ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

NYÁRI NORBERT

Elektronikus aláírás az eSzemélyi igazolvánnyal – egy innováció diffúziója Magyarországon

Témavezető: Dr. habil Kerti András

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024. november 4.

Tartalomjegyzék

1 Summary

The tradition of document signing dates back centuries, beginning with wax seals, progressing through paper-based signatures, and culminating in digital signatures. Digital signature technology has been available for decades. Since 2014, the legal framework for electronic signatures has also been established in both the EU and Hungary, based on the eIDAS [1] regulation ("Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC").

The regulation, among other things, governs the use of electronic identity cards (eID cards) and electronic signatures (eSignatures) that are equally accepted in the EU member states.

Of course, one can also purchase a certificate for electronic signature from a market participant service provider in Hungary, such as Netlock Kft. or Microsec Zrt. However, in my thesis I would like to examine the matter of the Hungarian eID card (called "eSzemélyi igazolvány") in detail, the electronic identification document which is freely available for the citizens. Therefore, I focus on the Hungarian eID card and its electronic signature function (eSignature) [2].

The Hungarian eID card is available since January 2016, but its electronic functions, like creating eSignatures are not spreading as fast as they could be. Identifying the factors that hinder the spread and devising strategies to overcome these obstacles is crucial. My thesis aims to examine the reasons for the underutilization of Hungarian eIDs from a new perspective: the perspective of diffusion research. Everett M. Rogers [4] began developing the theory of Diffusion of Innovations (DOI) in the 1960s, thereby establishing the methodology of diffusion research.

First, I assume that citizens are distrustful of electronic signatures as a "new" technology for some reason. The "new" is in quotation marks because, according to the DOI, the novelty of an innovation is to be interpreted in a given social system, so although electronic signatures are not objectively "new", they are still considered new to people living in Hungary [4].

Examining the issue from the perspective of trust did not necessarily validate the aforementioned assumption, so I redirected my investigation towards technology acceptance. However, discussing the acceptance of technology is premature if it has not yet reached its potential users. This leads us to diffusion research, which explores the factors influencing the spread of technology and how the diffusion process can be accelerated [4].

2 A kutatás előzményei

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 [1] (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” 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 Magyarországon, 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 elhárítani.

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 (DOI) 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 modell 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].

3 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, a végfelhasználók szemszögéből elvégzett, nyílt forrásból elérhető anyagok felhasználásával készített 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.

Kutatási kérdések

K1: Mi a legfőbb oka annak, hogy Magyarországon az eSzemélyi igazolvány elektronikus funkció nem széleskörben elterjedtek?

K2: Hogyan segítheti az eSzemélyi igazolvány kockázatainak azonosítása az okmány elektronikus funkcióinak terjedését Magyarországon?

K3: Melyik a legalkalmasabb elmélet az eSzemélyi igazolvány jelenségének modellezésére a felmerülő információbiztonsági kockázatok figyelembevételével?

K4: Hogyan lehetne a legjobban elősegíteni az eSzemélyi igazolvány elektronikus funkcióinak terjedését Magyarországon?

Hipotézisek

H1: Magyarországon az eSzemélyi igazolvány és elektronikus funkcióinak széleskörű terjedését legfőképp a bizalom hiánya hátráltatja.

Feltevésem szerint Magyarországon az eSzemélyi igazolvány elektronikus funkcióinak terjedését a bizalom hiánya hátráltatja. Az egyik ilyen elektronikus funkció az elektronikus aláírás, melyet további fejezetekben bemutatott statisztikák alapján a jogosultak csak igen alacsony százaléka igényel az okmányához – ezt később részletesen látni fogjuk. Az évszázados 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.

H2: Az eSzemélyi igazolvány elterjesztését segítő megoldás kialakításakor fel kell használni az azonosított kockázatokkal kapcsolatos információkat, mert azok az információbiztonsági szempontok érvényre jutásán túl a potenciális felhasználók eSzemélyi igazolványba vetett bizalmát is növelni fogják, ezáltal gyorsítva a terjedést.

