ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS TERVEZET

NYÁRI NORBERT

Elektronikus aláírás az eSzemélyi igazolvánnyal – egy innováció diffúziója Magyarországon

Témavezető: Dr. habil. Kerti András

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024. április 2.

TARTALOMJEGYZÉK

BEVEZETÉS

A tudományos probléma megfogalmazás

Az emberiség életében a dokumentumok hitelesítésének hosszú évszázadokra visszanyúló hagyománya van, kezdve a viaszos pecséttől, a papír alapú aláíráson keresztül a digitális aláírásig. A digitális aláírás, mint technológia már évtizedek óta elérhető, és a ráépülő, jogi környezetben is értelmezett elektronikus aláírás feltételei az EU-ban és így Magyarországon is adottak.

Az Európai Unió területén az elektronikus aláírás jogi környezetét az eIDAS rendelet [1] alapozza meg 2014 óta. A rendelet szabályozza többek között a tagországokban egységesen elfogadott elektronikus személyazonosító kártyák (eID card) és az elektronikus aláírás (eSignature, eAláírás) használatát.

Elektronikus aláíráshoz természetesen piaci szolgáltatótól is lehetséges tanúsítványt vásárolni, úgymint a Netlock Kft. vagy a Microsec Zrt. Jelen disszertációban azonban az állampolgárok számára a legtermészetesebb módon elérhető, ingyenes elektronikus aláírás kérdéskörét szeretném részletesen megvizsgálni, ezért a továbbiakban az eSzemélyi igazolványra és annak eAláírás funkciójára koncentrálok [2].

2016 januárja óta Magyarországon is elérhető az eIDAS-nak megfelelő elektronikus funkciókkal rendelkező személyazonosító igazolvány eSzemélyi néven. Az okmány számos előnnyel rendelkezik, melyek azonban az állampolgárok mindennapi életében különböző okoknál fogva nem használhatók ki teljes mértékben [3].

Az elektronikus aláírás az eSzemélyi igazolvánnyal – mint azt később látni fogjuk – nem terjed olyan ütemben, mint ahogy az lehetséges lenne. Fontos feltárni, hogy mely tényezők akadályozzák a terjedést, továbbá azt is, hogyan lehetne ezeket az akadályokat megszüntetni.

Jelen disszertáció az eSzemélyi igazolvány funkciói kihasználatlanságának okait hivatott megvizsgálni egy új nézőpontból. Everett M. Rogers [4] az 1960-as években kezdte el kidolgozni a Diffusion of Innovations néven ismertté vált elméletét, megalapozva ezzel a diffúziókutatás módszertanát.

Először is abból a feltételezésből indulok ki, hogy az állampolgárok valamilyen okoknál fogva bizalmatlanul fordulnak az elektronikus aláíráshoz, mint „új” technológiához. Az „új” azért van idézőjelben, mert a Diffusion of Innovations szerint egy innováció

újdonsága egy adott társadalmi rendszerben értelmezendő, így bár az elektronikus aláírás objektíve nem „új”, a Magyarországon élők számára mégis újdonságnak számít [4].

Mint azt később látni fogjuk, a kérdést a bizalom irányából megközelítve nem feltétlenül igazolódott be a fenti feltételezés, így vizsgálódásomat a technológia elfogadottság irányába folytattam. Látva azonban az állampolgárok mindennapi gyakorlatát és a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság által rendszeresen közreadott eSzemélyi igazolványra vonatkozó statisztikákat [5] könnyen arra a megállapításra juthatunk, hogy a kérdés mégsem a technológia elfogadottságáról szól. Nem beszélhetünk ugyanis egy technológia elfogadottságáról, ha az még el sem jutott a potenciális felhasználókig. Ezzel el is érkeztünk a diffúziókutatáshoz, melynek segítségével azt vizsgálhatjuk, hogy a technológia terjedését mi befolyásolja és azon hogyan lehetséges gyorsítani [4].

A diffúziókutatás egészen más szemszögből vizsgálja a jelenségeket, mint a különféle technológia elfogadottsági modellek (például TAM, UTAUT). A Diffusion of Innovations model a diffúziót alapvetően négy meghatározó tényezőre osztja fel: maga az innováció (innovation), az idő (time), a kommunikációs csatornák (communication channels), valamint a társadalmi rendszer (social system) [4].

Ha az eSzemélyi igazolványra és annak elektronikus funkcióira úgy tekintünk, mint egy innovációra, amely a társadalmi rendszerünkben újdonságként jelentkezett 2016-ban, akkor a jelenségre alkalmazhatók a Diffusion of Innovations fogalmai és alapelvei. Azóta megközelítőleg nyolc év telt el, de a szóban forgó azonosító okmányra valójában még mindig tekinthetünk innovációként, mert a tárolóelem (chip) csak 2021 augusztusa óta kötelező [3, 4].

Célkitűzések

Célom egyrészt az eSzemélyi igazolvány és elektronikus funkcióinak terjedését gátló tényezők feltárása, kiindulva abból a feltevésből, hogy az állampolgárok valamilyen oknál fogva bizalmatlanul fordulnak az elektronikus okmányhoz.

Egy kockázatelemzés keretében feltárásra kerülnek az okosokmánnyal kapcsolatos és annak használata közben felmerülő kockázatok, az ISO/IEC 27005:2022 nemzetközi szabványban leírt kockázatértékelési módszertan alkalmazásával.

Cél továbbá a Diffusion of Innovations modellel összhangban egy diffúziós terv kialakítása, amely magában foglalja az eSzemélyi igazolvány elektronikus funkciónak

terjedését segítő eljárásokat, eszközöket és módszereket – végig szem előtt tartva az információbiztonságot. Az okmánnyal kapcsolatos kommunikációt az állampolgárok számára átláthatóvá és érthetővé kell tenni. A magyar eSzemélyi szolgáltatásait és azok igénybevételi módjait hatékonyan kell kommunikálni az állampolgárok irányába. Végső soron: meg kell találni a módját, hogy az elektronikus aláírás az eSzemélyi igazolvány használatán keresztül az állampolgárok mindennapjainak természetes velejárója legyen.

A téma kutatásának hipotézisei

Hipotézis 1: Magyarországon az eSzemélyi és elektronikus funkcióinak terjedését a bizalom hiánya hátráltatja.

Feltevésem szerint Magyarországon az eSzemélyi igazolvány elektronikus funkcióinak terjedését a bizalom hiánya hátráltatja. Az egyik ilyen az elektronikus aláírás, melyet további fejezetekben bemutatott statisztikák alapján a jogosultak csak igen alacsony százaléka igényel az okmányához – ezt később részletesen látni fogjuk. Az évszádos múltra visszatekintő, hagyományos aláírásban jobban megbíznak az emberek, mint a technikai eszközökkel támogatott elektronikus aláírásokban. Ez hátráltatja az eAláírás funkció terjedését – ezért kiemelt jelentőségű az emberek elektronikus aláírásokba vetett bizalmának kérdéskörét alaposan megvizsgálni.

Hipotézis 2: Az eSzemélyi igazolvány és annak elektronikus funkcióinak terjedését segítené egy teljeskörű kockázatelemzés elkészítése az ISO/IEC 27005:2022 szabvány alapján.

Az eSzemélyi igazolvány elektronikus használati eseteit teljesen átszövi az információbiztonság. Tudomásom szerint korábban nem került publikálásra az ISO/IEC 27005:2022 alapján végzett kockázatelemzés az okmány vonatkozásában. Ennek elvégzését több szempontból is fontosnak találom. Egyrészt az ISO/IEC 27005 szabványt némiképp mellőzöttnek érzem a többi kockázatértékelési keretrendszerhez képest – később kifejtem –, ezért annak alkalmazhatóságát is szeretném megmutatni.

Másrészt az új szabványverzióban megjelent a kockázatok feltárására az esemény alapú megközelítés. Ezt a módszert alkalmazom az eSzemélyi igazolvány kockázatainak feltárására annak érdekében, hogy szilárd alapokon nyugvó információbiztonsági szempontokkal egészíthessem ki a terjedést elősegítő diffúziós tervet.

Hipotézis 3: Az eSzemélyi igazolvány és annak elektronikus funkcióinak elterjedtségét úgy kell megközelíteni, mint egy diffúziókutatási problémát.

Meglátásom szerint sajnálatos módon az eSzemélyi elektronikus aláírásra történő használatának lehetősége nincs a köztudatban.

Feltevésem szerint ennek alapvető oka az, hogy az eSzemélyi igazolvány elektronikus funkcióról nem jutott el elegendő információ az állampolgárokhoz ahhoz, hogy a mindennapokban eredményesen használni tudják azokat. A problémát úgy kell megközelíteni, mint egy innováció diffúzióját. Ebben a konkrét eseteben is beazonosíthatók a Diffusion of Innovations módszertanban meghatározott alapfogalmak és szereplők.

A modellt alkalmazva az eSzemélyi igazolványon, mint innováción, könnyebben felszínre kerülhetnek a terjedést esetlegesen hátráltató tényezők.

Hipotézis 4: Az eSzemélyi igazolvány és annak elektronikus funkcióinak elterjedését nagyban segítené egy diffúziós terv.

Még tovább követve az előbbi gondolatmenetet, a Diffusion of Innovations elveit alkalmazva kialakítható a feltárt hiányosságok orvoslására egy olyan diffúziós terv, amely jelentős mértékben felgyorsítaná az okmány funkcióinak terjedését. A keretrendszerben felhalmozott tapasztalat segíthet továbbá elkerülni olyan buktatókat, melyek létezését még csak nem is sejtjük.

Új utakat kell találni az elektronikus aláírás használatának népszerűsítésére, egyszerűsíteni szükséges a használati eseteket, és új használati eseteket kell bevezetni.

Kutatási módszerek

Kutatásaim során először is szekunder kutatásként áttekintettem a személyi okmányok fejlődéstörténetének releváns mérföldköveit, a digitális aláírást, az elektronikus aláírást, a bizalmat érintő szakirodalmat annak érdekében, hogy kellőképpen szilárd alapról indulhasson az új tudományos eredmények felépítése. Az 1. fejezetben röviden kitérek a személyazonosító okmányok fejlődéstörténetére, továbbá elemzem a bizalom a személyi adatokkal, okmányokkal, ügyintézéssel, szerződéskötéssel kapcsolatos összetevőit.

Primer kutatásként egy kockázatelemzés keretében információbiztonság és informatikai biztonság szempontból vizsgálom az eSzemélyi azonosító okmányt és elektronikus funkciót, figyelemmel a posztkvantum kriptográfia digitális aláírásra (amely az elektronikus aláírások technológiai alapját képezi) gyakorolt lehetséges hatásaira is.

További primer kutatást hajtottam végre kvalitatív módszerekkel. Az elektronikus aláírás széleskörű elterjedését gátló tényezők feltárását céloztam meg. Fókuszcsoportos beszélgetéssekkel igyekezetem feltárni többek között azt is, hogy milyen oktatási és kommunikációs megoldások befolyásolnák pozitívan az emberek attitűdjét az elektronikus aláírással szemben. Olyan mélyebb összefüggések feltárása volt a cél, amelyek kvantitatív módszerekkel csak nehezen lettek volna felszínre hozhatók.

Ezt követően az eSzemélyi igazolványt, mint innovációt a Diffusion of Innovations keretrendszer kontextusába helyezve az okmány elektronikus funkcióinak elterjedését segítő eljárásokat, módszereket kerestem, melynek eredményeként a 4. fejezetben bemutatásra kerülő diffúziós terv jött létre.

1 AZ ESZEMÉLYI IGAZOLVÁNY

A személyek azonosítására a fényképes igazolványok terjedtek el az elmúlt évtizedekben. Meglepő tény, hogy az első fényképes, személyazonosítására alkalmas igazolványok csak az első világháborút követően jelentek meg, holott már az 1840-es évektől lehetséges volt a fényképek készítése.

Mint azt korábban említettem, az eSzemélyi igazolvány egy 2016 januárjától igényelhető, tároló elemmel, vagy chip-el rendelkező személyazonosító okmány, amely számos előnyös tulajdonsággal rendelkezik.

Megfelel az eIDAS rendeletben foglaltaknak, ezért az Európai unió Területén útiokmányként is használható, a rajta tárolt tanúsítvánnyal aláírt dokumentumok elektronikusan hitelesnek tekintendők az EU-ban.

Természetesen a hagyományos értelemben vett személyazonosító okmányként is használható, de értekezésem szempontjából az – elmúlt években egyre bővülő – elektronikus képességei a legérdekesebbek.

Ebben a részben bemutatom az eSzemélyi igazolvány előzményeit, képességeit és az azokban rejlő lehetőségeket, melyekről két korábbi írásomban is említést tesztek (Nyári [2], Nyári és Kerti [6]).

1.1 Előzmények és kontextus

Az első ismert fényképes belépőkártya William Notman 19. századi fényképész nevéhez köthető, aki az Amerikai Egyesült Államokban 1876-ban megrendezésre került „Centennial International Exhibition” világkiállításra készített fényképes, sorszámozott, névre szóló jegyeket („photographic ticket”) [7].

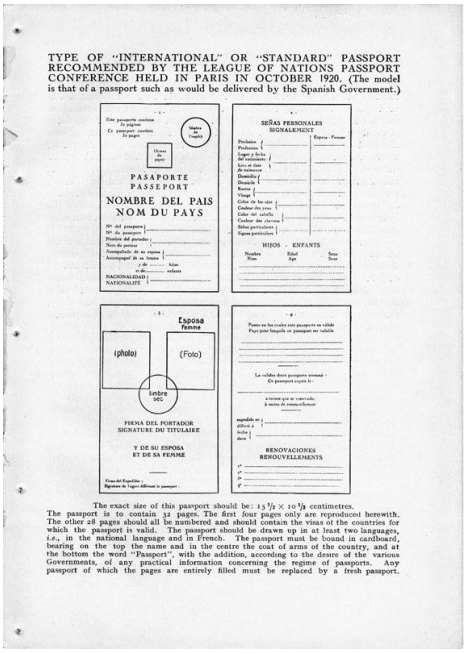
Doulman, és Lee [8] szerint a fényképes igazolványok széleskörű terjedése csak az 1910-es évektől kezdődött el. A fényképes okmányok megbízható megoldást jelentettek egészen a fényképezőgépek széleskörű elterjedéséig, ami a bűnözők számára megkönnyítette a hamis igazolványok készítését [9].

Az 1870-es évek második felében Sir William Herschel jelentős áttörést ért el az ujjlenyomatok alkalmazásának terén. Egyrészt kidolgozott egy osztályozási rendszert Sir Francis Galtonnal, másrészt pedig elsőként javasolta, hogy egy vádlott ujjlenyomatát vegyék fel a bírósági anyagok közé [9, 10].

Az 1900-as évek elején vezették be a Scottland Yardon a Galton-Henry-féle ujjlenyomat osztályozási rendszert, de akkoriban nem volt kivitelezhető, hogy minden állampolgártól ujjlenyomatot vegyenek [9].

Hollandiában alakították ki az első decentralizált személyi szám rendszert 1849-ben, de csak 1940-től kezdtek el személyi azonosító igazolványokat kiadni az állampolgároknak. Ezzel megközelítőleg egyidőben az Amerikai Egyesült Államokban elkezdődött a társadalombiztosítási számot tartalmazó kártyák (Social Security Number Cards) kiadása, az első köteget 1936-ban bocsátották ki [9].

Az 1930-as évektől kezdve világszerte kezdtek az egyes országok saját személyi azonosító rendszereket kidolgozni. Svédországban plébániák – mint helyi ügyfélszolgálati irodák – végezték személyi számok kiadását a helyi lakosoknak, 1947-re minden állampolgár rendelkezett ilyen számmal. Izraelben 1948-ban, az állam megalakulását követően népszámlálás keretében osztották ki a személyi számokat [9].



TYPE OF "INTERNATIONAL" OR "STANDARD" PASSPORT RECOMMENDED BY THE LEAGUE OF NATIONS PASSPORT CONFERENCE HELD IN PARIS IN OCTOBER 1920. (The model is that of a passport such as would be delivered by the Spanish Government.)

PASAPORTE
PASSEPORT
NOMBRE DEL PAIS
NOM DU PAYS

SEÑAS PERSONALES
SIGNALEMENT

HIJOS - ENFANTS

Esposa
Femme

(photo)

(Foto)

FIRMA DEL PORTADOR
SIGNATURE DU TITULAIRE

Y DE SU ESPOSA
ET DE SA FEMME

RENOVACIONES
RENOUVELLEMENTS

The exact size of this passport should be: 15 1/2 × 10 1/2 centimetres. The passport is to contain 32 pages. The first four pages only are reproduced herewith. The other 28 pages should all be numbered and should contain the visas of the countries for which the passport is valid. The passport should be drawn up in at least two languages, i.e., in the national language and in French. The passport must be bound in cardboard, bearing on the top the name and in the centre the coat of arms of the country, and at the bottom the word "Passport", with the addition, according to the desire of the various Governments, of any practical information concerning the regime of passports. Any passport of which the pages are entirely filled must be replaced by a fresh passport.

1. Ábra A Népszövetség által javasolt útlevél formátuma. Forrás: Leauge of Nations Photo Archive [11]

Az 1960-as és 1970-es években már több országban is elektronikus formában tartották nyilván a személyi azonosító adatokat, például Svédországban 1967-től, Franciaországban 1973-tól [9].

1946-ben megalakult a Nemzetközi Polgári Repülési Szervezet (rövidítve ICAO, International Civil Aviation Organization), az ENSZ szakosított intézménye. Az ICAO egyik legnagyobb eredménye az 1980-as években a gépi olvasásra alkalmas útlevelek

keretrendszerének kialakítása volt. Később, 2003-ban az ICAO beépíti az útlevelekbe a biometrikus azonosítást szolgáló adatokat [12].

1.1.1 Kártya formátumú és elektronikus személyazonosító okmányok

Az ISO/IEC 7810-es szabvány [13] első változata 1985-ben jelent meg, a legfrissebb változata 2019-es. A szabvány meghatároz 4 különböző méretet a kártya formátumú igazolványok számára. Leggyakrabban az ID-1 jelűt használják igazolványok, bankkártyák készítéséhez, amely 85,6 mm x 53,98 mm x 0,76 mm méretű.

Az ISO/IEC 7816 szabványcsalád [14] az integrált áramkört (más néven tárolóelem, smart card) tartalmazó kártyák szabványos leírását tartalmazza. A legújabb smart cardot tartalmazó kártyák képesek lehetnek adattárolásra (például fénykép, telefonszámok, biometrikus azonosítók), tanúsítvány tárolásra, kriptográfiai műveletek végrehajtására is.

A 2000-es években jelent meg a ISO/IEC 14443-es szabványcsalád, amely az érintés nélküli személyazonosításra alkalmas smart card-ot tartalmazó kártyákról szól. A mikrochip az érintésmentes kártyán RFID technológián keresztül kommunikál a kártyaolvasóval. Általában az olvasási távolság legfeljebb 10 cm körül van, annak érdekében, hogy a véletlen (vagy rossz indulatú) leolvasásokat elkerüljük [9, 15].

Ahogyan azt Szádeczky [16] is említi, Európai Unió-szerte több országban, többek között hazánkban is tároló elemmel ellátott kártya formátumú személyazonosító igazolványok vannak forgalomban.

1.1.1.1 Elektronikus aláírás

Az elektronikus aláírás története a 19. század közepén kezdődik. Az 1881-1886 közötti Amerikai Polgárháború alatt távíróberendezéseken küldött bizonyos üzeneteket közös megegyezés alapján elfogadták hitelesítő adatként, ezt bizonyítja a New Hampshire-i Legfelsőbb Bíróság egyik 1869-es jogi esete [17].

Wright [18] 1990-es írásában a fax készülékeken (1980-as évektől) keresztül továbbított papír alapon aláírt dokumentumok esetében kettősségről számol be. Elmondása szerint az óvatos alkalmazók minden esetben postai úton is továbbították az eredeti, papír alapú dokumentumot a faxolást követően. A kettősség abból ered, hogy akkoriban egyes állami hivatalok az USA-ban már elfogadtak faxon keresztül beküldött kérvényeket. Továbbá a telexen (ami egy a faxnál is régebbi technológia) keresztüli kommunikáció esetében – legalábbis bizonyos iparágakban – a jogi értelemben vett elköteleződés akkoriban teljesen egyértelmű volt.

Korábbi írásomban (Nyári [19]) részletesen bemutattam a világ különböző országaiban alkalmazott, jogilag is elfogadott elektronikus aláírási sémákat, így a kanadai PIPEDA szabályozást és az Egyesült Államoknak szövetségi és állami törvényeit (például a 2000-ben kiadott „Electronic Signatures in Global and National Commerce Act" (ESIGN Act)).

Jelen kutatás szempontjából a legfontosabb azonban az EU területén érvényes szabályozás, az eIDAS (electronic IDentification, Authentication, and trust Services) rendelet, szabatos megnevezésén „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". A rendelet 2014-ben lépett hatályba, egyik fő célja az egységes digitális piac (Digital Single Market, DSM) támogatása az EU-tagállamok számára [19, 1].

Az eIDAS határokon átnyúlóan és az egyes tagországokon belül is érvényesül. Egységesíti az elektronikus azonosítás (electronic Identification, eID) használatát, meghatározza az „elektronikus bizalmi szolgáltatásokat" (electronic Trust Services, eTS), biztosítja az elektronikus aláírások jogi érvényességét az EU tagállamaiban, és megteremti az elektronikus bizalmi szolgáltatások európai belső piacát [19, 1].

Alapvetően háromféle elektronikus aláírást határoz meg: „elektronikus aláírás" (korábbi nevén egyszerű elektronikus aláírás), „fokozott biztonságú elektronikus aláírás" (AES – nem tévesztendő össze a fejlett titkosítási szabvánnyal, amely egy kriptográfiai algoritmus) és „minősített elektronikus aláírás" (QES). A továbbiakban erre az utóbbi elektronikus aláírási modellre koncentrálok [19, 1].

A legnagyobb bizonyítóerővel a minősített elektronikus aláírások bírnak. Ehhez az elektronikus aláírásfajtához ugyanis a jogszabály a kézi aláírásokkal megegyező joghatást rendel. Vannak azonban megkötések, melyeknek a minősített aláírások készítése során meg kell felelni: „minősített elektronikus aláírást létrehozó eszközzel" kell előállítani „elektronikus aláírás minősített tanúsítványának" használatával [19, 1].

Mivel az eSzemélyi igazolvány minősített elektronikus aláírás létrehozására alkalmas, ezért a továbbiakban arra fókuszálok.

Az elektronikus aláírás napjainkban legfontosabb implementációja erősen támaszkodik különféle kriptográfiai algoritmusokra, úgymint a nyílt kulcsú rejtjelezőalgoritmusokra és különféle hash-függvényekre [19].

A nyílt kulcsú algoritmusok, mint például az RSA (Rivest-Shamir-Adleman) sajátossága, hogy nagy számításigényű matematikai problémákon alapulnak. A nagy számítási igény biztosítja, hogy feltörésük ne legyen normál időben kivitelezhető. Elméletben azonban léteznek ugyan olyan kvantumszámítástechnikai algoritmusok, amelyek a feltöréshez szükséges időt nagyban lerövidítik, gyakorlatilag azonban egyelőre nem állnak rendelkezésre valódi kvantumszámítógépek, melyeken ezek futtathatók lennének [19].

A kvantumszámítástechnika területén hónapról hónapra új eredmények születnek, és bár jelenleg a kvantumszámítógépek nem jelentenek közvetlen veszélyt a ma korszerűnek számító kriptográfiai algoritmusokra, létfontosságú figyelemmel kísérni az új eredményeket. Szem előtt kell tartani, hogy a valódi kvantumfölény bekövetkezésekor a jelenleg használatos nyilvánoskulcsú rejtjelezések jelentős része normál időben megfejthetővé válik [19].

A nyílt kulcsú algoritmusok esetében is különösen fontos a kulcselosztás: a nyílt kulcs bárkivel megosztható, a privát kulcsot pedig kizárólag annak tulajdonosa ismerheti. Erre jelent megoldás az ún. nyilvános kulcsú infrastruktúra (Public Key Infrastructure - PKI).

Andrew S. Tannenbaum [20] szerint a nyilvános kulcsú infrastruktúrák tanúsító hatóságok (CA – Certification Authorities) és regionális hatóságok (RA – Regional Authorities) alkalmazásával oldják meg a felhasználók azonosításának problémáját. Ezekben a rendszerekben a tanúsítványok ún. „bizalmi láncban” vagy „tanúsítási láncban” foglalnak helyet. A bizalmi lánc azt jelenti, hogy minden kiadott tanúsítványt a felette levő szint aláír. Erről részletesen írtam korábbi cikkemben (Nyári [21]), melyben kitértem a jelenleg is használt megoldások a posztkvantum érából várható fenyegetéseire is. [20, 21].

Erdősi [22] doktori értekezésében részletesen foglalkozott az elektronikus aláírás történetével, technikai megoldásaival, biztonsági kérdéseivel és a magyar társadalomba való beágyazottságával. Jelen értekezés fókuszában azonban az elektronikus aláírások egy speciális esete, az eSzemélyi igazolvánnyal történő elektronikus aláírás áll.

1.1.1.2 Elektronikus azonosítás

Az eIDAS [1] lefekteti az elektronikus azonosítás keretrendszerét is az Európai Unió területén. Az eID okmányok minden szükséges adatot tartalmaznak elektronikus formában is a személyazonosság megállapításához. A rendelet így definiálja az elektronikus azonosítást: „a természetes vagy jogi személyt, illetve jogi személyt

képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata".

Az egyes tagországok egymás elektronikus azonosítási megoldásait elismerik közigazgatási szervek nyújtotta szolgáltatások igénybevétele esetén, feltéve, hogy azok az eIDAS-nak megfelnek és biztonsági szintjük eléri vagy meghaladja a szolgáltatáshoz előírt biztonsági szintet [1].

A különféle eID megoldások tárolóelemén megtalálható az igazolvány tulajdonosának fényképe, a személyi adatai, amelyek egyébként az okmányról szabad szemmel is leolvashatók, továbbá a tulajdonos ujjlenyomata (opcionálisan). A technológia fejlődésének köszönhetően egyre inkább az érintésmentes eID megoldások terjednek, a módszerek között az NFC képes mobiltelefonok alkalmazása is megjelent [23].

1.1.2 Európai digitális identitás

Az Európai Unió Tanácsa 2023 novemberében tette közzé 15149/23 számon a korábban eIDAS 2.0 néven ismert módosítási javaslatot [24], melynek célja az Európai Digitális Identitás létrehozása az eIDAS rendelet módosításával.

1. Táblázat European Digital Identity Wallet pilot projektek és használati esetek, Forrás: saját szerkesztés az Európai Bizottság honlapja alapján

Projekt megnevezése	Használati esetek
Potential European Consortiums for Digital Identity (POTENTIAL)	• digitális eKözigazgatási szolgáltatások elérése • bankszámla nyitás • mobiltelefon SIM kártya igénylés • mobil vezetői engedély • szerződések aláírása • orvosi receptek kiváltása
NOBID Consortium (NOBID)	• fizetési tranzakciók jóváhagyása
Digital Credential for Europe (DC4EU) Consortium	• jelentkezés álláshirdetésre (iskolai végzettségek igazolása) • társadalombiztosítási ellátásokhoz való hozzáférés
EU Digital Identity Wallet Consortium (EUWC)	• utazás (digitális útiokmány) • szervezeti digitális identitás • fizetési tranzakciók jóváhagyása

Az Európai Digitális Identitás Tárca (European Digital Identity Wallet, EUDI) egy olyan, a nemzeti eID megoldásokra épülő új szolgáltatás, amely EU-szerte elfogadott elektronikus azonosítási szolgáltatást fog megvalósítani, lehető téve elektronikusan tárolt

jellemzőink (például iskolai végzettség,) hiteles, igazolt megosztását a különféle szolgáltatásokkal [24].

Amint az az Európai Bizottság honlapján olvasható [25] az éles kiadás előtt négy nagyszabású pilot projekt fut 2023. április 1-je óta az EU tagországaiban. A referencia EUDI forráskódját a github.com forráskódkezelő szolgáltatáson keresztül tették elérhetővé. A fenti táblázatban (1. Táblázat) láthatjuk a négy pilot projektet és az általuk biztosított használati esteket.

A honlap szerint Magyarország a fentiek közül az orvosi receptek kiváltását és a digitális útiokmányt érintő projektekben vesz részt [25].

1.1.3 Személyazonosító okmányok Magyarországon

Nagy és Papp szerint [26] hazánkban a második világháború előtt nem volt kötelező személyazonosításra szolgáló irat kiváltása, erre alkalmas országszerte elfogadott okmánytípus nem is igazán létezett. A második világháborút követően vált kötelezővé az akkor még személyi igazolványnak nevezett okmányok kiváltása, melyet a 2000-es évektől a kártya formátumú személyazonosító igazolvány és a lakcímet igazoló hatósági igazolvány (köznyelvben: lakcímkártya) váltott fel.

1.1.3.1 Személyi igazolvány

1857-től ún. Igazolási Jegyet adtak ki az állampolgároknak, amely még nem tartalmazott fényképet, csak azonosító adatokat és személyleírást. Ez egy nem kötelező, személyazonosításra használható igazolás volt, ami a későbbi személyi igazolvány ősének tekinthető [26].

1927-től még mindig Igazolási Jegynek hívták, de már a személyleírás helyett fényképet tartalmazott, de továbbra sem volt kötelező. Kiadására a rendőrhatóság volt jogosult [26].

A 70.300/1937. BM számú rendelet olyan egyedileg sorszámozott igazolvány kiadását írta elő, amely hitelt érdemlően bizonyítja a személyazonosságot. Tíz számjegyű azonossági számmal látták el, amely jellegében hasonlít a későbbi személyi számra. Az azonossági számot az anyakönyvi kerület számából, az anyakönyvi évfolyam számából és a születési anyakönyvi bejegyzés számából képezték [26].

A második világháborút követően, 1946-ban a 253.600/1946. (VII. 30.) BM rendelet [27] kötelezővé tette a lakcímváltoztatások bejelentését. A bejelentő lap igazolta ugyan a bejelentett lakcímet, de kötelező, arcképes személyi igazolvány hiányában azt bárki felhasználhatta. 1949-ben egyszeri lakcímbejelentésre kötelezte a lakosokat az új

állampolgársági törvény, de személyazonosító okmány rendszeresítésére még mindig nem került sor [26].

1954-től volt először kötelező minden 16 év feletti állampolgár számára arcképes személyi igazolványt kiadni. A rendelet kétféle igazolvány kiállítását tette lehetővé: állandó vagy ideiglenes személyi igazolvány. Meghatározta az igazolvány formátumát, adattartalmát (fénykép, család és keresztnév, nők esetében leánykori név, születési hely és idő, foglalkozás, szakképzettség, katonai igazolvány száma, állampolgár, anyja neve, apja neve, a tulajdonos aláírása, a kiállító hatóság szárazbélyegzőjének lenyomata) [26].

1969-től 14 év lett a kötelező kiváltás alsó korhatára. A 18 év alatti gyermekek nevét és születési adatait be kellett vezetni a szülők személyi igazolványába. Különböző érvényességi időt határoztak meg az eltérő korcsoportoknak [26].

1979-től a személyi számot (lásd 1.1.3.2 fejezet) is fel kellett tüntetni a személyi igazolványban és 1981-et követően csak személyi számmal ellátott igazolványok voltak érvényesek [28, 26].

1985-től a személyi igazolványnak tartalmaznia kellett az okmány tulajdonosának egyetemi doktori címét és tudományos fokozatát, továbbá nyugdíjas esetében annak tényét és a nyugellátás folyósítási törzsszámát [26].

A rendszerváltást követően 1990-től formai és tartalmi változásokon ment keresztül a személyi igazolvány. A borítón a „MAGYAR KÖZTÁRSASÁG” felirat és a Magyar Köztársaság koronás kiscímere látható [26].

Az Alkotmánybíróság 1991-ben alkotmányellenesnek minősítette a személyi szám használatát, ezért az kikerült a személyi igazolványból is [29]. 1992-től az igazolvány már csak a személy nevét, születési helyét, idejét, az állampolgárságot, anyja nevét, lakcímét, arcképét, saját kezű aláírását, a személyazonosító igazolvány sorszámát és az érvényességi időt tartalmazta [26, 30].

2000-től a személyi igazolványt két másik, a személyazonosító igazolvány és a lakcímet igazoló hatósági igazolvány váltotta fel, amelyek már kártyaformátumúak voltak [26].

1.1.3.2 Személyi szám

Magyarországon 1974-ben „A Magyar Népköztársaság Elnöki Tanácsának az Állami népességnyilvántartásról szóló 1974. évi 8. számú törvényerejű rendelete” [31] írta elő a személyi szám használatát, de a tényleges bevezetésre csak 1978 októberében került sor,

amikor is a „személyi szám, illetőleg a személyi lap kiadásáról és használatáról” szóló KSH rendeletben megjelentek a részletszabályok [32].

1982-től „1982. évi 17. törvényerejű rendelet az anyakönyvekről, a házasságkötési eljárásról és a névviselésről” [28] alapján a születési anyakönyvi kivonatokban fel kellett tüntetni a személyi számot. Továbbá a személyazonosításra szolgáló igazolványokban is szerepeltetni kellett az azonosítót. A rendelet hatálybalépésekor a személyi igazolványok erre nem voltak felkészítve, ezért külön ezt a célt szolgáló matricával kellett beragasztani [26].

Az „1986. évi 10. törvényerejű rendelet az állami népességnyilvántartásról” [33] hatályon kívül helyezte az 1974-es állami népesség-nyilvántartásról szóló rendeletet és előírta, hogy a számítógépes nyilvántartásokban azonosító adatként kell használni a személyi számot.

A 25/1986. (VII. 8.) MT rendelet [34] meghatározza a kötelezően nyilvántartandó adatok körét, amely a következőket foglalta magában: a személyi szám, a név, a születési adatok, lakcímadatok, iskolai végzettség valamint a családtagok személyi számai. 1990-ben a 102/1990. (VII. 3.) MT rendelet [35] apróbb módosításokat eszközölt az előbbi rendeletben, de a lényegén nem változtatott.

1991-ben az Alkotmánybíróság 15/1991. (IV. 13.) határozata [29] alkotmányellenesnek nyilvánította a fenti törvényerejű rendeletekben és az azok részletszabályait tartalmazó MT rendeletekben leírt cél nélküli személyes adatok gyűjtését, és hatályon kívül helyezte a fenti rendeleteket.

Csak öt évvel később, 1996-ban a „személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról” szóló törvény [36] rendelkezett arról, hogy milyen azonosítók lépjenek a személyi szám helyébe. Bevezetésre került adóügyekben az adóazonosító jel (a köznyelvben gyakran – tévesen – adószámként hivatkoznak rá), az egészségügyben a társadalombiztosítási jel (TAJ szám), lakcím ügyekben pedig a személyi azonosító (a korábbi személyi szám, a köznyelvben még gyakran így hívják). Így elkerülhető, hogy a különféle nyilvántartásokból egyetlen azonosító ismeretében egy állampolgár összes adata lekérdezhető legyen.

A jogszabály jelenleg hatályos változata meghatároz egy ún. „összerendelési nyilvántartást”, amely azt hivatott megkönnyíteni, hogy a fentebb leírt azonosítók kezelésére jogosult szervek együttműködése gördülékenyebben történhessen. Az

összerendelési nyilvántartásban az állampolgárok összes említett azonosítójának (és még egyéb, jelen írás szempontjából nem releváns azonosítók) rejtjeles képe szerepel, amiből nem lehet következtetni az eredeti azonosítóra. [36]

Továbbá azt is kimondja a jogszabály, hogy minden egyes azonosítóról egy külön hatósági igazolványt kell kiadni, melyek mindegyike csak egy azonosítót tartalmazhat (például adókártya – adóazonosító jel). [36]

A Nemzetbiztonsági Hivatal 2008-as évkönyvében javaslatot tett egy új, személyi szám jellegű univerzális azonosító bevezetésére, amely elősegíthetné a feketegazdasággal szembeni hatékonyabb fellépést. Írásukban más európai országokban (Dánia, Svédország) használt egyedi azonosítókra hivatkoznak. Ehhez azonban az alkotmány módosítására lett volna szükség – ez következik a 15/1991. (IV. 13.) AB határozat [29] megállapításaiból –, ezért ez a javaslat nem valósult meg [37].

1.1.3.3 Személyazonosító igazolvány és az eSzemélyi igazolvány

Magyarországon 2000-től a kártyaformátumú személyazonosító igazolvány és a lakcímet igazoló hatósági igazolvány váltotta fel a korábbi személyi igazolványokat.

Jelen tanulmány szempontjából, azonban 2016. január 1-je hozta meg a legfontosabb fordulatot. Ekkortól igényelhető ugyanis hazánkban az eIDAS rendeletnek megfelelő eSzemélyi igazolvány néven ismert, smart carddal rendelkező személyazonosító igazolvány [38].

Korábbi cikkemben (Nyári [2]) leírtam, hogy az eIDAS rendelet egy egységes modellt definiál az elektronikus aláírások alkalmazására az Európai Unió területére. Az úgynevezett eSzemélyi a magyar megfelelője az állampolgárok azonosítására szolgáló igazolványnak, melyet az eIDAS meghatároz. Az eSzemélyi képes személyre szóló digitális tanúsítvány (és még további személyi adatok, azonosítók) tárolására.

Számos használati eset említhető az igazolvány vonatkozásában: dokumentumok (például gépjármű, vagy ingatlan adásvételi szerződések) elektronikus aláírása, hitelesítés eKormányzati szolgáltatások használatához. Az igazolvány előnyeinek kihasználáshoz szükség van egy számítógépre, és egy ahhoz csatlakoztatott kártyaolvasó készülékre (okostelefonnal és az eSzemélyiM applikációval 2022 óta kiváltható) [2].

A tárolóelemmel rendelkező eSzemélyi igazolványok különféle adatok tárolására alkalmasak, például: digitális tanúsítvány elektronikus aláíráshoz, baleset esetén értesítendő személyek telefonszáma, lakcím adatok, azonosítószámok (adóazonosító jel,

TAJ szám, személyi szám), ujjnyomat stb. Ezen adatok csak a smart card feloldása – vagyis a helyes PIN kód megadása – után olvashatók ki [2].

