NEMZETI KÖZSZOLGÁLATI EGYETEM

Közigazgatás-tudományi Doktori Iskola

Erdősi Péter Máté

Az elektronikus aláírások fejlődése, jellemzői és ezek mérhetősége a közigazgatásban

Doktori (PhD) értekezés

TÉZISFÜZET

Témavezető: Dr. Muha Lajos, főiskolai tanár

Budapest, 2020

1 Az értekezés témája, célja

Az elektronikus aláírás (electronic signature) fogalmát széles körben használják a világban, és mára beszivárgott a hétköznapi gyakorlatba és a jogba is a világ legtöbb országában. A fogalom konzisztens használatát nem segíti, hogy az elektronikus aláírás értelmezése számos átalakuláson ment keresztül az elmúlt négy évtizedben, továbbá használata során sokszor keveredik a digitális aláírás (digital signature), az azonosítás (identification), hitelesítés (authentication) és feljogosítás (authorization) információbiztonsági és a bizalom (trust, reliance), hitelesség (authenticity), szavahihetőség (trustworthiness) köznyelvi fogalmakkal. Az elektronikus aláírásnak számos aspektusa jelent meg a jogalkotási és a jogalkalmazási területeken, például használható fokozott biztonságú elektronikus aláírás (advanced electronic signature) vagy minősített elektronikus aláírás (qualified electronic signature) is az elektronikus folyamatokban, továbbá azt a kérdést sem egyszerű megválaszolni, hogy az elektronikus aláírások közül melyiknek van teljes bizonyító ereje vagy melyik alkalmas az írásbeliség alaki követelményének kielégítésére. Ezek a kérdések a kezdetek óta jelen vannak, a terület jeles szakemberei már 2000-ben feltették maguknak azt a kérdést, hogy létezik-e „egyetlen helyes" elektronikus aláírási struktúra, illetve a kockázatokat felmérve az a kérdés is megfogalmazódott, hogy „egyáltalán szükséges nekünk ez az infrastruktúra?". A kérdésre egyértelmű válasz azóta sem született, de az biztosra vehető, hogy valamilyen hitelesítési technológia alkalmazása nélkül nem lehetséges megbízható módon használni az internetes technológiákat, mivel egy egyszerű elektronikus levél tartalmában és küldőjében sem lehet megbízni önmagában általános esetben[1]. A fogalmi zavart jól jelzi, hogy az elektronikus leveleknél aláírásnak (signature) nevezték már a kezdetek óta a levelek végére automatikusan odaillesztett, előre megírt záradékokat, amely, ha nem aláírási céllal készült, hanem a levél küldője a kedvenc idézetét osztotta meg minden levele végén, akkor nem volt megfeleltethető az elektronikus aláírás fogalmának sem, és teljes mértékben különbözött a digitális aláírás kriptográfián alapuló fogalmától.

Az elektronikus aláírás fogalmát 2014 óta az eIDAS-rendelet[2] írja le az Európai Unió területén, amely szerint az elektronikus aláírás olyan elektronikus adat, amit egy másik elektronikus adathoz csatolnak, és amit az aláíró (signatory) aláírásra használ. Az aláírás fogalma tehát az aláírni szándékozó személy tevékenységén és az azt kiszolgáló folyamaton alapul, mivel olyan természetes személyt (natural person) kell alatta érteni, aki éppen aláírási szándékkal végez valamilyen tevékenységet, azaz aláír. Ennek

[1] Bob Thomas (a BBN-TENEX munkatársa) 1974 júliusában ezt a kérdést tette fel az RFC 644-ben: „Hogyan lehet egy internetes levél címzettje 'bizonyos' abban, hogy az aláírás – például a név a 'FROM' mezőben – hiteles; vagyis az üzenet valóban az állított forrásból jött?"

[2] eIDAS rendelet alatt a továbbiakban az Európai Parlament és a Tanács 910/2014/EU rendeletét (2014. július 23.) értjük.

ismeretében a következő implicit kérdéseket veti fel az elektronikus aláírás az aláírást értelmezni kívánó entitás számára:

- az aláíró természetes személy? (a szubjektumra vonatkozik)
- az aláírásként szereplő adat csatolható-e másik adathoz? (a kapcsolódási funkcióra vonatkozik)
- az aláíró mely elektronikus adatokon hozott létre aláírást? (a kapcsolt objektumra vonatkozik)

Magyarországon 2014-ig a jogi személyek (legal person) és a természetes személyek (natural person) aláírása nem különült el definíció szintjén, mindkét entitás képes volt elektronikus aláírást létrehozni. Az eIDAS rendelet hatályba lépését követően az Európai Unió megkülönbözteti a jogi személyek aláírását a természetes személyek aláírásától, és külön szóval is illeti. Ez a fogalom az elektronikus bélyegző (electronic seal), létrehozója pedig kizárólag jogi személy lehet. Az elektronikus aláírás és bélyegző fogalmai között erőteljes hasonlóság van. Ebből adódóan a fentiekhez hasonló három kérdés fogalmazható meg az elektronikus bélyegző értelmezésének tárgyában is.