Az eSzemélyi igazolvány elektronikus használati eseteit teljesen átszövi az információbiztonság magas szintjére való igény. Több szempontból is fontosnak találom egy, az eSzemélyi igazolvány végfelhasználóinak szemszögéből elvégzett kockázatelemzés

elvégzését. Egyrészt a kockázatelemzés során feltárt kockázatok kezelése növeli a megoldás biztonságát, másrészt pedig a biztonság növelése érdekében tett intézkedések ezen felül a felhasználók bizalmára is pozitív hatással vannak. A kockázatelemzést az ISO/IEC 27005:2022 szabvány alapján végeztem el, annak ellenére, hogy a Magyarországon jelenleg hatályos jogszabályi környezet nem ezt írja elő.

A szabvány legújabb verziójában megjelent a kockázatok feltárására az esemény alapú megközelítés, amely lehetőséget biztosít a kockázatok különböző absztrakciós szinteken (stratégiai és operatív szcenáriók) történő megvizsgálására. Ezt a módszert alkalmazom az eSzemélyi igazolvány kockázatainak feltárására annak érdekében, hogy szilárd alapokon nyugvó információbiztonsági szempontokkal egészíthessem ki a terjedést elősegítő diffúziós tervet.

H3: Az eSzemélyi igazolvány és elektronikus funkciói elterjedtségének modellezésére a legalkalmasabb elmélet a Diffusion of Innovations, kiegészítve a „kockázatok" diffúziós folyamat összetevővel.

Meglátásom szerint sajnálatos módon az eSzemélyi elektronikus aláírásra történő használatának lehetősége nincs a köztudatban. Feltevésem szerint a bizalomhiány mellett az információhiány is egy további, a terjedést gátló tényezőként van jelen.

Az eSzemélyi igazolvány, mint innováció kérdéskörét 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.

H4: Az eSzemélyi igazolvány és elektronikus funkciói elterjedését legjobban egy, a Diffusion of Innovations elméleten alapuló diffúziós terv segítené.

Még tovább követve az előbbi a gondolatmenetet, a DOI elveit alkalmazva kialakítható a feltárt hiányosságok kiküszöbölésére 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.

A diffúzió alapvetően fizikában, kémiában és biológiában használatos fogalom. Latin eredetű szó, melynek jelentése szétfolyás, elterjedés. A diffúzió egy alapvető tulajdonsága, hogy külső erőhatás nélkül történik. Átvitt értelemben pontosan ez történik az eSzemélyi igazolvány esetében is. 2016-ban bevezetésre került az új okmány, majd az évek során egyre bővültek az elektronikus szolgáltatásai, és mindenféle különösebb külső beavatkozás

(reklámkampány, oktatás stb.) nélkül „diffundált” (vagy éppenséggel nem „diffundált”) a magyar lakosság körében.

Annak érdekében, hogy a terjedés nagyobb ütemben történhessen, a diffúziós folyamatot meg kell támogatni külső impulzusokkal is. Új utakat kell találni az elektronikus aláírás használatának népszerűsítésére, egyszerűsíteni szükséges a használati eseteket, és új használati eseteket kell bevezetni.

4 Vizsgálati 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. Értekezésem 1. fejezetében röviden kitérek a személyazonosító okmányok fejlődéstörténetére, továbbá elemzem a bizalom összetevőit a személyi adatokkal, okmányokkal, ügyintézéssel, szerződéskötéssel kapcsolatban.

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 beszélgetésekkel 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 az értekezésem 3.6. alfejezetében részletezett diffúziós terv jött létre.

5 Új tudományos eredmények

Doktori értekezésem eredményeként az alábbi téziseket fogalmazom meg.