Felmerül a kérdés, hogy hogyan teljesül az az előbbi szakaszban részletezett követelmény miszerint az állampolgárok számára a különböző területeken létrehozott (adóügyek, társadalombiztosítás stb.) különböző azonosítóit egymástól elkülönülő hatósági igazolványon kell kiadni. Közelebbről megvizsgálva az eSzemélyi chipjén tárolt azonosítókra vonatkozó szabályokat (414/2015. (XII. 23.) Korm. rendelet [39]) feltűnik, hogy a tárolóelem valójában nem az azonosítókat, hanem azok létezésének tényét rögzíti, idézem: „Annak tényét, hogy társadalombiztosítási azonosító jellel, adóazonosító jellel, személyi azonosítóval és lakcímmel a kiállítás időpontjában rendelkezik-e”. Így valójában az azonosítók „kiolvasása” a különböző szolgáltatások használata során nem az okmányból – ahogyan azt az eSzemélyivel kapcsolatos tájékoztatóanyagok sugallják –, hanem központi nyilvántartásokból történik. Valószínűsítem, hogy a közérthetőség kedvéért fogalmaznak úgy a tájékoztató anyagok, mintha közvetlenül az okmányról történne az azonosítók kiolvasása. Az egyszerűség kedvéért a továbbiakban magam is így használom az azonosítók kiolvasásának/tárolásának fogalmát.

Az igazolvány főbb felhasználási területei: elektronikus azonosítás, közösségi közlekedés, postai küldemények átvétele, külföldi utazás és úti okmány (EU-n belül) valamint elektronikus aláírás (eAláírás) [2].

Jelen értekezés a használati esetek közül nagyobb hangsúlyt fog helyezni az okosokmány elektronikus aláírás funkcionalitására, mert – mint azt később látni fogjuk – annak elterjedtsége igen alacsony az állampolgárok körében, továbbá az értekezés egyik célja az eSzemélyi igazolvánnyal történő elektronikus aláírás terjedésének elősegítése.

1.2 Hardver- és szoftverkövetelmények

Az eSzemélyi igazolvány elektronikus képességeinek kihasználásához hardveres szempontból szükséges egy személyi számítógép és egy kártyaolvasó. A kártyaolvasó kiváltható az eSzemélyiM mobilalkalmazással, egy WIFI és NFC képes mobil eszközzel, valamint egy WIFI hálózattal [40, 41].

Ami a szoftvereket illeti: szükséges telepíteni az eSzemélyi kliens alkalmazást, a kártyaolvasó hardver vezérlőprogramját, valamint az elektronikus aláírás használatához a „Kormányzati Elektronikus Aláíró és Aláírásellenőrző Szoftvert” (KEAASZ). A hardver vezérlőprogramja kiváltható az „eSzemélyiM mobilapp kártyaolvasó

segédprogram – QR generator” nevű programmal, ami egy virtuális kártyaolvasót és egy, a csatlakozást segítő QR kód generátort valósít meg. Továbbá még egy szoftver telepítése szükséges egy Android vagy iOS operációs rendszerű mobileszközre [41, 6].

A fenti, PC szoftverek telepítésének az előfeltétele a Java Runtime Environment és a Microsoft .NET Framework 4 futtatókörnyezetek telepítése [41].

1.3 Az eSzemélyi igazolvány képességei

1.3.1 Tárolt adatok

A tárolóelemmel rendelkező eSzemélyi igazolványok számos adat tárolására alkalmasak. Egyrészt minden adat megtalálható rajtuk, ami az okmányon szabad szemmel is olvasható, így elektronikusan is elérhetők a 4T adatok (név, születési hely, születési idő és anyja neve), a nem, az arckép, az ujjnyomat (csak 6. életévüket betöltöttek esetén), az aláírás, az állampolgárság, a lakóhely címe, a tartózkodási hely címe, a személyi azonosító, az okmányazonosító, az okmány lejárata, a kiállító hatóság, a kiállítás dátuma és az eSzemélyi elektronikus azonosítója. Ezen felül opcionálisan tartalmazhatja a tulajdonos származási helyét és nemzetiségi nevét [3, 2, 6].

A tárolóelem az igénylő választása szerint tartalmazhatja továbbá az adóazonosító jelet, a TAJ-számot, 2 db vész esetén értesítendő telefonszámot, tanúsítványt az eAláírás funkcióhoz és a tulajdonos e-mail címét [3, 2, 6].

1.3.2 Elektronikus azonosítás

Az elektronikus azonosítás funkció használatakor a tárolt adatok kiolvasására nyílik lehetőség személyes ügyintézés során. A szolgáltatás elektronikusan intézhető ügyek esetében is használható feltéve, hogy az okmány tulajdonosa rendelkezik a kártyaolvasás hardveres és szoftveres előfeltételeivel [42].

Az adatok kiolvasása csak az alábbiak teljesülése esetén történhet:

- arra jogosult szerv kezdeményezi,
- az adat kiolvasása szükséges az ügyintézéshez és
- az okmány tulajdonos hozzájárult a művelethez [42].

A hozzájárulás az elektronikus azonosítás funkcióhoz rendelt 6 jegyű PIN kód megadásával történik [42].

Az eSzemelyi.hu információs portál [42] szerint alábbi ügyekben használható a funkció:

- Ügyfélkapu regisztráció otthonról

- Okmányérvényesség ellenőrzése
- Chipen található adatok és az ahhoz hozzáférési jogosultsággal rendelkező szervezetek ellenőrzése
- TAJ kiolvasása egészségügyi ellátás során, valamint sürgős esetben
- eRecept kiváltása
- Adóügyek intézése eSzemélyivel
- Személyi azonosító kiolvasása az ügyintézés során
- Lakcímadat kiolvasása az ügyintézés során
- Vészhelyzet esetén értesítendő telefonszám
- Elektronikus azonosítás online közigazgatási ügyek intézéséhez

Az orvosok az elektronikus azonosítás funkció használatával hitelesítik magukat az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) rendszerben [42].

1.3.3 Közösségi közlekedés

A MÁV-START Zrt. és a DKV Debreceni Közlekedési Zrt. esetében már lehetséges papír alapú bérletszelvény helyett az eSzemélyi igazolványhoz kapcsolni a jegyeket és bérleteket [42].

A MÁV-START Zrt. esetében az ún. „digitális vasúti bérleteket” lehet hozzárendelni az eSzemélyihez, ezt a jegypénztárakban, vagy a MÁV applikációban lehet megtenni [42].

A debreceni tömegközlekedésben, a DKV Zrt.-nél bérletek és napijegyek kapcsolhatók az eSzemélyihez. Az összekapcsolás a jegyértékesítési pontokon személyesen vagy a DKV honlapján online lehetséges [42].

1.3.4 eRecept kiváltása

Gyógyszertári receptek kiváltására is alkalmazható az eSzemélyi igazolvány. Ebben az esetben a tárolt TAJ szám kerül kiolvasásra az elektronikus azonosításra szolgáló PIN kód megadását követően. A TAJ szám alapján a gyógyszertár dolgozója az EESZT rendszer használatával pedig hozzáfér a (köznyelvben: a Felhőben lévő) recepthez [42].

1.3.5 Elektronikus útiokmány

Európai országokban, ahol elfogadott a személyi igazolvány útlevél helyett és rendelkezésre áll a szükséges infrastruktúra, lehetséges az ún. automatizált határbelépés. Az okmányról beolvasásra kerülnek az azonosításhoz szükséges adatok, majd egy automatizált arcfelismerés történik a beléptető kapunál, melynek során az okmányon

tárolt fényképpel összeveti a rendszer a belépéskor készített képet. Egyezés esetén a kapu engedélyezi a belépést [42].

Magyarországra ilyen módon belépni az eSzemélyi használatával jelenleg kizárólag a Budapest Liszt Ferenc Nemzetközi Repülőtéren lehetséges, 18 év feletti magyar állampolgároknak [42].

1.3.6 Elektronikus aláírás az eSzemélyi igazolvánnyal

A magyar eSzemélyi használatával – feltéve, hogy az okmány tartalmaz minősített tanúsítványt – bármely állampolgár létrehozhat minősített elektronikus aláírást, amely köszönhetően az eIDAS következetes nemzetközi és nemzeti alkalmazásának, az EU bármely tagállamában a hagyományos, kézi aláírással egyenértékűen elfogadott lesz. Teljes bizonyító erővel rendelkező magánokiratok is létrehozhatók elektronikus ügyintézés során (magánjogi és közigazgatási jogi ügyekben egyaránt) [2].

A „414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól” meghatároz a minősített tanúsítványokkal kapcsolatosan egy ún. tranzakciós limitet, ami a maximális értéke annak a pénzügyi felelősségvállalásnak, amelyet az aláíró az elektronikus aláírásával tehet. Az eSzemélyi igazolványon található tanúsítványokat a NISZ Zrt. állítja ki, a tranzakciós limit pedig az előbbi jogszabály alapján 50 000 000,- Forint [2, 39].

Alapvetően a magyar igazolványon található tanúsítvánnyal kizárólag magáncélú esetekben írhatnak alá az állampolgárok, vagyis cég képviseleti minőségében nem használhatják eSzemélyi igazolványukat dokumentumok aláírásra a cégek képviselői – még egyéni vállalkozók sem [2]. 2023 januárjától a Szerepkör-Tanúsító Platform Szolgáltatás (SZTSZ) bevezetésével ez azonban megváltozott (lásd. 1.5. alfejezet).

1.3.7 Postai küldemények átvétele

Postai küldemények átvételénél az eSzemélyi igazolvány két funkciója is érintett. Egyrészt a címzett azonosítása megtörténhet az elektronikus azonosítás segítségével, másrészt a küldemény átvételét hitelesíthető az elektronikus aláírás funkcióval. A kézbesítő postástól kérni kell az aláíráshoz használható PDA használatát [42].

1.4 Az eSzemélyiM mobilalkalmazás

2022 tavaszától elérhető az eSzemélyiM mobilalkalmazás a Google Play Áruházban és az Apple App Store-ban. Az alkalmazás használatának előfeltételei: legalább Android 7 vagy iOS 13 operációs rendszer, NFC képesség, WIFI képesség és Internet kapcsolat.

A használatával elérhetővé válnak az eSzemélyi igazolvány szolgáltatásai: kiolvashatók a tárolt adatok, ellenőrizhető az elektronikus funkciók állapota, lehetővé válik a PIN kódok kezelése (aktiválása, megváltoztatása), az elektronikus azonosítás, valamint az elektronikus aláírás is. Az Andoroidos mobileszközök vezeték nélküli kártyaolvasóként is csatlakoztathatók számítógépekhez, így kiválthatók az USB-s kártyaolvasó készülékek is. Ehhez arra is szükség van, hogy mobileszköz és a PC ugyanahhoz a WIFI hálózathoz kapcsolódjanak [43].

1.5 A Szerepkör-Tanúsító Platform Szolgáltatás (SZTSZ)

A magyar kormány 2016-ban az „1004/2016. (I. 18.) Korm. határozat a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról” [44] kormány határozatban jóváhagyta a „Kormányzati hitelesítés szolgáltatás (Gov CA) kiterjesztése” megnevezésű projektet, melynek céljai:

- az elektronikus ügyintézést segítő technológiák elterjesztése az államigazgatásban,
- eIDAS rendeletnek és részletszabályaiból eredő kötelezettségeknek való megfelelés.

Az IdomSoft Zrt. „Kormányzati hitelesítés szolgáltatás (Gov CA) kiterjesztése” c. weboldala [45] szerint 2021-ben a projekt hatóköre kibővítésre került az ún. „szerepkör-tanúsító platform szolgáltatás” (SZTSZ) megvalósításával.

Az SZTSZ egy kiegészítő szolgáltatás az eSzemélyi eAláírás funkciójához. A szolgáltatás használatával egy elektronikus aláírással hitelesített dokumentum egy 5 napos, rövid lejáratú – lényegében csak az aláíráskor érvényes – szerepkörtanúsítvánnyal egészül ki, amelyet a szerepkör-tanúsító szolgáltató állít ki. A kiegészítő tanúsítvány célja annak igazolása, hogy az aláíró személy az aláírás pillanatában adott szerepkörrel rendelkezik, tartalmazza a személy adott szervezetben betöltött tisztségét, beosztását, esetleg rendfokozatát [45, 46, 47].

2021-ben a szerepkör-tanúsítás szolgáltatás jogi környezetét „Az egyes eljárások korszerűsítését és a polgárok biztonságának további megerősítését célzó intézkedésekről szóló 2021. évi CXX. törvény” [48] több jogszabály módosításával készítette elő. „Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény” [49] szerepkör-tanúsításra vonatkozó rendelkezései 2023. január 1-jétől hatályosak [46].

A T/1620. számú iromány szerint (törvényjavaslat „Magyarország biztonságát szolgáló egyes törvények módosításáról”) [46] az SZTSZ legelőször a közfeladat ellátásának érdekében és a közfeladat ellátásának igazolására lesz használatos. A Kormány az IdomSoft Zrt.-t jelölte ki szolgáltatónak.

Az SZTSZ-re vonatkozó hatályos rendelkezések a 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól [47] joganyagban olvashatók.

Az SZTSZ elsődleges nyilvántartása a „2020. évi CLXII. törvény a Kormányzati Személyügyi Döntéstámogató Rendszerről” törvényben [50] szabályozott Kormányzati Személyügyi Döntéstámogató Rendszer (a továbbiakban: KSZDR). A KSZDR nyilvántartja többek között az államigazgatásban és rendvédelemben – bizonyos kivételekkel – dolgozók személyügyi adatait [47].

Így lehetővé válik, hogy egy az államigazgatásban dolgozó magánszemély az eSzemélyi igazolványán tárolt eAláírásra szolgáló tanúsítvánnyal úgy írjon alá elektronikusan egy dokumentumot, hogy egyidejűleg az államigazgatásban betöltött tisztsége, beosztása is hitelt érdemlően tanúsításra kerüljön.

1.6 Az eSzemélyi igazolvány statisztikái

A Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkársága honlapján [5] rendszeresen közzéteszi az eSzemélyi igénylésével kapcsolatos statisztikákat. 2020-ig visszamenőleg havi bontásban olvashatók az adatok, azt megelőzően 2016-től 2020-ig összesítve.

Az alábbi táblázatban (2. Táblázat) láthatjuk a 2000.01.01. óta kiállított érvényes igazolványok statisztikáit. 2015.12.31-éig volt lehetséges régi típusú kártya formátumú személyazonosító igazolvány (nem eSzemélyi igazolvány) igénylésére. Jól látható a táblázatból, hogy ezek száma évről évre csökken, de még mindig egy – a lakosságszámhoz mérten – jelentősebb, egy milliónál is nagyobb darabszámú érvényes példány van forgalomban.

2021.08.01-je óta már csak tárolóelemmel rendelkező kártya formátumú igazolványt lehet igényelni – addig még opcionális volt a tárolóelem. Szükségszerűen a chip nélküli okmányok – hiszen újat ezekből sem lehet igényelni – darabszáma csökken az idő előrehaladtával. Az előbbi típusokba tartozó érvényes okmányok fogyatkozása nem meglepő, miután azokból új példányt igényelni nem lehet, ezért idővel le fognak járni.

Ami sokkal érdekesebb, hogy a 2016.01.01. után kiadott chipes eSzemélyi igazolványok darabszáma nem mutat – ha nem is szigorúan, de – legalább monoton növekedést. A 2021 decembere és 2022 decembere közötti időszakban a visszaesés az érvényes eSzemélyi igazolványok darabszámában vélhetően annak köszönhető, hogy a COVID járvány alatt a 38/2022. (II. 11.) számú kormányrendelet [51] a 2020. március 11-e és 2022. május 31-e között lejárt személyazonosító okmányok érvényességi idejét egységesen 2022. június 30-ában határozta meg a veszélyhelyzetre tekintettel.

2. Táblázat Személyazonosító igazolvány igénylések 2000.01.01 óta, Forrás: https://nyilvantarto.hu/statisztikak [5]

Megnevezés	2020 decemberig	2021 decemberig	2022 decemberig	2023. decemberig
2000.01.01 óta kiállított érvényes kártyaformátumú személyazonosító igazolványok száma	nincs adat	nincs adat	8 893 672	8 995 479
2000.01.01 - 2015.12.31 között kiadott érvényes SZIG	3 387 250	2 622 235	1 870 019	1 160 368
2016.01.01 után kiadott érvényes chipes eSZIG	5 880 848	7 186 858	6 564 904	7 402 374
2016.01.01 - 2021.08.01. között kiadott érvényes chip nélküli eSZIG	539 419	583 942	458 749	432 737

Az is előfordulhat azonban, ahol más fényképes igazolványt használnak az állampolgárok személyazonosító igazolvány helyett. Konkrét esettel 2022-ben végrehajtott kutatásomban (Nyári [2]) is találkozhatunk, ahol az egyik résztvevőnek azért nem volt személyazonosító igazolványa, mert vezetői engedélyt használt helyette.

A KSH „Népesség korév és nem szerint” [52] táblázata alapján 2023. január 1-jén az országban 4 625 260 fő férfi, 4 974 484 fő nő (összesen 9 599 744) élt. Fentiek alapján lakosság 93,7%-a rendelkezik kártya formátumú személyazonosító igazolvánnyal és 81,6%-a eSzemélyi (chipes vagy chip nélküli) igazolvánnyal.

Az alábbi táblázatból (3. Táblázat) láthatjuk, hogy még mindig vannak forgalomban 2000.01.01-je előtti személyi igazolványok, igaz ezek darabszáma ugyancsak természetes módon csökken. Az „érvényességi információ nélkül kiállított” kategóriába azok az okmányok tartoznak, melyek azon személyek okmányai, akinek már lejárt a régi típusú személyi igazolványuk, de 2000.01.01-óta nem adtak le igénylést új, kártya formátumú igazolványra.

3. Táblázat Érvényes régi típusú személyi igazolványok, Forrás: https://nyilvantarto.hu/statisztikak [5]

Megnevezés	2021. december vége	2022. december vége	2023. december vége
Érvényes régi típusú (füzet, könyv) SZIG - határidő nélküli kiállítású	361 368	127 232	111 172
Érvényes régi típusú (füzet, könyv) SZIG - érvényességi információ nélkül kiállított	nincs adat	147 551	125 389

Az „Az eSzemélyi okmány igénylések statisztikája” c. táblázatot (lásd 1. számú függelék) a https://nyilvantarto.hu oldalon közzétett statisztikák felhasználásával készítettem. A táblázatban az évenkénti személyazonosító igazolvány igénylési darabszámai látszanak összesítve és funkciók szerinti bontásban. Az adatok sajnálatos módon azt nem tartalmazzák, hogy jelenleg hány érvényes okmány van forgalomban funkció szerinti bontásban, de azért következtetéseket így is lehet levonni a táblázat alapján.

A tárolóelemes igénylések százalékos aránya az összes igényléshez képest az adott évben szinte a teljes időszakban emelkedő tendenciát mutatott (kivéve a 2018-as évet.) 2021 augusztusától pedig kizárólag chipes kártya igényelhető – ezért 100%-os az arány 2022-től.

2021. augusztus 2-a óta kötelező a 6 év felettieknek az ujjnyomat adása, ettől csak akkor tekintenek el a hatóságok, ha az igénylő állampolgár az ujjnyomat adására fizikailag képtelen [38]. 2021-es évig látható, hogy az állampolgárok ujjnyomat adási hajlandósága emelkedett. A kötelező ujjnyomat vétel előírását követően pedig 90% fölé emelkedett az ujjnyomatot tároló okmányok aránya.

A vészhelyzet esetén értesítendő telefonszám megadása az igénylők 27-31%-ára volt jellemző 2016 és 2023 decembere között. Ezt meglepően kevésnek tartom, tekintve, hogy igen hasznos funkció lehet például balesetek esetén.

A kezdetektől fogva a legnagyobb hajlandóságot az igénylők az Adóazonosító jel és a TAJ-szám megadására mutattak. Mindkét adat az okmányok több mint 80%-ára rákerült az egyes években. A legmagasabb arány 2022-ben és 2023-ban 95% körüli volt.

Az éves adatokból egyértelműen látszik, hogy a lakosok csak igen kis hányada igényelt eAláírás funkciót az okmányához. Ez az arány a legmagasabb 2016-ban volt 5,14%-kal.

A következő számításban – pontos adatok hiányában – azzal a becsléssel fogok kalkulálni, hogy 2016 óta minden évben az eAláírás funkcióval igényelt okmányok

teljesen új igénylések voltak (nem pedig elveszett/megrongálódott iratok pótlása, lejárt okmányok meghosszabbítása stb.) – ez majdnem biztosan nem így van, de ezzel a módszerrel az ismert adatokból egy legfeljebb érték meghatározható az ilyen típusú okmányok darabszámára. Kimondható, hogy 2016 óta legfeljebb 349 725 db eAláírás funkcióval rendelkező eSzemélyi igazolvány lehet forgalomban.

Az eAláírás funkció igénylésére jogosult körre vonatkozóan a KSH „Népesség korév és nem szerint" [52] adatsorából látható, hogy 2023. január 1-jén az országban összesen 8 304 909 fő 14 éves vagy annál idősebb lakos élt. Ezt az adatot a fentiekkel összevetve láthatjuk, hogy a jogosult lakosság legfeljebb 4,21 %-a rendelkezik elektronikus aláírásra használható személyazonosító okmánnyal.

A Belügyminisztérium 2022. január – decemberi [53] és a 2023. január – decemberi időszakra [54] vonatkozó Elektronikus közszolgáltatásokat összefoglaló monitoring jelentések szerint az eSzemélyiM mobilalkalmazást 115 650 db mobileszközre telepítették a 2022-es bevezetéstől 2023 decemberének végéig (4. Táblázat).

4. Táblázat Az eSzemélyiM mobilalkalmazás platformok szerinti telepítési darabszámai 2022-2023-ban, Forrás: saját szerekesztés a https://nyilvantarto.hu/hu/statisztikak [53, 54] alapján

	2022.	**2023.**	**Összesen**
IOS	24 575	33 901	58 476
Android	23 493	33 681	57 174
Összesen	48 068	67 582	115 650

Ez százalékosan azt jelenti, hogy az eAláírás használatára jogosult állampolgárok mindössze 1,39%-a, az eAláírással (feltéve, hogy mindenki, aki telepítette rendelkezett eAláírással) rendelkezőknek pedig 33,07%-a telepítette fel az alkalmazást.

1.7 Az eSzemélyi jelenlegi helyzete

Zámbó [55] 2018-as cikkében arról számolt be, hogy az eKormányzati szolgáltatásokba az ügyfélkapu volt a legnépszerűbb bejelentkezési mód, holott az eSzemélyivel történő bejelentkezést biztonságosabbnak ítéli. Megállapítja, hogy az állampolgárok számára túlságosan új megoldás az eSzemélyi elektronikus azonosítás funkciója és speciális eszközök beszerzése is szükséges annak használatához.

2022-ben fókuszcsoportos kutatást hajtottam végre (Nyári [2]) két csoporttal, melynek hipotézise az volt, hogy az állampolgárok bizalmatlanságból nem használják az eAláírás funkciót. Az első csoportban a 18-30 évesek, a másodikban a 31-65 évesek képviseltették magukat. A beszélgetések során elértük az elméleti telítettséget. Az összegyűjtött

adatokon a Grounded Theory elemzést nyílt kódolási megközelítéssel végeztem. Az így kapott kódokat ezután axiális kódolás segítségével kategóriákba csoportosítottam, végül egy alapkategóriát hoztam létre a kategóriák összefogására.

Az elemzés rámutatott, hogy nem a bizalom hiánya a legfőbb akadálya az elektronikus aláírások magyarországi elterjedésének. Bár gátló tényezőként megjelenik, de az alapvető problémát az okozza, hogy az állampolgárok nincsenek tisztában a magyar okosokmány lehetőségeivel, aminek okai feltehetően a felhasználási esetek hiánya, a megfelelő kommunikáció hiánya és az ebből eredő tájékozatlanság [2].

A kutatásban résztvevők szerint a fiatalabb és a középkorú korosztály számára nem okozna problémát a megengedett maximális értékhatárig kötelezettség vállalásra használni az eAláírás szolgáltatást. A problémát inkább az okozza, hogy saját bevallásuk szerint nincsenek tudatában annak, hogy egyáltalán milyen használati esetei vannak az eSzemélyinek és az elektronikus aláírásnak. Valamint úgy vélik, hogy a szükséges infrastruktúra sem áll rendelkezésre a technológia napi szintű alkalmazásához. Mellesleg az értékhatár pontos értékét egyik résztvevő sem ismerte [2].

A megkérdezettek alapvetően ismerethiányban szenvednek a digitális aláírás-elektronikus aláírás témakörében. Nem tudják a különbséget a két fogalom között, nem ismerik a technológia működését. Ez utóbbi természetesen nem elvárható egy informatikai előképzettséggel nem rendelkező állampolgártól, de az okmány magabiztos használathoz feltétlenül szükséges mélységű ismeretekkel vitathatatlanul rendelkezniük kellene [2].

A résztvevők többsége még csak felszínesen sem ismeri a digitális aláírás technológiát, de még felhasználói szempontból sem. A legtöbben abban sem voltak biztosak, hogy az okmányukon van-e eAláírás szolgáltatás, vagy, hogy a tárolt tanúsítvány meddig érvényes [2].

A beszélgetésekből az a sajnálatos tény is megállapítást nyert, hogy gyakran már az okmány igénylése során a Kormányablakok dolgozóitól sem kapnak az igénylők kellő mértékű tájékoztatást az eSzemélyi igazolvány képességeiről, szolgáltatásairól. Ennek okainak megállapítása azonban nem célja jelen értekezésnek [2].

A kutatásban résztvevők olyan esetekről is beszámoltak, melyekben az ügyintézők inkább negatívan nyilatkoztak az eSzemélyi okmányról, átadásakor közölték, hogy „úgysem jó semmire”, mert nem áll rendelkezésre a szükséges infrastruktúra [2].

Itt tennék egy rövid kitérőt a saját tapasztalataimra is, melyeket a megfigyelés kvalitatív módszerével a saját Kormányablak béli, eSzemélyi igazolvánnyal kapcsolatos ügyintézéseim során szereztem. Eddig négy alkalommal volt ilyen ügyintézési feladatom, ebből kettő teljesen gördülékeny és pozitív élmény volt. Ezeket nem részletezem.

Egy másik esetben azonban közel két órára „lefoglaltam" három fő ügyintézőt azzal az igényemmel, hogy szeretném megújítani az elektronikus aláírásra szolgáló tanúsítványomat az igazolványomon. A fennakadásnak az ügyintézők nem megfelelő kiképzésén túl infrastrukturális okai is voltak – éppen nem működött a rendszer.

Egy további alkalommal az ügyintéző hozzáállás béli hiányosságaival szembesültem, kétségbe vonta ugyanis, hogy nekem valóban szükségem van elektronikus aláírásra az eSzemélyi igazolványomon, továbbá azt is, hogy egyáltalán szükség van-e rá.

Visszatérve a kutatásra, a megkérdezettek jelezték, hogy ha lennének különféle tájékoztató anyagok, leírások, útmutatók a kártyaolvasó kiválasztásához, megvásárlásához az nagy segítség lenne számukra. Ilyen jellegű tájékoztató anyagok azonban nem kis számban, a kor elvárásainak megfelelően léteznek és hozzáférhetők az eszemelyi.hu portálon. Nyilvánvaló, hogy az interjúalanyok nem voltak tisztában az említett információs portál létezésével [2].

Az eSzemélyi igazolvány használati eseteinek hiánya és az ismerethiány ok-okozati összefüggést mutat: azért sem rendelkeznek információkkal a saját eSzemélyi igazolványaikról (tanúsítvány lejárata stb.) és általában a megoldásról, mert nem szükséges számukra, és nem jár előnnyel az eSzemélyi szolgáltatásainak napi szintű igénybevétele [2].

A megkérdezettek szerint végsősoron azért nem terjednek el az eSzemélyi igazolvány elektronikus funkciói, mert fizikai kártyaolvasó készülék szükséges azok használatához. Ezzel kapcsolatban több – szintén ismerethiányra visszavezethető – problémát is jeleztek: nem tudják, hogy milyen típusú kártyaolvasóval kompatibilis az eSzemélyi, pénzbe kerül megvásárolni és nem érzik megtérülő befektetésnek a vásárlást. Hangsúlyoznám, hogy az eszemelyi.hu információs portálon ezzel kapcsolatban is vannak anyagok – a résztvevők ezeket sem ismerték. Továbbá szerintük könnyítené a használatot egy mobilalkalmazás, amellyel kiváltható lenne a kártyaolvasó. Ilyen alkalmazás 2022 óta elérhető – és már a kutatás végrehajtásának idején is elérhető volt – eSzemélyiM néven, de sajnálatos módon ezzel nem voltak tisztában [2].

1.8 Az eSzemélyi további lehetőségei

Mint azt korábban említettem a 2023. január 1-jétől elérhető SZTSZ szolgáltatás lehetővé teszi, hogy az államigazgatásban és a rendvédelemben dolgozók a saját eSzemélyi igazolványuk eAláírás funkciójával úgy hitelesítsenek elektronikus dokumentumokat, hogy a szervezetük, az abban betöltött tisztségük, a beosztásuk és akár a rendfokozatuk is igazolásra kerüljön egy szerepkör-tanúsítványban.

A szolgáltatás tervezett életútja nem ismert számomra, de a szolgáltatás jellegéből következik, hogy további állami nyilvántartások bevonásával a jogosultak köre jelentős mértékben bővíthető lenne (többek között az egyéni vállalkozók és egyéni ügyvédek számára). Az „Egyéni vállalkozók nyilvántartása" alapul szolgálhatna az egyéni vállalkozók szerepkör-tanúsítványának kiállításához, az egyéni ügyvédek esetében pedig a „Magyar Ügyvédi Kamara" nyilvántartása lehetne irányadó. Így az induló vállalkozásoknak nem kellene piaci szereplőktől elektronikus aláírásra szolgáló tanúsítványokat vásárolniuk annak érdekében, hogy papírmentes ügyvitelt alakíthassanak ki.

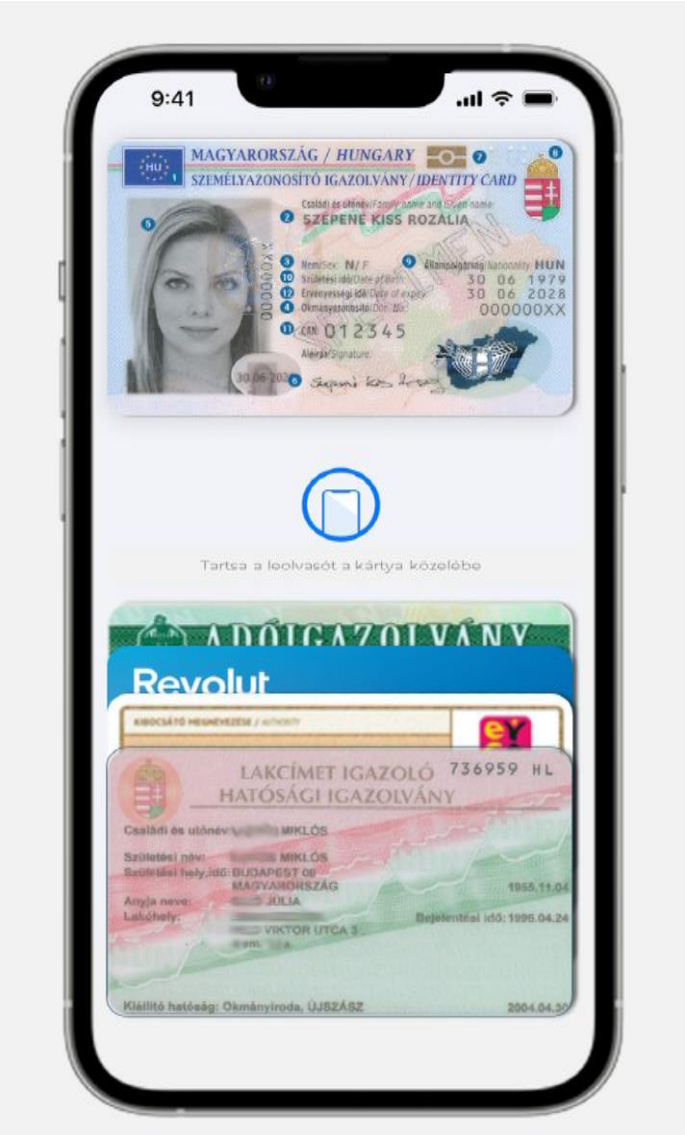
Korábban említett kutatásom (Nyári [2]) résztvevői szerint a magánszemélyek tekintetében – látva a bankkártyák példáját – érdemes lenne fontolóra venni olyan mobilalkalmazás kialakítását, amely – a technikai előfeltételek rendelkezésre állása esetén például NFC – teljes egészében kiválthatná még az eSzemélyi igazolványt is. Így elérhető lenne, hogy az okmány elektronikus funkcióinak használatához – az egyszeri regisztrációt leszámítva – még a kártyára se legyen szükség. Megfontolandó lenne az okmányt képessé tenni arra, hogy digitális pénztárcába rögzíthető legyen.

Itt emelném ki az Európai digitális identitáshoz kapcsolódó magyar programot, a Nemzeti Digitális Állampolgárság Programot, melynek keretében éppen ezzel a képességgel fog bővülni az eSzemélyi szolgáltatásköre.

1.9 Nemzeti Digitális Állampolgárság Program

2022 decemberében a Digitális Magyarország Ügynökség közzétette a Nemzeti digitális állampolgárság program c. dokumentumot [56], amely összhangban a korábban már említett Európai digitális identitással (lásd 1.1.2.) összhangban kijelöli a magyar eKözigazgatási szolgáltatások felhasználóbarát továbbfejlesztési irányait, szem előtt tartva a XXI. századi technikai, digitalizációs megoldásokat. A dokumentum szerint az új rendszerelemek kialakítása 2023-ban megkezdődik és „az állampolgárok 2026-ra

szinte minden ügyüket digitálisan, elsősorban mobilalkalmazások segítségével intézhetik”.



2. Ábra A Digitális személyi adattárca mobilalkalmazás látványterve. Forrás: Nemzeti digitális állampolgárság program [56]

A dokumentum szerint négy digitális alapszolgáltatás fogja jelenteni az új rendszer alapját: az eSzemélyazonosítás, az ePosta, az eDokumentumkezelés és az eFizetés [56].

„A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól” szóló törvény [47] alapvetően 2024. július 1-jén lép hatályba bizonyos rendelkezéseinek kivételével. A következő fontos mérföldkő szeptember 1-jén lesz, a törvény szerint akkor indul ugyanis a digitális személyi adattárca szolgáltatás, amely egy mobilalkalmazás segítségével lehetővé fogja tenni az állampolgárok számára személyazonosságuk igazolását és dokumentumok elektronikus aláírását.

1.10 Összefoglalás

A fejezetben röviden ismertettem a személyazonosításra szolgáló okmányok fejlődéstörténetének – jelen értekezés szempontjából – legjelentősebb mérföldköveit. Bemutattam továbbá az egyik várható továbbfejlesztési irányt is a European Digital Identity-t, mely korszerű megoldásainál fogva minden bizonnyal nagyban hozzájárulna az elektronikus okmányok széleskörű elterjedéséhez. Ennek magyarországi implementációja a Nemzeti Digitális Állampolgárság Program keretében fog megvalósulni.

A fejezetben bemutattam a magyar – az eIDAS rendelettel kompatibilis – eSzemélyi igazolvány képességeit, alkalmazásának hardveres és szoftveres előfeltételeit.

Az általam összegzett és ismertetett belügyminisztériumi statisztikákból látható, hogy az eSzemélyi okmány ugyan eljutott az állampolgárok túlnyomó többségéhez, de annak képességeit csak alig használják ki. Ez abból is látszik, hogy a jogosult lakosság létszámához képest milyen kevesen igényelték például az eAláírás funkciót.

A leírtakból világosan következik, hogy az eSzemélyi igazolvány elektronikus aláírás funkcionalitása az SZTSZ használatával alkalmazható lenne Kormányablak dolgozói, orvosok, ügyvédek, egyéni vállalkozók számára hivatalos ügyekben, jogkörükben eljárva. Ez anyagi előnnyel is járna az említett körök számára, hiszen nem lenne szükséges közel 100.000 Ft-os éves díjért cserébe piaci szereplőktől elektronikus aláíró tanúsítványt vásárolni.

A korábban végrehajtott kutatásom eredményei (Nyári [2]) azt támasztják alá, hogy az eSzemélyi igazolvány képességeivel nincsenek tisztában az állampolgárok, vagyis a használathoz szükséges információk nem jutottak el hozzájuk.

Fentiekből az is következik, hogy nem a bizalom hiánya a legfőbb oka a terjedés lassú ütemének, ezért a 1. számú hipotézisemet elvetem.

A felvetett problémák modellezéséhez szükséges egy alkalmas keretrendszert választani, erről és a kiválasztott módszertanról, az eSzemélyi igazolványra történő alkalmazásáról olvashatunk részletesen a 3. fejezetben.

Előbb azonban meg kell vizsgálni az okmány használatának biztonsági kérdéseit is, ezért a következő fejezetben egy kockázatelemzést fogok ismertetni, amely az eSzemélyivel és szolgáltatásaival kapcsolatos kockázatokat mutatja be.

2 AZ ESZEMÉLYI IGAZOLVÁNY KOCKÁZATAI

A nemzetközi és hazai szakirodalom egyaránt részletesen tárgyalja az eID okmányok lehetséges kockázatait. Kübler [57] az észtországi, a svájci és az európai unió béli eID megoldások példáin keresztül mutatja be az elektronikus azonosítási rendszerek lehetőségeit és kockázatait számba véve az összes érdekelt felet.

Edu, Hooper, Maple és Crowcroft [58] állítása szerint az eID megoldásokkal kapcsolatosan felmerülő kockázatok azonosítása, kiértékelése és azok esetleges hatásának felmérése kulcsfontosságú, hiszen a működési problémák, a kompromittálódás, vagy a visszaélés súlyos anyagi károkat okozhatnak az állam, a társadalom, illetve az állampolgárok számára. Vizsgálódásuk hangsúlya az érdekelt felek beazonosításán van.

Edu, Hooper, Maple és Crowcroft [59] egy másik munkájukban ugyancsak a nemzeti elektronikus azonosítási megoldások (NeID – National electronic IDentification) kockázatait vizsgálják azokat forrás szerinti kategóriákba csoportosítva.

Koller [60] az eSzemélyi igazolvány és az eSzemélyiM mobilalkalmazás elektronikus azonosítás funkcióját vizsgálta információbiztonsági szempontból. Szádeczky [61] 2017-es cikkében részletesen kifejti a tárolóelemmel rendelkező okmányok, mint például az elektronikus útlevél és az eSzemélyi igazolvány működési módját, biztonsági veszélyeit és az azok ellen való lehetséges védekezési megoldásokat.

