, a jogszabályi környezetnek megfelelően az azonosításhoz kapcsoltan.

Kulcsszavak: **elektronikus azonosítás, elektronikus dokumentum hitelesítése, ügyfélszolgálat, elektronikus ügyfélkapcsolat, biometria, aláírás, íráskép**

Immár közismert ténynek tekinthető, hogy egy szervezet működésével összefüggő adminisztrációs teher csökkentésében kulcsszerepe van a tisztán elektronikus működési modellre történő átállásnak, mivel a papírformájú iratok kezelése, előírások szerinti megőrzése jelentős terhet jelent mind humánerőforrás oldalról, mind a tárolási kapacitás oldaláról tekintve. Bár impresszív számok jelzik az ügyfelek informatikai lehetőségeinek bővülését, például Magyarországon a személyek internet hozzáférése 79% (Eurostat, 2017), a személyes ügyfélkapcsolat teljes mértékben nem számolható fel. Ennek oka jelentős részben az emberi attitűd. Példának tekinthetjük, hogy bár az elektronikus vásárlások esetében markánsan emelkedő trend figyelhető meg, azonban még mindig igen jelentős a személyes formát választók aránya. Magyarországon az elektronikus vásárlási formára részvételi hajlandóságot az aktív korú népesség 27%-a mutat (Eurostat, 2016), míg az elektronikus fizetések és csoportos megbízások aránya a teljes forgalom 38,9%-a (MNB, 2017). Emellett egyes ügytípusoknál azok tartalmából, vagy biztonsági követelményeiből következik, hogy az ügyféllel személyesen kell találkozni. Ahhoz, hogy a szervezet belső működése teljesen elektronikus formára váltson, meg kell oldani, hogy a személyes ügyfélszolgálaton is elektronikus formát alkalmazzanak. Célszerű megvizsgálni, hogy a szolgáltatók által hozzáférhető (beszerezhető, K+F szakaszán túljutott) technológiák közül melyik javasolható az ügyfélszolgálaton történő elektronikus hitelesítés bevezetésére. A vizsgálat során különös figyelmet kapott a közszolgáltatások ügyfélszolgálati rendszereinél történő alkalmazhatóság, mert ezek esetében mindenképp széles, eltérő digitális írástudású és attitűdű ügyfélkörrel kell számolni.

Elektronikus ügymenet jelenlegi alkalmazási gyakorlatai

Hagyományos megközelítés

Az ügyfelekkel való kapcsolattartás elektronizálásának egyik szokásos fejlesztési iránya, amikor az ügyfél papíralapú jognyilatkozatát rögzítik, majd utólag digitalizálják és a digitalizált formát rögzítik az informatikai rendszerbe, a feldolgozás így elektronikus dokumentum alapján történhet.

Ez azonban nem teljes értékű megoldás, két okból sem. Egyrészt a dokumentum más szervezetet is érintő ügyintézéshez is kellhet (fogyasztóvédelem, bíróság stb.), emiatt nem lehet ömlesztve, strukturálatlanul tárolni. Lényegében a papíralapú iratkezelés összes szolgáltatását fenn kell tartani, azaz a hatékonyság növelés csak részleges lehet a szervezetnél. Emellett ekkor a tárolási és feldolgozási rendszerrel kapcsolatos biztonsági követelmények is lényegesen magasabbak, hiszen az elektronikus dokumentum (mint szkennelt irat) önmagában nem tekinthető hitelesnek. A megoldás zárt rendszerben való tárolást követel meg, mely biztosítja a forrásadatok sértetlenségét, azonban egy informatikai biztonsági probléma (a rendszer elvi zártságának sérülése) esetén a visszaállásnál akár az összes papír újra digitalizálásának szükségessége is felmerülhet, lévén ügyfél hitelesítése ténylegesen nincs az elektronikus dokumentumokon (illetve az elektronikus nyilvántartásban).

Elektronikus aláírás alkalmazása

Másik, elvben alkalmazható út az ügyféltől az elektronikus aláírás megkövetelése. Ilyen megoldásra külföldön korábban voltak elképzelések, főleg a közigazgatási területen. Magyarország is elkezdte bevezetni az elektronikus személyi igazolványt, ami elektronikus aláírás létrehozására is használható. A megoldás nagy előnye az erős jogszabályi alátámasztottság a kapcsolódó bizalmi szolgáltatás alapján (eIDAS, 2017), valamint a problémamentes bizonyító erő. Ezen megoldás esetében azonban az elvi elképzelések és a valóság lényegesen eltértek egymástól. Jó példa erre a széles körű alkalmazási szándékkal bevezetett osztrák Bürgerkarte (Bürgerkarte, 2017) esete. Bár elvben széles körű elektronikus hitelesítő szerepre alkalmas, mind a kártya elterjedése, mind az elektronikus aláírás-

ra alkalmazása korántsem tekinthető általánosnak. Bár az osztrák lakosság 70%-a (Wiki, 2017) bekapcsolódik ez elektronikus kapcsolattartásba, az elektronikus aláírás használatnál 2014-ben csak 18%-os volt az arány. Az időközben megjelent mobiltelefonos (okostelefonos) hitelesítési lehetőség érezhetően javított a helyzeten (2014-ben 15 ezer kártyaregisztráció, 30 ezer okostelefonos alkalmazás regisztráció). Az ausztriai számok alapján elmondható, hogy a fokozódó elterjedés mellett sem lehetne csak erre a hitelesítési módra ügyfélszolgálati kiszolgálást alapozni, s ez esetben még számításba sem vettük a kártyával el nem látható (például külföldi állampolgárok) kiszolgálásának szükségességét. Magyarországon még a Bürgerkarte első generációs változatának megfelelő fizikai kártya bevezetése folyik (e-Személyi), s az igazolványhoz elektronikus aláírás létrehozásához szükséges tanúsítvány igénylése nem kötelező. Mindezek alapján egy szolgáltató számára nem megoldás az ügyfelek elektronikus aláírására való hagyatkozás, annak használatát ugyan indokolt lehetővé tennie, de egyedüli megoldást az elektronikus jognyilatkozati formára semmiképp nem jelent.

Terjedő rossz példa

Egyes szolgáltatók alkalmaznak egy olyan – az ügyfelekkel való korrekt eljárás szempontjából erősen vitatható – megközelítést, ahol a jóváhagyást egy táblaszámítógépen (tableten), történő kézi aláírás elektronikus képének tárolásával oldják meg. E megoldás mögött ugyanis nincs megfelelő jogi felhatalmazás, a digitális aláíráskép rögzítése és tárolása egyedül a postatörvényben (2012. évi CLIX. törvény) szerepel a küldemény átadásának igazolására. A törvény hatálya alá tartozó ügyletekben a módszer alkalmazásának célja egyrészt nem általános jognyilatkozat tétel hitelesítése, másrészt az ott szereplő „ellenkező bizonyításig" kitétel alapján a két tanúval igazolt, a vélelmezett átadási helytől fizikailag eltérő helyen tartózkodás a bíróság előtt legalább is vitatottá teheti a posta állítását. Mivel a sima íráskép elemi eszközökkel másolható, akár egy korábbi aláírás alapján készített, a kijelzőre fektetett fólia segítségével fizikai átírással hamisítható, így ez a megoldás a szolgáltatók számára érdemi jognyilatkozatok rögzítésére nem megfelelő.