Tekintettel arra, hogy az elektronikus aláírásokhoz számos további jellemző csatlakozik, felmerül a kérdés, hogy lehetséges-e az elektronikus aláírás jellemzőit dimenzionálni és milyen alapelvek mentén. Dimenzionálás alatt elsősorban az elektronikus aláírások halmazának feloszthatóságát értjük, és lefedjük a dimenziók meghatározásával, illetve az egyes dimenziók értékkészleteinek rögzítésével. Társadalmi célú felhasználásra nem látszik indokoltnak a dimenzió induktív definícióját alkalmazni úgy ahogyan ezt a topológia számára megalkották – és ahogy ezt van Dalen 2005-ben leírta, de a mérhetőséghez nyilvánvaló módon szükséges valamilyen metrika definiálása a meghatározott dimenziókon. A fogalmak tisztázását, az elektronikus aláírás tulajdonságainak egyértelműsítését követően válik lehetővé az elektronikus aláírások leírására egy olyan metrikus tér definiálása, ahol két elektronikus aláírás távolsága egyrészről mindig nemnegatív, másrészről akkor és csak akkor nulla, ha a leírásukban kizárólag ugyanazok a tulajdonságok szerepelnek. Ebből a definícióból az is következik, hogy két elektronikus aláírás nemcsak akkor lesz nulla távolságra, ha ugyanazon dokumentum ugyanazon aláíró által ugyanabban az időben megtett aláírására, vagyis önmagának bitszinten azonos másolatára vonatkozik, hanem akkor is, ha – egy absztrakciós szintet megalkotva – ugyanolyan tulajdonságokkal írható le. Informatikai értelemben, azaz a gyakorlati megvalósításban nem lesz szükségszerűen azonos két ugyanolyan tulajdonságokkal rendelkező elektronikus aláírás, sőt, jellemzően különböző bináris reprezentánsok lesznek ebben a leíró térben ugyanazon a helyen. Ha létezik, csak egy ilyen metrika biztosíthatja az elektronikus aláírás teljesebb körű tárgyalását elméletben (in thesi) és gyakorlatban (in praxi), a társadalomban és a társadalom működését normativizáló jogban egyaránt.

Végül felmerül az a kérdés is, hogy az elektronikus aláírások általános leírására alkalmas dimenziók használhatók-e az elektronikus ügyintézés során bármilyen változtatás nélkül, azaz van-e értelme megkülönböztetni az elektronikus aláírások általános és közigazgatási felhasználását. A megkülönböztethetetlenségnek az lenne a feltétele, hogy a közigazgatás külön sajátos szabályok előírása nélkül legyen képes kibocsátani és befogadni elektronikus aláírásokat, illetőleg elektronikusan aláírt tartalmakat.

Az eIDAS rendelet a tagállamok közigazgatási rendszerei számára csak részben tette kötelezővé az előírások alkalmazását, nem kell például a közigazgatási belső eljárások lebonyolítására szolgáló és ehhez bizalmi szolgáltatásokat igénybe vevő rendszerekre az eIDAS-rendelet előírásainak vonatkozniuk. A harmadik felek számára is elérhető nyilvános bizalmi szolgáltatásokra nézve viszont kötelezően kell érvényesíteni az európai előírásokat.

Mivel Magyarországon az ügyfelet megilleti az elektronikus ügyintézési jog az elektronikus ügyintézést biztosító szerv előtt, illetőleg az elektronikus ügyintézés valódi alternatíva a közigazgatási hatósági ügyek intézése során (lásd Ákr.) életveszély kivételével az ügyfél kezébe adva a döntési jogot 2018. január 1-től a kapcsolattartás módjáról, a normativitást biztosítva az elektronikus ügyintézés szabályait a közigazgatás külön rendeletben tette közzé. A 137/2016 (VI. 13.) Kormányrendelet az elektronikus ügyintézést nyújtó szervezetekre, a kiadmányozásra, az alkalmazható bizalmi szolgáltatásokra és a felügyeleti szervre terjed ki (a továbbiakban EüszR.). A Magyar Köztársaság már korábban is élt a külön előírások definiálásának jogával a közigazgatási ügyek elektronikus intézése vonatkozásában, amit Magyarország 2012-től folytatott, ez indokolttá teszi az általános célú vizsgálatok kiterjesztését a közigazgatásra vonatkozó speciális előírásokra is, amivel a civil és a privát szféra mellett a közszférát is be lehet vonni az elemzésbe.