Hazai [62] szerint A Nemzetbiztonsági Szakszolgálat Szakértői Intézet hatásköre az új okmányok esetében az ún. okmányvédelmi rendszerterv elkészítése, amelyben meghatározásra kerülnek a szóban forgó biztonsági okmány esetében alkalmazandó védelmi előírások, melyek biztosítják az okmányvédelmi kategóriának megfelelő védelmet. Ez alapján készül el a Szádeczky [61] által is említett okmányvédelmi terv. Ezek a dokumentumok azonban nem nyilvánosak.

Mint azt a korábbiakban láthattuk, az eSzemélyi igazolvány egy elektronikus azonosító okmány, mely megannyi elektronikus funkcionalitással rendelkezik, és a tulajdonosának bizonyos személyes adatait is tárolni képes. Előnyei mellett azonban kockázatokat is hordozhat magában, melyeket szükséges feltárni annak érdekében, hogy a megoldás ne csak hasznos, hanem biztonságos is legyen. Jelen fejezet célja egy átfogó kockázatelemzés bemutatásán keresztül felhívni a figyelmet az okmány használata során felmerülő információbiztonsági kockázatokra annak érdekében, hogy a növekedjen a

megoldás általános biztonsága és emelkedjen a vele kapcsolatos információbiztonsági tudatosság szintje.

Sajnos a kártya funkciói közel sem széleskörűen elterjedtek a magyar lakosság körében. Egy teljeskörű kockázatértékelés elvégzése az okmány általános biztonságának javításán túl elősegítheti új funkciók hatékony kialakítását és bevezetését is.

Az okmány funkcióinak használatához két PIN kód (elektronikus azonosítás és elektronikus aláírás) ismeretére és kártya fizikai birtoklására is szükség van. A megfelelő szintű információbiztonsági tudatosság hiányában könnyen félvállról vehetők a kártya elvesztése, ellopása esetén felmerülő kockázatok.

Sajnos jelenleg Magyarországon az elektronikus bizalmi szolgáltatások és az elektronikus aláírási szolgáltatások a 2012. évi CLXVI. törvény [63] értelmében nem minősülnek létfontosságú rendszerelemeknek. Idővel azonban, ahogy a dokumentum használata egyre jobban beépül a mindennapi életbe, az állampolgárok függése vélhetően erősödni fog az elektronikus bizalmi szolgáltatásoktól és az elektronikus aláírási szolgáltatásoktól, különös tekintettel a Nemzeti Digitális Állampolgárság Program keretében megvalósuló digitális adattárcára.

Az elektronikus bizalmi szolgáltatók és az elektronikus aláírási szolgáltatások létfontosságú rendszerelemként való azonosításának és kezelésének meg kellene jelennie a magyar jogi környezetben is. Az infrastruktúra megfelelő védelméhez eljárások és bevett gyakorlatok (best practices) kidolgozása szükséges, ahogyan azt Somogyi és Nagy [64] a pénzügyi szektorral kapcsolatban megfogalmazta.

Az eSzemélyi igazolvány kockázatainak felméréséhez meglátásom szerint célszerű az ISO/IEC 27000 szabványcsaládot használni, mert egy szervezet tanúsíthatja az ISO/IEC 27001:2022 [65] alapján létrehozott információbiztonsági irányítási rendszerét (ISMS – Information Security Management System). Továbbá a MIBIK (Magyar Informatikai Biztonsági Keretrendszer) [66], amely az informatikai biztonság irányításának, követelményeinek és vizsgálatának magyar keretrendszere, ami nagymértékben kapcsolódik az említett nemzetközi szabványhoz, mivel az a vonatkozó nemzetközi ISO szabványokon (ISO/IEC 17799 szabvány, amely az ISO/IEC 27002 elődje), műszaki jelentéseken, NATO Tanácsi Memorandumokon és az Európai Unió előírásain alapul [67].

A fejezetben bemutatott, az eSzemélyi igazolvány kockázatértékelése az ISO/IEC 27005:2022 szabvány iránymutatásai alapján készült. A nemzetközi szabvány fogalmait és lépéseit felhasználva meghatároztam az okmány külső és belső kontextusát, majd az eseményalapú (event-based risk identification) és a vagyontárgy alapú (asset-based risk identification) kockázatazonosítási megközelítések kombinált alkalmazásával beazonosítottam a különböző kockázati forgatókönyveket. Végül bemutattam ezek kiértékelésének módját.

Egy átfogó kockázatelemzés nagyban segítheti az eKözigazgatási szolgáltatások hatékony bevezetését és működtetését. Az eSzemélyi okmányon elvégzett, ISO/IEC 27005:2022 szabványon alapuló kockázatértékelés során azonosított kockázatok alapul szolgálhatnak a megfelelő információbiztonsági bevált gyakorlatok (best practices) és képzési anyagok tervezéséhez és kidolgozásához.

Korábban az eSzemélyi igazolványról – ismereteim szerint – nem publikáltak az ISO/IEC 27005:2022 szabvány alapján kockázatelemzést. Az itt bemutatott eredmények hozzájárulhatnak a meglévő használati esetek biztonságosabbá tételéhez, de felhasználhatók új használati esetek tervezésekor és implementálásakor is, szem előtt tartva az IT biztonságot.

Ahogyan arról korábbi cikkeimben (Kerti és Nyári [67], Nyári és Kerti [68]) írtam, számos nemzetközi és nemzeti szabvány, ajánlás foglalkozik kockázatelemzéssel, a különböző módszerek száma körülbelül 200 [69]. Jelen értekezésben az információbiztonsági kockázatokra összpontosítok ezért az általános célú vagy nem információbiztonság fókuszú módszereket/szabványokat (például ISO 31000 – Kockázatelemzés, ISO/SAE 21434 – Közúti járművek kiberbiztonsági tervezése) kizárom.

Korábbi írásaimban (Kerti és Nyári [67], Nyári és Kerti [70], Nyári és Kerti [68]) bemutattam a különféle kockázatelemzéssel és szoftverminőséggel foglalkozó nemzetközi szabványokat. A NATO NIAPC katalógusa (NATO Information Assurance Product Catalog - NATO információbiztosítási termékkatalógus) és az Európai Unió Kiberbiztonsági Ügynökségének (ENISA) hivatalos honlapján elérhető termékkatalógus ugyan tartalmaz információkat a különféle módszertanokról (CRAMM, NIST SP 800-30, ISO/IEC 27005 stb.), de sajnálatos módon ezek nincsenek naprakész állapotban tartva.

Ismertettem a magyarországi viszonyokat kitérve a Közigazgatási Informatikai Bizottság (KIB) által 2008-ban Magyar Informatikai Biztonsági Ajánlások (MIBA) címmel

közzétett ajánlásokra, azok iránymutatásaira az ISO/IEC 27001 megfelelésre és a kockázatelemzések elvégzésére vonatkozóan [67].

Korábbi írásaimban (Kerti és Nyári [67] és Nyári és Kerti [68]) levezettem, hogy hogyan lehet kombináltan alkalmazni az ISO/IEC 27005 és a NIST SP 800-30 szabványokat, valamit azt is, hogy miért érdemes az ISO/IEC 27005:2022 nemzetközi szabványt használni az eSzemélyi okmány kockázatelemzésére.

Részletesen bemutattam az ISO/IEC 27005 szabvánnyal kapcsolatos szakirodalmat: hogyan alkalmazták a szabványt különböző területeken, úgymint az eKözigazgatási szolgáltatások, az eID-k, a közösségi közlekedési rendszerek, vagy a kiberbűnözés megelőzése. Az írásból nyilvánvalóvá válik a megfelelő részletességgel kivitelezett kockázatértékelés fontossága is. Elvégzése nagyban hozzájárul egyrészt az új szolgáltatások biztonságtudatos kialakításához, másrészt azok sikeres bevezetéséhez. Bemutattam a kockázatkezelés fontosságát és hasznosságát az elektronikus személyazonosító okmányok terén [68].

Az ISO/IEC 27005:2022-ben bevezetésre került az ún. esemény alapú kockázatazonosítási megközelítés, melynek alkalmazhatóságát szeretném bemutatni jelen fejezetben. Emellett azonban szubjektív oka is vannak annak, amiért az ISO/IEC 27005:2022 nemzetközi szabványt választottam, az ugyanis meglehetősen alulértékeltnek tűnik Magyarországon, mivel a Magyar Szabványügyi Testület hivatalos honlapján (mszt.hu) nem vásárolható meg, és nem is fordították le magyar nyelvre. Szeretném bemutatni, hogy a szóban forgó szabvány alkalmazása számos gyakorlati előnnyel jár.

Ahhoz, hogy egy eID rendszer kritikus stratégiai eszközzé váljon, széles körben használtnak, bizalomra méltónak, robusztusnak és hozzáférhetőnek kell lennie. Ennek eléréséhez kulcsfontosságú az eID rendszerek kockázatainak azonosítása és értékelése a potenciális fenyegetések azonosításától kezdve, valószínűségük és hatásuk felmérésén keresztül kockázati szintjük alapján történő rangsorolásukig [59].

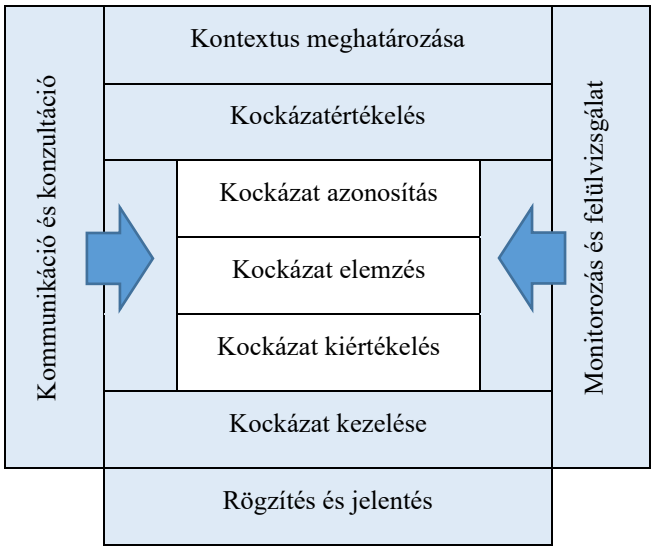
A megfelelő infrastruktúra-védelem kialakításához elengedhetetlen lenne a magyar elektronikus személyazonosító igazolvány (beleértve az elektronikus aláírási funkcionalitást is) megfelelő kockázatelemzése. Ennek figyelembevételével elvégeztem a magyar eID átfogó kockázatelemzését.

A továbbiakban nem írom ki a szabvány évszámát („:2022”), és ahol „ISO/IEC 27005”-ként hivatkozom rá, ott alapértelmezés szerint a 2022-es kiadást értem. A következő részekben az említett szabvány egy lehetséges alkalmazási módját mutatom be.

2.1 Kockázatkezelés az ISO/IEC 27005 szabvány alapján

Az ISO/IEC 27000 család meglehetősen sok szabványból áll. A legnépszerűbb az ISO/IEC 27001, mivel a szervezetek a szabvány alapján tanúsíthatják az Információbiztonsági Irányítási Rendszerüket (Information Security Management System - ISMS). Az ISO/IEC 27002 szorosan kapcsolódik az előbbihez, mivel útmutatást ad az ISO/IEC 27001 bevezetéséhez/megvalósításához. Az ISO/IEC 27005 a kockázatkezelés miként jéről szól, ezt használtam jelen disszertáció írásakor [67, 68].

A családban vannak ágazatspecifikus szabványok, amelyeket érdemes megemlíteni: az ISO/IEC 27033 útmutatást ad a hálózatbiztonsági kockázatok azonosításához és kezeléséhez. Ezen túlmenően az ISO/IEC 27034 irányelveket ad a különféle szoftverek, alkalmazások biztonságára vonatkozóan, legyen szó akár saját fejlesztésű, akár harmadik féltől származó alkalmazásokról. A vonatkozó szabványokat minden olyan léptékű hardver/szoftver fejlesztési projektekben, érdemes alkalmazni, mint például az eID megoldások [67, 68].



3. Ábra Kockázatértékelés lépései az ISO/IEC 27005 szerint. Forrás: saját szerkesztés az ISO/IEC 27005 alapján [71]

Fenti ábra (3. Ábra) az ISO/IEC 27005 szabvány szerinti kockázatértékelési módszertan lépéseit ábrázolja.

2.1.1 Kontextus meghatározása

A Kontextus meghatározása (Context Establishment) fázisban részletesen le kell írni az eID belső és külső környezetét, beleértve a jogi környezetet (nemzeti és nemzetközi szabályozás), a vonatkozó szabványokat. Meg kell határozni az Információbiztonsági Kockázati Kritériumokat is, mint például a Kockázat Elfogadási Kritériumot (RAC – Risk Acceptance Criteria) és a kockázatértékelés elvégzésének kritériumait. Ezt követően a módszertant (kvalitatív vagy kvantitatív) úgy kell kiválasztani, hogy az ismételt kockázatértékelés következetes és összehasonlítható legyen [71, 68].

2.1.2 Kockázatértékelés

2.1.2.1 Kockázat azonosítás

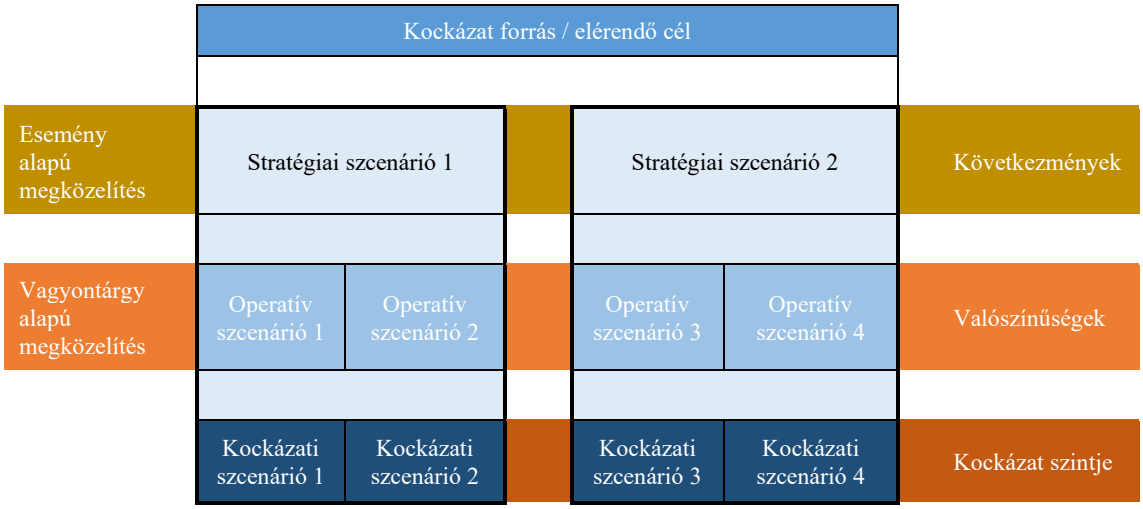
Ezután a Kockázatértékelés (Risk Assessment) szakaszban a kockázatazonosítás (Risk Identification) allépés következik. A szabvány 2022-es verziója a vagyontárgy alapú (Asset-based approach) megközelítés mellett bevezeti az új, eseményalapú (Event-based approach) megközelítést. A két különböző módszer kombinációját érdemes használni, mert azok különböző részletességgel tárják fel a kockázatokat. Az eseményalapú megközelítés használatával a kockázatok forrásából, a támadók lehetséges motivációiból és a támadások által elérendő célokból kiindulva számba vesszük az egyes üzleti vagyontárgyak kockázatait egy stratégiai szempontú kockázatazonosítás végrehajtásának érdekében, mely ugyan nem terjed ki minden részletre, de a következmények feltárására kiválóan alkalmas. Az esemény alapú megközelítés eredményeként létrejönnek az ún. stratégiai szcenáriók vagy stratégiai forgatókönyvek (Strategic Scenario) [71].

Ezzel szemben a vagyontárgy alapú megközelítés sorra veszi az érintett vagyontárgyakat és azok sérülékenységeit. Majd sorra veszi a sérülékenységeket potenciálisan kihasználni képes fenyegetéseket. Ezáltal meghatározásra kerülnek az ún. operatív szcenáriók vagy operatív forgatókönyvek (Operational Scenario) [71].

Az operatív szcenáriókhoz valószínűségeket rendelünk [71]. A bekövetkezési valószínűség meghatározásakor célszerű figyelembe venni a korábban esetlegesen bekövetkezett incidenseket is, melyek gyakorisága alapján következtetéseket lehet levonni a bekövetkezés valószínűségére. A „Using the Methods of Probability Theory Analyzing Logs of Electronic Information Systems” c. cikkemben (Nyári [72]) bemutattam, hogy hogyan alkalmazhatók a valószínűségszámítás módszerei elektronikus információs rendszerek naplóinak elemzése során, nemkívánatos események

előrejelzésére. Ugyanezen módszer kockázatkezelések végrehajtása során is hasznos lehet, hiszen korábbi incidensek gyakoriságának eloszlása alapján megbecsülhető a következő előfordulás időpontja.

Az alábbi ábrán (4. Ábra) látható az esemény és a vagyontárgy alapú megközelítés kapcsolata.



4. Ábra Esemény alapú és vagyontárgy alapú megközelítés kapcsolata, Forrás: saját szerkesztés ISO/IEC 27005 [71] alapján

Minden operatív szcenárió besorolható egy stratégiai szcenárió alá, ez képezi le azt a helyzetet, hogy egy stratégiai cél elérésére több lehetséges támadás/útvonal létezhet. Egy stratégiai és egy operatív szcenárió páros képez egy kockázati szcenáriót (Risk Scenario) [71].

A kockázati szcenárió szintje (Level of Risk) meghatározható a stratégiai szcenárió következményének súlyosságából (Consequences) és az operatív szcenárió valószínűségéből (Likelihood) [71].

Jelen értekezés megírásához a fent említett két megközelítés előbb leírt kombinációját alkalmaztam, azonban tartalmi korlátok miatt nem közlöm az egész elemzést részletekbe menően.

Nagyon fontos a kockázattulajdonosok (Risk owners) meghatározása minden azonosított kockázathoz, mivel ők rendelkeznek felhatalmazással, felelősséggel és hatáskörrel az azonosított kockázatok kezelésére [71, 68].

2.1.2.2 Kockázat elemzés

Ezután következik a Kockázatelemzés (Risk Analysis), ahol a korábban rögzített kritériumok alapján meghatározásra kerülnek a kockázati szintek. Ebben az állépésben be kell vonni a kockázattulajdonosokat, és konzultálni kell velük, mivel ők a területük

szakértői, akik a legpontosabb becsléseket tudják adni. Ez egy erősen szubjektív folyamat, számos bizonytalansággal (személyes, módszertani vagy rendszerszintű). A szubjektivitás csökkentése érdekében célszerű egy értékelő csoportot alkalmazni egyetlen személy helyett [71, 68].

2.1.2.3 Kockázat kiértékelés

Az információbiztonsági kockázatok értékelése (Risk Evaluation) lépés kevésbé szubjektív, mert az azonosított kockázatok előző lépésben megállapított szintjeit össze kell hasonlítani a kockázatelfogadási kritériumokkal. Az elfogadásról szóló döntés meghozatalakor be kell szerezni a kockázattulajdonosok beleegyezését is. Gyakorlatilag az elfogadott kockázatok nem igényelnek mérséklést (Mitigation), csak monitorozást. Ez a lépés kifinomultabb módon is végrehajtható, ha különböző kockázati osztályokhoz (például adatvédelmi kockázatok, működési kockázatok, nem megfelelőségi kockázatok) különböző elfogadási kritériumok kerülnek meghatározásra [71, 68].

2.1.3 Kockázatkezelés

Az elfogadható szintet meghaladó kockázatok kezelést igényelnek, amely a következő, Kockázatkezelés (Risk Treatment) nevű szakaszban történik. Az ISO/IEC 27005 [71] szabvány szerint négy, egymással kombinálható módszer létezik a kockázatok kezelésére:

- Elkerülés (Avoidance): a szóban forgó kockázatnak kiszolgáltatott tevékenységeket vagy műveleteket le kell állítani annak érdekében, hogy a bekövetkezés valószínűségét nullára csökkentsük.
- Módosítás (Modification): csökkenteni kell a bekövetkezés valószínűségét vagy a következmények súlyosságát (vagy akár mindkettőt).
- Megosztás (Sharing): harmadik fél bevonása (például alvállalkozó, biztosító) a kockázat következményeinek megosztására.
- Megtartás (Retention): jól informált döntés a kockázat megtartására általában a felső vezetés részéről, ami azt jelenti, hogy változtatás nélkül tovább folytatjuk a kockázatos tevékenységet vagy műveletet.

A kockázatkezelési lehetőségek megvalósításához szükség lehet ellenőrzésekre (Control). A javasolt 93 ellenőrzés szerepel az ISO/IEC 27001 [65] szabványban, négy témára osztva: szervezeti, emberi, fizikai és technológiai. Az ellenőrzéseket tovább lehet osztani preventív, detektív és javító osztályokra. Az ISO/IEC 27001 követelményeként létre kell hozni a Nyilatkozat az alkalmazhatóságról (Statement of Applicability) című

dokumentumot, amely tartalmazza a szükséges és a kizárt ellenőrzések listáját – indoklással együtt. Egyéni ellenőrzéseket is bevezethetünk, de kizárólag jól dokumentált módon [68].

Az ISO/IEC 27001 [65] szabvány az ún. kockázatkezelési terv (Risk Treatment Plan) elkészítését is előírja. Ehhez a dokumentumhoz a kockázattulajdonosok jóváhagyása is szükséges. Meg kell határoznia, hogy a szervezet hogyan kívánja kezelni a kezelést igénylő kockázatokat. Szinte minden esetben a folyamat végén marad ún. maradvány kockázat – ez természetesen a kockázattulajdonosok jóváhagyásával lehetséges. A kockázatkezelés azonban nem része jelen disszertációnak.

A kockázatértékelésnek tervezett időközönként megismételhető folyamatnak kell lennie, a különböző időpontokban végzett felmérések eredményeinek konzisztensnek és összehasonlíthatónak kell lenniük. Ezenkívül az időszakos kockázatértékelésnek az üzleti tevékenység szerves részét kell képeznie. A kockázatértékelést idővel folyamatosan fejleszteni kell, felül kell vizsgálni a módszertant, finomítani kell a különböző kockázati kritériumokat stb. [71, 68].

A lehetséges támadók és motivációik listájának kidolgozását tűztem ki célul a lehető legtöbb szempontot figyelembe vevő kockázatelemzés elkészítéséhez. A következő részben bemutatom, hogy a fenti fogalmak, módszertan és kritériumok hogyan alkalmazhatók a magyar eSzemélyi igazolványra. Tartalmi korlátok miatt azonban csak a kockázatelemzés sarokpontjait fogom bemutatni.

2.2 Az eSzemélyi kockázatértékelésének végrehajtása

Jelen fejezet célja egy kockázatértékelés bemutatása, amely az eSzemélyi igazolvány és a használatához szükséges hardver és szoftver megoldások kliens és infrastruktúra oldalon felmerülő kockázatait tárja fel. Az eredmények elősegíthetik az eSzemélyi megoldás biztonságtudatos továbbfejlesztését, továbbá rámutathatnak a terjedést lassító tényezőkre. Cél továbbá egy olyan alapvonal felállítása, amelyre épülve további kockázatértékelések végezhetők.

Az ISO/IEC 27005 szabvány alapvetően szervezetek kockázatértékelésére használható, mint azt korábban láttuk. Ez az értelmezés azonban kiterjeszthető: jelen értekezés szempontjából egy egész országot, Magyarországot kell vizsgálni, mert az állampolgárok nagy része valamilyen szinten érintett az eSzemélyi igazolvánnyal kapcsolatban. A

következőkben ismertetem a magyar elektronikus azonosító okmánnyal kapcsolatos kockázatkezelés javasolt menetét.

2.2.1 Kontextus meghatározása (Context establishment)

2.2.1.1 Külső kontextus

Az eSzemélyi tágabb értelemben vett környezetét főként hazánk EU tagsága határozza meg, így a külső kontextus egyik legnagyobb összetevője az Európai Unió és a digitális egységes piac jogszabályi környezete, beleértve például az eIDAS rendeletet. Továbbá itt kell megemlíteni azokat a nemzetközi szabványokat (ISO/IEC 27033 hálózatbiztonsági, ISO/IEC 27034 alkalmazásbiztonsági stb. szabványokat), melyeket egy ilyen volumenű rendszer fejlesztésekor és üzemeltetésekor célszerű alkalmazni. Ezeket korábbi cikkemben részletesen kifejtettem (Nyári és Kerti [68]), jelen értekezésben tartalmi korlátok miatt nem szerepeltetem.

Az eSzemélyi igazolvány ún. biztonsági okmány a 86/1996. (VI. 14.) Korm. rendelet [73] alapján. Személyazonosság igazolására alkalmas igazolvány lévén az „A" okmányvédelmi kategóriába tartozik, ezáltal minden összetevőjét védeni kell a teljes vagy részleges hamisítás ellen. Ezeknél az okmányoknál alkalmazni kell a kémiai, fizikai, technikai, technológiai és adminisztratív eljárásokat. Tekintettel arra, hogy elektronikus tárolóelemmel is rendelkezik, előbbiek mellett a digitális védelmi módszereket is alkalmazni kell [61, 73].

A 2252/2004/EK rendelet [74] meghatároz a tagállamok által kibocsátott útiokmányokra minimumkövetélmenyeket. Többek között előírja az ICAO 9303-as dokumentumban előírtak alkalmazását is. A minimumkövetelmények az eSzemélyi igazolványra is vonatkoznak, hiszen az útiokmányként is használható az EU területén [62, 74].

A Nemzetbiztonsági Szakszolgálat Szakértői Intézet hatásköre az ún. okmányvédelmi rendszerterv elkészítése, amelyben meghatározásra kerülnek a szóban forgó biztonsági okmány esetében alkalmazandó védelmi előírások, melyek biztosítják az okmányvédelmi kategóriának megfelelő védelmet. Ez alapján készül el az okmányvédelmi terv. Ezen dokumentumok azonban nem nyilvánosak [62, 61].

A személyes adatok az eID megoldások egyik legértékesebb vagyontárgyai, ezért az olyan értékeket, mint az anonimitás, a titoktartás és az ellenőrzés, prioritásként kell kezelni az eID rendszerek tervezése, fejlesztése és telepítése során. A szilárd jogi és szabályozási keretek azt is biztosítják, hogy az eID rendszereket hatékonyan és

átláthatóan irányítsák, mivel egyértelmű szabályokat és előírásokat biztosítanak a személyes adatok gyűjtésének, felhasználásának és megosztásának kezelésére [59].

Az adatvédelemre általában olyan normák és gyakorlatok vonatkoznak, amelyek védik az emberi autonómiát, identitást és méltóságot. Ezek a normák szabályozzák az egyének azon szabadságát, hogy hozzájáruljanak személyazonosságuk (például testük, adataik és jó hírnevük) felfedéséhez vagy ellenőrzéséhez [59].

2.2.1.2 Belső kontextus

A vizsgálat magában foglalja az eSzemélyi igazolvány tároló elemét, az azon tárolt adatokat, az NFC kommunikációt a tárolóelem és a kártyaolvasó készülék között. Mivel a kártyaolvasó helyett mobileszköz használatára is sor kerülhet, ezért az eSzemélyiM mobilalkalmazást futtató mobileszköz és az eSzemélyi kliens programot futtató számítógép és kettő közötti kommunikációs csatorna is ide értendő. Továbbá az eSzemélyi mobilalkalmazás, az eSzemélyi kliens, a KEAASZ aláírószoftver, valamint a QR kód generátor szoftver is részét képezi a vizsgálat hatókörének.

A belső kontextus részét képezik továbbá a magyar jogszabályok, a Belügyminisztérium, a Kormányablakok, külső alvállalkozók, például a NISZ Zrt.-t, mint számos magyar e-kormányzati szolgáltatás, köztük az elektronikus aláírás funkció fejlesztője és üzemeltetője, valamint az Idomsoft Zrt., mint az eSzemélyi infrastruktúra fejlesztője és üzemeltetője, a különféle elektronikus közigazgatási szolgáltatások, végül pedig az eSzemélyi igazolványra jogosult magyar állampolgárok [68].

Korlátozó tényezőként felmerül, hogy külső megfigyelőként nem férek hozzá a magyar állam és az alvállalkozói között létrejött különböző szerződésekhez, sem az azokban foglalt kontrollokhoz, sem az eSzemélyi igazolványra vonatkozó okmányvédelmi tervhez, sem a korábbi kockázatértékelések eredményeihez.

A tárolóelemmel rendelkező okmányok, mint például az elektronikus útlevél és az eSzemélyi igazolvány rendelkeznek különféle védelmi megoldásokkal az adatok észrevétlen kiolvasása ellen, például kriptográfiai (rejtjelezési algoritmusok és hash függvények) megoldások alkalmazásával [61].

Az elektronikus útlevelek esetében alkalmazott ún. Basic Access Control (BAC) hozzáférés védelmi megoldás az eSzemélyi igazolvány eÚtiokmány szolgáltatásának használata során is elérhető. Az okmányról számítógéppel leolvasható résznek (MRZ, Machine Readable Zone) adataiból generálódó hozzáférési kulcs feltörési ideje azonban

bizonyítottan felgyorsítható az entrópiájából fakadó 35 évről akár 3 órára is. Az okmányban rögzített ujjnyomat tárolására azonban már az Extended Access Control (EAC) módszer használatos, amelynek alapjait az ICAO 9303-as dokumentuma határozta meg, de a megvalósítás nem egységes az EU egyes tagországaiban [61].

Alkalmazható az ún. PACE (Password Authenticated Connection Establishment, Jelszóval Hitelesített Kapcsolatfelépítés) módszer is az eSzemélyi esetében. Ez a megközelítés az okmányról szabad szemmel leolvasható CAN (Card Access Number, Kártya Hozzáférési Szám) alkalmazásával biztosítja az illetéktelen hozzáférés elleni védelmet. A kártyáról történő hozzáférés előtt a kártyaolvasón be kell állítani ezt a kódot, majd az adatok kiolvasásakor a készülék ezzel az azonosítószámmal hitelesíti magát a kártya felé [61, 75].

2.2.1.3 Kockázatvállalási hajlandóság (Risk appetite) meghatározása

A szervezet kockázatvállalási hajlandóságának alacsonynak kell lennie, mivel az állampolgárok személyes adatai és a személyazonosságuk biztonsága forog kockán. Ezen túlmenően a magyar elektronikus azonosító okmány elektronikus aláírási funkciójával pénzügyi tranzakciók és szerződések is jóváhagyhatók. Nincs helye indokolatlan kockázatvállalásnak, ha az emberek vagyonáról, személyes adatairól vagy magánéletéről van szó [68].

2.2.2 Kritériumok

2.2.2.1 Kockázat-elfogadási kritérium

A javasolt kockázat-elfogadási kritériumok következmény-lehetőség alapon (Consequence-Possibility Based) a következők: minden alacsony szint feletti kockázatot mérsékelni kell. A kockázati mátrix színkódjait az alábbi táblázatban láthatjuk [68].

5. Táblázat Kockázati szintek színkódjai, Forrás: saját szerkesztés ISO/IEC 27005 [71] alapján

Osztályok	Kockázat értékelés	A kockázat szintje
Alacsony (zöld)	Elfogadható kockázat módosítás nélkül	Nagyon alacsony, Alacsony
Mérsékelt (narancssárga)	Irányítás alatt tartva elfogadható	Közepes
Magas (piros)	Elfogadhatatlan	Magas, Nagyon magas

2.2.2.2 Következmények

Az ISO/IEC 27005 szabvány [76] „A” mellékletének táblázatai alapján kvalitatív megközelítést használok a kockázati szintek, valamint egy kombinált kvantitatív-

kvalitatív megközelítést a következmények és a valószínűségek meghatározásakor az alábbiak szerint [68].

A Központi Statisztikai Hivatal (KSH) közzétett statisztikái [77] alapján 2023 októberében a teljes munkaidőben foglalkoztatottak nettó átlagkeresete havi 389 300 Ft volt, ami évi 4 671 600 Ft-ot jelent. Mint korábban említettem, az eSzemélyi okmány maximum 50 000 000 Ft értékű szerződés esetén használható elektronikus aláírásra. Ez a határ a magyar éves átlagkereset több mint tízszerese.

Az előbbi tények figyelembevételével a lenti táblázat (6. Táblázat) a következmények osztályozási skáláját mutatja be.

6. Táblázat Következmények kombinált kvalitatív-kvantitatív skálája. Forrás: saját szerkesztés ISO/IEC 27005 [71] alapján

	Kvalitatív skála szervezetekre	**Kvantitatív skála állampolgárokra**	
Következmény	**Leírás**	**Minimum értékhatár**	**Maximum értékhatár**
Katasztrofális	A szervezet keretein túlmutató, egész szektorra kiterjedő	4 000 000 Ft	50 000 000 Ft
Kritikus	A szervezet számára végzetes	400 000 Ft	3 999 999 Ft
Súlyos	A szervezet számára súlyos következmények	150 000 Ft	399 999 Ft
Jelentős	A szervezet számára jelentős	5 000 Ft	149 999 Ft
Mérsékelt	A szervezet számára elhanyagolható		4 999 Ft

A leírás oszlopban látható a kvalitatív skála, mely az ország és az infrastruktúra fejlesztő/üzemeltető esetében alkalmazandó. A minimum értékhatár és a maximum értékhatár pedig a kvantitatív skála, mely az állampolgárok vonatkozásában használatos.

2.2.2.3 Valószínűségek

Az alábbi táblázat (7. Táblázat) az ISO/IEC 27005 szabványon alapuló kvalitatív-kvantitatív valószínűségi skálát tartalmazza.

7. Táblázat Valószínűség kombinált kvalitatív-kvantitatív skálája. Forrás: saját szerkesztés ISO/IEC 27005 [71]

	Kvalitatív skála	**Kvantitatív skála**
Valószínűség	**Leírás**	**Előfordulási gyakoriság**
Majdnem biztos	A kockázati forgatókönyv bekövetkezésének valószínűsége nagyon magas.	Hetente többször
Nagyon valószínű	A kockázati forgatókönyv bekövetkezésének valószínűsége magas.	Havonta egyszer
Valószínű	A kockázati forgatókönyv bekövetkezésének valószínűsége szignifikáns.	Évente egyszer
Kissé valószínűtlen	A kockázati forgatókönyv bekövetkezésének valószínűsége alacsony.	Tízévente egyszer
Valószínűtlen	A kockázati forgatókönyv bekövetkezésének valószínűsége nagyon alacsony.	Évszázadonként egyszer

2.2.2.4 Kockázati szint mátrix

A kockázati szinteket a korábban ismertetett színkódokkal az alábbi táblázat (8. Táblázat) tartalmazza. A színkódoknak köszönhetően a különböző osztályok vizuálisan jól el vannak különítve, hogy segítsék a döntést, hogy egy kockázatot kezelni kell, vagy elfogadható-e kezelés nélkül.

8. Táblázat Kockázati szint mátrix. Forrás: saját szerkesztés ISO/IEC 27005 27005 [71]

Valószínűség	**Következmény**				
	Katasztrofális	**Kritikus**	**Súlyos**	**Jelentős**	**Mérsékelt**
Majdnem biztos	Nagyon magas	Nagyon magas	Magas	Magas	Közepes
Nagyon valószínű	Nagyon magas	Magas	Magas	Közepes	Alacsony
Valószínű	Magas	Magas	Közepes	Alacsony	Alacsony
Kissé valószínűtlen	Közepes	Közepes	Alacsony	Alacsony	Nagyon alacsony
Valószínűtlen	Alacsony	Alacsony	Alacsony	Nagyon Alacsony	Nagyon alacsony

2.2.3 Potenciális támadók

Mint azt korábban említettem a stratégiai szcenáriók meghatározásához több dologra is szükség van: a kockázati források, a motivációk és az elérendő célok meghatározása. Jelen kockázatértékeléshez a szabvány „A” mellékletében szereplő példa felsorolásokat vettem alapul.

Az eSzemélyi igazolvány infrastruktúrája kiberbűnözők, de akár ellenérdekelt országok titkosszolgálatai számára is célpont lehet. Kiemelten védendők az eSzemélyi

igazolvánnyal létrehozott elektronikus aláírások és az azokhoz esetlegesen hozzácsatolt, az SZTSZ szolgáltatáson keresztül létrehozott attribútum tanúsítványok is [60].

A szabvány [71] a hagyományos vagyontárgy alapú megközelítés esetében ugyan megkülönbözteti a szándékos, a véletlen és a környezeti fenyegetéseket, mint kockázatforrásokat, de az esemény alapú megközelítés példáiban csak szándékosságot feltételező kockázatforrásokat említ.

Alapvetően támadókat sorol fel, akik valamilyen feltett szándékkal indítanak támadást egy rendszer ellen, de a listában nem szerepelteti például a képzetlen felhasználót, aki bár nem szándékosan, de ugyancsak forrása lehet bizonyos kockázatoknak. A kockázatforrások közé felvettem a „Képzetlen felhasználó” elemet. Lásd a táblázatot a 2. számú függelékben.

Más oldalról megközelítve inkább sérülékenységként kellene értelmezni az óvatlan felhasználók által megnyitott információbiztonsági réseket. A stratégiai szcenáriók szintjén más mód azonban nem áll rendelkezésre ezen kockázatok megjelenítésére, így az egységes kezelése érdekében szükséges e kiegészítést megtenni.

A magyar eSzemélyi igazolvány és háttérinfrastruktúrája esetében a közvetlenül ezeket célzó támadók jelentős tudással és erőforrással kell, hogy rendelkezzenek a sikeres támadások végrehajtásához. Az ilyen volumenű támadásokhoz az ellenérdekelt államok, esetleg hacker csoportok rendelkezhetnek megfelelő erőforrásokkal. Az infrastruktúrára különösen nagy veszélyt jelenthetnek a bosszúálló forrásból származó kockázatok is.

Az egyes állampolgárok személyes adatainak megszerzésére, identitásának ellopására irányuló törekvések a social engineering módszereivel már akár szervezett bűnözői csoportoktól is eredhetnek.

A terrorszervezetek esetében a stratégiai szintű forgatókönyvek nagyon hasonlítanak az államhoz köthető forrásból származó forgatókönyvekhez, a jelentős különbség – ahogyan a szabvány [71] is írja – a támadások összetettségében van és nagyobb hangsúllyal szerepelnek a rombolást célzó támadások. A következmények elszenvedése jellemzően nagyobbrészt az államra esne. A szcenáriók bemutatása egyrészt redundáns lenne, másrészt nem tartom valószínűnek, hogy terrorszervezetek támadást indítanának az eSzemélyi infrastruktúra ellen, ezért ezeket nem ismertetem.