Fizikai eszközök alkalmazása

A személyes megjelenésnél történő ügyintézéshez a szolgáltató által rendszeresített eszköz megkövetelése sem járható út. Az otthoni bankoláshoz több bank eseti kódot generáló „tokeneket" biztosít, amelyet az egyes tranzakciók megerősítésére alkalmazni kell, de értelemszerűen az ügyfélnél ez vagy ott van, vagy sem, így a személyes ügyfélszolgálat speciális eszközhöz kötése a gyakorlatban problémákhoz, konfliktusokhoz vezethet. Emellett jogi bizonyító ereje is korlátozott, nem hozható létre vele teljes bizonyító erejű magánokirat. Nem véletlen, hogy jellemzően az ilyen eszközöket biztosító bankok sem követelik meg ezek alkalmazását a bankfiókban.

Mindezek alapján más utat kell keresni a széles ügyfélkör kiszolgálásához. Olyan megoldás kell, aminél elektronikusan jön létre az irat, az ügyfélnek elektronikusan bemutatható s elektronikusan hitelesíttethető. (Kis kockázatú esetekben lehet „bemondásra" ügyet intézni, de általános kapcsolattartási megoldásként az ilyen egyszerűsítés nem alkalmazható, azaz szükséges valamilyen jognyilatkozat hitelesítési megoldás.) A megoldás nem érinti a papíralapú ügyfélpéldány létrehozhatóságát – elektronikus formáról másolatként kiadható – a cél annak elősegítése, hogy a szolgáltatónak ne kelljen papírformában iratot kezelni, őrizni.

Jogi háttér

Szerencsére Magyarországon is jelentősen előrelépett a jogalkotás, és bevezette bemutatott probléma kezelésére is alkalmas „azonosításra visszavezetett dokumentumhitelesítés" megközelítést. E megközelítés lényege, hogy az elektronikus dokumentumot (elektronikus aláírással vagy bélyegzővel) hitelesítésszolgáltató hitelesíti, a személyhez rendelés előzetes azonosításon alapul. Ez megjelenik a 2015. évi CCXXII. törvényben (1.§ 5.), de ami a piaci szolgáltatók számára még fontosabb, e logikára épülő kézi aláírásra visszavezetett hitelesítési forma külön nevesítve megjelenik a Polgári perrendtartásban (325.§ (1) h.).

Már itt szükséges kiemelni, hogy a jogszabályi háttér tehát önmagában egy biometrikus adat dokumentumon történő elhelyezését nem tekinti megfelelő bizonyító erejű megoldásnak, egy személy azonosítása ugyanakkor önmagában még nem igazolja a jognyilatkozatát. A dokumentum hitelessége ez esetben egyrészt a jognyilatkozatot tevő személy megfelelő azonosításán alapul, másrészt gondoskodni kell az azonosított személy dokumentumhoz rendeléséről. Megoldást kell tehát keresni az ügyfelek számára elfogadható azonosítási és ehhez kapcsolódó vagy ezzel kombinált dokumentumhoz rendelési mechanizmusra.

Az informatikai háttér

Az informatikai alkalmazások azonosítási metódusai három faktoron alapulnak (tudás, birtoklás, illetve tulajdonságalapú azonosítás). Az állami szervezetek jelentős részére kötelező erővel bíró 41/2015. (VII.15.) BM-rendelet az egyes kockázati besorolásokhoz konkrét elvárásokat fogalmaz meg, ebben a magasabb védelmi szintet igénylő rendszereknél már két faktor együttes meglétét írja elő. E szabályozás megállapításait a nem kötelezett szervezetek számára is célszerű figyelembe venni, ezért ennek előírásaira a cikkben is támaszkodunk. Indokolt az egyes faktorokra épülő hozzáférhető megoldások áttekintése, mivel sok esetben ezek az azonosításra bevezetett megoldások olyan feltételezéssel élnek, melyek nem teljesen illeszkednek a gyakorlathoz. Az egyes feltételezések és gyakorlatban előforduló megvalósulásuk a következő:

– „csak a személy tudja": a jelenlegi gyakorlatban ez egy igen leegyszerűsített, túlegyszerűsített komponens, amely általában egy PIN-kód vagy jelszó ismeretét jelenti. Jelenleg „statikus" elemről van szó, még ha változtatható is, aligha van olyan felhasználó, aki

minden tranzakció után megváltoztatja. A kódok, illetve jelszavak megjegyezhetősége azok hosszát, bonyolultságát és változtatási periódusát is jelentősen korlátozza, Jelen egyszerűsített formájában, amennyiben a válaszadás statikus elemet érint, a válasz (kód, jelszó) megadása kifigyelhető. Egy mai okostelefon videóképessége bőven elég, hogy viszonylag távolról (így egy szobán, ügyfélszolgálaton belülről) a kód megadása rögzíthető legyen. Itt ki kell emelni, hogy az azonosítás, hitelesítés kockázatánál a figyelem nagyrészt az ismeretlen bűnöző támadásának kivédésére irányul. A gyakorlatban azonban a kriminalisztikában ismert kategória az egymást ismerők közötti bűneset, nem egyszer az alkalmazott, munkatárs a bűnelkövető. Mindezek miatt, bár jelszavas azonosítással ellátott ügyfélkapu-azonosítóval közel 3,5 millió személy rendelkezik Magyarországon, a „tudásra" épülő faktor önmagában, biztonsági kockázata miatt nem tekinthető érdemi védelmi komponensnek. (Nem jelen cikk tárgya, de e faktor dinamikus tudáskiértékelési mechanizmusra építve egy perspektivikus azonosítási irány, ez azonban még nem tekinthető kiforrott technológiának, nincsenek meg a széles körű bevezetési feltételei.)

– „csak a személy birtokában van az eszköz": mind az azonosításnál, mind az elektronikus aláírásnál alapfeltételezés, hogy a szolgáltató által biztosított eszköz (chip kártya, token) kizárólag a hozzá rendelt személy birtokában van. Ez a feltételezés azonban a gyakorlatban nem tud teljesülni. Amint mindennapos használati eszközzé válik valami, onnan kezdve a „védettsége" megváltozik. Egy páncélszekrény kulcsát vélhetőleg gondosan elzárja az őrzője, a lakáskulcsát azonban alighanem a legtöbb ember a táskájában hagyja az irodájában, nem zárja el, amíg rövid időre elhagyja a helyiséget. Hasonló sorsa van ezeknek az elektronikus eszközöknek. Az eszközök őrzési problémája elsősorban a rövid idejű hozzáféréssel elkövetett csalások esélyét növeli, egy ügyfélszolgálaton ez kevésbé probléma. Sokkal inkább gond, hogy az ügyfélnek eleve rendelkeznie kellene egy eszközzel (külön költség ennek rendszeresítése és fenntartása a szervezetnek is), s az igazán jelentős gond, hogy nem garantálható, hogy ügyintézésnél nála lesz. Az elektronikus személyi igazolvány általánossá válásával ez „teoretikusan" alkalmas forma (az azonosítási képessége nem opcionális, mint az aláíró képesség), de a gyakorlatban igencsak megakaszthatja az ügyintézést, ha az ügyfél esetlegesen más igazolvánnyal igazolja magát (például egy útlevelet felmutató külföldit ugyanúgy ki kell szolgálni), azaz a szolgáltatónak párhuzamos ügyintézési modelleket kellene fenntartania.