Érintőlegesen kitekintve az alkotmányok hitelesítésére azt találjuk, hogy Angliában a Magna Chartát I. János kézzel írta alá, az Aranybullát II. András az aranypecsétjével hitelesítette, az Amerikai Egyesült Államok alapító okiratát pedig minden alapító atya a saját kézi aláírásával látta el az irat 4. oldalán. Az aláírásoknak tehát olykor különleges jelentőségük van, mint helyhez, időhöz és kontextushoz kötött tevékenység. Ez a jelentőség azonban csak egy adott társadalomban érvényesülhet, amennyiben az nem globális. A magyar közigazgatás szempontjából az értekezés a „Magyary Zoltán Közigazgatás-Fejlesztési Program (MP 12.0) – a haza üdvére és a köz szolgálatában” vonatkozásában az alábbi célokhoz kapcsolható:

- az elektronikus közigazgatás kiterjesztése (3.2.3.1.), és
- az adminisztratív terhek csökkentése (3.2.3.2.).

2 A kutatás hipotézisei, céljai, módszerei

Hipotézis: Az elektronikus aláírások az őket leíró jellemzők segítségével mérhetővé tehetők, és az egyes aláírástípusok egyértelműen jellemezhetők egy alkalmas metrikus térben.

Az elektronikus közigazgatás mérésére számos módszertan jött létre az elmúlt időszakban. Az elektronikus közigazgatásban a kezdetektől fontos szerepet játszott az elektronikus dokumentumok hitelesíthetősége, azonban az alkalmazott megoldások mérésére vagy mérhetőségére kevés információval rendelkeztünk idáig.

Az elektronikus aláírás szabályozási igénye maga után vonta a fogalom szabatos definiálásának igényét is. Az eIDAS által az európai jogrendbe beemelt definíció alapján az elektronikus aláírás olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ. Ebből a definícióból automatikusan nem következik az elektronikus aláírások mérhetősége (a triviális mérhetőségen kívül), ezért jogosan tehető fel az a kérdés, hogy lehetséges-e mérni az elektronikus aláírást nem triviális módon, más szóval: létezik-e egy vagy több olyan metrika, amely minden egyes elektronikus aláíráshoz egy konkrét és egyedi értéket rendel hozzá, és alapjául szolgálhat az elektronikus aláírások összehasonlításának. A hipotézis igazolható, ha létezik legalább egy olyan metrikus modell, amelyikben elhelyezhető minden ismert elektronikus aláírás, és amelyik különböző aláírástípusokhoz különböző értékeket rendel hozzá, a hipotézist viszont el kell vetni, ha nem hozható létre ilyen modell sem elméletben, sem pedig a gyakorlatban. Ilyen értelemben nem valamiféle „jóság” kimutathatósága volt az alapvető célkitűzésem, hanem az, hogy minden elektronikus aláírást a saját tulajdonságai alapján reprezentálni lehessen egy arra alkalmas modellben, amely lehetővé teszi az aláírástípusok különbségeinek a vizsgálatát is.

A kutatás során a digitális aláírásra, az elektronikus aláírásra és az elektronikus hitelességre vonatkozó eredményeket és követelményeket tekintettem át, amelyből absztrakciót alkalmazva definiáltam az értékelés alapjául szolgáló dimenziókat. Tekintettel arra, hogy az elektronikus aláírás nem műszaki fogalom, ellenben műszaki tartalomból lett társadalmi szinten definiálva, a technológiák társadalmi beágyazódásához szükséges mechanizmusokat is elemeztem, a releváns jogi háttérrel és társadalmi konstrukciókkal együtt, ezek időbeni megjelenését és változásait követve a digitális aláírás fogalmi (elméleti), majd műszaki (gyakorlati) megjelenésétől az elektronikus aláírás globális (társadalmi) elterjedési és használati igényéig bezárólag. Az elektronikus aláírás térben és időben történő változásait és a változások kölcsönhatásait megvizsgálva eljutottam az elektronikus aláírás ontogenezisének értelmezéséhez.