Az ideológiai aktivisták esetében a támadások rombolásra, zavar okozásra és különféle ideológiák terjesztése irányulnak az elkövető kilétének leplezésével [71]. A szcenáriók a

részhalmazát képezik az előbbi csoportnak, így a tartalmi korlátok miatt ezeket sem mutatom be.

Az amatőr támadókat figyelembe véve a kihívásból vagy szórakozás céljából végrehajtott támadások jöhetnek szóba. Alapszintű támadások végrehajtására képesek, motivációjuk kevésbé komoly jellegénél fogva általában a támadások következménye is kevésbé súlyos [71], így az ebből a forrásból eredő kockázatok részletes bemutatását mellőzöm.

A patológiás támadók esetében is jellemzően a működés megakadályozására vonatkozó támadások a hangsúlyosabbak, de néha megjelenhetnek a haszonszerzésre irányulók is [71]. Ugyancsak jelentős átfedés mutatkozik az államhoz köthető forrásból származó esetekkel, így ezeket a szcenáriókat sem fogom részletezni.

A 2. számú függelékben zöld háttérszínnel kiemelten jelölöm azokat a kockázati forrásokat, melyekkel a fentiek alapján a továbbiakban foglalkozom: államhoz kötődő, szervezett bűnözés, bosszúálló, képzetlen felhasználó. Tartalmi korlátok miatt tehát nem ismertetem a következő kockázatforrásokból eredő forgatókönyveket: terrorista. ideológiai aktivista, amatőr, patológiás támadó.

2.2.3.1 Lehetséges motivációk

Az alábbi táblázat (9. Táblázat) ugyancsak a szabvány alapján készült. Felsorolja a támadók lehetséges motivációit. Alapvetően ez a táblázat sem fejezi ki az óvatlan felhasználó motivációit, ezért ezt a listát is kiegészítettem egy tétellel: „Jóhiszemű használat”. A kockázatforrások esetében tett kiegészítésem következetes végigviteléhez ez is feltétlenül szükséges.

9. Táblázat Motivációk listája. Forrás: saját szerkesztés ISO/IEC 27005 [71] alapján

Megnevezés	Leírás
Hódítás	Erőforrások vagy gazdasági piacok hosszú távú megszerzése, politikai hatalom megszerzése vagy értékek érvényesítése.
Megszerzés	Határozottan támadó megközelítés, erőforrások vagy előnyök megszerzése által vezérelve.
Megelőzés	Támadó viselkedés egy harmadik fél tevékenységének korlátozására.
Fenntartás	Ideológiai, politikai, gazdasági vagy társadalmi helyzet fenntartására irányuló erőfeszítések.
Védekezés	Szigorúan védekező, vagy kifejezetten fenyegető attitűd (például megfélemlítés) felvétele egy egyértelműen megjelölt ellenfél agresszív viselkedésének megelőzése, vagy cselekményének megakadályozása, lassítása stb. érdekében.
Túlélés	Egy entitás mindenáron történő védelme, ami rendkívül agresszív cselekedetekhez vezethet.
Jóhiszemű használat	Egy informatikai rendszer jóhiszemű használata a rendeltetés szerinti cél elérése érdekében, ám nem biztonságtudatos használata.

2.2.3.2 Elérendő célok

Az elérendő célok listáját (3. számú függelék) is bővítettem egy elemmel a szabvány által biztosított példa táblázathoz képest, ez pedig nem más, mint a „Jóhiszemű felhasználás”, amely azt hivatott kifejezni, hogy a felhasználó a rendszert annak szándék szerinti célja elérésre használja.

2.2.4 Következmények

Az eID megoldásokkal kapcsolatosan felmerülő kockázatok azonosítása, kiértékelése és azok esetleges hatásának felmérése kulcsfontosságú, hiszen a működési problémák, a kompromittálódás, vagy a visszaélés súlyos anyagi károkat okozhat az állam, a társadalom, illetve az állampolgárok számára. A kockázatokat az érdekelt felekre gyakorolt hatásának vizsgálatával együtt kell azonosítani [58, 71].

2.2.4.1 Érdekelt felek

Egy eID rendszer kialakításába és megvalósításába be kell vonni az összes érintett felet, ami biztosítja, hogy a rendszer fejlesztése során az érdekelt felek összes felmerülő aggálya látótérbe kerüljön. Az érintettek bevonása segíthet azonosítani továbbá a fokozott figyelmet igénylő magas kockázatú területeket, és hatékonyabb kockázatkezelési stratégiák kidolgozását teszi lehetővé [59].

Alapvetően három érdekelt fél azonosítható: a kormányzat, az állampolgárok, valamint az eID megoldásra támaszkodó gazdasági szereplők. A kormányzat, mint a nyilvántartások vezetéséért, az eID-k kiadásáért és a különféle eKormányzati szolgáltatásokért felelős ügynökségek összessége értendő [58]. Ide sorolom az eID megoldás fejlesztésében és üzemeltetésében résztvevő alvállalkozókat.

Az állampolgárok csoportja az eID megoldások végfelhasználói, akik az eID kártyák használatával igénybe veszik a különféle eKormányzati szolgáltatásokat, az eAzonosítás vagy az eAláírás funkciót. További érdekelt félként a teljes társadalmi rendszer is megemlíthető [58].

A megoldásra támaszkodó gazdasági szereplők az eSzemélyi igazolvány esetében jelen állapotban még nem értelmezhető, de ebbe a kategóriába fognak esni a piaci szolgáltatásokat (például online bankszámlanyitás, SIM kártya regisztráció) az eAzonosítással kiegészítő szolgáltatók. Az eAzonosítás elfogadása idővel kötelező lesz a Digitális Állampolgárság Program keretében [58, 56].

Az egyes hatásokra az Edu, Hooper, Maple és Crowcroft [58] által javasolt csoportosítást használom: hírnévre gyakorolt, gazdasági, emberi jogi, társadalmi, politikai, működési, fizikai, adatvédelmi és pszichológiai hatások. A következőkben pedig ezeket alkalmazom az eSzemélyi igazolvány vonatkozásában.

2.2.4.2 Kormányzatra gyakorolt hatások

A felmerülő kockázatok a kormányzat hírnévre is hatással lehetnek: az eSzemélyi rendszerbe vetett bizalom nagyban befolyásolja a megoldás elterjedtségét. A bizalom hiánya az eKormányzati szolgáltatások mellőzésére sarkallhatja az állampolgárokat. A kormányzat hírneve jelentős mértékben sérülhet egy eSzemélyi infrastruktúra leállás, vagy személyes adatok kiszivárgása esetén.

A gazdasági hatások vonatkozásában Edu, Hooper, Maple és Crowcroft [58] kiemeli, hogy az Amerikai Egyesült Államokban 2011-ben mintegy 3,3 millió USD munkanélküli járadék került kifizetésre csalók részére. Jól láthatóan közvetlen és közvetett gazdasági/pénzügyi hatásai is lehetnek a kockázatoknak. A csalók által okozott károkon túl felmerülhetnek a működési hibák/sérülékenységek feltárásából és javításából eredő költségek, vagy a szolgáltatás kiesés okozta elmaradt bevételek is.

A kormányzat eKormányzati szolgáltatásokat használ fel az átláthatóság, a méltányosság és a jól irányított szolgáltatások megteremtése érdekében, és minden állampolgárnak jogot biztosít az egyenlő bánásmódra az eKormányzati szolgáltatásokhoz való egyenlő hozzáférési lehetőségen keresztül is. A rendszerből valamilyen módon kizárt felhasználókra gyakorolt hatásokat vizsgálni kell [58].

Edu, Hooper, Maple és Crowcroft [58] szerint egy eID rendszer hatékonyságának és eredményességének mérése is fontos. A kormányzat az állampolgárok szemszögéből szolgáltatónak tekinthető, így végső célja az általános társadalmi jólét javítása, valamint a polgárok igényeinek kielégítése kell, hogy legyen.

Az eSzemélyi infrastruktúrát érintő incidenseknek jelentős társadalmi károsító vagy akadályozó hatása lehet a kritikus infrastruktúra-szektorra, befolyásolva az állampolgárok életvitelét és a társadalomban való interakcióját, szélsőséges esetben akár nemzetbiztonsági kockázatot is jelenthet.

Működési hatások alatt azok a hatások értendők, melyek az eSzemélyi infrastruktúra és a különféle eKormányzati szolgáltatások működőképességét közvetve vagy közvetlenül érintik.

A fizikai hatások a fizikai értelemben vett kormányzati tulajdon, vagyontárgyak és erőforrások megrongálódására vagy megsemmisülésére vonatkoznak [58]. Ideértendő az eSzemélyi infrastruktúra egésze, a különböző, az üzemeltetéshez kapcsolódó épületek, az infrastruktúra elemek, a támogató személyzet és a különféle felszerelések.

2.2.4.3 Az állampolgárokra gyakorolt hatások

Az állampolgárokra az eID rendszerek átláthatósága, használhatósága, hozzáférhetősége, elérhetősége, adatvédelme és biztonsága van a legnagyobb hatással [58]. Nincs ez másként a magyar eSzemélyi igazolvány esetében sem.

Adatvédelemi hatások tekintetében az egyik legfontosabb vagyontárgy az eSzemélyi infrastruktúrában és az eSzemélyi igazolvány tárolóelemén tárolt személyes adat. Ezen adatok kompromittálódásának hatásai egyénenként különbözhetnek. Mivel azokat csak a végfelhasználók érzik közvetlenül, így azok felmérése kívülállóként igen nehézkes [58].

Előfordulhat, hogy egy támadás az érintett állampolgárokat alapvető jogaikban korlátozzák [58]. A magyar rendszer vonatkozásában ilyen lehet például az EESZT rendszerből történő egészségügyi adatok kiszivárgása sértve ezáltal az önrendelkezéshez való jogot.

A kompromittálódott eID rendszer akadályokat állíthat a végfelhasználók elé az eKormányzati szolgáltatásokhoz való hozzáférések tekintetében, ezáltal gátolva a társadalmi rendszer hatékony működését [58]. Az eRecept példáját emelném ki, melynek működésképtelenné tétele az egész társadalomra hatással lenne.

Egy támadásnak pszichológiai hatásai is lehetnek, melyek lefutása adott esetben hosszabb lehet, mint a pénzügyi/gazdasági hatásoké. Kényelmetlenséget, frusztrációt okozhat az is, ha egy állampolgár hosszú távon, többszöri próbálkozásra sem fér hozzá egy eKormányzati szolgáltatáshoz, továbbá a kiberbűnözők más nevében elkövetett bűncselekményei következményeként előfordulhat, hogy az identitás lopás áldozatát vonják felelősségre a tényleges elkövető helyett [58].

Ezen túlmenően a támadást elszenvedett állampolgárok számára komoly anyagi veszteséget okozhatnak a kiberűnözők által a nevükben, az identitásuk ellopásával végrehajtott pénzügyi tranzakciók [58].

2.2.4.4 Gazdasági szereplőkre gyakorolt hatások

Az eSzemélyi infrastruktúrára építő gazdasági szereplőkre gyakorolt hatások jelenleg még ugyan nem értelmezhetők Magyarországon, de a Nemzeti Digitális Állampolgárság Program kiteljesedésével azzá válnak majd.

A gazdasági társaságok kizárólag egy robusztus és megbízható eID infrastruktúra hasznait élvezhetik, létfontosságú számukra a felhasználók hiteltérdemlő azonosítása a csalások kizárása érdekében. A rendszer kompromittálódása által okozott hatások bírságok, kompenzációs kifizetések és elmaradt haszon (akár veszteség) formájában jelentkezhetnek [58].

A gazdasági szereplő működését és hatékonyságát negatívan befolyásolhatja az igénybe vett eID infrastruktúra kiesése. Ennek következménye lehet a hírnévre gyakorolt hatás. A gazdasági társaság hírnevén is csorbát ejthet ugyanis egy eID infrastruktúra kiesés, ezáltal az ügyfelek a gazdasági szereplőbe vetett bizalma is sérülhet [58].

Az eSzemélyi infrastruktúra szolgáltatás kiesése esetén az állampolgárok szemszögéből az lenne érzékelhető, hogy nem tudják igénybe venni a piaci szereplő szolgáltatásait az eAzonosítás használatával. Megjegyzem, hogy ez nem csak a piaci szereplő hibájából történhet, hanem a kormányzatéból is.

A gazdasági társaságok kockázatai a teljes társadalmi rendszerre is hatással lehetnek, például munkahelyek kerülhetnek veszélybe, ellátási láncok sérülhetnek, szolgáltatáskiesések következhetnek be [58].

2.2.5 Stratégiai kockázati szcenáriók

Amint az látszani fog az azonosított kockázatoknál nem kizárólag az eSzemélyi igazolvány jelenleg is működő használati eseteit vettem figyelembe. Igyekeztem az Európai Digitális Identitás (1.1.2) és a Nemzeti Digitális Állampolgárság Program (1.9) által előrevetített újabb funkcionalitások kockázatait is felmérni, hiszen, ahogyan azt korábban is állítottam, a megfelelő kockázatelemzés segíthet új használati esetek biztonságos kifejlesztésében, bevezetésében.

Célszerű „fentről lefelé” haladva a stratégiai szcenáriók meghatározásával elkezdeni a kockázatok azonosítását. Ezt követően kerül sor azok alábontására az operatív szcenáriók meghatározásával és besorolásával.

A korábban már említett munkákban (Kübler [57], Edu, Hooper, Maple és Crowcroft [59], Szádeczky [61]) alkalmazott csoportosítási módszereket összegezve és az ISO/IEC

27005 stratégiai-operatív megközelítései alapján újrarendezve az alábbiak szerint osztályozhatók az eSzemélyi igazolvány kapcsán felmerülő stratégiai kockázati forgatókönyvek.

Az első és legfontosabb az *adatvédelmi kockázatok* kategóriája. Az emberek hajlamosak bizalmatlanul viszonyulni a szervezetekkel szemben, félve attól, hogy azok személyes adataikat saját céljaikra is felhasználják. Az eID rendszerek tervezése és kivitelezése során kiemelten fontos a beépített adatvédelem (privacy-by-design) alapelv [57]. Ezen túlmenően a már korábban is említett szoftverminőség központú nemzetközi szabványok alkalmazás is erősen megfontolandó.

Az eID rendszerek kiküszöbölik ugyan a papír alapú rendszerek bizonyos hátrányait – biztonsági funkcióik által –, mégis az adatok sérülésének, hibájának és elvesztésének komoly kockázatát is magukban hordozhatják. Bizonyos sérülékenységek lehetővé tehetik például az adatok engedély nélkül bevitelét, módosíthatóságát vagy akár törlését is [59].

Az eID rendszerek jelentős mennyiségű személyes adatot tartalmaznak beleértve az állampolgárok biometrikus jellemzőit (fénykép, ujjnyomat) is. Egy, az eID adatbázisok elleni sikeres támadás tömeges mértékű identitáslopáshoz vezethet [59].

A felhasználó hozzájárulása nélkül történő profilalkotás, megfigyelés, információgyűjtés és adatmegosztás olyan lehetséges visszaélések, melyek valószínűsége fokozódik megfelelő adatvédelmi szabályozás hiányában [59].

A *megszemélyesítési kockázatok* bár nem érintik a rendszer egészét, de az azokat elszenvedő állampolgárok számára igen súlyos következményekkel is járhatnak [59]. Személyes adataikhoz való jogosulatlan hozzáférés által akár anyagi káruk is keletkezhet.

Ennek egyik alesete az identitáslopás, amikor létező, érvényes identitás megszerzése a cél. A másik aleset pedig a szintetikus identitások létrehozása, mely előbbitől eltérően hamis identitás létrehozását feltételezi a támadások végrehajtásához [59].

Informatikai biztonsági kockázatok is felmerülhetnek az eID infrastruktúrák üzemeltetése során, például a centralizált adatbázisok esetében, melyek egyetlen expozíciós (és meghibásodási) pontként a potenciális támadók célpontjai lehetnek. Ezt kiküszöbölendő az adatok elosztott tárolását érdemes előnyben részesíteni [57].

A terjedelmi korlátok sajnos nem teszik lehetővé, hogy az összes azonosított forgatókönyvet részletesen kifejtsem, de néhányat ismertetni fogok a továbbiakban.

Az átláthatóság növelése érdekében a különböző kockázati forrásokból eredő forgatókönyveket külön táblázatokba csoportosítottam. Elsőként az államhoz köthető stratégiai szcenáriók ismertetése következik.

2.2.5.1 Államhoz köthető stratégiai szcenáriók

Az államhoz köthető támadások esetében – ahogyan a szabvány is leírja – jelentős támadási potenciált feltételeztem. Jellemzően a titkosszolgálatok rendelkeznek erőforrásokkal ilyen kiterjedésű és intenzitású támadások kivitelezéséhez. Az állami szintű támadások következménye összhangban azok intenzitásával többnyire a súlyosabb tartományban mozog és inkább az államot és a társadalmat érinti, semmint az állampolgárokat közvetlenül, ahogyan azt a lenti táblázatban (10. Táblázat) is olvashatjuk.

Az első sorban a kockázat forrás szerepel, a második sor a forgatókönyvek fejléce (Cél, Kategória, Stratégiai szcenárió, Érdekelt felek, Hatás, Következmény). A többi kockázati forrás esetében már csak néhány szcenáriót fogok bemutatni.

Az „Elektronikus aláírások hitelesnek látszó meghamisítása titkosszolgálati tevékenység leplezése céljából” forgatókönyv szerint a támadók képesek meghamisítani elektronikusan aláírt dokumentumokat. Érvényesnek látszó szerződéseket köthetnének ártatlan állampolgárok nevében. Egy ilyen támadásban a kormányzat és a megszemélyesítést elszenvedett állampolgárok érintettek.

„Állampolgár identitásának ellopása titkosszolgálati tevékenység leplezése céljából” forgatókönyv esetében egy ellenérdekelt titkosszolgálat a felderítési tevékenységének leplezése érdekében, állampolgárok nevében történő bankszámla nyitást, SIM kártya vásárlást valósíthatna meg.

Mint az alábbi táblázatból világosan kitűnik, az államhoz köthető forrásból származó kockázatok jellemzően valamilyen titkosszolgálati tevékenységgel (például kémkedés, befolyásolás) összefüggésben merülnek fel.

A specializált csapat forrásból származó kockázatok esetében ugyanazon stratégiai forgatókönyveket azonosítottam, mint az államhoz kötődők esetén, így azokat a redundancia elkerülése érdekében nem ismertetem.

10. Táblázat Államhoz köthető kockázati forrásból származó stratégiai kockázati szcenáriók, Forrás: saját szerkesztés

Forrása	Államhoz köthető				
Cél	**Kategória**	**Stratégiai szcenárió**	**Érdekelt felek**	**Hatás**	**Következmény**
Kémkedés	Megszemélyesítési	Politikai vezető/stratégiai fontosságú cég vezetője identitásának ellopása	Kormányzat	hírnév, politikai, gazdasági, adatvédelmi	Katasztrofális
	Megszemélyesítési	Állampolgár identitásának ellopása titkosszolgálati tevékenység leplezése céljából	Kormányzat, Állampolgár	hírnév, gazdasági, pszichológiai, adatvédelmi	Kritikus
	Megszemélyesítési	Hamis identitás létrehozás titkosszolgálati tevékenység leplezése céljából	Kormányzat	hírnév, gazdasági	Kritikus
	Adatvédelmi	Tömeges információszerzés az eSzemélyi infrastruktúrából	Társadalom	hírnév, gazdasági, adatvédelmi	Katasztrofális
	Adatvédelmi	Rejtjeles csatornák észrevétlen monitorozása felderítés céljából	Kormányzat, Gazdasági szereplők	gazdasági, adatvédelmi	Katasztrofális
	Megszemélyesítési	Elektronikus aláírások hitelesnek látszó meghamisítása titkosszolgálati tevékenység leplezése céljából	Kormányzat, állampolgár	hírnév, gazdasági, adatvédelmi, pszichológiai	Katasztrofális
Működés megakadályozása	IT biztonsági	Országgyűlési/önkormányzati választások, népszavazás megzavarása	Kormányzat, társadalom	hírnév, gazdasági, működési	Katasztrofális
	IT biztonsági	eKormányzati szolgáltatások működésének megzavarása	Kormányzat, társadalom, gazdasági szereplők	hírnév, gazdasági, működési	Kritikus
	IT biztonsági	Létfontosságú rendszerek működésének megzavarása az eSzemélyi infrastruktúra működésképtelenné tételével	Kormányzat, társadalom, gazdasági szereplők	hírnév, gazdasági, működési	Katasztrofális
Befolyásolás	Megszemélyesítési	Véleményvezér identitásának ellopása ideológia/fake news terjesztése céljából	Társadalom	hírnév, gazdasági, adatvédelmi, pszichológiai	Súlyos
	Megszemélyesítési	Hamis identitás létrehozása ideológia/fake news terjesztése céljából	Társadalom	hírnév, gazdasági	Jelentős
Stratégiai előpozícionálás	Megszemélyesítési	Politikai vezető/stratégiai fontosságú cég vezetője identitásának ellopása	Kormányzat	hírnév, gazdasági, adatvédelmi, pszichológiai	Katasztrofális
	Megszemélyesítési	Hamis identitás létrehozása ideológia/fake news terjesztése céljából	Társadalom	hírnév, gazdasági	Jelentős
	Megszemélyesítési	Iskolai végzettséget igazoló irat hamisítása beépülés elősegítésére	Kormányzat, társadalom	hírnév, gazdasági	Jelentős
	Megszemélyesítési	Útiokmány hamisítása beépülés elősegítésére	Kormányzat, társadalom	hírnév, gazdasági	Kritikus

A továbbiakban terjedelmi korlátok és tördelési megfontolások miatt csak legfeljebb egy-egy stratégiai szcenáriót fogok részletesen bemutatni.

2.2.5.2 Szervezett bűnözéshez kötődő stratégiai szcenáriók

Ami a szervezett bűnözői csoportokat illeti, már egészen más képet mutat a stratégiai szcenáriók listája, legnagyobb hangsúly a haszonszerzésen van és a célpontok már inkább az állampolgárok. Bizonyos rosszindulatú tevékenységek a szervezett bűnözői csoport befolyásának, hatásterének növelésére, általános értelemben vett terjeszkedésére is irányulhatnak. A teljesség igénye nélkül az alábbi forgatókönyvek merülhetnek fel:

- Állampolgár kárára elkövetett csalás
- Állampolgár identitásával illetéktelenül végrehajtott tranzakció (ingatlan, gépjármű, SIM kártya stb.)
- Hamis recept kiváltása illegális gyógyszerkereskedelem miatt
- Illegális tevékenységet végző hálózat kiépítése (bankszámla nyitás, SIM kártya vásárlás stb.)
- Iskolai végzettséget igazoló irat hamisítása beépülés elősegítésére
- Útiokmány hamisítása beépülés elősegítésére
- eSzemélyi igazolvány eltulajdonítása

Ezek közül az alábbi táblázatban (11. Táblázat) részletezett forgatókönyvet emelném ki, az „Állampolgár kárára elkövetett csalás” megnevezésűt, mely alapvetően az állampolgárok vagyonának megszerzésére irányuló támadásokat foglalja magában.

11. Táblázat Szervezett bűnözéshez köthető kockázati forrásból származó, Állampolgár kárára elkövetett csalás stratégiai kockázati szcenárió, Forrás: saját szerkesztés

Kockázat forrása	Szervezett bűnözés
Szcenárió megnevezése	Állampolgár kárára elkövetett csalás
Cél	Haszonszerzés
Kategória	Adatvédelmi
Érdekelt felek	Állampolgár
Hatás	Gazdasági, adatvédelmi
Következmény	Katasztrofális

2.2.5.3 Bosszúállókhoz köthető stratégiai szcenáriók

A bosszúállók kategóriájába eső lehetséges támadók komoly problémákat okozhatnak az eSzemélyi infrastruktúra üzemeltetői számára. Általában csalódottak, megkeseredettek, ebből eredően motivációjuk a károkozás például a korábbi munkahelyüknek. Gyakran rendelkeznek kulcsfontosságú információkkal a rendszerekről, melyekkel korábban

dolgoztak ezért azokban jelentős károkat tudnak okozni. Céljuk általában a működés megzavarása [71].

Jelen témakör szempontjából az eSzemélyi, a Nemzeti Digitális Állampolgárság Program informatikai fejlesztői, üzemeltetői állományába, a Kormányablak ügyintézői állományába tartozó munkavállalók érdemlik a legnagyobb figyelmet, hiszen olyan ismeretek birtokában lehetnek, olyan rendszerekhez rendelkezhetnek hozzáféréssel, melyek az eSzemélyi infrastruktúra biztonsága szempontjából kiemelten fontosak.

Az alábbi szcenáriók merülnek fel:

- Országgyűlési/önkormányzati választások, népszavazás megzavarása
- eKormányzati szolgáltatások működésének megzavarása imázsrombolás céljából
- Létfontosságú rendszerek működésének megzavarása az eSzemélyi infrastruktúra működésképtelenné tételével

2.2.5.4 Képzetlen felhasználókhoz köthető stratégiai szcenáriók

Végül az általam az egységes kezelhetőség érdekében bevezetett „Képzetlen felhasználók” csoportja következik. Motivációjukat tekintve alapvetően a rendszerek rendeltetésszerű használatára törekszenek, de sajnálatos módon felelőtlenek vagy képzetlenek az információbiztonság területén, ezért tevékenységük – ugyan nyilvánvalóan nem minősül támadásnak, de mégis – kockázatok megjelenéséhez vezethet.

Olyan forgatókönyvekben érintettek, mint

- Az eSzemélyiM mobil alkalmazás használata nyílt WIFI kapcsolaton keresztül
- PIN és/vagy PUK kódok együtt tárolása az eSzemélyi igazolvánnyal
- Az eSzemélyi szolgáltatás használata a PIN és/vagy PUK kód nyilvánosságra hozásával
- Az eSzemélyi igazolvány elvesztése

Kiemelném a „PIN és/vagy PUK kódok együtt tárolása az eSzemélyi igazolvánnyal” forgatókönyvet, mert ez sajnálatos módon jelen van a mindennapokban. Az eszemelyi.hu [78] információs portál részletesen leírja az igénylés folyamatát, az elektronikus funkciók aktiválásának menetét.

12. Táblázat Képzetlen felhasználóhoz kötődő kockázati forrásból származó, PIN és/vagy PUK kódok együtt tárolása az eSzemélyi igazolvánnyal stratégiai kockázati szcenárió, Forrás: saját szerkesztés

Kockázat forrása	Képzetlen felhasználó
Szcenárió megnevezése	PIN és/vagy PUK kódok együtt tárolása az eSzemélyi igazolvánnyal
Cél	Rendeltetésszerű felhasználás
Kategória	Adatvédelmi
Érdekelt felek	Állampolgár
Hatás	Gazdasági, adatvédelmi
Következmény	Katasztrofális

Az igénylés során az igénylő megkapja az elektronikus azonosítás aktiválásához szükséges kódkártyát tartalmazó zöld, és az elektronikus aláírás funkció (feltéve, hogy igényelte) aktiválásához szükséges kódkártyát tartalmazó kék borítékot. A kódkártyákon szerepel egy-egy aktiváló PIN kód. Az eSzemélyi igazolványt alapesetben csak 8 nappal később veheti át. Az aktiválás elvégezhető bárhol Internetkapcsolat, a megfelelő szoftverek és hardverek alkalmazása mellett, akár otthon is [78].

Az információs portál, és a Kormányablak dolgozók is – ezt a korábban is említett tapasztalataim alapján állítom – felhívják a figyelmet arra, hogy a Kormányablakban a helyszínen is lehetséges az aktiválás az ügyintézők segítő útmutatásával [78]. Ez egy kényelmi szolgáltatás azok számára, akik nincsenek az aktiváláshoz szükséges tudás birtokában, de sajnálatos módon azt feltételezi, hogy a kódkártyákat az igénylő vigye magával a Kormányablakba, így az okmány és a kódkártyák együtt tárolódnak a Kormányablakból távozást követően. Elvesztés esetén teljes kontrolt szerezhet egy támadó az okmány elektronikus funkciói felett.

Egy további személyes tapasztalatot az eRecept funkció alkalmazása során szereztem, mely az „Az eSzemélyi szolgáltatás használata a PIN és vagy PUK kód nyilvánosságra hozásával” forgatókönyvhöz kapcsolódik. Az eSzemélyi igazolványomról szerettem volna kiolvastatni a TAJ számomat a „felhőben” tárolt recept kiváltáshoz, felmerült azonban egy sajnálatos körülmény, miszerint a kártyaolvasó terminál kábele túlságosan rövid volt, így nem tudtam beírni a PIN kódom. A gyógyszerész – teljes jóindulattal – felajánlotta, hogy diktáljam a kódomat, majd ő beírja. Nyilván – biztonságtudatos lévén – nem egyeztem bele, de más, kevésbé hozzáértő eSzemélyi használó esetén bekövetkezhet az érzékeny információk kiszivárgása ily módon.

2.2.6 Vagyontárgyak

A stratégiai szcenáriók alábontásához az operatív szcenáriók azonosítása szükségeltetik, melynek előfeltétele, hogy tisztában legyünk a védendő vagyontárgyakkal. A 2. számú

függelék bemutatja az eSzemélyi kapcsán beazonosított vagyontárgyakat zöld háttérszínnel kiemelve az elsődleges/üzleti kategóriába esőket.

2.2.7 Operatív kockázati szcenáriók

2.2.7.1 Hardveres és infrastrukturális kockázati szcenáriók

Ebbe a kategóriába esnek azok a kockázati forgatókönyvek, melyek a rendszer különböző hardverelemeinek sérülékenységeit érintik. Ideértendők úgy a kliens, mint a szerver oldalon felmerülő kockázatok, valamint a teljes infrastruktúrát érintők is.

A hardverek kockázatait tekintve a véletlen és a szándékos backdoor-ok beépítése, vagy olyan rejtett funkciók implementálása is felmerül, melyek lehetővé teszik akár ellenérdekű országok számára a hardvereszközön zajló kommunikáció észrevételen megfigyelését/megváltoztatását [60]. A számítógépek BIOS/UEFI programja és a beépített hardvereszközök vezérlőprogramjai is tartalmazhatnak sérülékenységeket így ezek frissítése is létfontosságú.

Speciális, irányított antennával akár több méterről is megvalósítható távoli leolvasás a rádiós interfészen keresztül működő kártyák esetében. A lehetséges támadások magukban foglalják a kártyán lévő adatok megismerését, vagy akár a kártya földrajzi mozgásának nyomon követését is [60].

2.2.7.2 Adatátviteli kockázati szcenáriók

Az adatátvitel tekintetében a rádiófrekvenciás kommunikációs megoldások közül a Bluetooth és az NFC kommunikációt kiemelendő. Meglátásom szerint a Bluetooth eszközök sérülékenységei kevésbé relevánsak az eSzemélyi igazolvány esetében, hiszen Bluetooth kapcsolat nem szükségeltetik az eSzemélyiM applikáció használatához. Az NFC valóban egy kritikus elem, hiszen előfeltétele a szoftver kártyaolvasóként való használatának. Kihangsúlyoznám továbbá az eSzemélyiM alkalmazást és a PC-t összekötő közös WIFI hálózat (lásd 1.4. szakasz) biztonságának fontosságát [60].

A nyílt kommunikációs hálózatok kérdésköre is itt merül fel, ezen hálózatok ugyanis hálózatok további kockázati tényezőket rejtenek magukban, lehetővé teszik a kiberbűnözők számára, hogy kihasználják a valódi eID-kkal hitelesített felhasználói munkameneteket [59].

Ehhez nagyon hasonló eset, amikor egy valós eID hitelesítő adatai kompromittálódnak, és a támadó azok és az eID felhasználásával a valódi jogosult nevében hitelesíti magát valamely szolgáltatásban [59].

2.2.7.3 Szoftveres kockázati szcenáriók

Az operációs rendszerek esetében a zero-day sérülékenységek kizárására irányuló tesztelés kiemelten fontos. Felhasználói oldalról az operációs rendszerekhez a gyártó által biztosított frissítéseket (biztonsági és/vagy funkcionális) telepítése kulcsfontosságú [60]. Ezeken túlmenően azonban az operációs rendszerek biztonságát befolyásoló rendszerparaméterek jelentőségét is kihangsúlyoznám, ugyanis ezek nem megfelelő beállítása is rejthet kockázatokat.

Ide sorolandók a különféle maleware-ek, így a zsarolóvírusok, az eKözigazgatási infrastruktúra megbénítására, a végfelhasználó adataiknak illetéktelen megszerzésére irányuló támadó kódok is. Az okmányhamisítás egy új módja is kialakulhat lehetővé téve akár ellenérdekű országok titkosszolgálatainak számára a digitális fedőokmányok létrehozását [60]. Kiemelten fontos vírusirtó szoftver telepítése és naprakészen tartása.

A szoftverrendszerek esetében együttműködési kockázatok is felmerülhetnek. Az eIDAS által definiált eID séma esetében ez nem merül fel, hiszen maga az eIDAS biztosítja a tagállamok nemzeti elektronikus azonosítóinak alkalmazhatóságát az egész EU területén. A nemzeti eID megoldásoknak együtt kell működniük úgy az eKormányzat, mint a privát szektor szolgáltatásaival [57, 59]. Ilyen jellegű kockázatok felmerülhetnek azonban az eSzemélyi igazolvány kapcsán, amikor is a Nemzeti Digitális Állampolgárság Program keretében a különféle szolgáltatók csatlakoznak az eAzonosítás szolgáltatáshoz.

Ebbe a kategóriába értendők a különféle kriptográfiai eljárásokat érintő kockázatok is. Korábbi cikkeimben (Nyári [19] és Nyári [21]) részletesen elemzem a posztkvantum kriptográfia várható hatásait a jelenleg használatos elektronikus aláírást megvalósító technológiákra. Jelen állás szerint közvetlen veszélyt nem jelentenek a kvantumszámítástechnika megoldásai, de mindenképpen figyelemmel kell kísérni az új eredményeket ezen a területen. Amint megalkotásra kerülnek az általános célú, nagyteljesítményű kvantumszámítógépek, az azokon futtatható algoritmusok (például Shor prímszámokra felbontó algoritmusa) valódi fenyegetést fognak jelenteni a jelenleg használatban levő nyílt kulcsú rejtjelezési eljárásokra, és hash függvényekre. A szimmetrikus rejtjelező algoritmusok nagyobb biztonságban vannak a posztkvantum éra fenyegetéseivel szemben.

Cikkemben (Nyári [19]) leírtam a különböző nemzeti és nemzetközi információbiztonsággal is foglalkozó szervezetek a posztkvantum éra fenyegetéseinek elhárítása érdekében tett erőfeszítéseit, így a német Szövetségi Kiberbiztonsági Hatóság

(BSI - Bundesamt für Sicherheit in der Infromationstechnik) és az Európai Unió Kiberbiztonsági Ügynökségének (ENISA) ajánlásait is.

Továbbá bemutattam az Amerikai Egyesült Államok szabványügyi testülete, a NIST (National Institute of Standards and Technology) pályázati programját (Post Quantum Cryptography Project – PQC Project), melynek célja új, kvantum biztos nyílt kulcsú kriptográfiai eljárások kialakítása és szabványosítása. A programhoz az Európai Telekommunikációs Szabványügyi Testület (ETSI - European Telecommunications Standards Institute) kvantumbiztos kriptográfia munkacsoportja (Quantum-Safe Cryptography (QSC) working group) is hozzájárult, továbbá ajánlást adott ki a kvantumbiztos megoldásokra való áttérés megkönnyítése érdekében [29].

A fent említett cikk megírása óta eltelt időben a NIST PQC programja a 4. fázisának végéhez ért, melynek keretében három FIPS szabvány tervezetre (FIPS 203, FIPS 204 és FIPS 205) várták az észrevételeket 2023 novemberéig. A szabványtervezetek kvantumbiztos kulcselosztási és digitális aláírási sémák leírását tartalmazzák. A következő mérföldkő a 2024. április 10-12 közötti Ötödik Posztkvatum Kriptográfia Standardizálási Konferencia (Fifth PQC Standardization Conference) [79].

Rodríguez [80] a „A quantum cybersecurity agenda for Europe” c. (Európai Kvantum Kiberbiztonsági Program) írásában kiemeli, hogy az elektronikus aláírással, a biztonságos internetes forgalommal kapcsolatos, ma használatos rejtjelezési eljárások védtelenek a kvantumszámítástechnikából eredő fenyegetésekkel szemben. Ami az új kriptográfiai megoldásokat illeti, az Európai Unió vélhetően a NIST szabványokat fogja követni a posztkvantum rejtjelezési eljárások vonatkozásában.

A technológiai fejlődés, úgymint a kvantumszámítógépek széleskörű elterjedése az állami forrásból eredő, zero-day sérülékenységek kihasználásához hasonló. Tegyük fel, hogy egy állam rendelkezik olyan kvantumszámítógéppel, melynek segítségével képes megtörni a ma használatos nyílt kulcsú kriptográfiára alapuló megoldásokat (például HTTPS protokoll, PGP stb.). Ameddig ezen képességét eltitkolni képes, különösen nagy információbiztonsági – akár nemzetbiztonságot is érintő – károkat okozhat, a titkosítottnak hitt kommunikáció könnyűszerrel történő visszafejtéséből következően.

2.2.7.4 Felhasználóhoz köthető kockázati szcenáriók

Koller [60] a felhasználók kockázatai kapcsán kiemeli, hogy egy rendszer felhasználója mindig lehet gyenge pont – legyen a rendszer bármilyen erős fizikai és logikai

védelemmel ellátva. Véletlen károkozás eredhet a rendszer felhasználóinak figyelmetlenségéből/fegyelmezettlenségéből valamilyen támadás (social engineering, phishing stb.) következményeként. A szándékos károkozás azonban már a rendszer felhasználójának a támadókkal való együttműködését feltételezi például anyagi ellentételezésért cserébe, zsarolás hatására.

Az eSzemélyi megoldáson keresztül szélsőséges esetben akár magas beosztású személyek identitásának ellopása is megvalósulhat, ami akár ellenérdekű országok érdekében állhat. Más államok kiberfölényhez juthatnak az elektronikus hitelesítésre szolgáló infrastruktúra kompromittálódása esetén. Ezen szempontok a jelen értekezés fókuszában álló elektronikus aláírás funkcióra is alkalmazhatók, figyelemre méltó kockázati tényezőként jelentkeznek ugyanis például az anyagi előny megszerzésére, ellenérdekű állam titkosszolgálata által identitás lopásra/hamisításra irányuló törekvések.

2.2.7.5 Az okmány életciklushoz köthető kockázati szcenáriók

Ami az identitás életciklust érintő kockázatokat illeti: a nem megfelelő identitás menedzsment – legyen akár véletlen, akár szándékos – lehetővé teheti kiberbűnözők számára az eID felhasználók jogosultságával való visszaélést. Gondoskodni kell az eID-k visszavonásáról a jogosultság megszűnésekor (például a jogosult halálakor) a csalások kizárása érdekében [59].