– „csak a személynek van", ezek a biometrikus jellemzők (például ujjnyomat, irisz kép) de ide soroljuk a kézi aláírást is. Ügyfélszolgálati azonosításra ez a faktor mindenben megfelel, hisz „mindig az ügyfélnél van". Biometrikus adatból többféle van, ezek alkalmazási feltételrendszere ugyanakkor erősen eltérő, s alkalmazásuk gyakran szintén olyan feltételezésen alapul, amely nem feltétlen igazolódik a gyakorlatban. Az elmélet abból indul ki, hogy ami a személynek „van", az nem hamisítható. Itt azonban nem lehet figyelmen kívül hagyni a felhasználási környezetet. Például egy ujjnyomat viszonylag könnyedén megszerezhető (elég kezébe adni egy megfelelő tárgyat), s az ujjnyomat „szimulálása" (a nem egyedi biometrikus jellemzők például hőmérséklet, nedvesség hozzáadása mellett is) megoldható technikai feladat. Egy arcképmás, a filmszakma maszkmestereinek munkái ezt igazolják, szintén nem tekinthető hamisíthatatlannak. A biometrikus adatok felhasználásánál ugyanakkor tekintettel kell lenni az Európai Parlament és Tanács személyes adatok védelmével kapcsolatos 2016/679. számú (GDPR) rendeletére, amely ezekre fokozott adatvédelmi követelményeket fogalmaz meg (például hatástanulmány szükségességét).

Ezekből az egyszerű példából is látszik, hogy az egyszerű elméleti megoldások a látens feltételezéseik miatt nem felelnek meg közvetlenül az elektronikus ügyfélkapcsolatok elvárásainak, a biometriára visszavezetett közvetett hitelesítés ugyanakkor alkalmasnak tűnhet az ügyfelek széles körénél történő közvetlen alkalmazásra. Mivel a magyar vállalati szféra és közigazgatás a technológiaváltás határára ért, és elkezdődött az elektronikus ügyintézésre áttérés, így indokolt annak a részletesebb vizsgálata, hogy milyen azonosítási és kapcsolódó hitelesítési formát célszerű alkalmazni az ügyfélszolgálatokon, erre hol és mely biometrikus technológia a legalkalmasabb.

A biometriai azonosítási és kapcsolódó hitelesítési formák alkalmazási lehetőségei

A biometrikus jellemzők és felhasználási lehetőségeik

Igen széles a biometrikus adatok köre (Saini, 2014), ezekből, a gyakorlati felhasználhatósági követelményekre tekintettel, azon technológiák vizsgálatára szorítkozunk, amelyek a magyar piacon hozzáférhetők, referenciával rendelkeznek, vagy legalább is bevezethetőségüket már idehaza vizsgálják, vizsgálták. A biometrikus adatra építkezésnél figyelembe kell venni, hogy az adat felvételezéséhez mennyiben szükséges magának az érintettnek a közreműködése, hisz a tudta nélkül történő felvételezés lehetősége nagyban növeli a felderíthetetlen visszaélés lehetőségét (ami a bevezetendő szolgáltatás fenntarthatóságára jelent kockázatot). Emellett természetesen lényeges mérlegelési szempont az alkalmazott technika társadalmi elfogadottsága is, például kriminalisztikai alkalmazása miatt humán ellenállás tapasztalható az ujjnyomat alkalmazásánál.

A biometrikus azonosítás alapja a személyhez rendelési mechanizmus kialakítása. Ennek előzetes ellenőrzésre alkalmas formája egy mintaadatbázis létrehozása. Hitelesítési – tehát nem azonosítási – célú felhasználásnál léteznek csak utólagos ellenőrzést lehetővé tevő megoldások

– amikor egy vitatott esetnél utólagos mintával történik az összehasonlítás -, ennek jogszabályi alátámasztottsága azonban nem egyértelmű.

A biometrikus adatok felhasználásánál kritikus szempont a hosszú távú állandóság kérdésköre. Egy kompromittálódott PKI-alapú kulcs letiltható, a személyhez teljesen új kulcs rendelhető, azonban ez nem tehető meg a személy minden biometrikus adatával. (A változtathatatlanság problémáján kombinált megoldással némileg segíteni lehet (kulcs+biometria), de ekkor a biometria eszközfüggetlenségének és állandó rendelkezésre állásának előnyét veszítjük el.) Ügyfélszolgálatokon történő alkalmazhatóság esetében előnyt élveznek azok a megoldások, ahol szükség esetén az adat cseréjére mód van. A következő néhány bekezdésben áttekintjük a piacon elérhető azonosítási megoldásokat:

– *ujjnyomat:* jelenleg legismertebb, legelterjedtebb megoldás. Előnye, hogy egyre pontosabb felismerő algoritmusok és igen olcsó, könnyen használható mintavevő eszközök léteznek, valamint egyes igazolványokon (így az útlevélen) ez az adat elektronikusan már szerepel, azaz személyhez rendeltsége államilag igazolt. Hátránya ugyanakkor, hogy az egyik legkönnyebben megszerezhető és hamisítható biometrikus adat. A képi forma megszerzése kifejezetten egyszerű, s az ellenőrzés kijátszása sem nehéz, figyelembe véve, hogy az egyéb jelenleg mérhető bőrjellemzők változnak, és nem egyediek (hőmérséklet, nedvesség, véráramlás). Figyelembe kell venni azt is, hogy csak a képi forma ellenőrzése oldható meg egyszerű (olcsó) eszközökkel, a kiegészítő adatok megbízható mérése jelentősen drágítja az ellenőrzési környezetet. Az ujjnyomat állandó, ezért adatbázisban tárolása társadalmi szinten szenzitív kérdéskör, az e-személyi kapcsán is tartós központi tárolás helyett csak a kártyán történő rögzítésre van lehetőség. Az ujjnyomathoz kapcsolódó kriminalisztikai kép miatt egy szolgáltató általi nyilvántartása sem tekinthető az ügyfeleknél széles körben elfogadtatható megoldásnak.
– *írisz kép:* az íriszkép-alapú biometrikus adatok a szem szivárványhártyájának részletes képén alapulnak, melyről megfelelő felbontású kép illegális megszerzése némileg bonyolultabb az ujjnyomathoz képest, de a technológia fejlődésére tekintettel korántsem megoldhatatlan. E témakörhöz kapcsolódó érdekes eset, hogy egy nagyfelbontású arcfelvétel, és egy évekkel később készült ismételt fotó alapján sikerült a portrékon szereplő személyek azonosságát az írisz kép nagyítása és összevetése alapján igazolni (Daugman, 2002), ami jelzi, hogy e technológia is lehetőséget ad a távoli, akár a személy tudtán kívüli leolvasásra, így nem zárja ki a személyiséglopást. Az azonosításhoz szükséges eszköz egyre egyszerűbb (egyes okostelefonokon is várhatóan megjelenő szolgáltatás), de ez is állandónak tekinthető adat, így az elfogadtatási problémák ennél is fellépnek.
– *vénakép* (Syazana-Itqan, 2016): nehezebben megszerezhető biometrikus adat a kéz érhálózat elhelyezkedéséről készülő mintavételezés. Az előbbieknél lényegesen kevésbé lehet feltűnés nélkül, az érintett tudomása nélkül mintát venni. Visszaélés szempontjából is magasabb védettséget jelent az ujjnyomathoz képest, ugyanakkor jóval bonyolultabb (költségesebb) ellenőrző eszközt igényel. A hazai bevezetési tapasztalatok alapján (stadion beléptető rendszerek) a bevezetésével szemben kifejezett idegenkedéssel is számolni kell. Mivel ez is állandó adat, a minta központi tárolása itt sem problémamentes.
– *arcképmás:* a maszkírozás jól ismert lehetőség a színház/film területéről, így még az antropológiai méretek vizsgálata sem jelent valódi garanciát egy tudatos, professzionális visszaéléssel szemben. Kiegészítő elemként természetesen szükséges a személyes megjelenésnél, de kizárólagos formában, különösen az okmányon szereplő kicsiny kép alapján, nem biztonságos. A technológia megbízhatóságát elsősorban az rontja le, hogy jelenleg 2D statikus képi feldolgozás dominál. A 3D észlelés (sztereo kamera) és a véletlenszerűen kért dinamikus kiértékelés (mosolyogjon, most húzza össze a szemöldökét) jelentősen javíthatja a felismerés pontosságát, egyelőre azonban a hozzáférhető, megfizethető technológiák nem ezen alapulnak.
– *hang:* a hang a leginkább külső körülmények miatt (azaz nem az ügyfél szándékából adódóan is) változó jellemző, hisz egy hideg ital, megfázás igen jelentős változást idéz elő, a torokfájás még a beszéd dinamikáját is jelentősen megváltoztatja. Emiatt az ügyfélkapcsolatokban e technológia széles körű alkalmazása (különösen önálló elemként) nem javasolt.
– *kézírás, kézi aláírás:* a legegyszerűbb, legismertebb biometrikus adat. Természetesen nem kizárólag a képi formát értjük alatta, hanem az írás további jellemzőit is (nyomáserősség, sebesség, ezek változási dinamikája). A legtöbb embernél az aláírás, de különösen egy szöveges írásminta jellemzői oly mértékben egyediek, hogy azonnali hamisítása igen nehéz. (Olyan szöveget elő lehet állítani, amely a személy írásának, aláírásának felel meg, de ellenőrzési eszközön történő írásnál, személyes ügyfélszolgálatnál, nyilván nem lehet mikrorobotot ráhelyezni az aláíró táblára.) A megoldás mögöttes adata nem állandó, egy aláírást megváltoztathat az ügyfél, kiterjesztve írásmintára pedig a „tudásalapú" elemmel is kombinálható. Az aláírásminta maga elfogadottan tárolt (lásd bankok gyakorlata), így elfogadtathatósága egyszerűbb. Ki kell ugyanakkor emelni, hogy az aláírásminta hagyományos azonosítás célú alkalmazása két okból is aggályos. Egyrészt ellentétben az ujjnyomattal, itt nem vélelmezhető, hogy nincs két egyforma aláírás, másrészt a mintaadatbázisban keresés funkció megvalósítása komoly adatvédelmi aggályokat vethet fel. Jelenleg általános bizonyító erő más azonosítási megoldással kombinálva a kézi

aláírásra visszavezetett hitelesítéshez kapcsolható (Polgári perrendtartás alapján).

Az ügyfelekkel való kapcsolattartás különböző formái

Az egyes azonosítási lehetőségek felhasználhatósága nagyban függ a felhasználás körülményeitől is. A felhasználási körülményeket az *1. ábra* szerinti alesetekre bonthatjuk, melyeket két fő szempont szerint különíthetünk el.

1. ábra

Az ügyfelek különböző nyilatkozattételi környezetei

		nyilatkozattétel helye	
		felügyelt	nem felügyelt
nyilatkozattétel eszköze	ellenőrzött	személyes ügyfélszolgálat	ügyfélszolgálati önkiszolgáló kioszk azonosítási eszközzel
	nem ellenőrzött	ügyfélszolgálati önkiszolgáló kioszk azonosítási eszköz nélkül	bárhol (pl. otthoni elérés) bárhogyan

A nyilatkozattétel helye esetében azt vizsgáljuk, hogy a nyilatkozattétel a szervezet szempontjából megbízható személy által felügyelt környezetben történik-e, ahol a speciális beavatkozások (eszköz megbontása, ujjnyomatadás helyett speciális eszközök igénybevétele stb.) kizárhatók, míg a nyilatkozattétel eszköze szerinti bontás esetében kérdés, hogy az eszköz, amelynek igénybevétele szükséges a nyilatkozatadáshoz, a szervezet számára ellenőrzöttnek tekinthető-e (ilyen például egy kártyaolvasó, az aláíró tablet).

a. *ellenőrzött eszközön, felügyelt* környezetben*:* itt a jognyilatkozat tétel olyan eszközön történik, amely garantáltan nem tartalmaz illegális elemet, és maga a nyilatkozattételnél a személyes megfigyelés illegális eszköz bevonásának kizárására biztosított. Nem lehet tehát speciális eszközöket a géphez illeszteni (például ujjnyomat szimulátort, ami fűtéssel, nedvesítéssel kombinált eszköz). Tipikusan ilyen helynek felel meg a megfelelően kialakított személyes ügyfélszolgálat.
b. *ellenőrzött eszközön, nem felügyelt* környezetben: ennél az ellenőrző eszköz (és így maga az ellenőrzési eljárás) ellenőrzöttnek, azaz megbízhatónak tekinthető, de már az ellenőrzési körülmények nem ismertek. Ilyen megoldás például a vizuális megfigyelés alatt álló önkiszolgáló kioszk telepítése az ügyfélszolgálaton. Az ilyen kioszk jellemzően azonosításkötelezetten nyújt szolgáltatást, ezzel nagyban csökkentve az információbiztonsági kockázatot. Az eszköz megbontására, nagyobb méretű visszaélési eszköz használatára nincs lehetőség (feltűnő beavatkozás), ugyanakkor az azonosítás folyamatának figyelemmel kísérése nélkül a visszaélés nem zárható ki. Egy ujjnyomat érzékelőnél például egy hamísított eszköz használata akár bekövetkezhet.
c. *nem ellenőrzött eszközön, felügyelt* környezetben: olyan kapcsolattartási helyek, ahol már magára az eszközre nem terjed ki a megbízhatósági vélelem. Ilyen környezetnek lehet tekinteni egy ügyfélszolgálaton a vizuálisan ugyan megfigyelt, de speciális azonosítási eszközök nélkül kialakított internetes végpontokat. Ezek jellemzően azonosítás nélkül nyújtanak szolgáltatást. Ilyen helyeken az azonosítást igénylő tranzakcióknál jelentős információbiztonsági kockázattal kell számolnia az ügyfélnek, hisz a mai komplex informatikai rendszerekben nehéz annak garantálása, hogy a felhasználó adataiból minden garantáltan törlődjön a rendszerből.
d. *nem ellenőrzött eszközön, ismeretlen környezetben végzett tranzakciók:* jellemzően ilyenek az otthonról az ügyfelek által végzett tranzakciók. Ilyennek minősül egy vizuális megfigyelés nélküli kioszk (például folyosón elhelyezve), ahol akár fizikai megbontás sem zárható ki teljesen.