T1: Az eSzemélyi igazolvány elektronikus funkcióinak terjedését legfőképp a használati esetek hiánya és a felhasználók információhiánya gátolja. (Kapcsolódó tudományos közlemények sorszáma: 1,2,3,4)

Értekezésem 1. fejezetében a H1 hipotézist a kutatásaim eredménye következményeként elvetettem, így az tézisként nem állja meg a helyét, helyette a fenti, T1 állítást fogalmaztam meg, amelyet kutatási eredményeim alapján igazoltam. Hátráltató tényező ugyan a bizalom hiánya, de sokkal nagyobb problémát jelent, hogy a potenciális felhasználók nincsenek tisztában az eSzemélyi igazolványban rejlő lehetőségekkel.

T2: Az eSzemélyi igazolvány elterjesztését segítő megoldás kialakításakor fel kell használni az azonosított kockázatokkal kapcsolatos információkat, mert azok az információbiztonsági szempontok érvényre jutásán túl a potenciális felhasználók az eSzemélyi igazolványba vetett bizalmát is növelni fogják ezáltal gyorsítva a terjedést. (Kapcsolódó tudományos közlemények sorszáma: 1,3,4,5,6,7,8)

Az eID rendszerek esetében annak fejlesztői, üzemeltetői számára törvényi előírás az adekvát kockázatelemzés elvégzése. Magyarországon, az eSzemélyi igazolvány infrastruktúrája, mint bizalmi szolgáltatás esetében a 7/2024 MK rendelet alapján kell elvégezni. Értekezésemben ettől eltérően egy új megközelítésben, az ISO/IEC 27005:2022 szabvány vagyontárgy alapú és eseményalapú megközelítésének kombinációját alkalmazva mértem fel és ismertettem az okmány kliens oldali megoldásaival kapcsolatosan felmerülő kockázatokat. Szakirodalomelemzésen keresztül támasztottam alá a kockázatelemzés fontosságát egy ilyen rendszer esetében.

T3: Az eSzemélyi igazolvány és elektronikus funkciói elterjedtségének modellezésére a legalkalmasabb elmélet a Diffusion of Innovations kiegészítve a „kockázatok" diffúziós folyamat összetevővel. (Kapcsolódó tudományos közlemények sorszáma: 1,2,4)

Értekezésem 3. fejezetében bizonyítottam, hogy a Rogers-féle DOI elmélet diffúzió fogalma kiegészíthető a kockázatok összetevővel, mely kiegészítést meg is tettem. Az innováció fejlesztése során azonosított és a terjesztése/terjedése során a potenciális elfogadók által érzékelt kockázatokat egyaránt kezelni kell. Az azonosított és az érzékelt kockázatok nem mindig esnek egybe. Különös figyelmet kell fordítani az érzékelt kockázatokra, tekintve, hogy ezek a felhasználók számára látványos és megnyugtató módon történő kezelése nem csak a biztonságot növeli, hanem a szóban forgó megoldásba vetett bizalom szintjét is.

T4: Az eSzemélyi igazolvány és elektronikus funkciói elterjedését legjobban egy, a Diffusion of Innovations elméleten alapuló diffúziós terv segítené. (Kapcsolódó tudományos közlemények sorszáma: 1,2,4)

Értekezésemben bemutattam az eSzemélyi igazolvány terjedését segítő diffúziós tervet, amely a kockázatok összetevővel kiegészített DOI elmélet szempontjai alapján készült. A diffúziós terv hangsúlyozza, hogy milyen fontos lenne a terjedés elősegítése érdekében az innováció tulajdonságainak megváltoztatása (érthetőbbé, átláthatóbbá kell tenni a használati eseteket, további használati eseteket kell bevezetni). Kezelni kell az előbbi tézispontban (T3) is említett kockázatokat, mindezt olyan szemlélettel, hogy az alkalmazott biztonságot növelő megoldások, eljárások az eSzemélyi igazolványba vetett bizalmat is növeljék a terjedés elősegítése érdekében.

A terv a diffúziós folyamatban résztvevő személyekre is kitér: oktatásban kell részesíteni a változásközvetítőket, be kell vonni a véleményvezéreket. Továbbá reklámkampányokkal, oktatási anyagokkal népszerűsíteni kell az eSzemélyi igazolványt.