Az eSzemélyi igazolvány esetében egyrészt a Kormányablakok üzleti folyamatai érintettek, másrészt pedig a kompromittálódott eAláírás tanúsítvány visszavonása.

2.2.8 Kockázatértékelés

Ebben a részben a tényleges kockázatértékelést mutatom be, első lépésként a kockázatazonosítás az egyik korábbi szakaszban (2.1) részletezett kombinált esemény és vagyontárgy alapú megközelítésével.

2.2.8.1 Kockázat azonosítás és elemzés

A kockázat azonosítás és kockázat elemzés allépéseket összevontan fogom ismertetni, egy-egy lépésben végeztem el ugyanis a stratégiai szcenáriók azonosítását (kockázat azonosítás) és következményük meghatározását (kockázat elemzés), valamint az operatív szcenáriók azonosítását (kockázat azonosítás) és előfordulási valószínűségük meghatározását (kockázat elemzés).

Ezt követően minden bemutatott stratégiai szcenárióhoz felsorolásra kerülnek az operatív szcenáriók, terjedelmi korlátok miatt azonban csak néhány példát ismertetek. A

„Vagyontárgyak” oszlopban vastagon szedetten szerepelnek az elsődleges vagyontárgyak.

13. Táblázat Politikai vezető/stratégiai fontosságú cég vezetője identitásának ellopása – államhoz köthető stratégiai szcenárió alábontása. Forrás: saját szerkesztés

Stratégiai szcenárió	Politikai vezető/stratégiai fontosságú cég vezetője identitásának ellopása – államhoz köthető		
Motiváció	**Operatív szcenárió**	**Vagyontárgyak**	**Valószínűség**
Hódítás	Okmány lemásolása	**A1**, **A3**, **A5**, **A6**, A10	Valószínűtlen
Hódítás	Beszivárgás az eSzemélyi infrastruktúrát üzemeltető szervezetekbe	**A7, A8**, A18, A19, A20, A21	Kissé valószínűtlen
Hódítás	Malware bejuttatása az eSzemélyi infrastruktúrába	**A7, A8**, A18, A19, A20, A21	Kissé valószínűtlen
Hódítás	Malware bejuttatása a célszemély eszközeire	**A1**, **A3**, **A5**, **A6**, A14, A15, A16, A17	Valószínű

Az alábbi táblázatban (14. Táblázat) az az államhoz köthető, igen valószínűtlen operatív szcenárió szerepel, amely fekete hattyú eseményként is felfogható. Bekövetkezése valószínűtlen, hatása azonban az egész digitális világra katasztrofális mértékben kihatna.

14. Táblázat Elektronikus aláírások hitelesnek látszó meghamisítása titkosszolgálati tevékenység leplezése céljából – államhoz köthető stratégiai szcenárió alábontása. Forrás: saját szerkesztés

Stratégiai szcenárió	Elektronikus aláírások hitelesnek látszó meghamisítása titkosszolgálati tevékenység leplezése céljából – államhoz köthető		
Motiváció	**Operatív szcenárió**	**Vagyontárgyak**	**Valószínűség**
Hódítás	Kvantumszámítástechnika alkalmazása az elektronikus aláírások hamisítására	**A9**, A18	Valószínűtlen

Alább látható (15. Táblázat) a hitelesítő kódok felelőtlen tárolását megvalósító lehetséges operatív szcenáriók listája, melyek következményeként a kódokon túl további elsődleges vagyontárgyak is sérülhetnek.

15. Táblázat PIN és/vagy PUK kódok együtt tárolása az eSzemélyi igazolvánnyal – Képzetlen felhasználó stratégiai szcenárió alábontása. Forrás: saját szerkesztés

Stratégiai szcenárió	PIN és/vagy PUK kódok együtt tárolása az eSzemélyi igazolvánnyal – Képzetlen felhasználó		
Motiváció	**Operatív szcenárió**	**Vagyontárgyak**	**Valószínűség**
Jóhiszemű használat	Kormányablakban történő aktiválás során az állampolgár magával viszi az aktiváláshoz szükséges borítékot	**A1, A2, A3, A4, A5, A6**	Nagyon valószínű
Jóhiszemű használat	Az állampolgár folyamatosan, a pénztárcájában együtt tárolja a PIN/PUK kódokat az okmánnyal	**A1, A2, A3, A4, A5, A6**	Valószínűtlen
Jóhiszemű használat	Az állampolgár az otthonában együtt tárolja a PIN/PUK kódokat az okmánnyal	**A1, A2, A3, A4, A5, A6**	Kissé valószínűtlen

Alább (16. Táblázat) láthatók az állampolgár kárára elkövetett csalás kivitelezését célzó operatív forgatókönyvek.

16. Táblázat Állampolgár kárára elkövetett csalás – szervezett bűnözés stratégiai szcenárió alábontása. Forrás: saját szerkesztés

Stratégiai szcenárió	Állampolgár kárára elkövetett csalás – szervezett bűnözés		
Motiváció	**Operatív szcenárió**	**Vagyontárgyak**	**Valószínűség**
Megszerzés	Telefonos/online adathalászat	**A1, A2, A3, A4 A5, A6, A9**	Valószínű
Megszerzés	Okmány lemásolása	**A1**, **A3**, **A5**, **A6**, A10	Valószínűtlen

A kockázatok azonosítását és elemzését a kockázatok kiértékelése követi.

2.2.8.2 Kockázat kiértékelés

Ebben a lépésben, amint azt korábban is írtam, nincsen szubjektivitás, hiszen mechanikusan ki kell választani a kockázati kritériumok meghatározásánál megalkotott kockázati szint mátrixból a kockázati szintet az azonosított kockázatok következményei és valószínűségei alapján. Az értekezés tartalmi korlátjai miatt csak néhány példát fogok megmutatni az azonosított kockázati szcenáriók közül az alábbi táblázatban (17. Táblázat).

Amint azt korábban is írtam egy kockázati szcenárió egy stratégiai és egy operatív szcenárióból áll össze, előbbihez következményt, utóbbihoz valószínűséget rendelünk a kockázat azonosítás és elemzés lépésekben, melyekből következik a kockázat szintje.

17. Táblázat Néhány példa a kockázatértékelésre. Forrás: saját szerkesztés

Stratégiai szcenárió	Operatív szcenárió	Következmény	Valószínűség	Kockázat szintje
PIN és/vagy PUK kódok együtt tárolása az eSzemélyi igazolvánnyal – Képzetlen felhasználó	Kormányablakban történő aktiválás során az állampolgár magával viszi az aktiváláshoz szükséges borítékot	Katasztrofális	Nagyon valószínű	Nagyon magas
Politikai vezető/stratégiai fontosságú cég vezetője identitásának ellopása – államhoz köthető	Okmány lemásolása	Katasztrofális	Valószínűtlen	Alacsony
Politikai vezető/stratégiai fontosságú cég vezetője identitásának ellopása – államhoz köthető	Beszivárgás az eSzemélyi infrastruktúrát üzemeltető szervezetekbe	Katasztrofális	Kissé valószínűtlen	Közepes
Politikai vezető/stratégiai fontosságú cég vezetője identitásának ellopása – államhoz köthető	Malware bejuttatása a célszemély eszközeire	Katasztrofális	Valószínű	Magas
Elektronikus aláírások hitelesnek látszó meghamisítása titkosszolgálati tevékenység leplezése céljából – államhoz köthető	Kvantumszámítástechnika alkalmazása az elektronikus aláírások hamisítására	Katasztrofális	Valószínűtlen	Alacsony
Állampolgár kárára elkövetett csalás – szervezett bűnözés	Telefonos/online adathalászat	Katasztrofális	Valószínű	Magas

A korábban ismertetett elfogadási kritériumok (5. Táblázat) alapján a „Nagyon alacsony”, illetve „Alacsony” szintű kockázatok nem igényelnek kezelést, a „Közepes” szintűek kontroll alatt tartva, biztonsági intézkedések bevezetésével elfogadhatók, a „Magas” és a „Nagyon magas” szintű kockázatok pedig minden esetben mérséklést igényelnek.

Terjedelmi korlátok ugyan nem teszik lehetővé a teljes kockázatelemzés részletezését, de az alkalmazott módszertan és a példák betekintést nyújtanak és jól érzékeltetik a kockázatelemzés jelentőségét.

Az ilyen módon azonosított és értékelt kockázatokat figyelembe kell venni termékek (eSzemélyi), szolgáltatások (eAláírás, eAzonosítás, eKormányzat stb.) fejlesztése, bevezetése és üzemeltetése során. Ennek egy lehetséges módját fogja többek között bemutatni jelen értekezés 3. fejezete.

2.3 Összefoglalás

Az ISO/IEC 27000 család meglehetősen sok szabványból áll. Az ISO/IEC 27001 alapján a szervezetek tanúsíttathatják információbiztonsági irányítási rendszerüket (ISMS). Az ISO/IEC 27002 szorosan kapcsolódik az előbbihez, mivel útmutatást ad az ISO/IEC 27001 bevezetéséhez. Az ISO/IEC 27005 a kockázatkezelésről szól, ezt használtam az értekezés írásakor.

Mint azt a fejezetben olvashattuk a világ számos országa alkalmaz ISO/IEC 27005 alapú kockázatértékelést az e-kormányzati szolgáltatások fejlesztése, továbbfejlesztése és működtetése során. Az új fejlesztések megvalósítása során végzett kockázatelemzések nagyban hozzájárulnak a megfelelő biztonság és felhasználói élmény kialakításához, végsősoron a sikeres megvalósításhoz.

Új tudományos eredményként kiemelném, hogy újrarendszereztem az ISO/IEC 27005:2022 fogalomrendszerével összhangban a korábban, más szerzők által meghatározott kockázati kategóriákat és az érdekelt felekre gyakorolt hatások kategóriáit.

A magyar eSzemélyi igazolvány átfogó kockázatelemzése a jelen értekezésben ismertetett módszer alapján nagyban hozzájárulhat a lehető legbiztonságosabb és legmegbízhatóbb szolgáltatás biztosítása érdekében.

Eredményeim tanúsítják, hogy az ISO/IEC 27005:2022 szabvány alkalmazható az eSzemélyi igazolványra a különféle kockázatok feltárása érdekében. A jelen tanulmányban bemutatott módszer természetesen további finomítást igényel. Mint korábban említettem, nem elég egyszer elvégezni a kockázatelemzést, rendszeres időközönként, folyamatosan finomítva a felmérési és az értékelési szempontokat, újra végre kell hajtani.

A kockázatértékelés ismételt elvégzése több okból is indokolt lehet: egyrészt az eSzemélyi igazolványhoz idővel új funkciók jelenhetnek meg, amelyek további kockázatokat rejthetnek, másrészt, az elterjedtség növekedése miatt. Jelenleg az eSzemélyi használata nem elterjedt, nem része a napi rutinnak, de a felhasználási esetek számának növekedésével az állampolgárok függése az okmánytól idővel nőhet, ezáltal új kockázatok merülhetnek fel, vagy megnőhet a meglévő kockázatok bekövetkezési valószínűsége.

Az ISO/IEC 27000-es szabványcsaládban vannak ágazatspecifikus szabványok is, amelyekre érdemes figyelemmel lenni: az ISO/IEC 27033 útmutatást ad a

hálózatbiztonsági kockázatok azonosításához és kezeléséhez. Ezen túlmenően az ISO/IEC 27034 irányelveket ad az alkalmazások biztonságára vonatkozóan, amely úgy harmadik féltől származó, mint saját fejlesztésű alkalmazásokon alkalmazható. A vonatkozó ágazatspecifikus szabványokat mindenképpen érdemes alkalmazni az olyan léptékű hardver/szoftver fejlesztési projektekben, mint például az eID sémák.

A fejezetben azt is bemutattam, hogy az ISO/IEC 27005:2022-ben megjelent eseményalapú megközelítés hogyan használható az eSzemélyi igazolvánnyal kapcsolatosan felmerülő kockázatok azonosítására.

A következő fejezetben az eSzemélyi igazolványt, mint innovációt fogom vizsgálni, és bemutatom, hogy hogyan feleltethető meg Everett M. Rogers Diffusion of Innovations elméletének a magyar okmány, továbbá azt is, hogy hogyan egészíthető ki a Rogers-féle elmélet kockázatértékeléssel.

3 AZ ESZEMÉLYI IGAZOLVÁNY, MINT INNOVÁCIÓ ÉS ANNAK DIFFÚZIÓJA

Napjainkban az elektronikus információs rendszerek egyre nagyobb mértékben jelen vannak a magyar közigazgatásban, elterjedésük minden állampolgártól fokozott digitális és számítógépes írástudást vár el. Mint azt az 1.3. részben bemutattam, az eSzemélyi igazolvány számos elektronikus funkcióval rendelkezik, mint például elektronikus azonosítás, ami a magyar eKormányzati szolgáltatások igénybevételét hivatott megkönnyíteni, vagy az eAláírás, melynek segítségével Európai Unió-szerte elfogadott bizonyító erővel rendelkező, elektronikusan aláírt dokumentumok hozhatók létre.

A helyzet azonban bonyolultnak tűnhet a felhasználók számára, mivel az eSzemélyi igazolvány használatának számos technikai követelménye van. Ennek eredményeként az alapvető számítógép-használati jártasság már nem elegendő, további ismeretek szükségesek, mint például az elektronikus aláírás alapjai.

Mint azt láthattuk az 1.6. alfejezetben is, az eSzemélyi igazolvány, mint személyazonosító okmány már szinte minden arra jogosult állampolgárhoz eljutott, de az elektronikus funkciók elterjedtségéről ugyanez nem mondható el. Jelen fejezet célja ennek a problémakörnek a vizsgálata.

Korábbi kutatásom (Nyári [2]) a témában azt mutatja, hogy a magyar állampolgárok súlyos információhiányban szenvednek az eSzemélyi okmánnyal és annak lehetőségeivel kapcsolatosan. Ennek oka az lehet, hogy nem jutnak el hozzájuk a szükséges tájékoztató anyagok, információk annak ellenére, hogy azok bőséges mértékben elérhetők a https://eszemelyi.hu információs portálon. A probléma tehát látszólag az igazolvánnyal kapcsolatos kommunikáció kérdése. Erről részletesebben olvashattunk az 1.7. alfejezetben. Azért hangsúlyozom újra, mert a modell alapjául szolgáló keretrendszer kiválasztásában ennek a ténynek fontos szerepe van.

Az elmúlt évtizedekben a kutatók többféle módszertant alkalmaztak a különféle technológiák elfogadottságának mérésére. A következő részben röviden bemutatom miért éppen a Diffusion of Innovations elmélet került kiválasztásra a számos releváns keretrendszer közül.

A megfelelő módszertan bemutatása után következik annak fogalmainak megfeleltetése az eSzemélyi igazolvány fogalomrendszerével. Végül pedig a modell alapján előrejelzéseket és továbbfejlesztési irányokat mutatok be a fejezet további részében.

3.1 A megfelelő módszertan kiválasztása

Korábbi írásomban (Nyári és Kerti [6]) összehasonlítottam a leggyakrabban használt módszertanokat (Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM), Technology-Organizatoin-Environment (TOE), a Unified Theory of Acceptance and Use of Technology (UTAUT) és Diffusion of Innovations (DOI)). A különféle módszertanok különböző szempontok figyelembevételével vizsgálják technológiák, új ötletek, innovációk elfogadottságát. A módszerek egy része az egyén szintjén, egy másik része szervezetek szintjén vizsgálja a különféle újdonságokat. Vannak közöttük pszichológiai alapokon nyugvó, általános értelemben vett viselkedéselméleti megközelítést alkalmazók, mint például a TPB, TRA és olyanok is, melyek már specializáltan technológia elfogadottságra készültek, mint például a TAM vagy az UTAUT. A különféle elméletek evolúciós úton, egymásra épülve, egymás eredményeit felhasználva, pontosítva alakultak ki.

A vizsgált okmány jellemzőit figyelembe véve az alábbi tulajdonságokkal rendelkező módszertan alkalmas:

- a jelenséget egy egész társadalmi csoport körében kell modellezni, nem csak egy szervezet kontextusában,
- egyéni szinten alkalmazhatónak kell lennie,
- a modellnek figyelembe kell vennie a jelenséggel kapcsolatos kommunikáció módját,
- a modell fókuszában egy technológiai újdonság kell, hogy álljon,
- figyelembe kell venni a jelenség időbeli lefutását.

Az említett cikkben részletesen kifejtem, hogy milyen logika mentén jutottam el a Diffusion of Innovations elmélet kiválasztásáig [6].

A továbbiakban az eSzemélyi igazolvány elektronikus funkcionalitásainak terjedését diffúziókutatási problémaként közelítem meg a Rogers-féle Diffusion of Innovations keretrendszer koncepcióinak és módszereinek alkalmazásával, helyenként más módszertanokból átvett fogalmakkal kiegészítve.

3.2 A Diffusion of Innovations módszertan ismertetése

1962-ben Rogers [4] kiadta a „Diffusion of Innovations” elmélet első változatát (DOI vagy Innovation Diffusion Theory – IDT), amelynek célja az új ötletek és technológiák terjedésének modellezése. Az elmélet az évek során több változáson is keresztülment, a

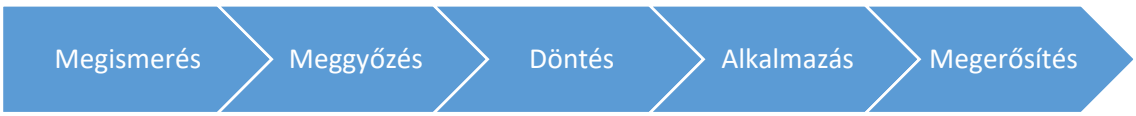
legfrissebb verziója 2003-ban látott napvilágot – ezt a változatát használtam fel jelen értekezés elkészítésekor.

Az elmélet magja és egyben az egyik legfontosabb fogalma a diffúziós folyamat, melyet Rogers négy további kulcsfontosságú tényezőre bont fel az alábbiak szerint: innováció, kommunikációs csatornák, társadalmi rendszer és idő [4].

Az innováció, mint a diffúziós folyamat egyik központi eleme több olyan tulajdonsággal is rendelkezik, melyek nagyban befolyásolják annak terjedési sebességét az adott társadalmi rendszer keretei között. Ezek a tulajdonságok a következők: relatív előny, komplexitás, kompatibilitás, kipróbálhatóság és megfigyelhetőség [4].

A terjedéshez az innovációt át kell adni a potenciális alkalmazók között. Ez a különféle kommunikációs csatornákon keresztül történhet. Ezen a téren a legnagyobb kihívást az emberek sokfélesége jelenti. Tovább nehezít a dolgon, hogy az emberek sokféleképpen lehetnek sokfélék például tudás szerint, meggyőződések szerint, iskolai végzettségek szerint, társadalmi-gazdasági státusz alapján [4].

Nyilvánvalóan időre van szükség minden új technológia elterjedéséhez, így az idő is a modell része. Minden potenciális alkalmazónak át kell esnie egy úgynevezett „innovációs döntési folyamaton” (5. Ábra), amelyben eldönti, hogy elfogadja-e az adott innovációt. Ez az innováció első megismerésétől annak elfogadásán vagy elutasításán keresztül a visszaigazolásig tart. [4]



5. Ábra Innováció döntési folyamat. Forrás: Rogers [4] alapján.

Végül a társadalmi rendszer fogalma: „egymással összefüggő egységek összessége, amelyek közös problémamegoldásban vesznek részt egy közös cél elérése érdekében”. Tagjai között vannak az innováció potenciális elfogadói is. Az elfogadók lehetnek magánszemélyek vagy szervezetek a szóban forgó innováció természetétől függően. Az elfogadási hajlandóság szerint (a leginkábbtól kezdve a legkevésbé hajlandókig) a következő kategóriákba sorolhatjuk a potenciális alkalmazókat: újítók, korai elfogadók, korai többség, késői többség és lemaradók [4].

A társadalmi rendszer fontos részei továbbá a véleményvezérek – azok a személyek, akik nagymértékben képesek befolyásolni más egyének véleményét [4].

A diffúziós folyamat egy nagyobb folyamatban foglal helyet, az Innováció fejlesztési folyamatban, mely az alábbi ábrán (6. Ábra) látható. A fejlesztési folyamat az innovációra való igény megfogalmazásától kezdve a kutatás-fejlesztési, a bevezetési lépéseken át egészen az innováció következményei bekövetkezéséig tart [4].

6. Ábra Innováció fejlesztési folyamat. Forrás: Rogers [4] alapján.

Jelen értekezés az eSzemélyi igazolvány elektronikus funkcióinak vonatkozásában az Innováció fejlesztési folyamat 5. pontjával, a diffúziós folyamattal foglalkozik (az ábrán narancsszínnel kiemelve), mivel a vizsgált okmány tekintetében az azt megelőző lépések már lezajlottak.

Rogers [4] állítása szerint diffúziós kutatásokat számos területen végeztek, mint például a mezőgazdasági tudomány, az egészségügy, a marketing stb.

3.2.1 A diffúziós folyamat

Rogers [4] szerint a diffúzió egy olyan folyamat, amely egy innovációt kommunikál egy társadalmi csoport tagjaival. Minden esetben szükség van valamiféle kommunikációs csatorná(k)ra az innováció és a vele kapcsolatos ismeretek közléséhez. Az alapfogalmak: az innováció (maga az újdonság), a kommunikációs csatornák, az idő és a társadalmi rendszer.

3.2.1.1 Innováció és jellemzői

Bármit tekinthetünk innovációnak, amit a potenciális alkalmazók újnak tartanak (ötlet, gyakorlat és így tovább), vagyis nem kell szükségszerűen objektíven újdonságnak lennie, elegendő, ha a vizsgált társadalmi rendszerben újdonságnak számít. Az innováció jellemzői nagyban befolyásolják az elterjedés sebességét és mértékét. Fontos hangsúlyozni, hogy ezeket a tulajdonságokat mindig a potenciális felhasználók által észleltek alapján kell értelmezni [4].

A komplexitás (complexity) az innováció összetettségét, bonyolultságát fejezi ki. A rendszerelemek, az elsajátítandó új információk, új technológiák minél nagyobb száma növeli a rendszer komplexitását a potenciális elfogadók szemszögéből nézve.

Lényegében azt fejezi ki, hogy a felhasználók mennyire tartják bonyolultnak és nehezen érthetőnek az innovációt [4].

Egy komplex innováció alkalmazása is járhat azonban előnyökkel, melyek miatt megéri arra áttérni. Ennek az előnyösségnek a kifejezésére a relatív előny (relative advantage) tulajdonságot határozta meg Rogers [4], amely leírja, hogy egy újdonság milyen mértékben előnyösebb a jelenleg is alkalmazott gyakorlathoz képest.

A diffúziókutatók hajlamosak abba a tévedésbe esni, hogy egy innovációt csak az előnyös tulajdonságai szempontjából vizsgálnak. Ezt Rogers [4] pro-innováció elfogultságnak (pro-innovation bias) nevezi. Ezzel a megközelítéssel könnyen szem elől téveszthető a potenciális alkalmazók nézőpontja, és így szinte érthetetlenné válik a kutatók számára, hogy adott esetben miért terjed túlságosan lassan egy innováció. Minden diffúziókutatásnál figyelembe kell venni a potenciális alkalmazók évrendszerét, legtöbb esetben ugyanis jó okuk van arra, hogy elutasítsanak egy innovációt. Ez többek között azért is történhet, mert nem jelent számukra akkora előnyt az alkalmazása, ami miatt megérné lecserélni a már működő megoldást.

Nagyban befolyásolja továbbá a potenciális alkalmazók elfogadási hajlandóságát az innovációk kompatibilitás (compatibility) tulajdonsága is, ami azt fejezi ki, hogy a vizsgált újdonság – az elfogadók szemszögéből – milyen mértékben hasonló a jelenleg használt megoldásokhoz. Minél inkább hasonlít az újdonság egy régi megoldásra, valószínűsíthetően annál könnyebben fog terjedni. Minél több új ismeret, új technológia megtanulására és használatára van szükség, annál inkább el fog húzódni a diffúziós folyamat [4].

A diffúziókutatók azonban ezen a ponton is elfogulttá válhatnak. Rogers [4] meghatározza az egyén hibáztató (individual blame bias), és a rendszer hibáztató (system blame bias) elfogultságokat is.

Az egyén hibáztató elfogultság (individual blame bias) esetén a kutatók abba a hibába esnek, hogy a potenciális alkalmazók hiányosságait (ismeret hiány, képzetlenség, hajlandóság hiánya stb.) hangsúlyozzák, és az innováció terjedésének fő akadályozó tényezőit a társadalmi rendszer tagjaiban látják [4].

A másik szélsőség a rendszer hibáztató elfogultság (system blame bias), mely esetben a kutató éppen az előbbi ellentétjeként alapvetően a társadalmi rendszert teszi felelőssé a diffúziós folyamat nehézségeiért. [4]

Segíthet a potenciális elfogadóknak, ha az innováció megfigyelhető, miközben azt más egyének alkalmazzák. Így következmények nélkül, ugyan nem elsőkézből, de megtapasztalhatják az innováció felhasználásával járó relatív előnyöket és a bonyolultságot. Ezt a tulajdonságot megfigyelhetőség (observability) néven fogalmazta meg Rogers [4].

Hasonlóképpen jótékony hatással van a terjedésre, ha az elfogadók különösebb következmények nélkül, gyakorlás céljából kipróbálhatják az adott újdonságot– ennek mértékét fejezi ki a kipróbálhatóság (trialability) [4]. Egy megoldás alkalmazásához szükséges gyakorlat megszerzése előtt frusztrálóan hathat ugyanis a felhasználókra, ha azt kizárólag éles helyzetben, a valódi hatás kiváltásával tudják használni.

Az innovációk egy további tulajdonsága az újraértelmezhetőség/újrafelhasználhatóság (reinvention). Előfordulhat ugyanis, hogy a felhasználók egy újdonságot nem (vagy nem kizárólag) az eredeti szándék szerint alkalmaznak/alkalmaznának. Egy innováció ezen tulajdonsága további segítséget nyújthat a terjedés sebességének fokozásában. [4] Ezt Rogers ugyan nem említi egy szinten az előbbiekkel, de meglátásom szerint ez éppolyan fontos, mint az előbbiek.

3.2.1.2 Társadalmi rendszer

A társadalmi rendszer Rogers [4] szerint „egymással összefüggő egységek összessége, amelyek közös problémamegoldásban vesznek részt egy közös cél elérése érdekében”, melybe beleértendők a potenciális elfogadók (adopters), a változásképviseletek (change agencies), a változásközvetítők (change agent) és a véleményvezérek (opinion leaders) is.

Rogers [4] szerint a „változásképviselet” (change agency) olyan szervezet, amely valamilyen módon érdekelt a vizsgált innováció elterjedésében/elterjesztésében, a „változásközvetítők” (change agent) pedig azok, akik aktívan részt vesznek az innováció terjedésének előmozdításában.

A véleményvezérek a társadalmi rendszer azon tagjai, akik – többnyire interperszonális csatornákon keresztül – erős befolyással vannak a többiek véleményére. Nagyban gyorsítható egy újdonság terjedése, ha beazonosítjuk a véleményvezéreket és elsők között őket „vesszük rá” az innováció alkalmazására. A rendszer többi tagja ad a véleményükre, ezért látva a véleményvezérek példáját nagyobb hajlandóságot fognak mutatni az újdonság átvételére [4].

Az elfogadók lehetnek magánszemélyek vagy szervezetek és tovább csoportosíthatók az elfogadási hajlandóságuk alapján a következő kategóriákba: újítók (innovators), korai elfogadók (early adopters), korai többség (early majority), késői többség (late majority) és lemaradók [4].

Az újítók általában aktívan keresik az újdonságokat a különféle kommunikációs csatornákon és kiterjedt kapcsolati körrel rendelkeznek. Mivel az elsők között alkalmazzák az innovációkat, általában nincs lehetőségük más egyének véleményére alapozni. Általánosságban képzettebbek és jobb anyagi lehetőségekkel rendelkeznek másoknál, ezért képesek akár anyagilag nem megtérülő innovációkat is kipróbálni [4].

Rogers szerint [4] a legtöbb társadalmi rendszerben a korai elfogadók között van a legtöbb véleményvezér. Ettől a csoporttól várja a rendszer többi tagja a segítséget az innovációs döntési folyamat lefutásához. A változásközvetítők ennek a csoportnak a meggyőzésével érhetik el a legjobb eredményeket, sőt ez a csoport járulhat hozzá legnagyobb mértékben a kritikus tömeg eléréséhez is.

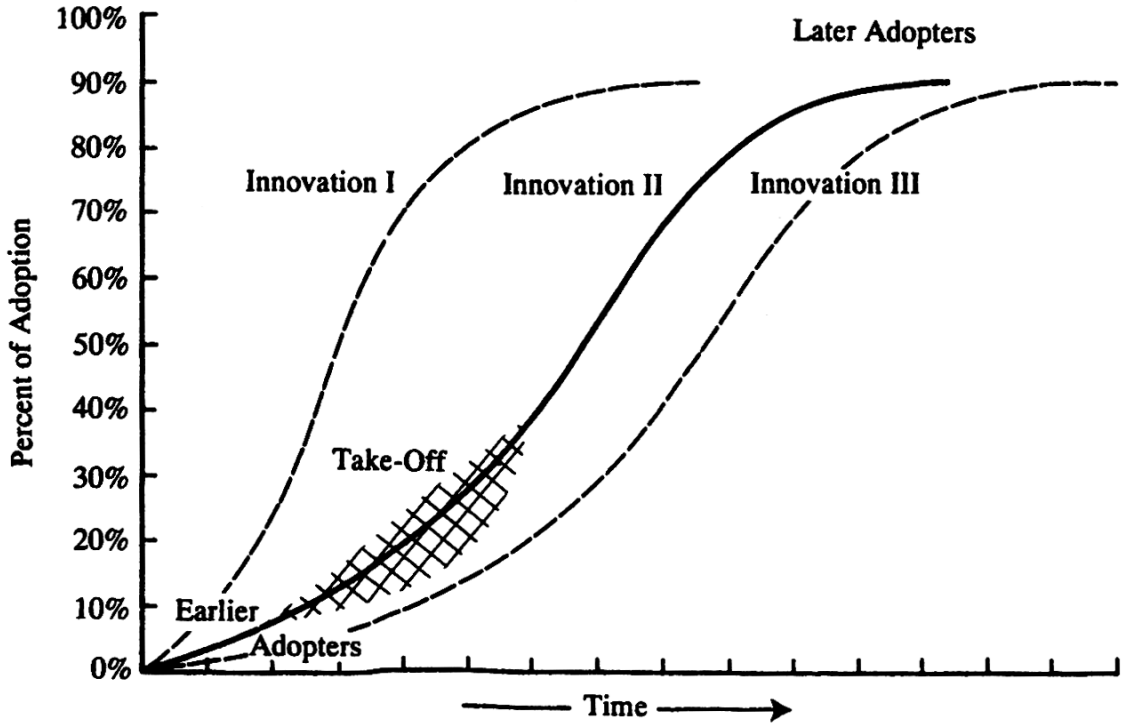
A korai többség tagjai csak ritkán véleményvezérek, általában ők képviselik a társadalmi rendszer legnagyobb hányadát, az egyharmadát. Az ő esetükben hosszadalmassá válik az innovációs döntési folyamat, nem akarják az elsők között elfogadni az innovációt, de lemaradni sem szeretnének a társadalmi rendszer többi tagjától. Tudatosság vezérli őket a döntésük meghozatalában [4].

A késői többségre a szkeptikusság a leginkább jellemző. A társadalmi rendszer átlagos tagjánál később alkalmaznak egy innovációt, ők az előző csoporthoz hasonlóan ugyancsak a populáció egyharmadát teszik ki. Csak akkor hajlandók elfogadni egy újdonságot, ha az alapvető szükségletté válik, vagy a társadalmi rendszer többi tagja irányából nagy nyomás nehezedik rájuk [4].

Végül a lemaradók: gyanakvóan kezelik az újdonságot és a változásközvetítőket, ők az utolsók az adott társadalmi rendszerben, akik átvesznek egy innovációt. Gyakran elszigeteltek a többiektől, a döntéseiket legtöbbször az alapján hozzák meg, hogy egy bizonyos dolgot hogyan szoktak a múltban megoldani. Rogers szerint az eredeti elnevezés „laggards” (magyarul lusta, lemaradó ember) félrevezető lehet, ugyanis a diffúzió kutatókban ezen csoport esetében könnyebben kialakulhat a korábban már említett egyén hibáztató elfogultság érzete, holott egyáltalán nem biztos, hogy az egyének hibája az innováció késői elfogadása [4].

3.2.1.3 Idő

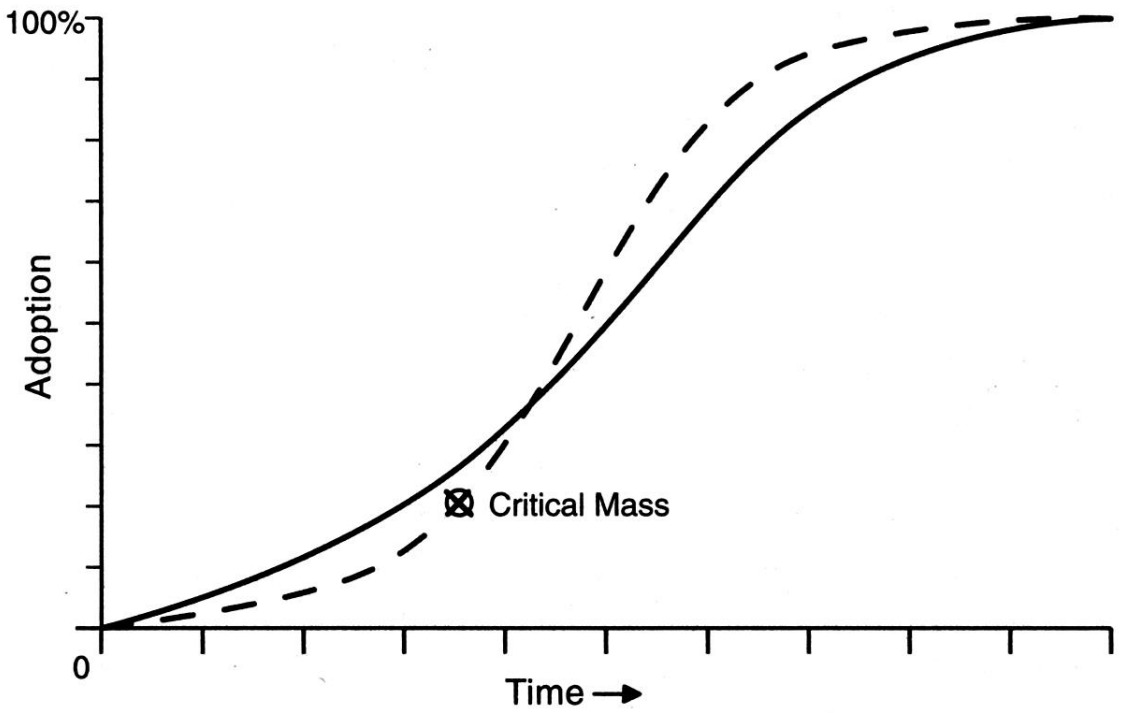
A diffúziós folyamat előrehaladásának szemléltetésére kiválóan alkalmas az elfogadottság aránya (rate of adoption, percentage of adoption) diagram, ami az elfogadók számának időbeli változását jeleníti meg egy kumulatív gyakoriság diagramon. Rogers szerint egy sikeres innováció elterjedése mindig az úgynevezett S-alakú görbe mintáját követi [4].



7. Ábra A diffúziós folyamat Forrás: Everett M. Rogers [4], 2003

Ha a szóban forgó innováció elfogadási aránya (rate of adoption) eléri az úgynevezett „kritikus tömeget", akkor a diffúziós folyamat önfenntartóvá válik, és egyre kevésbé lesz szükség a változásképviseletek és -közvetítők közreműködésére [4].

A két ábrát összevetve (7. Ábra és 8. Ábra) láthatjuk, hogy a felszállásként (take-off) megjelölt szakasz indítóeseménye a kritikus tömeg elérése. Az is megfigyelhető, hogy az S-alakú görbe mely szakaszában „lépnek be" a különböző elfogadó csoportok.



8. Ábra A kritikus tömeg, Forrás: Everett M. Rogers [4], 2003

3.2.1.4 Kommunikációs csatornák

Az újdonságok terjedéséhez szükség van kommunikációs csatornákra, melyek lehetnek a tömegmédia (mass media) csatornái (például tévé, rádió, Internet) vagy akár interperszonális csatornák is. A tömegmédia előnye természetesen, hogy a társadalmi rendszer igen sok résztvevőjéhez eljuthat, meggyőzőereje diffúziós szempontból azonban kisebb lehet, mint az interperszonális csatornákon terjedő információké [4].

Kihívást jelent a társadalmi rendszer tagjainak sokfélesége a tudás, a vallási/politikai meggyőződés, az iskolai végzettség, a társadalmi-gazdasági státusz stb. alapján [4].

Két fontos, alapvetően a szociológiában használatos fogalmat érdemes kiemelni a homofíliát (homophily) és a heterofíliát (heterophily). Az előbbi, a homofília annak a mértékét határozza meg, hogy két egymással interakcióba lépő egyén mennyire hasonlít egymásra a társadalmi helyzetüket illetően (tudás, végzettség, meggyőződés stb.). A heterofília ennek éppen az ellenkezőjére, a különbözőségre helyezi a hangsúlyt [4].

Két egyén, akik hasonló társadalmi helyzettel rendelkeznek általában véve sokkal gördülékenyebb, hatékonyabb kommunikációt folytatnak egymással, mint azok, akik nagymértékben különböznek ilyen téren. Az ebben az értelemben hasonló egyének egymástól tanácsot is hajlamosabbak elfogadni, mint másoktól [4].

Fontos ezt a tényezőt figyelembe venni, amikor a véleményvezérek beazonosítása és a változásközvetítők kiválasztása történik. Az egyes társadalmi csoportok meggyőzése hatékonyabban történhet, ha olyan személyiség közvetíti feléjük a befogadásra szánt üzenetet, akivel könnyebben tudnak azonosulni.

3.3 eKormányzati szolgáltatások diffúziója

Ebben a szakaszban a Diffusion of Innovations keretrendszer korábbi alkalmazásai mellett ki fogok térni különböző országok eKormányzati (eGovernment) szolgáltatásainak népszerűsítésével, alkalmazásával foglalkozó kutatásokra is. A Diffusion of Innovations módszert számos területen alkalmazták már az első megfogalmazásától számított közel hét évtizedben.