A kutatás fő módszereként a szintézisen alapuló modellalkotást választottam. A modell dimenzióinak meghatározásához felmértem az elektronikus aláírások ismert és

lehetséges jellemzőit, az egyes jellemzőket összefoglaló dimenziókban meghatároztam az értékekként számításba vehető elemeket. A modell mérhetőségének megteremtéséhez leképezést definiáltam a modell és egy többdimenziós euklideszi vektortér között, eközben a mérhetőség biztosításához numerikus értékeket rendeltem minden olyan elemhez, amely kategorikus attribútumként volt csupán leírható. Ezt követően kategorizáltam a már rögzített elemeket, a kategóriákat elneveztem dimenzióknak, és megvizsgáltam az egyes dimenziók egymástól való esetleges függőségét is statisztikai módszerek alkalmazásával. Mivel az attribútumok nem folytonos, hanem diszkrét változók, és nem két, hanem több változó közötti összefüggésrendszert kellett elemezni, a CATPCA (főkomponens-analízis kategorikus változókon) statisztikai módszert választottam ehhez alapul. A modell értékkészletében felhasznált elemeket alapvetően három forrásból gyűjtöttem össze a szintézist megelőzően:

- az elektronikus aláírásokra vonatozó műszaki szabványokból,
- magyar, európai és nemzetközi jogszabályok előírásaiból, valamint
- a tudományos adatbázisokban fellelhető publikációk kulcsszavas keresése és a találatok áttanulmányozása során kiemeltem az elektronikus aláírások és bélyegzők, illetve a digitális aláírások valamely aspektusának a tárgyalásával kapcsolatosan megjelenő egyes attribútumokat.

A fentiek során feltárt, összegyűjtött és dimenzióként validált jellemzőket egy absztrakt modell segítségével foglaltam rendszerbe. Az elektronikus aláíráshoz szorosan nem köthető attribútumokat is megvizsgáltam és döntöttem a modellben való megjelenítésükről vagy elutasításukról. A modellt ezt követően alkalmaztam empirikus mintákra, és következtetéseket vontam le a modell kimeneteinek értékelése alapján. A kapott eredményekből kidolgozott klaszterek segítésével a modell eredményeinek alkalmazhatóságára adtam példát.

Az értekezés egyik külön fejezetében elemzem a kézírásos aláírás és a digitális aláírás emelt biztonsági szintű alkalmazhatóságát a jogszabályi háttér és következményeinek bemutatásával, ami elvezetett a fokozott biztonságú biometrikus elektronikus aláírás fogalmának létrejöttéhez, amely így integrálhatóvá vált a modellbe is. A fogalom létezésének szükségszerűségét dedukcióval, a fogalom gyakorlati tartalommal való kitölthetőségét pedig egy prototípus empirikus leírásával támasztottam alá.

A társadalmi integráció és az innovációk elterjedése vizsgálatához a technológiai innovációk társadalmi használatához szükséges tudást és annak potenciális elterjedési mechanizmusait is bemutatom kiegészítő elemként, a digitális tanúsítványoknak a magyar elektronikus társadalomban való penetrációjának valós adatokon nyugvó elemzésével és az adatokból való konzekvenciák levonásával együtt.

3 Az értekezés felépítése és a vizsgálat leírása

Az értekezés hét fő fejezetben tárgyalja az elektronikus aláírások és bélyegzők tulajdonságait és ezek mérhetőségét. Az értekezés felépítése pontosan tükrözni a vizsgálat lefolytatásának kettősségét, vagyis a kérdés társadalmi és technológiai oldalról való megközelítésének szükségességét. A bevezető gondolatokat követően a 2. fejezet az elektronikus aláírás társadalmi beágyazódását tekinti át, a hitelesség történelmi elemzésén, a társadalmak evolúciós kérdéskörén és annak a technológiára gyakorolt mérhető hatásain keresztül a bizalom és a hitelesség kapcsolódásának feltárásával együtt, ideértve a hitelesség időben változó dinamikájának a leírását is. A fejezet megközelítésmódja technológiai, arra a kérdésre próbál választ adni ez a fejezet, hogy az aláírási technológiák hogyan bukkantak fel társadalmi szinten. Nem lehet elhagyni a magyar közigazgatás által kialakított speciális szabályok ismertetését sem, hiszen az elektronikus ügyintézés volt az elmúlt időszakban a legnagyobb motorja az elektronikusan aláírt dokumentumok használatának, és számos olyan új elemmel gazdagította az elektronikus ügyintézési folyamatokat, amelyek kapcsolódtak az elektronikus aláírásokhoz vagy azok valamely jellemzőjéhez. Ez a fejezet kitér még a digitális tanúsítványok elosztásának a számosságból adódó problémájára, ha azokat állampolgári szinten kell előállítani, mivel ilyen tapasztalattal Magyarország a kormányzati hitelesítésszolgáltató megindítását megelőzően nem rendelkezhetett. A probléma vizsgálatához egy olyan egyszerűsített modell (R.M.) lett megalkotva, amelynek a működése analitikus képlettel nagy valószínűséggel nem írható le. A közigazgatási kiegészítések rávilágítottak arra, hogy ma az ügyintézők preferenciája a személyes ügyintézés felé fordul, de arra is, hogy az ügyek elektronikus intézése folyamatosan jelen van és egyre növekszik a használati arány. A biztonsági kérdések tárgyalása zárja a 2. fejezetet.