Az ügyfélszolgálat szempontjából az a) eset minőségileg eltérő kezelést igényel a többi esettől. A személyes megjelenésnél az ügyintéző kontrollja a jelenlegi jogfelfogásban magasabb biztonsági szintet jelent, eleve sok olyan ügylet van, ami kizárólag személyes megjelenéssel végezhető. Persze ide sorolhatók az ügyfelekkel való egyéb személyes találkozáson alapuló ügyintézés is (szolgáltató helyszíni kiszállása), ha az alkalmazott ellenőrzött informatikai eszköz a szolgáltató munkatársa birtokában van. Ez a tipikus ügyfélszolgálati ügyintézési eset, aminél a bevezetésben megfogalmazott problémát meg kell oldani. A többi esetnél már korlátozottabb szolgáltatási kör, az otthoni eléréshez eltérő, szűkített szolgáltatási portfólió és azonosítás társulhat. Például a b) eset szerinti azonosítást végző kioszk esetében megkövetelhető megfelelő eszköz (például kártya) megléte, azaz érdemi önkiszolgálást a kockázat kézben tarthatósága érdekében csak ennek birtokában lehet végezni.

Jelen cikk kifejezetten az ügyfélszolgálatokon alkalmazható technológia kiválasztásának körülményeire szorítkozik, így a továbbiakban az a) eset szerinti ügyfélszolgálatok jellemzőivel foglalkozunk.

Az ügyfélszolgálati környezet kockázati tényezői

Az ügyfélszolgálaton az ügyfél és ügyintéző egyszerre van jelen, ahol az ügyfél tevékenységét az ügyintéző felügyeli, „tanúsítja". A gyakorlatban azonban ez sem ilyen egyszerű, mivel két emberi szereplőnél egyformán előjöhet biztonsági kockázat, nem kizárható az ügyintéző általi visszaélés, ezt igazolja, hogy még a magas biztonsági szintet igénylő okmánykiadásnál is előfordult büntetőjogi következményekkel járó visszaélés.

Az ügyfélszolgálatokon előforduló esetleges visszaélések csökkentése és a visszaélések lehetőségének kizárása a szolgáltatók alapvető célja, mivel az inkorrekt viselkedéssel létrehozott jognyilatkozatok súlyos anyagi veszteséggel és hosszas peres eljárásokkal járhatnak. Az

ügyintéző, illetve az ügyfél magatartásán alapuló ügyfélszolgálati kockázati eseteket a *2. ábra* nevesíti.

2. ábra

Az ügyfél, illetve ügyintéző magatartásformáinak kockázati tényezői

		ügyintéző	
		korrekt	inkorrekt
ügyfél	korrekt	normál eset	személyiség lopás
	inkorrekt	személyiség lopás vagy szabály kijátszása	összejátszás

a. *ügyfél és ügyintéző korrekt:* itt csak a tranzakció hosszabb távú igazolása az érdekes, akár a szervezet által hitelesített dokumentum is elég lenne, különös követelményt ez az eset nem támaszt, így külön szempontot nem jelent a technológiaválasztáshoz.

b. *ügyfél korrekt, de ügyintéző inkorrekt:* ez az eset ma még kevés figyelmet kap, de a jövőben előtérbe kerülhet, ha a kézi aláírás visszaszorul. Meg kell akadályozni, hogy az ügyintéző más nevében illegális tranzakciókat végezhessen, jognyilatkozatokat tehessen. A technológia szempontjából erre a jelenlegi válasz a birtokláson alapuló eszköz igénybevétele, mint amelyen az elektronikus személyi igazolvány. Azon túl, hogy, mint feljebb kimutattuk, teljes körű ügyfélkör lefedésre nem alkalmas, az eszköz birtoklása sem jelent garantált személyhez rendelést. Például családon belüli visszaélésnél az ügyintéző elhozhatja házastársa kártyáját, felhasználva családjogi nyilatkozatra.

c. *ügyfél inkorrekt, ügyintéző korrekt:* ebben az esetben a birtoklásalapú azonosítás csak látszat biztonságot jelent. Önmagában eleve nem ismert, kihez tartozik egy chip-kártya, tehát csak hitelesítésre vagy elektronikus azonosításra használva más személyiségével ügyet lehet intézni. Ez lehet időlegesen eltulajdonított kártya (például családon belül a házastárs tudta nélkül, ahol a PIN-kód ismerete is megoldható), de tudatos visszaélés is (például nyelvtudás igazolása esetén egy állampolgársági eljárásban, más személy jelenik meg a vizsgálaton). Ha az ügyintéző gondos, és az igazolványon lévő fénykép alapján is azonosít, valamelyest korlátozódik a lehetséges visszaélések köre, de a maszkírozási lehetőség miatt valójában még így is igen széles körű visszaélésekre lesz lehetőség (nem beszélve például egy kínai vagy mongol születésű ügyfélről, akiknél európai archoz szokott ügyintéző a fénykép alapján történő azonosítást csak igen nagy hibaaránnyal tudja elvégezni). Az ügyfél csalási szándéka ellen ellenőrzött környezetben elsősorban a biometrikus adatok alkalmazásával lehet védekezni, ami speciális eszközök alkalmazása nélkül lényegében kizárja az ügyintéző megtévesztésének lehetőségét.

d. *ha ügyfél és ügyintéző összejátszik* (amire több konkrét feltárt bűnügy a gyakorlati példa), akkor közösen jelentősen nagyobb kockázatot jelentenek az illegális tranzakciókra. Ha ügyintéző előtt kell igazolni állampolgárságot, s az ügyintézőt lefizették, akkor nem fogja vizsgálni, hogy az aláíró kártyához tartozó személy azonos-e a megjelenttel, s még hangfelvétel, képfelvétel sem fogja igazolni a visszaélést (megfelelő öltözet, némi maszkírozás). Ilyen esetben a szolgáltatók sincsenek védve egy előnytelen megállapodás megkötésétől. Ilyen esetben is a biometria jelenti a megfelelő korlátozást. E szempontból eltérően viselkednek az egyes biometriai jellemzők. Egy műujj, műtenyér, vagy akár az írisz-ellenőrzést becsapó műszem alkalmazása – lévén messzebbről nem látni, mit tesznek az ellenőrző eszközre, még csak-csak elképzelhető. A kézírás hamisítása viszont igen nehéz, hisz a képi hasonlóságot gyakorlással meg lehet ugyan tanulni, az egyéb jellemzők (nyomáserősség, dinamika) egyezéséhez azonban már sokkal komolyabb eszközháttér és felkészülés kell. Különösen igaz ez, ha nem aláírás, hanem szövegminta alapján történik az ellenőrzés. E megközelítés hatékonysága és biztonsága az íráskép ellenőrzési technológiák további fejlődése estén, dinamikus mintaszövegek alapján történő ellenőrzés esetén még jelentősen javítható, hiszen minimális az esélye annak, hogy a visszaélő ilyen esetre fel tudjon készülni, a kért szöveget a célszemély írásának megfelelően tudja reprodukálni.