Zhang, Xu és Xiao [81] egy metaanalízis keretében vizsgáltak korábbi tanulmányokat az eKormányzati szolgáltatások diffúziójának témakörében és megállapításaik szerint alapvetően négy téma köré lehet csoportosítani a releváns írásokat:

- az eKormányzati szolgáltatások terjedését befolyásoló tényezők,
- az eKormányzati szolgáltatások diffúziós rendszere és alkalmazásuk,
- az eKormányzat terjedésének hatása a kormányzati szervekre és az alkalmazottakra,
- az IKT-infrastruktúrák és az eKormányzat elterjedése közötti kapcsolat.

A felhasználók elégedettsége az eKormányzati szolgáltatásokkal meglehetősen jó hatással van azok jövőbeli elterjedésére, a széles körű elfogadás mintegy „húzóerőként” jelentkezhet a diffúziós folyamatban. Az eKormányzat terjedési folyamata a fejlődő országokban továbbra is lassú. Az új ötletek terjedése tervszerűen vagy akár spontán is megtörténhet. A legtöbb tanulmány elsősorban a tervezett diffúziós folyamatra (vagy formális diffúziós folyamatra) összpontosított, míg a spontán diffúziós folyamatot (vagy informális diffúziós folyamatot) figyelmen kívül hagyták [81].

Ezenkívül a diffúziós folyamattal foglalkozó tanulmányok többsége a nemzeti és állami szintre összpontosított, míg kevés tanulmány foglalkozik a kormányzati ügynökségek közötti diffúziós folyamattal. Továbbá kevés tanulmány vizsgálta a diffúziós folyamat befolyásoló tényezőit, például harmadik feleket [81].

Wang, Doong és Lin [82] tanulmányukban a tömegmédiában történő reklámozás, az ismerősök közötti interakciók és a kettő kombinációjának a tajvani elektronikus adóbevallás kitöltő rendszer (tax e-filing system, TEFS) diffúziójára gyakorolt hatását

vizsgálták három diffúziós modell – köztük a Diffusion of Innovations-el – alkalmazásával, felhasználva a tajvani pénzügyminisztérium összesített éves adatait.

A domináns faktornak az interperszonális csatorna bizonyult. A tajvani kormányzat az eKormányzati szolgáltatásait korábban főként a hírességek tévében vagy rádióban sugárzott hirdetésein keresztül népszerűsítette. Bebizonyosodott azonban, hogy ezek hatása igen korlátozott a diffúziós folyamatra [82].

Megállapítást nyert továbbá, hogy az eKormányzati infrastruktúra kiépítésére fordított hatalmas befektetések kizárólag a megfelelő marketingstratégiák kidolgozásával együtt hozhatják meg az állampolgárok számára a kényelmes digitális életet. A szerzők javaslata szerint könnyen megosztható Internetes hirdetésekkel kell népszerűsíteni (közösségi médián keresztül) a megoldást. Javasolják továbbá a relatív előnyök növelését is, amely az elégedett felhasználókon keresztül fel fogja erősíteni az interperszonális csatornák hatását [82].

Bass [83] a Rogers-féle Diffusion of Innovations keretrendszer fogalmait matematikai alapokra helyezte 1969-ben. Egy differenciálegyenlettel modellezi új termékek elterjedését egy adott populáció körében. A modellje kitűnően használható diffúziós folyamatok előrejelzésében.

A Bass modellre a későbbiekben még ki fogok térni részletesebben, mert az eSzemélyi korábban már hivatkozott BM statisztikai adatait felhasználva magam is alkalmaztam a modellt az eSzemélyi elektronikus funkciói diffúziójának előrejelzésére.

Ram [84] az innovációkkal szemben tanúsított ellenállásról szóló cikkében két fő tényezőt azonosított: az érzékelt kockázatot (perceived risk) és a kognitív ellenállást (cognitive resistance). Szerinte az innováció módosítására és a kommunikációjára irányuló stratégiákkal hatékonyan csökkenthetők az érzékelt kockázatok. Mint azt a későbbiekben látni fogjuk a Diffusion of Innovations a korábbi kutatások során gyakran kiegészítésre került az érzékelt kockázat fogalommal és jelen értekezésben az eSzemélyi igazolvány vonatkozásában is értelmezésre kerül.

Baldunčiks [85] 2016-os írásában Lettországban vizsgálta az elektronikus aláírás diffúzióját. Cikkében úgy hivatkozik az eAláírásra, mint új szolgáltatásra. Állítása szerint az online bankoláshoz kellőképpen hasonlít az elektronikus aláírás innováció bizonyos szempontok alapján, ezért az online bankolásra vonatkozó megkérdezéses felmérés adataiból készített előrejelzést Bass módszerével az elektronikus aláírás szolgáltatás

várható terjedésére. Eredményeiből az interperszonális kommunikációs csatornák és a Rogers-féle kipróbálhatóság fontossága válik nyilvánvalóvá.

Folorunso, Vincent, Adekoya és Ogunde [86] a különféle közösségi média platformok (Facebook, MySpace stb.) elterjedtségét vizsgálták standardizált kérdőíves felméréssel egyetemi hallgatók körében alkalmazva a Rogers-féle innováció jellemzőket. Eredményeik szerint a kipróbálhatóság és a kompatibilitás volt a legfontosabb szempont az elfogadási döntés meghozásakor.

Al-Jabri és Sohail [87] Szaúd-Arábiában 330 mobil bank felhasználó kérdőíves felmérésének adatin alkalmazták a Rogers-féle elméletet kiegészítve az érzékelt kockázat (Perceived Risk) fogalommal. A következtetéseik szerint az érzékelt kockázat negatívan befolyásolta az elfogadást, a kipróbálhatóság, és a komplexitás nem voltak különösebb hatással, a relatív előny, a kompatibilitás és a megfigyelhetőség pedig pozitívan befolyásolták. Kiemelték, hogy a bankoknak törekedniük kell az ügyfeleik által észlelt kockázatok csökkentésére azáltal, hogy speciális garanciákat kínálnak az ügyfelek védelmére, valamint azzal, hogy kiemelten kezelik a panaszaikat.

Yeloglu és Sagsan [88] írásukban szintén innovációként kezelik a török eKormányzati szolgáltatások összességét. Hangsúlyozzák az érthetőség, az olvashatóság, az egyszerű navigáció – vagyis az alacsony komplexitás – fontosságát. Ugyan nem használják az érzékelt kockázat kifejezést, de megállapítják, hogy a felhasználók szívesebben használnak olyan szolgáltatásokat, melyek hitelesnek és biztonságosnak tűnnek számukra.

Magyarországon is alkalmazták már a Diffusion of Innovations keretrendszert. Láng, Letenyei és Siklós [89] 2003-ban végeztek kérdőíves felmérést a Kaposvári kistérségben, melynek célja a számítógéphasználat terjedésének vizsgálata volt. Végkövetkeztetésük szerint a vizsgált régióban az adatokra illeszthető lett volna egy diffúziós modell, de valójában nem diffúzióról volt szó, mivel alapvetően nem interperszonális úton terjedt a számítógéphasználat, hanem intézményeken keresztül (például iskolák, munkahelyek). Szerintük ilyen esetekben nincs szükség a Rogers-féle kritikus tömeg elérése a diffúzió terjedésének fenntartásához.

Erdősi [22] is említi a Diffusion of Innovations-t, amikor is a különböző potenciális elfogadói csoportok (innovátorok, korai elfogadók stb.) Rogers által definiált statisztikai eloszlása alapján a KHS adatait figyelembe véve meghatározza a magyar viszonyok között értelmezett elfogadói csoportok számosságát az elektronikus aláírás elfogadására

vonatkozóan. Jelen értekezés azonban ennek egy részhalmazával, az eSzemélyi igazolvány eAláírás funkciójával foglalkozik.

Schmidt [90] a diplomamunkájában a Németországban alkalmazott eIDAS szerinti elektronikus személyazonosító igazolvány kapcsán használta fel a TAM-mal kombinálva 2022-ben a Diffiusion of Innovations-t. A 3.2. alfejezetben leírt „innováció fejlesztési folyamat"-ból ő sem vizsgálta a „Diffúzió és elfogadás" előtti lépéseket ugyanazon okokból, melyekből magam sem – azok a lépések a vizsgálat időpontjában már lezajlottak.

A tanulmány szerint Németországban „neuer Personalausweis" (Új Személyi igazolvány), röviden nPA-ként hivatkoznak az okmányra. Végkövetkeztetésében ismerteti, hogy mely problémák akadályozzák a nPA diffúzióját Németországban, több javaslatot is megfogalmazva többek között a hasznosság („Usefulness") – ami a Rogers-féle relatív előnnyel egyenértékű – növelésére vagy az elektronikus okmánnyal foglalkozó közalkalmazottak képzésére vonatkozóan is [90].

Yera, Arbelaitz, Jauregui és Muguerza [91] kutatásukban az e-kormányzati szolgáltatások elterjedését, gyakorlati felhasználását elemzik Európa-szerte (26 EU-tagország) az Európai Unió statisztikai hivatala (Eurostat) adatai alapján. Meghatározták az EGUI (e-Government Usage Index) indexet, amelyet az „Eurostat's Community Statistics on Information Society" (CSIS) évenként végrehajtott megkérdezéses kutatásainak az eKormányzati szolgáltatások használatára vonatkozó kérdései alapján számítottak ki. Az eKormányzat használatának négy szintjét határozták meg (nagyon magas, magas, alacsony és nagyon alacsony). Magyarország vonatkozásában 2020-ban az „alacsony" értéket állapították meg. Ezek az eredmények alátámasztják a BM statisztikákból az 1.6. fejezetben levont következtetéseimet is.

Kumar, Mukerji, Butt és Pesaud [92] a Kanadai eKormányzati szolgáltatásokat vizsgálták a TAM módszertan segítségével. Megállapításaik szerint kulcsfontosságú, hogy a különféle szolgáltatások alaposan megtervezett, a célcsoport igényeit legjobban kielégítő weboldalakon keresztül legyenek elérhetők. Hangsúlyozzák, hogy a felhasználók által érzékelt információbiztonsági kockázat (Perceived Risk) is különösen fontos tényező az eKormányzati szolgáltatások alkalmazása során. Az észlelt kockázatokat adatvédelmi aggályokra és rendszerbiztonsági aggályokra bontották.

Lényeges elem annak megteremtése, hogy az állampolgárok biztonságosan lebonyolíthassák az online tranzakciókat a bizalom szintjének és az eKormányzati

szolgáltatások elfogadási arányának növelése érdekében. A magasabb szintű elégedettség – amelyet nagyrészt az határozz meg, hogy a szolgáltatások mennyire tudnak gazdag, problémamentes, biztonságos és megbízható élményt nyújtani – magasabb szintű elfogadáshoz vezet [92].

Korábbi cikkemben (Nyári és Kerti [70]) bemutattam, hogy az ISO/IEC 25010 szoftverminőség követelményeit és értékelési szempontjait meghatározó (SQuaRE) szabvány – melynek azóta már megjelent a 2023-as változata – alkalmazása nagy mértékben hozzá tud járulni a szoftverek biztonságához, így akár az érzékelt kockázat csökkentéséhez is.

3.4 Az eSzemélyi igazolvány elhelyezése a Diffusion of Innovations keretrendszer kontextusában

Jelen szakasz címei többé-kevésbé megegyeznek az előző szakaszban találhatókkal – ez azonban nem véletlen, ugyanis azt mutatom be, hogyan alkalmazhatók a Diffusion of Innovations keretrendszer fogalmai az eSzemélyi igazolványra vonatkoztatva.

Az Innováció fejlesztési folyamattal részleteiben nem foglalkozom, ez ugyanis új termékek kifejlesztése, bevezetése során a leghasznosabb. Új használati esetek bevezetésekor javasolt az alkalmazásának megfontolása. Terjedelmi korlátok miatt kizárólag a diffúziós folyamat alapfogalmait feleltetem meg az eSzemélyi igazolvány fogalomrendszerével.

Alábbiakról egy korábbi cikkemben (Nyári-Kerti [6]) már ejtettem szót, de a következő szakaszokban részletesebben fejtem ki az eSzemélyi – Diffusion of Innovations megfeleltetést, mint az említett írásban.

3.4.1 Innováció

Rogers [4] szerint még egy viszonylag régi technológia is innovációnak tekinthető egy társadalmi rendszer keretein belül, ha az újnak számít a tagok számára. Az eSzemélyi igazolvány 2016. január 1-től érhető el az állampolgárok számára, de a chip csak 2021 augusztusa óta kötelező [39].

Ahogyan ezt az 1.6. alfejezetben is láthattuk a BM Adatnyilvántartásokért Felelős Helyettes Államtitkárság statisztikái alapján a jogosultak igen kis százaléka igényelte az évek során az okmány elektronikus aláírási funkcióját, így a személyazonosító igazolvány és annak elektronikus funkciói innovációnak tekinthetők [5]. A továbbiakban az

elektronikus aláírás funkció előfordulási gyakoriságát használom az eSzemélyi elektronikus funkcióinak elterjedtségének mérésére.

Az eSzemélyi igazolvány, mint innováció komplexnek tekinthető, hiszen használatához több szoftver és kártyaolvasó (vagy NFC-képes mobileszköz) szükséges, amint az láthattuk a 1.2. szakaszban is.

Kompatibilitását tekintve merőben eltér az állampolgárok által napi rutinként használt papír alapú aláírási megoldástól. Bár használata valamelyest hasonlíthatna az „érintős" bankkártyák használatához, a használati eseteik lényegesen különböznek egymástól, továbbá a szükséges infrastruktúra sincs teljes mértékben kiépítve.

Sajnos az állampolgároknak nincs lehetőségük igénylés előtt következmények nélkül kipróbálni, vagy akár megfigyelni a megoldást, így nem túl kedvező a helyzet a kipróbálhatóság és a megfigyelhetőség szempontjából sem.

Használatának előnyeként kiemelhető, hogy az elektronikus aláírással időt és papírt (ezek által végső soron pénzt) lehet spórolni, de az állampolgárok egyéni megítélésétől függ, hogy ez milyen mértékű relatív előnyt jelent számukra a megszokott megoldáshoz képest. Az előnyök értékelésekor természetesen figyelembe kell venni a magas komplexitást és a viszonylagosan alacsony kompatibilitást.

Ahogyan azt korábban láthattuk többféle szempontból is lehet elfogultan vizsgálni az innovációkat. Az első fejezetben olvasottak alapján könnyen gondolhatnánk azt, hogy jómagam valamelyest pro-innováció elfogult (pro-innovation bias) szemlélettel közelítem meg a kérdést. Vagyis túlságosan nagy jelentőséget tulajdonítok az eSzemélyi igazolvány előnyeinek. Pontosan ennek ellensúlyozására született meg a 2. fejezet, melyben módszeresen áttekintettem az okosokmány használatának árnyoldalát is.

Kerülendő az egyén-hibáztató (individual blame bias) megközelítés is, vagyis nem szabad minden problémát az eSzemélyi igazolvány potenciális felhasználóira hárítani. Mindig abból a feltételezésből kell kiindulni, hogy aki már – hangsúlyozom – ismeri az innovációt és mégis elutasítja, annak jó oka volt e döntés meghozatalára. Nem jár számára akkora relatív előnnyel, ami miatt érdemes használnia, nincsenek az életében olyan használati esetek, amelyek indokolttá tennék, túlságosan komplex a számára stb.

Ami a rendszer-hibáztató elfogultságot (system blame bias) illeti, korábbi cikkemben (Nyári [2]), valamint a korábbi fejezetekben ennek nyomai is megjelentek. Hajlamos voltam ugyanis a kormányablaki tájékoztatás hiányosságaira fogni a terjedés lassú

ütemét. Minden bizonnyal e mögött is méltányolható okok rejlenek például az igénylési folyamat hosszadalmasabb lenne, ha a kormányablaki tisztviselők még reklámkampánnyal, oktatással is foglalkoznának, ami esetlegesen növelné az elégedetlen ügyfelek számát. Az igénylési folyamatnak, a kormányablaki dolgozók felkészültségének és hozzáállásának további vizsgálata és kifejtése nem célja az értekezésnek, de további kutatási irányként érdeklődésre számot tartónak találom.

A Diffusion of Innovations szerint az innovációk terjedése szélesítheti a társadalmi rendszeren belül a különböző csoportok közötti társadalmi-gazdasági szakadékot. Ez az eSzemélyi igazolvány esetében is egy valós problémává válhat hosszú távon. Elképzelhetőnek tartom, hogy amikor a hagyományos, eSzemélyi igazolványt nem igénylő megoldások elkezdenek visszaszorulni, akkor a rosszabb anyagi lehetőségekkel rendelkező, a digitális írástudást nélkülöző állampolgárok hátrányos helyzete tovább fokozódik. Ez azonban a korábban említett nyomásként is felfogható, ami ösztönözheti a lemaradókat az innováció átvételére.

Az innovációk egy további jellemzője az újrafelhasználhatóság (reinvention), ezt azonban nehezen értelmezhetőnek tartom az eSzemélyi igazolvány esetében. Egyrészt informatikai szempontból is, másrészt jogszabályok által is meglehetősen kötött ugyanis, hogy mire használható az okmány. Szoftverfejlesztői tapasztalatomra alapozva azonban úgy gondolom, hogy a felhasználók meglepően kreatívok tudnak lenni. Az újrafelhasználási esetek megjelenéséig is várnunk kell azonban. Amíg ilyen alacsony számban vannak forgalomban eAláírással rendelkező okmányok, addig nem számíthatunk különösebben nagy kreativitásra.

Egy ide vonatkozó ötletet azonban már a diffúziós folyamat jelen állapotában is felmerül: érdemes lenne kiterjeszteni a korábban említett SZTSZ szolgáltatást például az egyéni vállalkozókra, ezzel is segítve a kisvállalkozásokat. Az Egyéni Vállalkozók Nyilvántartásában (ami a nyilvantarto.hu-n keresztül elérhető) minden szükséges adat szerepel ahhoz, hogy az összeköthető legyen az SZTSZ-szel. Bővebben lásd a 4.1.1.5. szakaszban.

Nem része ugyan a Diffusion of Innovations keretrendszernek a hagyományos, Rogers-féle felfogásban, de – mint azt korábban is jeleztem – értekezésemben az innováció tulajdonságai között az érzékelt kockázatot is figyelembe veszem tekintettel arra, hogy egy olyan innováció áll a vizsgálat középpontjában, amelynek jelentős információbiztonsági vonatkozásai vannak.

Korábbi fókuszcsoportos kutatásom (Nyári [2]) során a résztvevőkkel folytatott beszélgetések során két, alapvetően pénzügyi/gazdasági kategóriába sorolható kockázat került azonosításra. Egyrészt az eAláírás alkalmazása során attól tartanának a résztvevők, hogy a másik fél valamilyen formában csalást követ el az ő kárukra (például ellopja a kártyájukon tárolt személyes adatukat). A másik, ennél jóval szerényebb hatással járó kockázatként a kártyaolvasó készülékbe való felesleges, nem megtérülő beruházást említették. További hasznos kutatási irányt jelenthet az eSzemélyi igazolvány használata során érzékelt kockázatok széleskörű vizsgálata.

Az érzékelt kockázat mellett egy további elemmel kiegészítem a Rogers-féle innováció értelmezést, ez pedig az „azonosított kockázat". Az érzékelt kockázat egy nagyon fontos összetevő, hiszen mint azt korábban olvashattuk nagyban befolyásolja a potenciális elfogadók hajlandóságát az innováció alkalmazására. Figyelembe kell azonban venni azt is, hogy a felhasználók által érzékelt kockázat nem minden esetben esik egybe az innováció használata során jelentkező valós kockázatokkal. Az azonosított kockázat, mint innováció jellemző, az innováció tervezése, bevezetése során elvégzett kockázatértékelés során feltárt kockázatokat és azok kezelési módját jelenti.

Mint azt a 2. fejezetben láthattuk az eSzemélyi igazolvány kapcsán számos kockázat felmerül úgy a mindennapi használat, mint az alkalmazott technológiák vonatkozásában. A példa kedvéért egy kockázati szcenáriót kiemelnék az azonosított kockázatok közül, a kifejtett kódkártyák kiosztását és a Kormányablakban történő aktiválást érintő „PIN és/vagy PUK kódok együtt tárolása az eSzemélyi igazolvánnyal" nevű forgatókönyvet, amely adminisztratív intézkedésekkel könnyen kezelhető lenne.

Az alkalmazott technológiát illetően – digitális aláírásról lévén szó – kiemelném cikkeimet (Nyári [21] és Nyári [19]), melyekben a poszt kvantum éra várható fenyegetéseit részletezem az eIDAS, a kriptográfia és általában véve az információbiztonság szemszögéből.

Ahogyan azt korábbi cikkemben (Nyári és Kerti [68]) is írtam egy ilyen mértékű hardver/szoftverfejlesztési projekt esetében, mint az eSzemélyi igazolvány különösen fontos a megfelelő kockázatértékelés elvégzése a sikeres bevezetés és a biztonságos mindennapi használat megteremtése érdekében.

Az eSzemélyi igazolványt támogató szoftverek információbiztonságot szem előtt tartó fejlesztése, karbantartása és üzemeltetése szintén különösen fontos. Kiemelném korábbi

írásomat (Nyári-Kerti [70]), melyben kitérek az ISO/IEC 25010 szoftverminőséggel kapcsolatos szabvány jelentőségére a szoftverfejlesztési projektek során.

3.4.2 Társadalmi rendszer, elfogadók, változásközvetítők

A „társadalmi rendszer" fogalma igényel a legkevesebb magyarázatot az eSzemélyi vonatkozásában. Ebben a diffúziókutatásban a „társadalmi rendszer" megegyezik az egész magyar társadalommal.

Minden magyar állampolgárnak fényképes igazolványt kell igényelnie (ez azonban lehet jogosítvány vagy útlevél is), valamint 14 éves kortól jogosult elektronikus aláírás funkcióval ellátott okmányra is. Lényegében ez a jogosulti kör ebben az esetben megfelel az elfogadók halmazának [39].

A fő változásképviselet maga Magyarország Kormánya. A legkézenfekvőbb módja a terjedés elősegítésének a reklámkampányok finanszírozása lenne, ám mint korábban írtam ez csak ritkán járul hozzá nagymértékben a terjedéshez. Sokkal inkább a közösségi médiákban való megjelenést lenne érdemes erősíteni.

További használati esetek bevezetésével vonzóbbá lehetne tenni az okosokmányt. A Budapesti tömegközlekedésben például még nem lehetséges eSzemélyi igazolvánnyal kiváltani a jegyeket, bérleteket.

Továbbá a Kormányablakok is tekinthetők változásképviseleteknek. A fő változásközvetítők az ügyintézők, akik segítik az állampolgárokat az okosokmány igénylési folyamata során. Az ügyintézők ugyanis minden egyes állampolgárral személyesen találkoznak – nem is egyszer – az igénylési folyamatban. Ezeket az alkalmakat ki lehetne használni az okosokmány módszeres és tervezett népszerűsítésére. De ugyanezen a ponton az innováció kipróbálhatóságának és a megfigyelhetőségének hiányosságain is lehetne valamelyest segíteni.

Korábbi cikkemben (Nyári [2]) is hangsúlyoztam, hogy ezen a területen lehetne javítani, és az ügyintézőknek nagyobb erőfeszítéseket kell tenniük az elektronikus dokumentum népszerűsítésére az igénylések kiszolgálása folyamán.

3.4.3 Idő

A diffúziós folyamat 2016. január 1-jén kezdődött. A szóban forgó személyazonosító okmány az évek során módosult. A chip eleinte opcionális volt, de 2021 augusztusa óta kötelező. 2022 tavaszán jelent meg az eSzemélyiM mobilalkalmazás, amely lehetővé teszi a hardveres kártyaolvasók kiváltását NFC- és WIFI-képes mobileszközökkel [3].

Az innováció és felhasználási esetei is folyamatosan fejlődnek, 2023 januárja óta az elektronikus aláírás funkcióhoz kapcsolódóan új szerepkör alapú hitelesítési megoldás (SZTSZ) érhető el, amely lehetővé teszi, hogy a felhasználók az elektronikusan aláírt dokumentumokat olyan attribútumtanúsítvánnyal egészítsék ki, amely hitelesen igazolja a pozíciójukat egy szervezetben. Ez azonban egyelőre csak az állami alkalmazottak számára elérhető [48].

Sajnos azonban a Belügyminisztérium már említett statisztikái szerint az elektronikus aláírás funkciót igénylő állampolgárok száma az évek során nem nőtt számottevően, lásd az alábbi táblázatot (18. Táblázat).

A honlapon elérhető adatok az elektronikus aláírás funkcióval igényelt új azonosító okmányok évi számát is tartalmazzák. Ezeket az igényléseket teljesen új igényeknek tekintve (nem pedig elveszett/sérült dokumentumok pótlására irányuló kérelmeknek) kiszámolható az új kérelmek kumulatív összege. Az adatok azt is mutatják, hogy a teljes, 9 599 744 fős lakosság körében 11 731 220 kártya igénylés történt az évek során. Magyarországon a 14 év felettiek száma 8 304 909 fő. [5, 52].

Az adatokon alkalmaztam a korábban említett Bass modellt az alábbiak szerint. Baldunčiks [85] és Van den Bulte [93] nyomán a Bass modell alapvetően a Rogers-féle diffúziós folyamat időbeli lefutásának modellezésére alkalmas.

Négy bemeneti paraméter felhasználásával képes az S-görbe és az elfogadások időbeli eloszlásának megbecslésére. A paraméterek az alábbiak:

- a piac befogadóképessége, amely azt fejezi ki, hogy a vizsgált termékből összesen hányat képes befogadni a piac
- az induló elfogadási érték: hány termék jelent meg a piacon a termék bevezetésekor
- az innovációs együttható (p) azt hivatott modellezni, hogy az innovációt milyen mértékben reklámozzák a tömegkommunikáció segítségével, nem függ a kumulatív összegtől
- az imitációs együttható (q), vagy más néven szájról-szájra (word-of-mouth) együttható, amely az interperszonális csatornák hatását hivatott kifejezni a kumulatív összegek alapján.

18. Táblázat Új eSzemélyi igazolvány igénylések, Forrás: Belügyminisztérium [5], 2023

	2016	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Új eSzemélyi	1 309 260	1 373 617	1 300 429	1 378 184	1 058 777	1 350 533	2 145 399	1 815 021
Új eSzemélyi kumulatív összeg	1 309 260	2 682 877	3 983 306	5 361 490	6 420 267	7 770 800	9 916 199	11 731 220
Új eSzemélyi eAláírással	67 348	122 520	37 523	25 509	20 743	16 246	27 980	31 856
eAláírás kumulatív összeg	67 348	189 868	227 391	252 900	273 643	289 889	317 869	349 725

Az évenkénti elfogadások számának meghatározásához az alábbi képletet alkalmaztam:

$$E_t = pB + (q - p)E_{t-1} - \frac{qE_{t-1}^2}{B}$$

ahol

E_t – az adott t évre vonatkozó becslése az elfogadások számának

p – innovációs együttható

q – szájról szájra együttható

E_{t-1} – az előző évre vonatkozó becslése az elfogadások számának

B – a piac befogadási képessége

A piac befogadóképessége 8 304 909 db, hiszen ennyien jogosultak elektronikus aláírás funkcióval eSzemélyi igazolványra.

Ha a q értéke nagyobb p értékénél, akkor a hagyományos S-görbét figyelhetjük meg. Magas p érték gyors indulást követően fokozatos lassulást eredményez. Ezzel szemben a magas q érték lassú indulást és a később szakaszban való begyorsulást okoz [85, 93].

A p értéke alacsonyabb a q értékénél, akkor az úgynevezett J-görbe figyelhető meg, ami a kevésbé kockázatos innovációkra (például élelmiszer, új mozifilm, zenei album) jellemző [93].

Előrejelzéshez célszerű egy olyan már létező és sikeresen elterjedt innovációt kiválasztani, ami hasonlít az aktuálisan vizsgált innovációhoz. A korábbi diffúziós adatokból meg lehet határozni q és p értékét, majd ezek alapján előrejelzések készíthetők [85].

Ilyen dokumentált innovációt magyar viszonyok között nem találtam. Próbáltam a magyar mobiltelefonelőfizetések darabszámára vonatkozó 2000 és 2021 közötti KSH

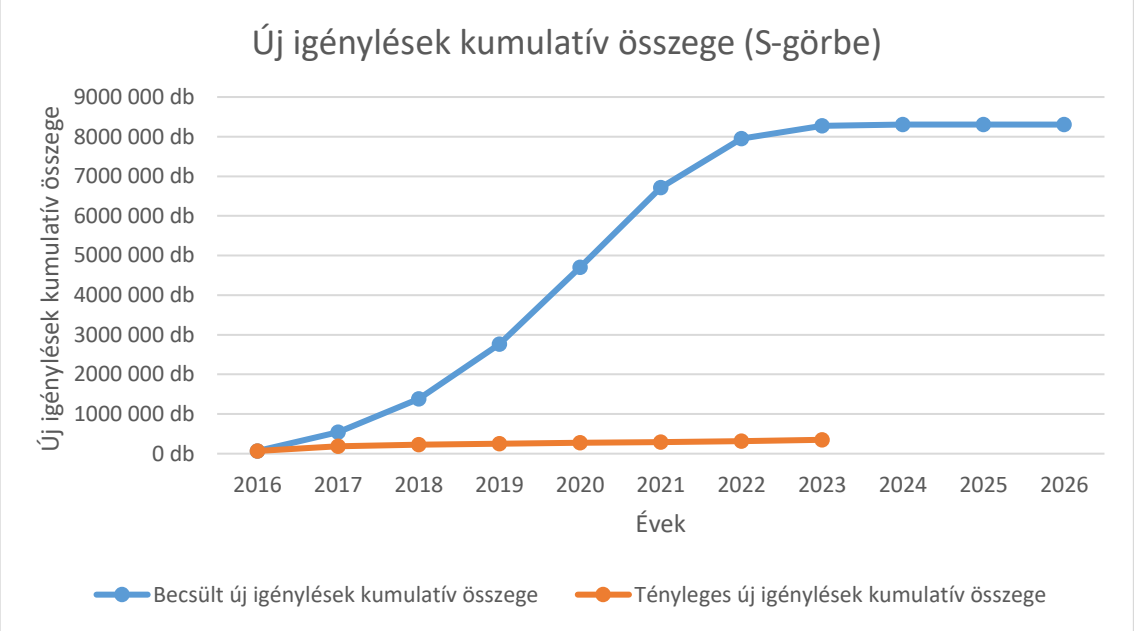
adatsorra [94] diffúziós görbét illeszteni, de nem illeszkedett, továbbá nem is igazán jó analógia az eSzemélyi igazolványra.

Igyekeztem továbbá a nemzetközi szakirodalomból q és p értékeket keresni referencia gyanánt, de az eSzemélyihez egyáltalában nem hasonlító innovációk merültek csak fel (például mikrohullámú sütő, elektromos autók). Annyi megállapítható, hogy q értéke tipikusan 0,01 és 1,5 között, p értéke pedig 0,0001 és 0,1 között mozog [83, 95]. Ebből kifolyólag kísérletezéssel próbáltam kiválasztani egy megfelelő q és p értéket az alábbiak szerint.

19. Táblázat A különböző forgatókönyvek paraméterezése, Forrás: saját szerkesztés

	Forgatókönyvek		
Paraméterek	**A**	**B**	**C**
Induló új igénylések	67 348 db	67 348 db	31 856 db
Innováció (p)	0,05	0,0035	0,25
Szájról szájra (q)	0,9	0,12	1,8
Befogadóképesség	8 304 909 db	8 304 909 db	8 304 909 db

Az alábbiakban három forgatókönyv modelljét fogom bemutatni, melyek paraméterezését a fenti táblázat (19. Táblázat) tartalmazza.



9. Ábra Meredek S-görbe 2026-ig, Forrás: saját szerkesztés

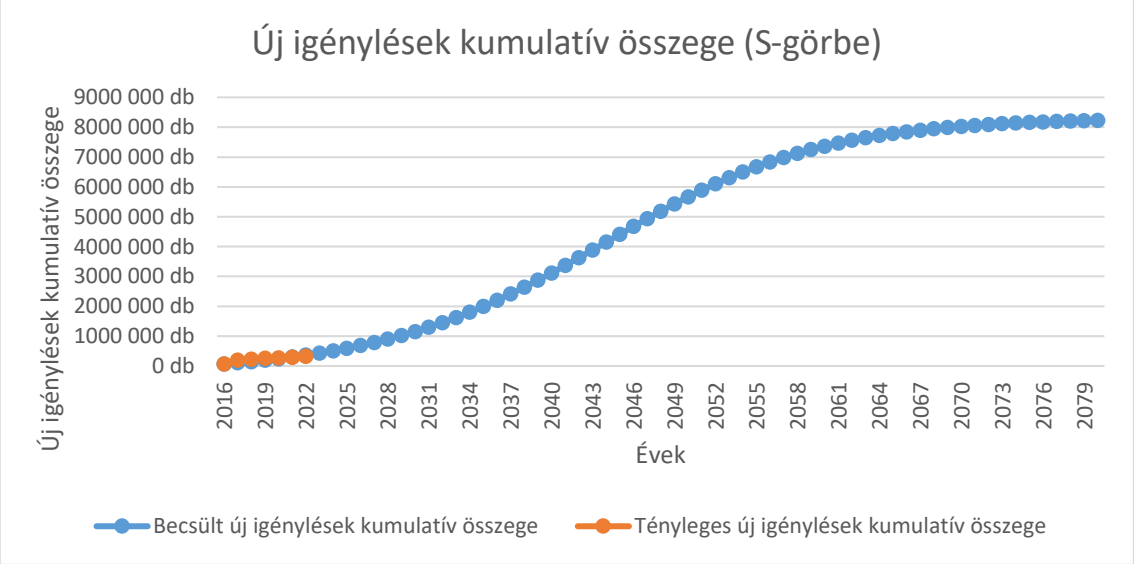
Tegyük fel, hogy a 2016-os induló új elektronikus aláírással igényelt eSzemélyi igazolványokkal számolva 2026 lett volna a céldátum (vö. Nemzeti Digitális Állampolgárság Program tervezett határideje) a teljes diffúzió elérésére az ideális Rogers-féle S-görbe lefutását követve, lásd 9. Ábra. P és q együtthatók (19. Táblázat – „A”

forgatókönyv) egyaránt viszonylag magas értéket képviselnek, ennek köszönhető a gyors indulás és emelkedés.

A valóság ettől azonban nagyon messze van, jól látható módon a tényleges igénylések száma lényegesen az ideális szint alatt maradt. A kritikus tömeget 2018-2019 között megközelítőleg 2 000 000 igénylésnél kellett volna elérnie a folyamatnak.

Pontosabban illesztve a becsült S görbe felszállás előtti szakaszát a tényleges igénylési adatokhoz 2016-2023 között az alábbiakat kapjuk. Lásd 19. Táblázat – „B" forgatókönyv és 10. Ábra.

Ebben a paraméterezésben p is q is viszonylag alacsony értékre kerültek beállításra. Ez azt fejezi ki, hogy az innovációt nem reklámozzák és szájhagyomány útján sem terjed igazán. Ez utóbbinak, mint tudjuk több oka is lehet (relatív előnyök hiánya, túl komplex stb.).



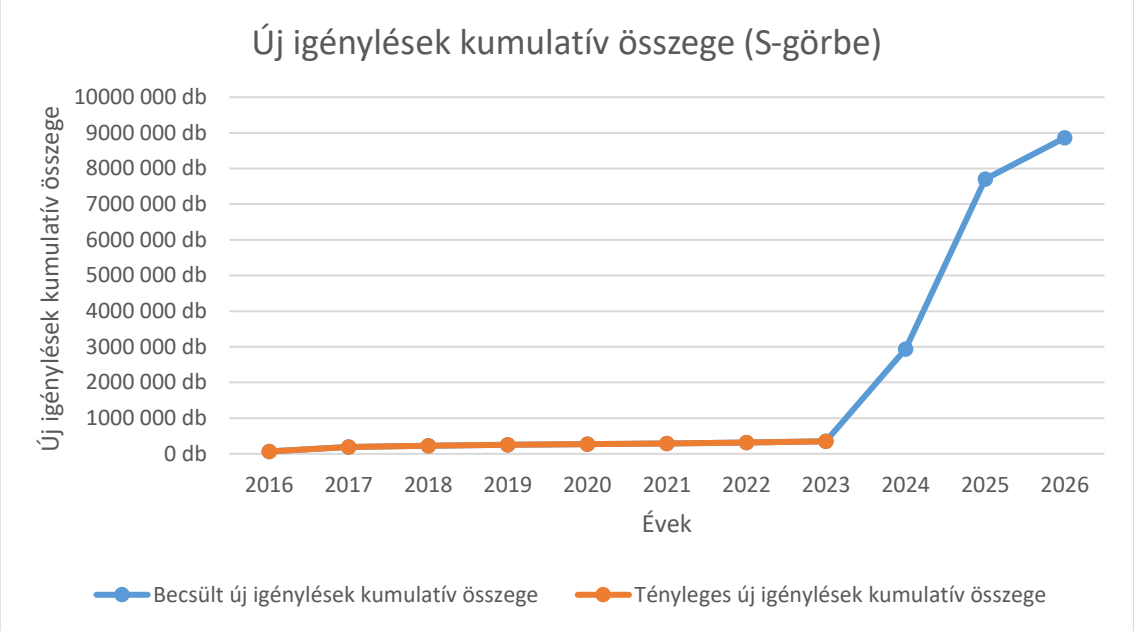
10. Ábra A tényleges igénylés adatokhoz legjobban illeszkedő S-görbe 2080-ig, Forrás: saját szerkesztés

A kritikus tömeg 2 000 000 és 3 000 000 darab körül alakulna 2037 környékén. A korábbiakban leírtakkal összhangban sajnos ez a modell látszólag elég jól közelít a valósághoz.

Figyelembe véve, hogy a digitális állampolgárság program a tervek szerint 2026-ra fogja elérni azt az állapotot, amikor az állampolgárok az ügyeik többségét digitális formában intézhetik, releváns az alábbi paraméterezésű Bass modell bemutatása is.

A p és a q értékek (19. Táblázat – „C" forgatókönyv) egyaránt magasak, ami azt jelenti, hogy az innováció erős promócióval megtámogatásra kerül és a szájhagyomány útján

való terjedési sebessége is elég magas. Az ábra szerint 2023 harmadik-negyedik negyedéve táján kellett volna elérni a kritikus tömeget 2 000 000-3 000 000 igényléssel.