A 3. fejezet az elektronikus aláírás koncepciójának az időbeli változását írja le. A fejezet megközelítésmódja a társadalomra fókuszál, arra a kérdésre próbál választ adni ez a fejezet, hogy a társadalmi szinten megjelenő problémákra a technológia hogyan tudott választ adni. Ehhez a hitelesség igényének megjelenését és az írásbeliséggel való kapcsolódását tekintettem át elsősorban. A fejlődési ív bemutatására megalkottam az elektronikus aláíráshoz kapcsolódó általam fontosabbnak tartott magyarországi események kronologikus listáját, amelyből átfogó képet lehet kapni a hazai történések időbeliségéről és egymásutániságáról. A jogszabályi háttér fontos társadalmi aspektus, hasonlóképpen az intézményesült technológiai rendszerekkel szemben támasztott bizalom másik fontos tényezője a nem rendeltetésszerű használat szankcionálásának a mértéke, azaz a jogos felhasználók érdekeinek a védelme is, ezeknek a bemutatásával zárul a 3. fejezet.

A 4. fejezetben rátérek az elektronikus aláírások és bélyegzők jellemzőinek a tematikus tárgyalására és a lehetséges dimenziók kiválasztását is elvégzem. Az egyes dimenziók függetlensége vagy egymástól való függőségének feltárása fontos tulajdonsága a modellnek, ezért a feltárt függőségeket táblázatos formában vizualizáltam. A dimenziók tárgyalását követően az elektronikus aláírás dimenziómodell megalkotása következik. Tekintettel arra, hogy a modell időben változhat, az egyes verziókat érdemesnek gondoltam verziókezelés alá vetni, így a dolgozatban ismertetett modell verziószámának az 1.1-et adtam, mivel a műhelyvitára bocsátott tervezet tartalmazta az 1.0 verziójú modellt, az azóta történt változások pedig indokolták a verziószám növelését. Megvizsgálva a lehetséges értékeket és az ábrázolás egyértelműségét, a következő formulával lehet meghatározni egy elektronikus aláírás (bélyegző) értékét olyan módon, amely az azonos típusú aláírásoknak azonos értéket biztosít:

$$V(ES) = \{D_1(ES); D_2(ES); \ldots, D_{14}(ES)\},$$

ahol ES az elektronikus aláírás/bélyegző, D_x pedig az aláíráshoz/bélyegzőhöz tartozó 14 dimenzió, $D_i(ES)$ pedig az ES aláírás/bélyegző adott dimenzióban felvett értékét jelöli (i=1, 2, …, 14), így V(ES) egy tizennégy természetes számból álló vektort fog jelenteni ebben a modellben. Az egyes dimenziókat és az értékek magyarázatát az alábbi táblázat rögzíti. Az értékkészleteket a dolgozat részletesen leírja.