Következtetések

Kiindulva abból, hogy a papíralapú kapcsolattartás mind biztonsági, mind hatékonysági okból vissza kell, hogy szoruljon, az ügyfelek által közvetlen végezhető elektronikus hitelesítés (elektronikus aláírás) elterjedési korlátai miatt a személyes ügyfélkapcsolatoknál azonosítás, és azt is felhasználva a jognyilatkozat elektronikus hitelesítése szükséges. Áttekintve a potenciális visszaélési lehetőségeket, a jelenleg széles körben kínált megoldások (így a jelszavas azonosítás, a chipes kártya alapú azonosítás), bár központi szolgáltatásra építve (451/2016. (XII.19.) Kormányrendelet, azonosításra visszavezetett dokumentumhitelesítés) igénybe vehető, kimutathatóan nem minden szituációra nyújtanak kellő védelmet, illetve csak az ügyfelek korlátozott körénél alkalmazhatók. Mivel az elektronikus kapcsolattartás általánossá válása csak most van folyamatban, így önmagában az, hogy a potenciális visszaélések még jelentős problémát nem jelentettek, nem igazolja, hogy a jövőben az egyre szélesebb körű felhasználás során ne válhatnának kritikus problémává. Emellett megfigyelhető, hogy egy technológia bevezethetősége nagyban függ a társadalmi elfogadtathatóságával, ami részben összefügg a megszokott, átlátható megoldásokhoz való hasonlatosságával. A legkönnyebben olyan megoldás vezethető be, amely nem igényel speciális, külön gondoskodást igénylő eszközt, ami az „ügyfél birtoklásán alapuló" kategória helyett az „ügyfél tulajdonságaira épülő" kategória előtérbe

kerülését jelentheti. Itt is hangsúlyozni kell, hogy ez nem a hagyományos „birtokláson alapuló" kategória megszűnését jelenti, itt eltérő ügyfélcsoport igényről van szó. Az okostelefonon valós idejű online életet élők számára az okostelefon szolgáltatási köre, majdan az azonosításba, akár közvetlen hitelesítésbe – elektronikus aláírásba – bevonása jelenti a kényelmes megoldást, de a szervezetek ügyfélkapcsolatainál ez csak egy csoportja az ügyfeleknek, ezért szükséges olyan megoldást (is) alkalmazni, ami az emberek szélesebb köre számára egyszerűen elérhető, s ez a biometrikus adatokra alapozás. A személyes kontaktusnál, ahol az ellenőrzés ellenőrzött környezetben, ellenőrzött eszközzel történhet, a biometrikus adatra, az aláírás- és írásminta-alapú (arra visszavezetett) hitelesítésre való alapozás igen perspektivikus megoldást kínál, jelentősen csökkentve több, másként nehezen kontrollálható kockázatot.

Az írásképalapú hitelesítési megoldás

A biometrikus megoldások jellemzőit áttekintve megállapítható, hogy a széles körben bevezethető, relatíve alacsony hamisíthatóságot biztosító megoldás az írásképre visszavezetett hitelesítés. Az embereknek a gyakorlatban egyedinek tekintett írásképe van (ami alatt nem önmagában az írás formája, hanem a létrehozó vektor, sebesség, íráserősség, gyorsulás is értendő). A kézírás alesete a kézi aláírás, ami jóval kevesebb információt jelent egy hosszabb szöveg kézi leírásához képest, de a hozzáférhető informatikai támogatások jelenleg az aláírásra koncentrálnak.

Lényeges szempont, hogy a biometrikus jellemzők állandósága felveti a másolhatóságot, ezért önálló elemként a jog hitelesítési formának nem ismeri el. A másolhatóság miatt nem járható út, hogy a kézírás biometrikus jellemzőit az irathoz csatoljuk, hisz a kézi aláírás jellemzői megszerezhetők (az adott ügyfél sokszor, sok helyen aláír), s utólagosan az iratra másolhatók, manipulálhatók. Ezt felismerve az elektronikus formában felvett kézi aláírás hitelesítésként történő alkalmazását a magyar jog külön jogszabályban meghatározott szolgáltatáshoz rendeli, s a hitelesítésnél az azonosításra visszavezetett dokumentum hitelesítési logikát követi.

Lehetséges kialakítások

A kézi aláírás elektronikus formájának hitelesítési célú felhasználásánál tehát a személyhez és aláíráshoz rendeltséget a szolgáltató igazolja, s nem a biometrikus adat, azaz azonosításra szükség van. A kézi aláírás beemelése a folyamatba ugyanakkor a visszaélések – más személy, vagy az ügyintéző személyiséglopása – kockázatát csökkenti. A szolgáltatás kialakításánál két, jellemzőit tekintve lényegesen eltérő megoldási mód férhető hozzá.

Mintatár nélküli megközelítés (a)

A minta nélküli megközelítésnél a biometrikus adatot (illetve abból képzett adatot) titkosítva rendelik a dokumentumhoz, ahol a titkosítás feloldása a szolgáltató kezében marad. E megközelítésnél nincs szükség előzetesen felvett és tárolt írásmintára, így viszonylag egyszerű informatikai megoldást igényel. Ennek összetettebb (adatvédelmi szempontból erősebben védett) formája, amikor a biometrikus adatot (titkosítva) egy külön szolgáltatónál tárolják, a dokumentumra ténylegesen csak az íráskép vizuális formája kerül rá. E megoldás előnye, hogy nem igényel előzetes regisztrációt, s csak az utólag vitatott jognyilatkozatoknál kell az arra jogosult hatóságnak a biometrikus adatot elkérnie és szakértővel – aktuálisan az érintett ügyféltől bekért minta alapján – ellenőriztetnie. A módszer alkalmazása elsősorban ügyféloldali védettséget jelent, így nem véd például az ellen, ha ügyfél tudatosan másképp írt alá, majd a későbbiekben a nyilatkozatot vitatja. Mivel az aláíró személyét a szolgáltató igazolja, így e megoldáshoz magas biztonsági szintű azonosítás szükséges, és az utólagos bizonyíthatóságról külön gondoskodni kell.