11. Ábra Nagyon meredek S-görbe 2023. tényleges igénylési adataiból kiindulva 2026-ig, Forrás: saját szerkesztés

A digitális állampolgárság nyújtotta előnyök, a digitális adattárcából elérhető kényelmi szolgáltatások meghozhatják azt a változást az innováció tulajdonságaiban (relatív előny növekedése, komplexitás csökkenése), melyek akár jelentős mértékben is felgyorsíthatják a diffúziót.

3.4.4 Kommunikációs csatornák

Nincsenek műsoron az elektronikus igazolványt népszerűsítő tévé-, rádió- vagy internetes reklámok, az eSzemélyi.hu információs portálon viszont minden olyan információ megtalálható, amely a dokumentum képességeinek és használatának megismeréséhez szükséges. Kellő részletességgel bemutatja a dokumentum lehetséges felhasználási eseteit is [42].

2022-ben végzett kutatásomból (Nyári [2]) azonban kiderült, hogy az állampolgárok nem rendelkeznek elegendő információval a dokumentumról, és nem ismerik a fent említett információs portált sem. A kutatásban résztvevők kiemelték azt is, hogy a dokumentum felhasználása beágyazható tévésorozatok és filmek történetébe a népszerűsítése érdekében.

3.5 Összefoglalás

Számos elmélet létezik a technológiák elfogadottságának vizsgálatára, amelyek különböző fogalomrendszereket alkalmaznak. A technológiák elfogadottságát azonban csak akkor tudjuk vizsgálni, ha azok már elérhetők a potenciális felhasználók számára. Az eIDAS-kompatibilis magyar eID kártya jelensége más megközelítést igényel, mivel elektronikus funkciói nem ismertek a polgárok körében. Mint az a fejezetben kifejtettek alapján látható a Diffusion of Innovations elmélet teljes mértékben alkalmas az eSzemélyi igazolvány jelenségének modellezésére, így a jelenséget diffúziókutatási problémaként kell felfogni. Fentiek alapján a 3-as számú hipotéziseimet igazoltnak tekintem.

A szóban forgó innováció meglehetősen összetett és kevésbé kompatibilis a magyar állampolgárok által jelenleg használt megoldásokkal. A diffúziós folyamat még korai fázisban van, mivel az eAláírás funkcióval rendelkező okmányok száma még közel sem érte el a kritikus tömeget.

Az eddigi igénylési gyakoriságok előző évi adatai alapján több becsült diffúziós görbét is bemutattam a fejezetben, melyek azt mutatták, hogy az ideális lefutású S-görbétől sajnálatos módon messze van a valóság. Továbbá bemutattam azt is, hogy az új e-aláírással rendelkező eSzemélyi kérelmeknek milyen ütemben kellene növekedniük ahhoz, hogy az S-alakú görbe kialakuljon.

A leghatékonyabb és leggyorsabb terjedés elérése érdekében diffúziós tervet kell kidolgozni, ami feltétlenül szükséges ahhoz, hogy idővel az eSzemélyi elektronikus funkciói teljeskörűen elterjedjenek és a polgárok magabiztosan használhassák azokat.

Jelen fejezetben bebizonyítottam, hogy az eSzemélyi igazolvány széleskörű elterjedésének fő akadályozója a nem megfelelően előkészített diffúzió. Mint azt fentebb olvashattuk a szükséges tájékoztató anyagok nem ismertek széles körben, nincs megfelelő szintű jelenléte a megoldásnak a különféle tömegkommunikációs csatornákon, valamint az innováció maga sem elég „erőteljes”, a Rogers-féle tulajdonságait áttekintve több helyen is hiányosságokkal küzd.

A fentebb bemutatott statisztikákat felhasználva bizonyítottam, hogy az igényelt eAláírással rendelkező eSzemélyi igazolványok száma nem éri el a Rogers-féle kritikus tömegnek megfelelő szintet. Ahhoz, hogy az okmány, mint innováció terjedése önfenntartó folyamattá váljon, az elkövetkező években a többszörösére kellene emelkedni

az évenkénti elektronikus funkciókkal igényelt személyazonosító igazolványok számának.

Új tudományos eredményként kiegészítettem a Rogers-féle innovációfogalmat az „azonosított kockázat” összetevővel, amely a vizsgált innováció fejlesztésekor, bevezetésekor végzett kockázatértékelés eredményeként feltárt kockázatok összessége. Jelentősége abban rejlik az érzékelt kockázathoz képest, hogy az innováció felhasználói által érzékelt kockázat és a valós kockázatok nem minden esetben vannak összhangban.

4 AZ ESZEMÉLYI IGAZOLVÁNY TERJEDÉSÉT SEGÍTŐ DIFFÚZIÓS TERV

Az előbbi fejezetben kifejtettem a megfeleltetést a DOI fogalmai és az eSzemélyi igazolvány, mint innováció között. Amint az jól látszik a keretrendszer alkalmas az eSzemélyi igazolvány jelenségének modellezésére.

Célom jelen fejezetben a korábban felvázolt modell alapján egy olyan diffúziós terv megfogalmazása – felhasználva a releváns szakirodalmat –, amely segíthet a szóban forgó innováció elterjedésében – figyelembe véve természetesen a Diffiusion of Innovations elméletben felhalmozódott több évtizedes tapasztalatot is.

4.1 A diffúziós terv áttekintése

Az 5. számú függelékben összefoglalom a megalkotott diffúziós terv leglényegesebb lépéseit madártávlatból, a következő szakaszokban pedig részletekbe menően kifejtem azokat.

A diffúziós terv a diffúziós folyamat minden elemét érinti. Az eSzemélyi igazolvány innováció-tulajdonságainak megváltoztatásával vonzóbbá tenné magát az okmányt a potenciális elfogadók számára. A társadalmi rendszer tekintetében beazonosításra és bevonásra kerülnének a véleményvezérek. A változásképviseletek nagyobb fokú bevonásával és a változásközvetítők képzésével tovább lehetne gyorsítani a terjedési folyamaton. A potenciális elfogadók biztonságtudatos képzése is létfontosságú a sikeres diffúzió szempontjából.

Mivel a diffúziós folyamat fókuszában az innováció áll, ezért az első és legfontosabb lépés az innováció megváltoztatása. Ezt olyan módon kell végrehajtani, hogy az a lehető legnagyobb mértékben támogassa a potenciális elfogadók mindennapi életét a lehető legkisebb ráfordítással (idő, pénz, energia).

4.1.1 Az innováció megváltoztatása (1. lépés)

Ebben a részben az innovációt és annak tulajdonságait fogom újra áttekinteni – de ezúttal olyan nézőpontból, hogyan lehetne javítani azokon.

A korábbiakban láthattuk, hogy az eSzemélyi igazolvány tulajdonságai/adottságai nem igazán előnyösek a diffúziós folyamat szempontjából. Jelen szakasz ezen hátrányok enyhítésére tesz javaslatokat. Először is ki kell alakítani a vizsgált innováció terjedéséhez szükséges infrastrukturális feltételeket.

4.1.1.1 Kipróbálhatóság növelése (1.1. allépés)

A kipróbálhatóság az igénylési folyamatba lenne beépíthető. Az igénylés végén az okmány átvételét az állampolgár akár az új eSzemélyi igazolványára telepített minősített tanúsítvánnyal, elektronikus aláírással is hitelesíthetné – ezzel biztosítva az első gyakorlati felhasználását az okmány elektronikus funkcióinak.

Továbbá a Kormányablakokban az eSzemélyi funkciónak használat közben való bemutatására szolgáló, homokozó (sandbox) üzemmódban futó kioszkok is telepíthetők lennének. Gyakorolni lehetne rajtuk az elektronikus azonosítást, az elektronikus aláírást – természetesen úgy, hogy a kilépést követően minden létrehozott fájl automatikusan törlődik.

Egy ilyen megoldás kialakításához felhasználható lenne a Funke és Senger [96] által 2014-ben bemutatott PersoSim nevű nyílt forráskódú, eID szimulációra használatos szoftver. A szimulált eID kártya egy virtuális kártyaolvasón keresztül tud csatlakozni a különféle eID-t alkalmazó szolgáltatásokhoz. A német elektronikus személyazonosító igazolványhoz („neuer Personalausweis” Új Személyi igazolvány) illesztve készítették. Alapvetően eID megoldások fejlesztéséhez és fejlesztői teszteléséhez készült a szoftver, éppen ezért egy homokozó üzemmódú, a kipróbálhatóságot fokozó megoldás fejlesztéséhez is hasznos lenne.

4.1.1.2 Komplexitás csökkentése (1.2. allépés)

Az eSzemélyi igazolvány, figyelembe véve a használatához szükséges szoftver és hardver követelményeket, egy komplex innováció, amint azt korábban bemutattam.

A hardverkövetelmények a 2022-es évtől kedvező irányba változtak, hiszen már lehetséges a fizikai kártyaolvasó készülék helyett NFC képes mobileszközt és az eSzemélyiM alkalmazást használni az okmányon tárolt adatok kiolvasásához. Ez a hardveres egyszerűsödés azonban a szoftveres követelmények oldalán hátrányosan jelentkezett, ugyanis eggyel több szoftver feltelepítése szükséges.

Összesen négy különböző szoftver telepítése szükséges az elektronikus aláírás használatához, ebből hármat a PC-re és egyet a mobileszközre kell telepíteni.

Először is szükség van az „eSzemélyi Kliens Kártyakezelő Alkalmazásra”, ami a kártyaolvasó segítségével az okmányon tárolt adatok kiolvasására alkalmas. Hardveres kártyaolvasó használata esetén is szükséges, hogy telepítsünk egy további szoftvert, a

kártyaolvasó készülék meghajtóprogramját, ilyen driver installálása azonban az eSzemélyiM mobil alkalmazás használata mellett is elvárt.

Manapság igen elterjedtek az erre a célra is alkalmas mobileszközök, így a potenciális felhasználók már csak anyagi megfontolásokból is ésszerű választásnak tarthatják a kártyaolvasók kiváltását mobileszközzel.

Ebben az esetben egy úgynevezett virtuális kártyaolvasó kerül telepítésre a felhasználók számítógépére. A virtuális kártyaolvasó és az NFC képes mobiltelefon közös WIFI hálózaton keresztül csatlakozik egymáshoz.

A kapcsolat beállításához szükség van az eSzemélyi Kliens alkalmazást futtató PC IP címére és a port számra, a csatlakozáshoz ezeket az adatokat az eSzemélyiM mobil alkalmazásban meg kell adni. Ennek kiváltására szolgál a „Virtual Smart Card QR generator" nevű alkalmazás, amely egy további szoftver, ami szükséges az eSzemélyi használatához.

A QR generator a https://api.qrserver.com/ webszolgáltatás segítségével egy olyan, az eSzemélyiM mobilalkalmazással beolvasható QR kódot generál, amely tartalmazza a csatlakozáshoz szükséges adatokat (IP cím és port szám).

A mobileszközön az NFC kapcsolatnak bekapcsolva kell lennie és ugyanarra a WIFI hálózatra kell csatlakoznia, mint az eSzemélyi Klienst futtató PC-nek. A sikeres csatlakozást követően az eSzemélyi okmányt a mobileszköz NFC érzékelőjének hatótávolságában tartva az eSzemélyi Kliens alkalmazás már képes a különböző kártyaolvasást igénylő műveletek végrehajtására.

Ezekkel a szoftverekkel az elektronikus azonosítás és az okmányadatok kiolvasása már használható, de ha az állampolgár az eAláírást is alkalmazni szeretné, akkor a Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver (KEAASZ) telepítése is szükséges.

Mint az fentiekből látszik, egy átlagos, felhasználói szintű informatikai tudással rendelkező állampolgár számára akár megoldhatatlan kihívást is jelenthet a szoftverek telepítése.

Legegyszerűbb megoldást egy olyan telepítőkészlet összeállítása jelenthetné, amely az összes az eSzemélyi igazolvány minden funkciójának használatához szükséges szoftvert és meghajtó programot tartalmazna.

További egyszerűsítést jelenthetne, ha a QR kód generátor komponens az eSzemélyi Kliens alkalmazás része lenne, ezzel is csökkenne a szükséges szoftverek száma.

Továbbá érdemes lenne megfontolni egy Service Discovery protokoll alkalmazását a virtuális kártyaolvasót futtató PC és az eSzemélyiM alkalmazást futtató mobileszköz közötti kapcsolat kiépítésére – így csak azokban a ritka esetekben lenne szükség a QR kód generálásra, amikor valamilyen oknál fogva mégis „kézi” konfigurációt igényel a kapcsolat kiépítése.

4.1.1.3 Kompatibilitás növelése (1.3. allépés)

A megszokott megoldásokkal való kompatibilitását illetően az eSzemélyi okmány legjobban talán az érintésmentes fizetésre alkalmas bankkártyákhoz hasonlít. Annyi különbség azonban mindenképpen van, hogy az okosokmányhoz két PIN kód is tartozhat – egyik az elektronikus azonosításhoz, a másik az elektronikus aláíráshoz.

A használati esetek hiányában azonban az állampolgároknak fel sem tűnik, hogy ez a megoldás hasonlít egy korábbihoz.

Ha több kártyaolvasó terminál lenne telepítve például postákon, gyógyszertárakban, Kormányablakokban, ahol az állampolgárok használhatnák az okmányukat küldemények átvételére, receptek kiváltására, felhasználó azonosításra, akkor a rutin részévé válhatna az okmány PIN kódjainak használata.

Más szempontból nézve viszont a hagyományos kézi aláíráshoz szinte semmilyen szempontból nem hasonlítható az elektronikus aláírás. Ezen a téren aláírópanelek alkalmazásával lehetne fokozni a kompatibilitást – hangsúlyozom – a komplexitás terhére. Ez abban nyilvánulhatna meg, hogy a PIN kód ellenőrzése helyett az eSzemélyi igazolványon rögzített aláírásmintával történő összevetés után váltódna ki az elektronikus aláírás funkció. Ez azonban további hardver és szoftvereszközök bevonását jelentené, ami növelné a komplexitást, és valószínűleg csak az idősebb generációk számára növelné a kompatibilitás érzetét.

4.1.1.4 Megfigyelhetőség növelése (1.4. allépés)

Az első pont a folyamatban, ahol a megfigyelhetőség javítható lenne, a személyes igénylési folyamat során jelentkezik. Az ügyintézők az igénylés befejezésekor akár egy, a saját eSzemélyi igazolványukkal hitelesített elektronikus dokumentumot is elkészíthetnének. Ezt oly módon kellene megvalósítani, hogy közben az igénylő egy külön monitoron megfigyelhesse, hogy mit kell csinálni a kártyával, a terminállal, és a

szoftverekkel az elektronikus aláírás létrehozásának érdekében. Ehhez szükséges lenne az SZTSZ kiterjesztése a kormányablaki ügyintézők részére, annak érdekében, hogy a szervezetben betöltött helyük is része legyen az elektronikus aláírásnak.

4.1.1.5 Relatív előny növelése (1.5. allépés)

A komplexitás csökkentése mellett a relatív előny növelése jelenthetné a legnagyobb húzóerőt az állampolgárok számára az innováció átvételére. További használati esetek kidolgozásával és bevezetésével nagyban javítható lenne az eSzemélyi igazolvány érzékelt relatív előny tulajdonsága. Olyan felhasználási eseteket kellene létrehozni, amelyek miatt igazán megérné az okosokmány elektronikus funkcióinak alkalmazását elsajátítani az állampolgároknak.

Elsőként ismét a Kormányablakokra térnék ki: időpontfoglalásra lehetőség van ügyfélkapu regisztráción keresztül. Ha a helyszínre érkezéskor használt sorszámhúzó berendezéseket alkalmassá tennék eSzemélyi okmány olvasására, akkor az időpontra érkezés tényét is jelezhetnék az állampolgárok az igazolványuk használatával. Nem egy e-mail üzenetben megküldött véletlenszerű kód megadására lenne szükség – ahogyan az jelenleg is működik, hanem a saját eAzonosításra szolgáló PIN kódjuk megadására az eSzemélyi igazolvány „érintését” követően.

Újabb példa, amely az államigazgatás keretein belül megvalósítható lenne: 2023 januárjában az állami alkalmazottakra bevezetett SZTSZ attribútum tanúsítvány szolgáltatás széleskörű kiterjesztése. Több olyan állami nyilvántartás is van, amelyek alapot képezhetnének az SZTSZ új felhasználói köreinek kiszolgálásához. Ezek a megoldások a kisvállalkozásokat a papírmentes működésre sarkallhatnák. Ilyen például az Egyéni vállalkozók nyilvántartása, vagy a Magyar Ügyvédi Kamara nyilvántartása. Ha az SZTSZ ezekből is képes lenne attribútum tanúsítványt hozzácsatolni az elektronikusan aláírt dokumentumokhoz, akkor egy egyéni vállalkozónak a papírmentes működéshez nem lenne szükséges piaci szereplőtől szervezeti tanúsítványt vásárolni.

A debreceni tömegközlekedésben és a MÁV-vonatokon már lehetséges eSzemélyi okmánnyal igazolni a bérlet vagy jegy érvényességét. A jegyet/bérletet mindkét esetben digitálisan kell megvásárolni, majd össze kell kapcsolni egy internetes felületen az eSzemélyi okmánnyal. Az állampolgárok jelentős részét ösztönözné az okmány használatára, ha ugyanez a BKK járatain is lehetséges lenne. A BKK jegy és bérletvásárlásra alkalmas automatáit is ki lehetne egészíteni az eSzemélyi olvasásához

szükséges funkciókkal ezzel akár azt is lehetővé téve, hogy eleve az okmánnyal összerendelt módon vásároljanak az utasok jegyeket/bérleteket.

Megfontolandó lenne a többi, jelenleg használatban levő hatósági igazolvány kiváltása az eSzemélyi igazolvánnyal, beleértve a diákigazolványt, a lakcímkártyát, a vezetői engedélyt, az adókártyát, valamint a TAJ-kártyát. A TAJ szám, az adóazonosító jel és a lakcímadatok már jelen állás szerint is rajta lehetnek az okosokmány tárolóelemén, a diákigazolvány és a vezetői engedély adataival kellene kibővíteni. Természetesen ennek igen jelentős infrastruktúra fejlesztési vonatkozásai is jelentkeznének. Ennek részletei már azonban már túlmutatnak jelen értekezés keretein.

Az eSzemélyiM mobilalkalmazást is ki lehetne egészíteni további funkciókkal, mint például elektronikus aláírással és aláírás ellenőrzéssel, így közvetlenül egy mobileszközön is keletkeztethetők lennének elektronikusan aláírt dokumentumok.

Számos további használati esetet lehetne megalkotni az okmányhoz, mint például az olvasójegyek kiváltása a könyvtárakban, elektronikus fizetés stb.

További nagy előny lenne, ha digitális pénztárcákba fel lehetne venni az okmányt. Ennek megvalósításával vélhetően nagyban fogja növelni a megoldás relatív előnyét az 1.1.2. szakaszban említett Európai Digitális Identitás és a Nemzeti Digitális Állampolgárság Program (1.9. alfejezet).

4.1.1.6 Újrafelhasználhatóság növelése (1.6. allépés)

Valószínűsítem, hogy az újrafelhasználhatóság valamelyest javulna, ha újabb és újabb használati esetek jönnének létre, de ez a jogszabályi környezet miatt csak korlátozott mértékben jelentkezne. Még ha találnak is az állampolgárok egy új felhasználási módot, amire a fejlesztők nem gondoltak, amíg annak szabályozási keretei nincsenek kialakítva, addig az hivatalosan úgysem lenne alkalmazható.

4.1.1.7 Érzékelt kockázatok kezelése (1.7. allépés)

A magyar lakosságra reprezentatív mintán szükséges lenne vizsgálni az eSzemélyi igazolvánnyal és használati eseteivel kapcsolatosan érzékelt kockázatokat, melyeket aztán össze kellene vetni a korábbi kockázatértékelés során azonosított kockázatok listájával. Az érzékelt kockázatok kezelése a diffúzió gyorsítására nagyobb hatást gyakorolna, mint az azonosított kockázatok kezelése. Az azonosított kockázatok kezelése pedig a megoldás biztonságához járulna hozzá nagyobb mértékben.

Két PIN kód tartozhat egy eSzemélyi igazolványhoz: eAzonosítás PIN és eAláírás PIN. Az előbbi pontosan hat, az utóbbi pontosan hét számjegy hosszú. A mai számítási kapacitásokat figyelembe véve a brute force támadásoknak eléggé kiszolgáltatottak a rövid jelszavak, PIN kódok. Az eSzemélyi esetében három-három próbálkozása van a felhasználónak a PIN kódok sikeres megadására, így a brute force támadás lehetősége gyakorlatilag ki van zárva.

Más módszerek alkalmazásával sokkal valószínűbb a PIN kódok támadók általi megismerése (egy lelesés begépelés közben, keylogger, social engineering stb.). Különösen fontos lenne a biometrikus azonosítás beépítése a rendszerbe. Az eSzemélyiM app használhatná akár mobileszközbe rögzített ujjnyomatos bejelentkezést is.

Ezt támasztja alá Szádeczky [16] írása is, melyben kiemeli a különféle biometrikus jellemzők (ujjnyomat, arckép stb.) lehetséges személyazonosítási felhasználásait az elektronikus személyazonosító okmányok (útlevél, eSzemélyi igazolvány) esetén.

Az eSzemélyiM és a PC összeköttetéshez közös WIFI hálózatra van szükség. Az eSzemélyiM mobil alkalmazást célszerű lenne olyan funkcionalitással kiegészíteni melynek keretében megbízhatóként jelölhetne meg a felhasználó egy WIFI hálózatot a csatlakozáskor és figyelmeztető üzenetet kapna, ha nem megbízható vezetéknélküli hálózatra csatlakozik.

4.1.1.8 Azonosított kockázatok kezelése (1.8. allépés)

Az azonosított kockázatok listáját össze kell vetni az érzékelt kockázatok listájával és a prioritási sorrend felállításakor figyelembe kell venni, hogy mely kockázati forgatókönyvek jelentek meg mindkét listában. A diffúzió gyorsítása érdekében az azonosított kockázatok kezelése során nagyobb prioritást kellene adni azoknak a kockázati forgatókönyveknek, melyek érzékelt kockázatként is megjelennek, hiszen ezek kezelése közvetlenül befolyásolná a felhasználók attitűdjét a megoldáshoz.

Természetesen ez nem azt jelentené, hogy a felhasználók által súlyosnak érzékelt, de valójában alacsony kockázati szintű forgatókönyveket felelőtlenül a valós veszélyeket rejtő forgatókönyvek elé soroljuk, de minden bizonnyal meg lehetne találni azt az arany középutas megoldást, amely kellőképpen járul hozzá a megoldás általános biztonságához és fokozza a felhasználók bizalmát a megoldás irányába.

4.1.2 Véleményvezérek azonosítása (2. lépés)

Be kell azonosítani az eSzemélyi igazolvány diffúzióját legjobban segíteni képes véleményvezéreket, hogy segítségükkel aktívan és hatékonyan előmozdítsuk a kártya előnyeinek terjedését.

Mivel a véleményvezérek a diffúziós folyamat több pontján is bekapcsolódhatnak az elfogadási ütem felgyorsításába, ezért az első és legfontosabb lépés azon közszereplők, hírességek beazonosítása, akik az állampolgárok szemében hitelesen tudják közvetíteni a szóban forgó innováció előnyeit. Erre láthattunk példát a COVID vakcinákat népszerűsítő kampány esetében is, amikor Győrfi Pált, az Országos Mentőszolgálat szóvivőjét alkalmazták a figyelemfelhívások, új információk közlésére [97].

Egy bizonyos időközönként megismételt, intenzív reklámkampány jelentős mértékben segítené elő az okosokmány használatának terjedését, feltéve, hogy a megfelelően kialakított infrastruktúra és a kellő relatív előnyt biztosító használati esetek rendelkezésre állnak.

4.1.3 Változásképviseletek és változásközvetítők beazonosítása (3. lépés)

A változásképviseletek és közvetítők beazonosítása és hathatós alkalmazása jelentősen felgyorsíthatná az eSzemélyi igazolvány terjedését.

Ahogyan azt korábban említettem a két legfőbb változásképviselet Magyarország Kormánya és a Kormányablakok. A fentebb kifejtettem, hogy további használati esetek kialakítására lenne szükség, amit a mindenkori magyar kormány akár a jogszabályi környezet alakításával és különböző támogatási programokkal is elősegíthetne.

A Kormányablakok ugyancsak fontos szereplők ebben a diffúziós folyamatban, hiszen az ott dolgozókon keresztül juthatnak első kézből információhoz az állampolgárok az eSzemélyi igazolványról. A Kormányablakokban kialakított megfelelő infrastruktúra és ügymenet szintén elősegíthetné a terjedést. Úgy kellene kialakítani a munkafolyamatokat, hogy az igénylés során úgy az ügyintézőnek, mint az igénylőnek szükséges legyen használnia a saját elektronikus okmányát.

4.1.3.1 Változásközvetítők képzése (3.1. allépés)

A Kormányablak dolgozói, mint kommunikációs csatornák vagy véleményvezérek is alkalmazhatók lennének a potenciális elfogadók különféle csoportokba tartozásától függetlenül. Az igénylési folyamat a legkézenfekvőbb pont, ahol az okmány használatához szükséges információk az állampolgárok részére átadásra kerüljenek.

További előnye, hogy nem igényel különösebb anyagi ráfordítást, mint például a sokat emlegetett reklámkampányok, mindössze annyi szükséges, hogy az ügyintézők megkapják a szükséges ismeretanyagot, melynek birtokában meggyőzően tudják népszerűsíteni az okosokmányt.

Az ügyintézők az eSzemélyi igazolvány irányába tanúsított attitűdjét is formálni lenne szükséges, de ez a téma már igazán túlmutat jelen disszertáció tartalmi és tematikus keretein egyaránt.

4.1.4 A potenciális elfogadók biztonságtudatosságot szem előtt tartó képzése (4. lépés)

Ahogyan azt korábban, a 3.4.2. szakaszban meghatároztam az eSzemélyi igazolvány kontextusában a társadalmi rendszer a teljes magyar társadalom, a potenciális elfogadók pedig a 14. életévüket betöltött eSzemélyi igazolvány és elektronikus aláírás igénylésére és használatára jogosult magyar állampolgárok.

A nemzeti köznevelésről szóló törvény [98] alapján Magyarországon alapszabályként a 6-16 éves kor közöttiekre vonatkozik a tankötelezettség. Nem lehet elégszer hangsúlyozni az információbiztonsági tudatosságra nevelés fontosságát. Az általános iskola utolsó évében és a középiskolai oktatás éveinek tantervébe célszerű lenne bevezetni az eSzemélyi igazolvány, az elektronikus közigazgatási szolgáltatások használatának bemutatását. Így a tanulók olyan tudásra tehetnének szert érettségiig, amely később nagyban megkönnyítené a mindennapjaikat, amikor közigazgatási ügyeket kell majd intézniük. Az eKözigazgatási szolgáltatások a közoktatásban való szerepeltetését Zámbó [55] is hangsúlyozta.

Ezt tovább lehetne folytatni a felsőoktatásban, ahol lehetőséget kellene biztosítani arra, hogy a hallgatók szabadon választható tantárgy keretében ismerkedhessenek az elektronikus közigazgatás lehetőségeivel.

4.1.5 Az eSzemélyi igazolvány jelenlétének fokozása a tömegkommunikációs csatornákban (5. lépés)

Fontos, hogy a különböző korosztályba tartozó potenciális elfogadók a számukra leginkább hiteles forrásból értesülhessenek az okosokmány képességeiről. Az eszemelyi.hu információs portál minden szükséges információt tartalmaz, azonban – ahogyan azt korábban is említettem már – az állampolgárok sok esetben még a portál létezésével sincsenek tisztában.

A modern trendeket lekövetve nem csak a tömegmédiában, hanem a közösségi médiákban is hirdetni kellene az eSzemélyi igazolványt és annak előnyeit. A korábban már említett, véleményvezérként beazonosított személyeknek a különféle, manapság széleskörben népszerű videómegosztó portálokon is közzé kellene tenniük olyan tartalmakat, amelyek az okosokmány használatára buzdítanak.

Ezzel kapcsolatosan már a korábban többször említett kutatásom (Nyári [2]) során is merültek fel ötletek. Elhangzott ugyanis, hogy TV sorozatokon, mozifilmeken keresztül is lehetne népszerűsíteni az okosokmányt.

Az országmárka fogalmát Nagy Beáta [99] az alábbiak szerint határozta meg: „A márka fogalmában említett név, kifejezés, külalak, szimbólum vagy egyéb sajátos vonások összessége nem csak termékre vagy szolgáltatásra, hanem országokra is hasonlóképpen értelmezhető. Hiszen az egyes államok és nemzetek is rendelkeznek szimbólummal, névvel, márkás nemzeti termékekkel, melyek által megkülönböztethetők más országoktól.”

Silva Novais [100] a 2023-as diplomamunkájában a TV sorozatok országmárkára (nation brand) gyakorolt hatását vizsgálta. Tanulmányából látszik, hogy a különféle sorozatokban vizuálisan szerepeltetett országmárka-élmény pozitív hatást fejt ki a fogyasztók magatartási szándékaira.

Dadashzadeh [101] az USA eKormányzati szolgáltatásai vonatkozásban azt írja a közösségi média megjelenésekkel kapcsolatosan, hogy a közösségi média eszközei jól használhatók a nagy tömegekkel való információcserére, továbbá hozzájárulhatnak az adott ügynökség céljainak eléréséhez felhasználva a nyilvánosság „kollektív találékonyságát”. Az egyéb kommunikációs csatornákhoz képest gyakran költségmegtakarítást is eredményezhet. Szerinte azonban a közösségi médiák igazi ereje a megszólított közönség fokozottabb elköteleződésében rejlik.

Írásában Dadashzadeh [101] bemutat egy stratégiai tervezési megközelítést, amelynek segítségével a közösségi média beruházások tervezhetők – mint ahogyan minden egyéb informatikai beruházást is szükséges tervezni. Javaslata szerint ésszerű „kicsiben kezdeni”, hogy tapasztalati úton kiderüljön, mely kezdeményezések működnek és melyek nem.

A mozgóképek pozitív hatásait a márkaépítésre és a közösségi média csatornák előnyeit az eSzemélyi igazolvány esetében is ki lehetne használni, a fentebb említett tanulmányok eredményeit megfelelőképpen átültetve.

A korábban említett TV és rádió hirdetésekhez hasonlóan a TV műsorok is felhasználhatók lennének az okosokmány népszerűsítésére. Célszerű lenne szappanoperák, mozifilmek történetének szerves részévé tenni az eSzemélyi igazolvány használatát.

Meg kell találni azt a történetet, melynek folyamába észrevétlenül bele lehet szőni az okosokmányt. Továbbá azonosítani kell azokat a színészeket, híresség̈eket, akik a lakosság számára hitelesen el tudják mondani az innovációval kapcsolatos információkat. A teljes részletességgel való kidolgozás azonban túlmutat jelen disszertáció keretein.

4.2 Összefoglalás

A fejezetben bemutattam egy lehetséges, az eSzemélyi igazolvány és elektronikus funkcióinak terjedését segítő diffúziós tervet, mely alapján többek között oktatási és reklám kampányokkal kellene népszerűsíteni az okosokmány elektronikus funkcióit és előnyeit. A fejezetben bizonyítottam továbbá, hogy az eSzemélyi, mint innováció Diffusion of Innovations szerinti tulajdonságait módosítani kell a terjedés gyorsítása érdekében többek között az alábbiak szerint:

a. komplexitás: a támogató szoftverrendszer egyszerűsítése
b. relatív előny: új, jól dokumentált és népszerűsített használati esetek bevezetése
c. megfigyelhetőség: már az igénylési folyamat során a kormányablaki dolgozók használhatnák a saját eSzemélyi igazolványukat.

A Nemzeti Digitális Állampolgárság Program vélhetően számos olyan változást fog hozni az innováció éppen a fent felsorolt jellemzőiben, melyek jótékony hatással lehetnek majd a terjedés ütemére. Annak hatásait a megjelenést követően kell majd értékelni.

A diffúziós terv végrehajtása során külön figyelmet érdemel az érzékelt kockázatok felmérése, mert ezek azonosítása, megértése és szükség esetén kezelése nagyban hozzájárulna a diffúzió felgyorsításához.

Ezek alapján a 4-es számú hipotéziseimet igazoltnak tekintem.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Az értekezés az eSzemélyi igazolvány előzményeinek áttekintésétől kezdődően bemutatta az eSzemélyi igazolványban rejlő lehetőségeket, az elterjedtségének jelenlegi helyzetét és a továbbfejlesztési irányokat. Bemutatásra került, hogy az SZTSZ szolgáltatás alá bevont alapnyilvántartások körének kibővítésével olyan további jogosulti csoportok alkalmazhatnák a szervezetben betöltött hely igazolására szolgáló attribútumtanúsítványokat, melyek számára kézenfekvő és anyagilag is előnyös lehetne az eSzemélyi elektronikus aláírás funkció használata.

Ezt követően ismertettem egy módszert az ISO/IEC 27005:2022 nemzetközi kockázatkezelési szabványban újonnan bevezetett eseményalapú megközelítés alkalmazására az eSzemélyi igazolvány vonatkozásában.

A kockázatértékelés külső és belső kontextusának, valamint a különböző kockázati kritériumok meghatározását követően a kockázatértékelés végrehajtása során először ún. stratégiai szcenáriók megfogalmazásával, az egyes kockázati forrásokból eredő magas absztrakciós szinten leírt forgatókönyvek és azok következményei kerültek listázásra. Ezt követően ismertettem, hogy a stratégiai szcenáriók hogyan bonthatók alá az azok megvalósítására alkalmas operatív szcenáriókra, melyek a támadók motivációjával, az érintett elsődleges és támogató vagyontárgyak, valamint a bekövetkezés valószínűségével együtt kerültek meghatározásra.

Egy stratégiai és egy operatív szcenárió páros meghatároz egy kockázati szcenáriót, melynek szintje a kockázati szint mátrix alapján egyértelműen meghatározható. A kiszámított kockázati szint alapján lehetséges a kockázat elfogadásáról vagy kezeléséről való döntés meghozatala.

Majd azt mutattam be, hogy az eSzemélyi igazolványra, mint innovációra tekintve alkalmazható a Everett M. Rogers-féle Diffusion of Innovations elmélet fogalomrendszere. Először is bemutattam magát a keretrendszert, majd annak kontextusába helyezve értelmeztem az eSzemélyi igazolvány eddigi eseményeit, jelenlegi helyzetét. A Bass-modell alkalmazásával készítettem különféle paraméterezések mellett az S-görbe lefutására lehetséges forgatókönyveket.

Ahogyan azt korábban is írtam, Rogers modelljében az innováció jellemzői közé korábban javasolták a kutatók az „érzékelt kockázat” felvételét. Ehhez képest egy további jellemzővel javaslom kibővíteni a Diffusion of Innovations elmélet innováció fogalmát,

az „azonosított kockázat”-tal. Ez azért szükséges, mert a felhasználók által érzékelt kockázat nem mindig esik teljesen egybe a valódi kockázatokkal.

Végül ismertettem egy lehetséges diffúziós tervet, amely elősegíthetné az eSzemélyi igazolvány diffúzióját az innováció jellemzőinek megváltoztatásával, véleményvezérek bevonásával, valamint érzékelt és azonosított kockázatok kezelésével.

Új tudományos eredmények

1. Összefoglaltam a személyazonosító okmányok fejlődéstörténetét, az eSzemélyi igazolvány jelenlegi helyzetét és tervezett továbbfejlesztési irányait.
2. Bebizonyítottam, hogy az eSzemélyi igazolvány elektronikus aláírás funkcionalitása az SZTSZ használatával alkalmazható lenne kormányablaki dolgozók, orvosok, ügyvédek, egyéni vállalkozók számára hivatalos ügyekben, jogkörükben eljárva.
3. Elkészítettem az eSzemélyi igazolvány átfogó, kliens oldali kockázatelemzését az ISO/IEC 27005:2022-ben bevezetett új, eseményalapú megközelítés alkalmazásával. Beazonosításra kerültek az eSzemélyi igazolvány lehetséges támadói, azok céljai, motivációi.
4. Újrarendszereztem az eID rendszerekkel kapcsolatosan a hazai és a nemzetközi szakirodalomban ismertetett kockázati kategóriákat az ISO/IEC 27005:2022 szabvánnyal összhangban.
5. Bemutattam, hogy az eSzemélyi igazolvány kombinálható lenne biometrikus azonosítással, ami nagyban növelné a megoldás biztonságát.
6. Bebizonyítottam, hogy az eSzemélyi igazolvány és elektronikus funkcióinak terjedése felfogható diffúziókutatási problémaként.
7. Bebizonyítottam, hogy az eSzemélyi igazolvány széleskörű terjedésének legfőbb akadályozója a nem megfelelően előkészített diffúzió.
8. Bemutattam, hogy az igényelt eSzemélyi igazolványok száma nem érte el a Diffusion of Innovations elmélet szerinti kritikus tömeg értékét.
9. Bemutattam az eSzemélyi igazolvány és elektronikus funkcióinak terjedését segítő diffúziós tervet.
10. Bebizonyítottam, hogy az eSzemélyi, mint innováció Diffusion of Innovations szerinti tulajdonságait módosítani kell a terjedés gyorsítása érdekében az alábbiak szerint:
    a. komplexitás csökkentése

b. kompatibilitás növelése
c. relatív előny növelése
d. megfigyelhetőség, kipróbálhatóság növelése
e. érzékelt kockázatok kezelése
f. azonosított kockázatok kezelése
g. újrafelhasználhatóság növelése

Ajánlások

Értekezésemet ajánlom olyan információbiztonsággal foglalkozó szakemberek részére, akik hasonló területen dolgoznak. Az eredmények hasznosak lehetnek biztonsági okmányok tervezésével, kivitelezésével foglalkozó szakemberek számára is.

Az eredményeim felhasználhatók továbbá más kutatók, doktoranduszok számára is, akik akár további kutatásokat is végezhetnek a közölt eredmények alapján. Ajánlom továbbá egyetemi oktatók figyelmébe is, akik az oktatási tevékenységük során is felhasználhatják bizonyos részeit.

Az eredmények hozzájárulhatnak az eSzemélyi igazolvány, a Digitális Állampolgárság hatékonyabb népszerűsítéséhez is.

További kutatást igénylő területként kiemelném az eSzemélyi igazolvány használata során érzékelt kockázatok vizsgálatát a magyar társadalomra nézve, egy reprezentatív mintán. Ezen kívül a Nemzeti Digitális Állampolgárság Program innovációinak diffúzója – szem előtt tartva az információbiztonsági szempontokat – is felmerülhet kutatási témaként.