D_i	Dimenzió	Leírás
D_1	Megjelenítés	Az aláírás kódolási szabványát jelöli
D_2	Aláírástípus	Az aláírás biztonsági szintjét jelöli (gyakorlatilag I/N módon)
D_3	Alaki bizonyító erő	Az aláíráshoz fűzött jogi vélelem
D_4	Komplexitás	Az aláírás részleteinek jelölése, ideértve a szabályzatok, időjel, érvényesítési adatok és időbélyegek aláírásba kerülésének jelzését
D_5	Érvényességi idő (nap)	Azt az időtartamot jelöli napban kifejezve, ameddig az aláírás ellenőrzését bármikor el kell tudni végezni
D_6	Tanúsítvány szabvány	Az aláíráshoz tartozó tanúsítvány létrehozási formátumát adja meg
D_7	Aláíró entitás	Az aláíró entitás kategóriáját jelöli
D_8	Aláíró algoritmus	Az ismert és elterjedten használt kriptográfiai aláíró algoritmusokat sorolja fel
D_9	Aláírás-létrehozó adat hossza	Az aláírás-létrehozó adat hossza bitben meghatározva
D_{10}	Aláírás-létrehozó adat tárolója	Az aláíráshoz használt adat tárolási helyét és módját specifikálja

D_i	Dimenzió	Leírás
D_{11}	Aláírás relációja	Az aláírás relatív pozícióját írja le több aláírás esetében
D_{12}	Aláírás elhelyezkedése	Az aláírások helyét rögzíti az aláírt adatokhoz viszonyítva
D_{13}	Tanúsítvány kiállítója	A tanúsítvány kibocsátójának típusa
D_{14}	Speciális attribútumok	További jellemzők (pl. magyar állampolgári, a magyar közigazgatásban használható)

1. táblázat: Az elektronikus aláírás dimenziómodell (forrás: saját táblázat)

A dimenziók értékeinek a meghatározása során három alapelvet próbáltam meg szem előtt tartani:

- ALAPELV 1: különböző aláírások esetében a modell különböző értékeket rendeljen az aláírásokhoz hozzá (a fentebb tárgyalt tipizálás figyelembevételével),
- ALAPELV 2: a hasonló aláírások távolsága legyen olyan, hogy meg lehessen különböztetni őket a nagyon eltérő aláírásoktól és egymástól is,
- ALAPELV 3: a hasonló aláírások közelsége adjon lehetőséget klaszterek kialakítására.

Ennek a három alapelvnek a szem előtt tartásával lettek definiálva a dimenziók értékkészletei. Az egyes értékek „jóságának" tükrözése az értékekben nem volt célom.

Az 5. fejezetben bemutatom, hogy az így kialakított elektronikus aláírás/bélyegző dimenziómodellben az egyes aláírások/bélyegzők reprezentálás hogyan történik, illetőleg milyen méréseket lehetséges elvégezni a különböző típusú aláírások és bélyegzők között. A mérhetőség kidolgozását elméleti megfontolásokkal kezdtem, amelyet a modell működésének valós példákon vett gyakorlati bemutatása követi. Két elektronikus aláírás *távolsága* alatt a következő értéket értjük (a képletet a vektorok távolságára az n-dimenziós euklideszi térben általánosan használt matematikai formula alapján készítettem el):

$$\sqrt{((D_1(ES_1) - D_1(ES_2))^2 + ((D_2(ES_1) - D_2(ES_2))^2 + \cdots + ((D_{14}(ES_1) - D_{14}(ES_2)^2}$$

és $T(V(ES_1);V(ES_2))$-vel jelöljük. A különbségek értelmezéséhez a vektorok abszolútértékeit hívjuk segítségül. Két elektronikus aláírás *különbsége* alatt a következő (abszolút)értéket értjük a továbbiakban (a képletet az n-dimenziós euklideszi térben a vektorok hosszának számítására általánosan használt matematikai formula alapján írtam fel):

$$\left| \sqrt{(D_1(ES_1))^2 + ((D_2(ES_1))^2 + \cdots + ((D_{14}(ES_1))^2} - \sqrt{(D_1(ES_2))^2 + (D_2(ES_2))^2 + \cdots + (D_{14}(ES_2))^2} \right|$$

és $K(V(ES_1);V(ES_2))$-vel jelöljük.

Az elektronikus aláírások csoportosításához a vektorok hosszértékei mellett a vektorok különbségvektorainak a hossza is felhasználható, mivel valamivel finomabb felbontásban mutatja meg az egyes aláírásokhoz tartozó vektorokból látható hasonlóságokat és különbségeket.