6 Az eredmények hasznosítási lehetősége

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 hatékonyabb népszerűsítéséhez, továbbá az itt megfogalmazott diffúziós terv kiindulási alapul szolgálhat a Digitális Állampolgárság Program terjesztését támogató terv kialakításához 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.

7 Irodalmi hivatkozások listája/ 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: 23 10 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] P. M. Erdősi, Az elektronikus aláírás mérése, Budapest: Nemzeti Közszolgálati Egyetem, 2019.

[22] 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].

[23] 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].

[24] 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].

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

[26] 253.600/1946. (VII. 30.) BM rendelet a bejelentési kötelezettség teljesitésének részletes szabályozása tárgyában, 1946.

[27] 1982. évi 17. törvényerejű rendelet az anyakönyvekről, a házasságkötési eljárásról és a névviselésről, 1982.

[28] 15/1991. (IV. 13.) AB határozat, 1991.

[29] 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról, 1992.

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

[31] 2/1978. (X. 28.) KSH A személyi szám, illetőleg a személyi lap kiadásáról és használatáról, 1978.

[32] 1986. évi 10. törvényerejű rendelet az állami népességnyilvántartásról, 1986.

[33] 25/1986. (VII. 8.) MT rendelet az állami népességnyilvántartásról szóló 1986. évi 10. törvényerejű rendelet végrehajtásáról, 1986.

[34] 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.

[35] 1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról, 1996.

[36] 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].

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

[38] 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól, 2015.

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

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

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

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

[43] 1004/2016. (I. 18.) Korm. határozat a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról, 2016.

[44] 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].

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

[46] 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól, 2023.

[47] 2021. évi CXX. törvény Az egyes eljárások korszerűsítését és a polgárok biztonságának további megerősítését célzó intézkedésekről, 2021.

[48] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, 2015.

[49] 2020. évi CLXII. törvény a Kormányzati Személyügyi Döntéstámogató Rendszerről, 2020.

[50] 38/2022. (II. 11.) számú kormányrendelet egyes lejárt okmányok érvényességének veszélyhelyzettel összefüggő meghosszabbításáról, 2022.

[51] 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: 23 10 2024].

[52] 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].

[53] 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].

[54] Belügyminisztérium, „Elektronikus közszolgáltatásokat összefoglaló monitoring jelentés 2024. január – június,” [Online]. Available: file:///C:/Users/nyari/Downloads/2024_I_felevi_adatokat_tartalmazo_monitoring_jelentes.pdf . [Hozzáférés dátuma: 23 10 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] 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.

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

[64] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról, 2013.

[65] 249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, 2017.

[66] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 2013.

[67] 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról, 2011.

[68] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági..., 2015.

[69] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról..., 2022.

[70] 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről, 2023.

[71] 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről, 2024.

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

[73] N. Nyári és A. Kerti, „A risk assessment of the Hungarian eID card," The Scientific Bulletin of the Land Forces Academy, 29. kötet, 1. szám, pp. 91-102, 2024.

[74] 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.

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

[76] ISO/IEC 27005:2022, 2022.

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

[78] 86/1996. (VI. 14.) Korm. rendelet a biztonsági okmányok védelmének rendjéről, 1996.

[79] 2252/2004/EK rendelet a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról, 2004.

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

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

[82] ISO/IEC 27005:2011, 2011.

[83] 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].

[84] I. Skierka, „When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia’s eID crisis,” Government Information Quarterly 40 (2023), 2023.

[85] A. Alrawais, „Security Issues in Near Field Communications (NFC),” International Journal of Advanced Computer Science and Applications (IJACSA) , 11. kötet, 11. szám, pp. 621-628, 2020.

[86] M. Pernpruner, R. Carbone, S. Ranise és G. Sciarretta, „The Good, the Bad and the (Not So) Ugly of Out-Of-Band Authentication with eID Cards and Push Notifications,” CODASPY ’20, March 16–18, 2020, New Orleans, LA, USA.

[87] P. Paganini, „Flaw allowing identity spoofing affects authentication based on German eID cards,” 22 11 2018. [Online]. Available:

https://securityaffairs.com/78314/hacking/german-eid-cards-hack.html. [Hozzáférés dátuma: 21 10 2024].