IRODALOMJEGYZÉK

[1] *The European Parliament and The Council of The Euroepean Union, "REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Official Journal of the European Union, 23 07 2014.,* 2014.

[2] N. Nyári, „Az eszemélyi és az elektronikus aláírás technológia helyzete és lehetőségei magyarországon," Biztonságtudományi szemle, 4. kötet, 2. szám, pp. 61-73, 2022.

[3] Belügyminisztérium, „eSzemélyi - Miért hasznos az eSzemélyi," [Online]. Available: https://eszemelyi.hu/az-eszemelyi/#miert-hasznos-az-eszemelyi. [Hozzáférés dátuma: 14 03 2024].

[4] E. M. Rogers, Diffusion of Innovations (5th edition), New York: Free Press, 2003.

[5] Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság, „Statisztikák," [Online]. Available: https://nyilvantarto.hu/hu/statisztikak. [Hozzáférés dátuma: 19 02 2024].

[6] N. Nyári és A. Kerti, „Selecting a suitable framework for modelling the spread of the Hungarian eID card," Interdisciplinary Description of Complex Systems, 22. kötet, 1. szám, pp. 129-141, 2024.

[7] R. Hall, G. Dodds és S. Triggs, The World of William Notman: The Nineteenth Century Through a Master Lens, Boston: David R. Godine Publisher Inc., 1993.

[8] J. Doulman és D. Lee, Every Assistance & Protection A History of the Australian Passport, Sydney: THE FEDERATION PRESS, 2008.

[9] M. Michael és K. Michael, Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants, New York: Information Science Reference, 2009.

[10] Lee, Henry C.; Ramotowski, Robert; Gaensslen, R.E. eds., Advances in Fingerprint Technology 2nd edition, New York: CRC Press, 2001.

[11] „Leauge of Nations Photo Archive," [Online]. Available: https://web.archive.org/web/20110719215431/https://bl-libg-doghill.ads.iu.edu/league-web/book/p63.html. [Hozzáférés dátuma: 20 02 2024].

[12] J. Doulman és D. Lee, Every Assistance & Protection A History of the Australian Passport, Sydney: THE FEDERATION PRESS, 2008.

[13] *ISO/IEC 7810:2019 Identification cards — Physical characteristics,* 2019.

[14] *ISO/IEC 7816-1: Cards with contacts — Physical characteristics,* 2011.

[15] *ISO/IEC 14443-1:2018 Cards and security devices for personal identification — Contactless proximity objects — Part 1: Physical characteristics,* 2018.

[16] T. Szádeczky, „Enhanced Functionality Brings New Privacy and Security Issues – An Analysis of eID," Masaryk University Journal of Law and Technology [Vol. 12:1, 12. kötet, 1. szám, pp. 3-27, 2018.

[17] *Howley v. Whipple, 48 N.H. 487,* 1869.

[18] B. Wright, „Fax Pacts," Law Prac. Mgmt., 16. kötet, 1990.

[19] N. Nyári, „The Future of eIDAS in the Light of Post-Quantum Cryptography," Biztonságtudományi szemle, 4. kötet, 1. szám, pp. 91-103, 2022.

[20] A. S. Tannenbaum, Computer Networks, New Jersey: Pearson Education, 2003.

[21] N. Nyári, „The Impact of Quantum Computing on IT Security," Biztonságtudományi Szemle, 3. kötet, 4. szám, pp. 25-37, 2021.

[22] P. M. Erdősi, Az elektronikus aláírás mérése, Budapest: Nemzeti Közszolgálati Egyetem, 2019.

[23] ENISA, „eIDAS compliant eID Solutions,” 15 03 2020. [Online]. Available: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions. [Hozzáférés dátuma: 15 03 2024].

[24] Council of the European Union, „15149/23 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity,” 11 2023. [Online]. Available: https://data.consilium.europa.eu/doc/document/ST-15149-2023-INIT/en/pdf. [Hozzáférés dátuma: 20 02 2024].

[25] European Comission, „EU Digital Identity Wallet Pilot implementation,” 19 07 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation. [Hozzáférés dátuma: 20 02 2024].

[26] P. Nagy és J. Papp, „Személyazonosító okmányok a XIX-XX. századi Magyarországon,” *Hajdú-Bihar Megyei Levéltár Évkönyve XXIX,* pp. 401-427, 2002-2003.

[27] *253.600/1946. (VII. 30.) BM rendelet a bejelentési kötelezettség teljesitésének részletes szabályozása tárgyában,* 1946.

[28] *1982. évi 17. törvényerejű rendelet az anyakönyvekről, a házasságkötési eljárásról és a névviselésről,* 1982.

[29] *15/1991. (IV. 13.) AB határozat,* 1991.

[30] *1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról,* 1992.

[31] *A Magyar Népköztársaság Elnöki Tanácsának az állami népességnyilvántartásról szóló 1974. évi 8. számú törvényerejű rendelete,* 1974.

[32] *2/1978. (X. 28.) KSH A személyi szám, illetőleg a személyi lap kiadásáról és használatáról,* 1978.

[33] *1986. évi 10. törvényerejű rendelet az állami népességnyilvántartásról,* 1986.

[34] *25/1986. (VII. 8.) MT rendelet az állami népességnyilvántartásról szóló 1986. évi 10. törvényerejű rendelet végrehajtásáról,* 1986.

[35] *102/1990. (VII. 3.) MT rendelet az állami népességnyilvántartásról szóló 1986. évi 10. törvényerejű rendelet végrehajtásáról rendelkező 25/1986. (VII. 8.) MT rendelet módosításáról,* 1990.

[36] *1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról,* 1996.

[37] Infostart, „A vagyonosok körmére nézne a Nemzetbiztonsági Hivatal," 18 04 2009. [Online]. Available: https://infostart.hu/belfold/2009/04/18/a-vagyonosok-kormere-nezne-a-nemzetbiztonsagi-hivatal-271938. [Hozzáférés dátuma: 19 03 2024].

[38] Belügyminisztérium, „Az eSzemélyi," [Online]. Available: https://eszemelyi.hu/az-eszemelyi/. [Hozzáférés dátuma: 20 02 2024].

[39] *414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól,* 2015.

[40] Belügyminisztérium, „eSzemélyi - Gyakran Ismétlődő Kérdések," [Online]. Available: https://eszemelyi.hu/gyakran-ismetlodo-kerdesek/. [Hozzáférés dátuma: 19 03 2024].

[41] Belügyminisztérium, „eSzemélyi - Letöltések," [Online]. Available: https://eszemelyi.hu/letoltesek/. [Hozzáférés dátuma: 15 03 2024].

[42] Belügyminisztérium, „eSzemélyi - Szolgáltatások," [Online]. Available: https://eszemelyi.hu/szolgaltatasok. [Hozzáférés dátuma: 19 03 2024].

[43] Belügyminisztérium, „eSzemélyiM mobilapplikáció," [Online]. Available: https://eszemelyi.hu/eszemelyim-applikacio. [Hozzáférés dátuma: 19 03 2024].

[44] *1004/2016. (I. 18.) Korm. határozat a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról,* 2016.

[45] IdomSoft Zrt., „”Kormányzati hitelesítés szolgáltatás (Gov CA) kiterjesztése”,” IdomSoft Zrt., [Online]. Available: https://idomsoft.hu/projektjeink/folyamatban-levo-eu-s-projektek/kormanyzati-hitelesites-szolgaltatas-gov-ca-kiterjesztese/. [Hozzáférés dátuma: 20 02 2024].

[46] *T/1620. törvényjavaslat Magyarország biztonságát szolgáló egyes törvények módosításáról,* 2022.

[47] *2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól,* 2023.

[48] *2021. évi CXX. törvény Az egyes eljárások korszerűsítését és a polgárok biztonságának további megerősítését célzó intézkedésekről,* 2021.

[49] *2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól,* 2015.

[50] *2020. évi CLXII. törvény a Kormányzati Személyügyi Döntéstámogató Rendszerről,* 2020.

[51] *38/2022. (II. 11.) számú kormányrendelet egyes lejárt okmányok érvényességének veszélyhelyzettel összefüggő meghosszabbításáról,* 2022.

[52] KSH, „22.1.1.3. Népesség korév és nem szerint, január 1.*,” [Online]. Available: https://www.ksh.hu/stadat_files/nep/hu/nep0003.html. [Hozzáférés dátuma: 19 02 2024].

[53] Belügyminisztérium, „Elektronikus közszolgáltatásokat összefoglaló monitoring jelentés 2022. január – december,” [Online]. Available: https://nyilvantarto.hu/letoltes/statisztikak/2022_evi_adatokat_tartalmazo_monitoring_jelentes_v2.pdf. [Hozzáférés dátuma: 20 02 2024].

[54] Belügyminisztérium, „Elektronikus közszolgáltatásokat összefoglaló monitoring jelentés 2023. január – december,” [Online]. Available:

https://nyilvantarto.hu/letoltes/statisztikak/Monitoring_adatok_2023_II_felev.xlsx. [Hozzáférés dátuma: 20 02 2024].

[55] A. E. Zámbó, „Rules for eID Management in the Public Sector (Hungary, 2018),” *CEE e|Dem and e|Gov Days Conference,* pp. 115-127, 2018.

[56] Digitális Magyarország Ügynökség, Nemzeti digitális állampolgárság program, Budapest: Digitális Magyarország Ügynökség, 2022.

[57] N. Kübler, „Electronic Identity: Risk or Opportunity for Digital Authentication?,” in *Burkhard Stiller, Muriel Franco, Christian Killer, Sina Rafati, Bruno Rodrigues, Eder Scheid, Rafael Ribeiro, Alberto Huertas, Eryk Schiller (szerk.) Communication Systems XIV*, Zürich, Switzerland, University of Zurich, 2021, pp. 7-27.

[58] J. Edu, M. Hooper, C. Maple és J. Crowcroft, „An Impact and Risk Assessment Framework for National Electronic Identity (eID) Systems,” *International Conference on AI and the Digital Economy (CADE 2023),* 2023.

[59] J. Edu, M. Hooper, C. Maple és J. Crowcroft, „Exploring the Risks and Challenges of National Electronic Identity (NeID) System,” *International Conference on AI and the Digital Economy (CADE 2023),* 2023.

[60] M. Koller, „Okoseszközök mint a személyi hitelesítésre alkalmas interfacetechnológia biztonsági vetületei,” Hadmérnök, 18. kötet, 1. szám, pp. 109-124, 2023.

[61] T. Szádeczky, „Adatvédelem és adatbiztonság az elektronikus okmányoknál,” Hadmérnök, XII. kötet, II. szám. különszám „KÖFOP”, pp. 181-195, 1017.

[62] L. Hazai, „Okmányvédelem, az NBSZ okmányvédelemmel kapcsolatos szakértői, hatósági tevékenysége,” Nemzetbiztonsági Szemle MMXV/III, MMXV. kötet, III. szám, pp. 60-100, 2015.

[63] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,* 2012.

[64] T. Somogyi és R. Nagy, „Cyber Threats and Security Challenges in the Hungarian Financial Sector,” Contemporary Military Challenges, 24. kötet, 3. szám, pp. 15-29, 2023.

[65] *ISO/IEC 27001:2022,* 2022.

[66] „Magyar Informatikai Biztonsági Keretrendszer (MIBIK),” KIB, 2008.

[67] A. Kerti és N. Nyári, „Software Development Teamwork from an Information Security Perspective,” Biztonságtudományi Szemle, 3. kötet, 3. szám, pp. 37-53, 2021.

[68] N. Nyári és A. Kerti, „A risk assessment of the Hungarian eID card,” The Scientific Bulletin of the Land Forces Academy, 1. szám, 2024.

[69] I. El Fray, „A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in Information Systems,” In: Cortesi A., Chaki N., Saeed K., Wierzchoń S. (eds) Computer Information Systems and Industrial Management. CISIM 2012. Lecture Notes in Computer Science, 7564. kötet, 2012.

[70] N. Nyári és A. Kerti, „Review of Software Quality Related ISO Standards,” Biztonságtudományi Szemle, 3. kötet, 2. szám, pp. 61-72, 2021.

[71] *ISO/IEC 27005:2022,* 2022.

[72] N. Nyári, „Using the Methods of Probability Theory Analyzing Logs of Electronic Information Systems,” Biztonságtudományi Szemle, 2. kötet, 4. szám, pp. 65-76, 2020.

[73] *86/1996. (VI. 14.) Korm. rendelet a biztonsági okmányok védelmének rendjéről,* 1996.

[74] *2252/2004/EK rendelet a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról,* 2004.

[75] Belügyminisztérium, „eSzemélyi - eÚTIOKMÁNY (ePASS),” [Online]. Available: https://eszemelyi.hu/partnereinknek/#epass. [Hozzáférés dátuma: 30 03 2024].

[76] *ISO/IEC 27005:2011,* 2011.

[77] KSH, „A bruttó átlagkereset 564 400 forint volt 2023 októberében, 14,0%-kal magasabb, mint egy évvel korábban,” 21 12 2023. [Online]. Available: https://www.ksh.hu/gyorstajekoztatok/ker/ker2310.html. [Hozzáférés dátuma: 15 03 2024].

[78] Belügyminisztérium, „eSzemélyi - IGÉNYLÉS,” [Online]. Available: https://eszemelyi.hu/igenyles/#kodok-es-jelszavak. [Hozzáférés dátuma: 18 03 2024].

[79] NIST, „Post-Quantum Cryptography PQC,” 26 02 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. [Hozzáférés dátuma: 15 03 2024].

[80] A. G. Rodríguez, „A Quantum Cybersecurity Agenda for Europe - Governing the transition to post-quantum cryptography,” 17 07 2023. [Online]. Available: https://www.epc.eu/content/PDF/2023/Cybersecurity_DP.pdf. [Hozzáférés dátuma: 15 03 2024].

[81] H. Zhang, X. Xu és J. Xiao, „Diffusion of e-government: A literature review and directions for future directions,” Government Information Quarterly, 31. szám, pp. 631-636, 2014.

[82] H.-C. Wang, H.-S. Doong és F.-C. Lin, „Determinants of E-Government Service Adoption: An Innovation Diffusion Perspective,” *International Conference on Wireless Communications, Networking and Mobile Computing,* pp. 3458-3461, 2007.

[83] F. M. Bass, „A New Product Growth for Model Consumer Durables,” Management Science, 15. kötet, 5. szám, pp. 215-227, 1969.

[84] S. Ram, „Successful Innovation Using Strategies to Reduce Consumer Resistance An Empirical Test,” Journal of Product Innovation Management, 6. kötet, 1. szám, pp. 20-34, 1989.

[85] J. Baldunčiks, „Diffusion of Innovations and its Forecast for E-Signature in Latvia,” Journal of Economics and Management Research, 4. kötet, 5. szám, pp. 145-157, 2016.

[86] O. Folorunso, R. O. Vincent, A. F. Adekoya és A. O. Ogunde, „Diffusion of Innovation in Social Networking Sites among University Students,” International Journal of Computer Science and Security (IJCSS), Volume (4): Issue (3), 4. kötet, 3. szám, pp. 361-372, 2010.

[87] I. M. Al-Jabri és M. S. Sohail, „Mobile Banking Adoption: Application of Diffusion of Innovation Theory,” Journal of Electronic Commerce Research, 13. kötet, 4. szám, pp. 379-391, 2012.

[88] H. O. Yeloglu és M. Sagsan, „The diffusion of e-government innovations in Turkey: A conceptual framework,” Journal of US-China Public Administration, 6. kötet, 7. szám, pp. 17-23, 2009.

[89] S. Láng, L. Letenyei és V. Siklós, „Információs technológia diffúzió. Információs technológia és szakismeretek terjedése a Kaposvári kistérségben,” in *Információs technológia és életminőség*, Budapest, BKÁE Szociológia és Szociálpolitika Tanszék, 2003, pp. 5-28.

[90] L. Schmidt, The Diffusion of the German eID Scheme, Westfälische Wilhelms-Universität, Münster: Chair for Information Systems and Information Management, 2022.

[91] A. Yera, O. Arbelaitz, O. Jauregui és J. Muguerza, „Characterization of e-Government adoption in Europe,” PLoS ONE, 15. kötet, 4. szám, 2020.

[92] V. Kumar, B. Mukerji, I. Butt és A. Persaud, „Factors for Successful e-Government Adoption: a Conceptual Framework,” Electronic Journal of e-Government, 5. kötet, 1. szám, pp. 63-76, 2007.

[93] C. Van den Bulte, „Want to know how diffusion speed varies across countries and products? Try using a Bass model," PDMA VISIONS, 26. kötet, 4. szám, pp. 12-15, 2002.

[94] KSH, „12.1.3.2. Mobiltelefon-előfizetések száma [ezer lakosra]*," [Online]. Available: https://www.ksh.hu/stadat_files/ikt/hu/ikt0027.html. [Hozzáférés dátuma: 19 02 2024].

[95] J. Massiania és A. Gohs, „The choice of Bass model coefficients to forecast diffusion for innovative products: An empirical investigation for new automotive technologies," Research in Transportation Economics, 50. kötet, pp. 17-28, 2015.

[96] H. Funke és T. Senger, „Der Open Source Simulator für den elektronischen Personalausweis," Datenschutz und Datensicherheit, 4. kötet, pp. 232-236, 2014.

[97] V. Pusztai, „Vizuális önkifejezési lehetőségek az újmédiában – Uniformizálódik-e a (képi) kommunikáció?," *Közösségi Kapcsolódások,* 1-2. kötet, pp. 136-145, 2021.

[98] *2011. évi CXC. törvény a nemzeti köznevelésről,* 2011.

[99] B. Nagy, „EGY ORSZÁG A VILÁG SZEMÉBEN A Nation Brand Index bemutatása Ausztria elemzésén keresztül," Tér és Társadalom, 22. kötet, 4. szám, pp. 205-219, 2008.

[100] A. R. Silva Novais, The impact of TV Series in Nation Brand Experience, Porto, Portugal: Faculdade de economia Universidade do Porto, 2023.

[101] M. Dadashzadeh, „Social Media In Government: From eGovernment To eGovernance," Journal of Business & Economics Research, 8. kötet, 11. szám, pp. 81-86, 2010.

[102] E. Higgs, Identifying the English. A History of Personal Identification 1500-Present, London: Continuum International Publishing Group, 2011.

[103] *The Metropolitan Police Act 1829 (10 Geo.4, c.44),* 1829.

[104] *168/1999. (XI. 24.) kormányrendelet a személyazonosító igazolvány kiadásáról és nyilvántartásáról,* 1999.

[105] T. Oliveira és M. F. Martins, „Literature Review of Information Technology Adoption Models at Firm Level," Electronic Journal Information Systems Evaluation, 14. kötet, 1. szám, pp. 110-121, 2011.

[106] H. O. Awa, O. U. Ojiabo és L. E. Orokor, „Integrated technology-organization-environment (T-O-E) taxonomies for technology adoption," Journal of Enterprise Information Management, 30. kötet, 6. szám, p. 893–921, 2017.

[107] M. Fishbein és I. Ajzen, Belief, attitude, intention and behaviour: An introduction to theory and research, Reading, MA: Addison-Wesley, 1975.

[108] T. J. Madden, P. S. Ellen és I. Ajzen, „A comparison of the theory of planned behavior and the theory of reasoned action," Personality and social psychology Bulletin, 18. kötet, 1. szám, pp. 3-9, 1992.

[109] I. Ajzen, „From Intentions to Actions: A Theory of Planned Behavior," in *In Kuhl, Julius; Beckmann, Jürgen (eds.). Action Control: From Cognition to Behavior*, Berlin, Heidelberg, Springer, 1985, p. 11–39.

[110] I. Ajzen, „The theory of planned behavior: Frequently asked questions," Human Behavior and Emerging Technologies, 2. kötet, 4. szám, pp. 314-324, 2020.

[111] F. D. Davis, „A technology acceptance model for empirically testing new end-user information systems: theory and results," *Doctoral Dissertation, MIT Sloan School of Management, MA,* 1986.

[112] V. Venkatesh és F. D. Davis, „A theoretical extension of the technology acceptance model: Four longitudinal field studies," Management Science, 46. kötet, 2. szám, pp. 186-204, 2000.

[113] N. Marangunić és A. Granić, „Technology acceptance model: a literature review from 1986 to 2013,” Universal Access in the Information Society, 14. kötet, pp. 81-95, 2015.

[114] G. C. Moore és I. Benbasat, „Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation,” Information Systems Research, 2. kötet, 3. szám, pp. 192-222, 1991.

[115] R. Ward, „The application of Technology Acceptance and Diffusion of Innovation models in healthcare informatics,” Health Policy and Technology, 2. kötet, 4. szám, pp. 222-228, 2013.

[116] V. Losova, „Technology Acceptance Model: A Case of Electronic Health Record in Estonia,” 2014.

[117] V. Venkatesh, M. G. Morris, G. B. Davis és F. D. Davis, „User Acceptance of Information Technology: Toward a Unified View,” MIS Quarterly, 27. kötet, 3. szám, pp. 425-478, 2003.

[118] NIST, „NIST SP 800-37 revision 2,” NIST, 2018.

[119] CRAMM, „CRAMM,” [Online]. Available: http://www.cramm.com/. [Hozzáférés dátuma: 30 04 2021].

[120] Putra, Fandi A., S. Hermawan, and R.P. Anggi., „Design of Information Security Risk Management using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute,” International Conference on Information Technology Systems and Innovation, 8. kötet, 4. szám, pp. 251-256, 2017.

[121] Muhamad Al Fikri et al., „Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency,” Procedia Computer Science - The Fifth Information Systems International Conference, 161. kötet, pp. 1206-1215, 2019.

[122] *SP 800-30 revision 1,* 2012.

[123] M. Vanhaeren, F. d'Errico, C. Stringer, S. L. James, J. A. Todd és H. K. Mienis, „Middle Paleolithic Shell Beads in Israel and Algeria," Science, 312. kötet, 5781. szám, pp. 1785-1788, 2006.

[124] A. Deter-Wolf, B. Robitaille, L. Krutak és S. Galliot, „The world's oldest tattoos," Journal of Archaeological Science: Reports, 5. kötet, pp. 19-24, 2016.

[125] C. G. Grajalez, „Ancient censuses," *Royal Statistical Society,* p. 21, 2013.

[126] T. E. Tomlins és J. Raithby, „Safe Conducts Act 1414," *The Statutes at Large, of England and of Great Britain: from Magna Carta to the Union of the Kingdoms of Great Britain and Ireland. Vol. II.,* p. 320–326, 1811.

[127] A. Bloch, „The body as a canvas: Memory, tattoos and the Holocaust," *The Sociological Review,* 2024.

[128] M. Matusz, „A szemelyi igazolójegy („dögcedula") fejlesztesi lehetősegei a telemedicina vonatkozásában," Hadmérnök, 13. kötet, 4. szám, pp. 370-380, 2018.

[129] S. Dehm, „Passport," in *Hohmann, Jessie and Joyce, Daniel (eds), International Law's Objects,* New York, Oxford University Press, 2018, pp. 342-356.

[130] J. L. Lyman, „The Metropolitan Police Act of 1829: An Analysis of Certain Events Influencing the Passage and Character of the Metropolitan Police Act in England," Journal of Criminal Law and Criminology, 55. kötet, 1. szám, pp. 141-154, 1964.

[131] K. Michael és M. Michael, Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants, New York: Information Science Reference, 2009.

[132] *ISO 31000:2018,* 2018.

[133] ENISA, „Cramm," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-

management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html. [Hozzáférés dátuma: 19 03 2024].

[134] NIAPC (NATO Information Assurance Product Catalogue), „CRAMM," [Online]. Available: https://www.ia.nato.int/niapc/Product/CRAMM_257. [Hozzáférés dátuma: 19 03 2024].

[135] ENISA, „European Union Agency for Cybersecurity," ENISA, [Online]. Available: https://www.enisa.europa.eu/. [Hozzáférés dátuma: 15 03 2024].

[136] NIAPC, „https://www.ia.nato.int," [Online]. Available: https://www.ia.nato.int/DocumentGenerator/repository/version/ea1f0a72-17ba-40cd-be71-3ad6704b96b7/CRAMM-Manufacturer's%20Brochure. [Hozzáférés dátuma: 19 03 2024].

[137] IT Governance, „Information Security and ISO27001 – an Introduction," [Online]. Available: https://www.itgovernance.co.uk/files/Infosec%20101v1.1.pdf. [Hozzáférés dátuma: 19 03 2024].

[138] ISO, „ISO," [Online]. Available: https://www.iso.org. [Hozzáférés dátuma: 14 03 2024].

[139] ISO, „iso.org," ISO, [Online]. Available: www.iso.org. [Hozzáférés dátuma: 19 03 2024].

[140] ENISA, „ISO/IEC 27001," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso27001.html. [Hozzáférés dátuma: 19 03 2024].

[141] MSZT, „Magyar Szabványügyi Testület - Az információbiztonság-irányítás szabványai," [Online]. Available: http://www.mszt.hu/hu-hu/szabvanyositas/hirek/2015/03/az-informaciobiztonsag-iranyitas-szabvanyai. [Hozzáférés dátuma: 19 03 2024].

[142] NAH, „NAH,” NAH, [Online]. Available: https://www.nah.gov.hu/. [Hozzáférés dátuma: 19 03 2024].

[143] NIAPC (NATO Information Assurance Product Catalogue), „NATO Information Assurance Product Catalogue,” [Online]. Available: https://www.ia.nato.int/NIAPC. [Hozzáférés dátuma: 19 03 2024].

[144] NIST, „NIST,” [Online]. Available: http://nist.gov. [Hozzáférés dátuma: 19 03 2024].

[145] ENISA, „SP800-30 (NIST),” [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_sp800_30.html. [Hozzáférés dátuma: 15 03 2024].

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

FÜGGELÉK

1. számú függelék: Az eSzemélyi okmány igénylések statisztikája, forrás: https://nyilvantarto.hu/hu/statisztikak [5]

Megnevezés	2016	2016 [%]	2017	2017 [%]	2018	2018 [%]	2019	2019 [%]	2020	2020 [%]	2021	2021 [%]	2022.	2022 [%]	2023.	2023. [%]
Igényelt állandó eSzemélyi igazolvány	1 309 260		1 373 617		1 300 429		1 378 184		1 058 777		1 350 533		2 145 399		1 815 021	
Chipes	1 191 260	90,99%	1 255 961	91,43%	1 185 072	91,13%	1 262 044	91,57%	986 511	93,17%	1 306 010	96,70%	2 145 399	100,00%	1 676 495	92,37%
Ujjnyomat	570 842	43,60%	588 531	42,85%	522 686	40,19%	543 005	39,40%	432 938	40,89%	831 582	61,57%	1 940 159	90,43%	1 640 400	90,38%
14 év felettiek	1 033 313	78,92%	1 107 830	80,65%	1 022 779	78,65%	1 041 182	75,55%	867 126	81,90%	1 016 910	75,30%	1 725 283	80,42%	1 447 097	79,73%
e-Aláírás funkció	67 348	5,14%	122 520	8,92%	37 523	2,89%	25 509	1,85%	20 743	1,96%	16 246	1,20%	27 980	1,30%	31 856	1,76%
Vészhelyzet esetén értesítendő telefonszám	-	-	413 749	30,12%	411 216	31,62%	427 079	30,99%	334 893	31,63%	418 220	30,97%	615 887	28,71%	490 102	27,00%
Adóazonosító jel	1 105 014	84,40%	1 174 714	85,52%	1 111 614	85,48%	1 183 792	85,90%	944 854	89,24%	1 244 106	92,12%	2 046 306	95,38%	1 560 820	85,99%
TAJ szám	1128175	86,17%	1186161	86,35%	1 114 470	85,70%	1 194 752	86,69%	942 502	89,02%	1 242 341	91,99%	2 039 934	95,08%	1 724 325	95,00%

2. számú függelék: Kockázatforrások. Forrás: saját szerkesztés ISO/IEC 27005 [71] alapján

Kockázatforrás	Példák
Államhoz kötődő	Államok, titkosszolgálatok. Általában profik hajtják végre ezeket a támadásokat, meg van képességük hosszan tartó támadások kivitelezéséhez, zero day sérülékenységek megvásárlásához, felfedezéséhez.
Szervezett bűnözés	Bűnszövetkezetek (maffiák, bandák). Online vagy személyes jelenlétet igénylő csalások, zsarolások, botnetek alkalmazása jellemzően vagyonszerzési célból. Néhány esetben megvan a képesség zero day sérülékenységek megvásárlásához, felfedezéséhez.
Specializált csapat	Kiberzsoldos, technikai szempontból általában magas IT-kapacitással. Tapasztal hackerek. Van lehetőségük interneten megvásárolható eszközökkel dolgozniuk. Legtöbbször az anyagi haszonszerzés motiválja őket.
Bosszúálló	Motivációja általában a bosszú, vagy az igazságtalanság érzete valamilyen ügy kapcsán. Elszántság jellemzi. Általában belső tudással rendelkezik konkrét informatikai rendszerekről, ami különösen veszélyessé teszi.
Képzetlen felhasználó	Jóindulatú felhasználó, de nem rendelkezik megfelelő IT képesítéssel és biztonsági tudatossággal.
Terrorista	Kiberterroristák, kiberkatonák. Általában nem túlságosan szofisztikált támadási módszerekkel dolgoznak. Céljuk a destabilizálás, pusztítás, működés meggátolása.
Ideológiai aktivista	Kiber-hacktivisták, szekták. Nagyon hasonlóak a kiberterroristákhoz, de kevésbé a pusztítás vezérli őket. A támadások célja általában ideológiák, üzenetek közvetítése.
Amatőr	Script-kiddies elég jó IT tudással. Alapszintű támadások kivitelezésére képesek, általában a kihívás, a szórakozás motiválja őket.
Patológiás támadó	Kóros vagy opportunista jellegű motivációkkal rendelkezik, néha haszonszerzés vezérli (csaló). Megvan a lehetőségük online elérhető támadó megoldások alkalmazására, vagy a támadás „alvállalkozó” számára kiadásra. Gyakran próbálnak belső erőforrásokat célba venni (például elégedettlen alkalmazottak).

3. számú függelék: Elérendő célok listája, Forrás: saját szerkesztés ISO/IEC 27005 [71] alapján

Elérendő cél	Leírás
Kémkedés	Hírszerző tevékenység (állami vonatkozású). A támadó sok esetben az információs rendszerbe történő hosszú távú telepítésre törekszik, teljes diszkrécióval. Kiemelt célpontok: a fegyvergyártás, az űrkutatás, a repülés, a gyógyszerszektor, az energiaipar és az állam bizonyos tevékenységei (gazdaság, pénzügy, külügy).
Stratégiai előpozícionálás	Előpozícionálás általában hosszú távú támadásra irányul, anélkül, hogy a célt egyértelműen meghatároznák (például távközlési hálózatok veszélyeztetése, tömeges információs internetes oldalak beszivárgása erős visszhangot kiváltó politikai vagy gazdasági befolyás megindítása érdekében). A számítógépek hirtelen és tömeges kompromittálása botnet létrehozása érdekében is ebbe a kategóriába sorolható.
Befolyásolás	Hamis információk terjesztésére, véleményvezérek mozgósítására a közösségi oldalakon, jó hírnév rombolására, bizalmas információk nyilvánosságra hozatalára, szervezetről vagy államról alkotott kép lerontására irányuló művelet. A végső cél általában attitűdök destabilizálása vagy módosítása.
Működés megakadályozása	Szabotázsművelet, amelynek célja például egy internetes oldal elérhetetlenné tétele, információtelítettség előidézése, digitális erőforrások használatának megakadályozása, fizikai objektum elérhetetlenné tétele. Az ipari rendszerek különösen kiszolgáltatottá és sebezhetővé válhatnak olyan informatikai hálózatokon keresztül, amelyekkel összekapcsolódnak (például parancsok küldése hardverkárosodás vagy kiterjedt karbantartást igénylő meghibásodás előidézésére). Az elosztott szolgáltatásmegtagadási támadások (DDoS) gyakran használt technikák a digitális erőforrások semlegesítésére.
Haszonszerzés	Közvetlen vagy közvetett pénzügyi haszonszerzést célzó művelet. Általában a szervezett bűnözéshez kötődően megemlíthetők: internetes csalás, pénzmosás, zsarolás vagy sikkasztás, pénzpiaci manipuláció, okmányok hamisítása, személyazonosság lopás stb. Néhány támadási módszer alkalmazhatja a fentebb felsorolt módszereket is (például kémkedés és adatlopás, zsarolóprogramok egy tevékenység semlegesítésére), de a végső cél továbbra is vagyoni haszonszerzés.
Kihívás, szórakozás	Művelet, amelynek célja egy exploit megvalósítása társadalmi elismerés, kihívás vagy egyszerűen szórakozás céljából. Bár a cél elsősorban szórakozás és különösebb ártási vágy nélkül történik, az ilyen típusú műveletek is súlyos következményekkel járhatnak az áldozatra nézve.
Rendeltetésszerű felhasználás	Jóhiszemű felhasználók használják a vizsgált informatikai rendszert annak rendeltetésszerű célja elérésre, de nem biztonságtudatos módon.

4. számú függelék: Vagyontárgyak az eSzemélyi infrastruktúrában. Forrás: saját szerkesztés

ID	Vagyontárgy	Vagyontárgy típusa	Érintett fél
A1	PIN kód az elektronikus aláíráshoz	Elsődleges/üzleti	Állampolgár
A2	PUK kód az elektronikus aláíráshoz	Elsődleges/üzleti	Állampolgár
A3	PIN kód az elektronikus hitelesítéshez	Elsődleges/üzleti	Állampolgár
A4	PUK kód az elektronikus hitelesítéshez	Elsődleges/üzleti	Állampolgár
A5	Az eSzemélyi igazolvány tárolóelemén tárolt személyes adat	Elsődleges/üzleti	Állampolgár
A6	Az eSzemélyi igazolványon tárolt elektronikus aláírásra használatos digitális tanúsítvány	Elsődleges/üzleti	Állampolgár
A7	Az eSzemélyi infrastruktúrában tárolt adatok	Elsődleges/üzleti	A magyar állam
A8	Az SZTSZ alapnyilvántartásaiban tárolt adatok	Elsődleges/üzleti	A magyar állam
A9	eAláírás funkcionalitással elektronikusan aláírt dokumentum	Elsődleges/Üzleti	Állampolgár
A10	eSzemélyi igazolvány	Támogató	Állampolgár
A11	Az elektronikus hitelesítéshez tartozó PUK kódot tartalmazó plasztik kártya	Támogató	Állampolgár
A12	Az elektronikus aláíráshoz tartozó PUK kódot tartalmazó plasztik kártya	Támogató	Állampolgár
A13	Hardveres kártyaolvasó készülék az eSzemélyi igazolványhoz	Támogató	Állampolgár
A14	Az eSzemélyiM mobilakalmazás	Támogató	Az eSzemélyi infrastruktúra fejlesztője
A15	Az eSzemélyiM mobilakalmazást futtató mobileszköz	Támogató	Állampolgár
A16	Az elektronikus funkciókhoz használt PC	Támogató	Állampolgár
A17	Az elektronikus aláíráshoz használt szoftver (KEAASZ)	Támogató	Az eSzemélyi infrastruktúra fejlesztője
A18	A magyar eSzemélyi infrastruktúra	Támogató	Az eSzemélyi infrastruktúra üzemeltetője
A19	Az eSzemélyi elektronikus aláírásához használt PKI infrastruktúra	Támogató	Az eSzemélyi infrastruktúra üzemeltetője
A20	eKormányzati szolgáltatások	Támogató	A magyar állam
A21	Az SZTSZ szolgáltatás	Támogató	Az eSzemélyi infrastruktúra üzemeltetője

5. számú függelék: Az eSzemélyi diffúziós terve, Forrás: saját szerkesztés

SSz	Leírás	Kapcsolódó DOI fogalom
1.	Az innováció megváltoztatása	Innováció
1.1.	Kipróbálhatóság növelése	Innováció, Kipróbálhatóság
1.2.	Komplexitás csökkentése	Innováció, Komplexitás
1.3.	Kompatibilitás növelése	Innováció, Kompatibilitás
1.4.	Megfigyelhetőség növelése	Innováció, Megfigyelhetőség
1.5.	Relatív előny növelése	Innováció, Relatív előny
1.6.	Újrafelhasználhatóság növelése	Innováció, Újrafelhasználhatóság
1.7.	Érzékelt kockázatok kezelése	Innováció, érzékelt kockázat
1.8	Azonosított kockázatok kezelése	Innováció, azonosított kockázat
2.	Véleményvezérek azonosítása	Társadalmi rendszer, kommunikációs csatornák
3.	Változásképviseletek és változásközvetítők beazonosítása	Társadalmi rendszer, kommunikációs csatornák
3.1.	Változásközvetítők képzése	Kommunikációs csatornák
4.	A potenciális elfogadók biztonságtudatosságot szem előtt tartó képzése	Társadalmi rendszer
4.1.	Az eSzemélyi és az elektronikus szolgáltatások szerepeltetése a közoktatásban	Társadalmi rendszer, Kommunikációs csatornák
4.2.	Az eSzemélyi és az elektronikus szolgáltatások szerepeltetése a felsőoktatásban	Társadalmi rendszer, Kommunikációs csatornák
5.	Az eSzemélyi igazolvány jelenlétének fokozása a tömegkommunikációs csatornákban	Kommunikációs csatornák
5.1.	Internetes, televíziós, rádiós hirdetések véleményvezérek bevonásával	Kommunikációs csatornák
5.2.	Az eSzemélyi igazolvány jelenlétének fokozása a közösségi médiákban véleményvezérek bevonásával	Kommunikációs csatornák
5.3.	Az eSzemélyi és az elektronikus szolgáltatások szerepeltetése magyar sorozatokban, TV- ill., mozifilmekben	Kommunikációs csatornák

KÖSZÖNETNYILVÁNÍTÁS

Mindenekelőtt köszönettel tartozom a páromnak, Vágány Diánának, a szüleimnek, a fiamnak és barátaimnak (kiemelendő: Péter Benjámin, Turbéki-Wertán Péter Bulcsú és Karánsebesy Ildikó) a sok-sok támogatásért, amit kaptam tőlük és a türelemért, amit velem szemben tanúsítottak az elmúlt időszakban. Külön elnézést kell kérnem drága kisfiamtól, Nyári Bencétől, amiért a doktori képzés miatt kevesebb időm jutott rá.

Köszönöm a témavezetőmnek, Kerti Andrásnak a konzultációkon a jó hangulatban zajló, igen konstruktív brainstorming alkalmakat. Rajnai Zoltánnak, Farkas Tibornak és Besenyő Jánosnak az iránymutatást a nemzetközi folyóiratok útvesztőjében. Farkasné Hronyecz Erikának és Lévay Katalinnak a doktori szabályzat közös értelmezésére fordított időt és energiát.