A 6. fejezet az európai szabályozás technológiafüggetlenségét mutatja be és ennek következményeként értelmezi a biometrikus kézírás jellemzőin alapuló fokozott biztonságú biometrikus elektronikus aláírás fogalmát. A vonatkozó szabványok számos olyan technológiai megoldást definiálnak, amelyek kielégítik a fokozott biztonságú elektronikus aláírással szemben támasztott magasabb szintű követelményeket, amelyek kriptográfiai titkos kulcs használatán alapulnak. A papíralapú világban az aláírás az aláíró kézírásához kapcsolódik, ennek az elfogadottsága a polgári társadalom óta nem kérdéses, és kialakultak a vitatható aláírások vizsgálatának módszerei és eljárásrendjei is. Kérdésként merült fel, hogy létezik-e az elektronikus világban olyan elektronikus aláírás, amely egyrészről az aláíró kézi aláírásán alapul, másrészről kielégíti a fokozott biztonságú elektronikus aláírással szemben támasztott magasabb szintű követelményeket. A kérdésre válaszként bemutattam egy az üzleti világban alkalmazott gyakorlati példát (prototípus), amelyet banki környezetben implementáltak. A fokozott biztonságú aláírás tárgyalását követően meghatároztam az ilyen aláírásokhoz kapcsolható tanúsítványok egy lehetséges felépítését. A nem minősített biometrikus aláíró tanúsítvány tartalmára adott koncepcionális javaslatom egy aláírási célú X.509v3 tanúsítvány és egy nyilvános kulcsot nem tartalmazó X.509v2 attribútumtanúsítvány „keresztezéséből” jött létre, figyelembe véve a biometrikus aláírás és környezete specialitásait.

A 7. fejezetben röviden kitértem az elektronikus aláírás/bélyegzés használatát elősegítő tudás átadásának létező, lehetséges és ajánlott formáira. Feltételezve, hogy legalább az elektronikus aláírás ellenőrzéséhez szükséges tudás elterjedése kívánatos, a probléma egyik eleme az, hogy az aláírás technikáit nem oktatják graduális szinten, és a felhasználói szintű oktatás sem eléggé elterjedt ahhoz, hogy kritikus tömegről tudjunk beszélni, más szóval az elektronikus aláírás oktatása alacsony szinten intézményesült idáig Magyarországon. Kérdés, hogy az elektronikus ügyintézés során hogyan képzelhető el ennek a tudásnak a hatékony felhasználást eredményező gyors elterjedése, ha graduális képzések nem vagy alig állnak rendelkezésre, továbbá az önkéntesen választható akkreditált képzési formák (ECDL) pedig évente 20 000–40 000 vizsgázót képesek befogadni? A választ a tudásmenedzsment eszközeiben véltem megtalálni.

4 Összegzett következtetések

4.1 Az elektronikus aláírás mérhetősége

Az elektronikus kommunikáció és adatok hitelességének biztosítása azok teljes életciklusában alapvető fontosságú a digitális állam működésében a katasztrófák elleni védekezés, a fenntartható fejlődés új dimenzióba helyezése, a digitális világ robbanásszerű fejlődése, a nemzetközi biztonsági környezetben beállt változások menedzselése érdekében. Az észt példa többszörösen megmutatta, hogy az egyetlen technológiai megoldásra alapozott elektronikus közigazgatás működése sérülékeny, azonban egyenrangú alternatív megoldások specifikálásával ez a sérülékenység jelentős mértékben csökkenthető. Az egyenrangúság feltételeül nyilvánvaló módon kínálkozik a megoldások értékeinek azonossága vagy szűk intervallumba való beszorítása. Az elektronikus aláírás dimenziómodell által lehetővé válik a gazdasági/biztonsági szempontok empirikus vizsgálata a közmenedzsment intézményi feltételeinek kutatásában, a tranzakcionális biztonság fejlesztésére fókuszálva. Továbbá a biztonság megvalósítása és fenntarthatósága alapvető fontosságú, valamint törvényi kötelezettség is Magyarországon és az Európai Unióban egyaránt, ennek során a hitelesség kiemelt szerepet kap a hacktivizmus terjedésével a hadüzenet nélküli háborúk időszakában. A hitelesség általános biztosításához nélkülözhetetlen valamely fejlett elektronikus aláírás vagy azzal egyenértékű technológiai megoldás használata. A hitelesség fenntartásához megelőző, feltáró és javító kontrollok is szükségesek, ezek közül a modell szervesen kapcsolható a digitális állam fenyegetései és a kiberkatasztrófák elleni védekezés feltáró kontrolljaihoz is.