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

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

[90] 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].

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

[92] 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.

[93] 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.

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

[95] 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.

[96] 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.

[97] 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.

[98] 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.

[99] 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.

[100] 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.

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

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

[103] 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.

[104] 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.

[105] 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].

[106] 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.

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

[108] V. Pusztai, „Vizuális önkifejezési lehetőségek az újmédiában – Uniformizálódik-e a (képi) kommunikáció?,” Közösségi Kapcsolódások, %1. kötet, összesen: %21-2, pp. 136-145, 2021.

[109] 2011. évi CXC. törvény a nemzeti köznevelésről, 2011.

[110] 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.

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

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

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

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

[115] 168/1999. (XI. 24.) kormányrendelet a személyazonosító igazolvány kiadásáról és nyilvántartásáról, 1999.

[116] 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.

[117] 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.

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

[119] 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.

[120] 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.

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

[122] 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.

[123] 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.

[124] 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.

[125] 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.

[126] 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.

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

[128] 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.

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

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

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

[132] 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.

[133] 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.

[134] SP 800-30 revision 1, 2012.

[135] 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.

[136] 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.

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

[138] 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.

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

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

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

[142] 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.

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

[144] ISO 31000:2018, 2018.

[145] ISO/IEC 27001:2022, 2022.

[146] 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].

[147] NIAPC (NATO Information Assurance Product Catalogue), „CRAMM,” [Online]. Available: https://www.ia.nato.int/niapc/Product/CRAMM_257. [Hozzáférés dátuma: 19 03 2024].

[148] ENISA, „European Union Agency for Cybersecurity,” ENISA, [Online]. Available: https://www.enisa.europa.eu/. [Hozzáférés dátuma: 15 03 2024].

[149] 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].

[150] 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].

[151] ISO, „ISO,” [Online]. Available: https://www.iso.org. [Hozzáférés dátuma: 14 03 2024].

[152] ISO, „iso.org,” ISO, [Online]. Available: www.iso.org. [Hozzáférés dátuma: 19 03 2024].

[153] 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].

[154] 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].

[155] NAH, „NAH,” NAH, [Online]. Available: https://www.nah.gov.hu/. [Hozzáférés dátuma: 19 03 2024].

[156] NIAPC (NATO Information Assurance Product Catalogue), „NATO Information Assurance Product Catalogue,” [Online]. Available: https://www.ia.nato.int/NIAPC. [Hozzáférés dátuma: 19 03 2024].

[157] NIST, „NIST,” [Online]. Available: http://nist.gov. [Hozzáférés dátuma: 19 03 2024].

[158] 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].

[159] 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek..., 2015.

[160] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezésé, 2016.

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

1. **N. Nyári** és A. Kerti, „A risk assessment of the Hungarian eID card," The Scientific Bulletin of the Land Forces Academy, 29. kötet, 1. szám, pp. 91-102, 2024.
2. **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.
3. **N. Nyári**, „The Future of eIDAS in the Light of Post-Quantum Cryptography," Biztonságtudományi szemle, 4. kötet, 1. szám, pp. 91-103, 2022.
4. **N. Nyári**, „Az eszemélyi és az elektronikus aláírás technológia helyzete és lehetőségei Magyarországon," Biztonságtudományi szemle, 4. kötet, 2. szám, pp. 61-73, 2022.

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

5. **N. Nyári** és A. Kerti, „Review of Software Quality Related ISO Standards," Biztonságtudományi Szemle, 3. kötet, 2. szám, pp. 61-72, 2021.
6. **N. Nyári**, „The Impact of Quantum Computing on IT Security," Biztonságtudományi Szemle, 3. kötet, 4. szám, pp. 25-37, 2021.
7. **N. Nyári**, „Using the Methods of Probability Theory Analyzing Logs of Electronic Information Systems," Biztonságtudományi Szemle, 2. kötet, 4. szám, pp. 65-76, 2020.