Mintaellenőrzést alkalmazó megközelítés (b)

A mintaalapú megközelítésnél aláírás-mintatárat állítanak fel, ahova az ügyfél biometrikus adatait szigorú személyazonosság-ellenőrzést követően veszik fel. Itt a hitelesítéskor a dokumentumon – az aláírás megszokott vizuális képen túl – csak a szolgáltató igazolása szerepel, hogy a hitelesítési célú aláírás megtörtént, és az aláírásminta egyezett a mintatárban az ügyfélhez rögzített mintával. E megoldás jól alkalmazható ott, ahol az ügyfél a szolgáltatás igénybevételéhez eleve kapcsolatba lép a szolgáltatóval (szerződéskötés), mert az ellenőrzött körülmények közt rögzíthető a minta (például négy szem elv alapján ügyfél igazolványában szereplő adatokhoz rendelve), a későbbi megjelenésekkor már nem igényel magas ellenőrzési szintet az azonosítás (mivel a mintaellenőrzés maga egy lényeges biztonságnövelő elem). A kézírásalapú hitelesítés ilyen módon történő alkalmazása mind az ügyfél, mind a szolgáltató számára magasabb védelmi szinttel rendelkezik, miközben az ügyfél számára a minden napos használata csekély teherrel jár (akár igazolvány bemutatása alapján ügyintéző általi azonosítás is elfogadható).

Alkalmazhatósági körülmények

A két megközelítés között különbség, hogy a mintatár nélküli (a) változat gyakorlatilag a papíralapú kézi aláírás elektronikus megfelelője (ott sem tudjuk, valójában ki ír alá, s valóban ez-e a megszokott aláírása), a mintaellenőrzést alkalmazó (b) változat viszont már ennél magasabb tényleges bizonyító erőt képvisel. (A technikai és elméleti különbség mellett sem szükségszerű, hogy a jogi megítélés mindkét esetben eltérő legyen.)

Megjegyzendő, hogy jogszabályok a papíriratnál is külön kezelik az egyszerű írásba foglalást a teljes bizonyító erejű magánokirattól. Ez utóbbinak felel meg, ha a teljes iratot az érintett kézírással írja, vagy gépírás estén az aláírását két tanúval igazolja. Cégek nevében eljáró személyeknek aláírási címpéldányt kell közjegyző előtt készíteniük és az eljárásokban bemutatniuk, a komolyabb kockázatú jogügyletekben pedig megjelent az ügyvédi ellenjegyzési kényszer. Ez érthető, ha a *2. ábrán* bemu-

tatott, ügyfél inkorrekt magatartásán alapuló kockázati tényezőket is figyelembe vesszük. Amennyiben az ügyfél csalni akar (például később a nyilatkozatát le akarja tagadni), aláírásminta nélkül nehezen szűrhető ki a szándékos aláírás-torzítás (papíresetben sem, például nem a megszokott kezével ír alá). Elsősorban a szolgáltatók számára problémás tehát, ha ügyfél valamire kötelezettséget vállal, de ezt oly módon írja alá, amit később letagadhat, mert még csak nem is hasonlít a valós aláírására.

A mintaalapú megközelítésnél a mintarögzítésnél elengedhetetlen az ügyfél előzetes és erős azonosítása (igazolvány), s az igazolványokon szereplő aláírás is támpont lehet egy gyanús esetben. Magánál a felhasználásnál (hitelesítési célú aláírásnál) viszont kis kockázatú esetben azonosításra elegendő a vélelem (bemondja a nevét, lévén aláírás mintájának egyeznie kell), magasabb kockázatnál – például szerződésmódosítás – is elég bemutatnia az igazolványát. Ez a papíralapú ügyintézésnél megszokott eljárás, azaz az ügyfelek számára nem jelent többlet terhet, szokatlan eljárást. Mivel maga a biometrikus adat csak az ellenőrzésben vesz részt, zárt rendszerű kialakítás szükséges (a dokumentum hiteléül szolgáló igazolás a tényleges ellenőrzés nélkül ne legyen kiállítható). Az aláírás-mintatár ugyanakkor egyes személyekben ellenérzést válthat ki (bár a bankoknál ez bevett gyakorlat a papírügyleteknél, így szerződéskötést alkalmazó szolgáltatóknál tömeges ellenkezéssel nem kell számolni). Megjegyezzük, hogy az aláírás-mintatár felállítása esetén az adatvédelmi jogszabályokra tekintettel a biometrikus adatbázisban keresés nem alkalmazható (azonosításra adatvédelmi okból nem használható a mintatár), így a mintaellenőrzés csupán ellenőrzési lehetőség arra, hogy az azonosított ügyfél aktuális írásmintája a tárolt mintával egyezik-e. A hazai szigorú adatvédelmi szabályokra tekintettel az esetleges közigazgatási felhasználásnál az összerendelési nyilvántartáson keresztül kellene az adatot ügyfélhez rendelni, hogy ezzel is csökkenthető legyen a támadások kockázata (önmagában a minta egyes biometrikus adatai felhasználhatatlanok).

A minta nélküli megoldásnál is szigorítható az ellenőrzés az azonosító igazolványon szereplő aláírás mintával való összevetéssel (jogosítvány, személyi igazolvány tartalmaz aláírás képet), de a normál üzleti tranzakcióknál ilyen mélységű ellenőrzés nem feltétlenül életszerű. A mintatáralapú, illetve mintarögzítés nélküli megoldás közül való választáshoz az adott ügyfélszolgálaton vizsgálni kell az esetleges hamis hitelesítés következményeit az ilyen módon intézendő ügyekre, s ezt kell összevetni az egyes megoldások bevezetési feltételeivel (költsége, elfogadottsága stb.).

Mindkét megközelítésre igaz, hogy az ügyintézéskor az ügyfelet mindenképp azonosítják, személyes ügyintézésnél tipikusan az ügyintéző által (jellemzően okmány alapon, de más technika is alkalmazható), s a jognyilatkozat megtételénél annak kiegészítését szolgálja az elektronikus eszközön (aláíró padon) készített kézi aláírás. Mintatár esetén az ügyintéző által végzett azonosítás a felhasználáskor (dokumentumhitelesítéskor) lehet alacsonyabb biztonsági szintű, lévén az aláírás egyezés ellenőrzése itt bizonyosságnövelő tényező. Lényeges kiemelni, hogy a Polgári perrendtartás. alapján joghatás csak az azonosítással kombinált hitelesítés esetén lehetséges, azaz teljes bizonyító erő csak akkor rendelhető e formához, ha az azonosítás megtörténik (ügyfél elektronikusan vagy az ügyintéző személyesen az azonosítást elvégzi), s a személyhez rendelést a dokumentumhoz rendelt igazoláson feltüntetik.

Mindkét megoldás szolgáltatóra épít (ezt a hazai jogszabály a bizonyító erőhöz megköveteli)., s mindkét megoldás alkalmazása a papíron megszokotthoz hasonló az ügyfelek számára. Az iratot előbb láthatja az aláíró eszközön, megfelelő programozás esetén a „szokott helyen" az irat alján ír alá, megjelenik az aláírásának képe, majd a hitelesítő záradék, amiben a szolgáltató igazolja a személy azonosságát (ki írta alá). A mintatár nélküli megoldásnál az adatvédelmi kockázatot jelentősen csökkenti, ha a biometrikus adatot nem csak titkosítják, de nem a dokumentummal tárolják, hanem a dokumentumra hivatkozással együtt külön szolgáltató őrzi vita esetére.

Mindkét megoldásra igaz, hogy a biometrikus adat felhasználását az Európai Parlament és Tanács GDPR-rendelete alapján adatvédelmi hatásvizsgálattal kell alátámasztani.

Kiterjesztési lehetőségek

Amíg az ujjnyomatnál elfogadott, hogy egyedinek tekinthető, addig az írásképnél ugyan valószínű, de ez nem igazolt, és jellegénél fogva „tanulható". A megoldás biztonsági szintjét ezért érdemes tovább növelni az aláírás mellett kézírási minta ellenőrzésével. Ennél az ügyfél mintaadáskor ellenőrző szavakat kézírással megad („tudásalapú" faktor bevonása), amelyet hitelesítéskor leír (de az iratra nem kerül rá). Mivel az aláírás-kezelő programok grafikus objektumot értékelnek, ezek a szavak az aláírással azonos módon értékeltethetők ki velük. Ez egy olyan speciális „tudásalapú" faktor, ahol a megfigyelhetőség csak korlátozottan növeli a kockázatot, lévén az adott szó leírásának biometrikus jellemzői távolról nem megfigyelhetők, így nincs mit „begyakorolni" (e kockázat megfelelő pult elrendezéssel, rálátás kizárással tovább csökkenthető).

A „tudásalapú" faktoros kiegészítés, az ügyfél által választott szó (vagy szavak) beépítése a hitelesítési folyamatba mind a mintatár nélküli (a), mind a mintaellenőrzést alkalmazó (b) megoldásnál alkalmazható. A mintaellenőrzést alkalmazó megoldásnál, lévén eleve van aláírás-mintatár, e technológiára építve viszonylag egyszerű a kézírásos jelszavak tárolása, kezelése. Mintaellenőrzés nélküli aláírás esetében kézírásos jelszó-mintatár felállításával hibrid megoldás hozható létre az aláírásminták tényleges tárolása nélkül, csökkentve az ügyintézői hitelesítési kockázatot, lévén a sima „tudásalapú" faktor mellett biometrikus („tulajdonságalapú" faktor) ellenőrzése is megtörténik.

A jövőben a felhasználók által kézírással megadott szavak (jelszavak) mintával összevetése akár a hagyományos azonosítási folyamatokba is beépülhet a nyomásérzékenységet is kezelő okostelefonos megoldások elterjedésével,

azaz nem csak a hitelesítési folyamat részese lehet a kézírás-felismerés.

További jövőbeni biztonságnövelő technika lehet mind az azonosításnál, mind a hitelesítési folyamatban a dinamikus, a számítógép által kiválasztott szöveg leíratása, de ehhez sokkal hosszabb írásminták tárolása, és a jelenleg kereskedelemben hozzáférhető felismerő algoritmusoknál összetettebb elemző programok kellenek, így ezzel a lehetőséggel még nem érdemes számolni.

Összefoglalás

A szervezetek, különösen a széles ügyfélkört kiszolgáló közszolgáltató szervezetek számára az elkövetkező időben kulcsfontosságú lesz a tisztán elektronikus belső működésre áttérés, azonban az ügyfélkapcsolatoknál ehhez olyan megoldást kell biztosítaniuk, amelyet a legkülönbözőbb, informatikai megoldásoktól idegenkedő ügyfélcsoportok is el tudnak fogadni. E követelmény kielégítésében segít a hatályos jogszabályok alapján megfelelő bizonyító erővel rendelkező, az íráskép elektronikus rögzítésén alapuló hitelesítési megoldás, ami nem helyettesíti, hanem kiegészíti az elektronikus hitelesítési megoldások – így különösen az okostelefonokra épülő szolgáltatások – kínálatát. A megoldásnál figyelemmel kell lenni arra, hogy önmagában a biometria jelenléte nem elegendő a jog által elismert bizonyító erőhöz, az ügyfél azonosítása is szükséges, s a dokumentumhitelesítési alkalmazásoknál a dokumentum teljes életciklusát figyelembe kell venni. Az ügyfelek számára megszokott aláírással történő hitelesítés elektronikus megfelelőjénél mind az előzetes aláírás-mintavételen, mind az e nélküli megoldás is kialakítható, eltérő tulajdonságaik miatt a felhasználási igények és lehetőségek alapján mérlegelve a választást. A tisztán kézi aláírás felismerésére épülő megoldások biztonsági szintje jelentősen növelhető egy „tudásalapú" elem beemelésével, amikor nem csak az aláírását, hanem egy előzetesen ügyfél által – szintén kézírással – adott jelszó mintát (is) figyelembe vesz a szolgáltató a hitelesítési igazolás kiadásánál.

Felhasznált irodalom

Daugman, J. (2002): How the Afghan Girl was Identified by Her Iris Patterns http://www.cl.cam.ac.uk/~jgd1000/afghan.html

Jain, A. K. – Bolle Ruud, M. - *Pankanti, S.* (eds.) (2006): Biometrics Personal Identification in Networked Society. New York: Springer

Jain, A. K. – Ross, A. – Pankanti, S. (2006): Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security, 1, p. 125–143.

Kuhn, D. R. et al. (2001): Introduction to Public Key Technology and the Federal PKI Infrastructure: (NIST SP 800-32). National Institute of Standards and Technology

Ratha, N. K. A. Senior – Bolle, R. M. (2001): Automated biometrics. in Proc. of ICAPR, Rio, Brazil, March 2001, p. 445-454.

Saini, R. – Rana, N. (2014): Comparison of Various Biometric Methods. International Journal of Advances in Science and Technology (IJAST), Vol 2 Issue I (March 2014)

Syazana-Itqan, K. – Syafeeza, A. R. – Saad, N. M. – Abdul Hamid, N. – Bin Mohd Saad, W. H. (2016): A Review of Finger-Vein Biometrics Identification Approaches. Indian Journal of Science and Technology, Vol 9(32), August 2016

Zhang, D. D. (2000): Automated Biometrics Technologies and Systems. The International Series on Asian Studies in Computer and Information Science, Vol. 7 (2000)

EIDAS (2017): http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32014R0910

Eurostat (2017): http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_ifp_iu&lang=en

Eurostat (2016): http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ec_ibuy&lang=en

Eüitv (2017): http://njt.hu/cgi_bin/njt_doc.cgi?docid=193173.337609

Pp (2017): http://njt.hu/cgi_bin/njt_doc.cgi?docid=305.331318

Bürgerkarte (2017): https://www.buergerkarte.at/

Wiki (2017): https://de.wikipedia.org/wiki/B%C3%BCrgerkarte

MNB Fizetési rendszer jelentés, 2017-07-01