4.2 A biometrikus aláírások alkalmazhatósága

A fokozott biztonságú biometrikus aláírás létezésének fel- és elismerésével a minősített biometrikus aláírás létrehozása is lehetővé válhat (a szükséges aláíró eszköz tanúsítását és a biometrikus aláíró tanúsítvány nemzetközi szabványosítását követően), amivel megteremthető a kézírással egyenértékű elektronikus kézírás lehetősége az EU-ban, és nem kizárólag nemzeti szinten. A bemutatott megoldás minősített tanúsítvánnyal és tanúsított aláíró eszközzel kiegészítve azonban már most is teljes bizonyító erővel rendelkező fokozott biztonságú elektronikus aláírást lenne képes biztosítani az e-közigazgatásban az elektronikus aláírási képességgel nem rendelkező polgárok számára. Ez a megoldás a digitális szakadék hatásának csökkenését vagy akár eltűnését eredményezheti, és független a digitális szegénységtől, valamint az e-részvétel (e-participation) minden területén nemzeti szinten is alkalmazható. A fokozott biztonságú biometrikus aláírás használatával a technológiai ellátottságtól és tudástól függetlenül minden polgár bevonható az e-közigazgatásba, teljes mértékben megvalósítható a minősített elektronikus vagy kézi aláíráson alapuló papírmentes e-közigazgatás.

5 Új tudományos eredmények

H1. Az elektronikus aláírások az őket leíró jellemzők segítségével mérhetővé tehetők, és az egyes aláírástípusok egyértelműen jellemezhetők egy alkalmas metrikus térben.

T1. Az elektronikus aláírás triviális mérhetőségén (azaz bináris számként való megjelenítésén) túl definiálható egy olyan metrikus tér – az elektronikus aláírás dimenziómodell –, amely az elektronikus aláírások és bélyegzők absztrahált tulajdonságain alapul, és mérhetővé teszi az elektronikus aláírásokat, illetve az elektronikus bélyegzőket is bármely környezetben. A modellben a mérés alapjául a dimenziók értékkészleteinek skaláris megjelenítése szolgál, amely lehetővé teszi az egyes elektronikus aláírásokhoz rendelt értékek numerikus ábrázolását. Az ábrázolást követően az eredményekkel algebrai műveletek végezhetők, például átlagszámítás, különbségek vagy távolságok értékeinek kiszámíthatósága, és az értékek jelentéseinek megfogalmazása alapján lehetséges értékelni a technológiailag különböző megoldásokat.

Ha rendszerszemléletben kívánjuk megfogalmazni a modell eredményét, akkor az elektronikus aláírások hatásait minden kapcsolódó társadalmi rendszerben lehetséges a modell segítségével explicit módon kifejezni, azonban a dimenzióknak az egyes társadalmakban alkalmazható értékkészleteit „bottom-up” módszerrel, alulról felfelé célszerű kialakítani. Ha minden egyes olyan értéket, amelyet valamely társadalom használ, bele tudunk illeszteni a modellbe, akkor az eredmény globálisan is teljes mértékben használható. Amennyiben minden historikus értéket is bele tudunk foglalni a modellbe, akkor az értéknek az időbeli változása is megjeleníthető lesz a modellben. Ez azt jelenti, hogy ez a modell egy olyan generalizált eszközt biztosít, amely mérhetővé teszi az elektronikus aláírások mint objektumok absztrakt tulajdonságai által definiálható rendszer kapcsolódási pontjait, mélységét és természetét minden további érintett rendszer számára.

A kapcsolatok feltárásához szükséges az aláírások hatásának társadalomtudományi eszközrendszerrel történő vizsgálata (itt jól használhatók lehetnek a gyenge konstrukciós, az erős konstrukciós vagy a technológiai determinizmus elméletek). A modellnek ugyanis szüksége van kategóriákra és a kategóriákon belül értékekre (ilyen például a különböző aláírástípusokhoz fűzött jogi vélelem a különböző társadalmakban). Az elektronikus aláírási rendszer vagy rendszerek önmagunkban is rendszereknek vagy alrendszereknek tekinthetők, amelyek önmagukra nézve is felvethetnek kérdéseket, de társadalmi aspektusból fontosabbnak látszik annak vizsgálata, hogy az elektronikus aláírás technológiai rendszere egyrészről milyen más társadalmi rendszerekkel van kapcsolatban és gyakorol rá hatást, illetve fordított irányban, milyen társadalmi rendszerek hatnak rá és hogyan. Az elsőre példa az e-közigazgatás közműve, illetve ennek

minden releváns alrendszere, míg a másodiknak a normatíva, a közigazgatási jog lehet egy jól körülhatárolt alkalmazási területe. Nemeslaki András felvetése így reálisnak látszik az elektronikus aláírás mint kollaboratív, mindenhová beépülő ICT-rendszer esetében is, vagyis az aláírások hatásainak társadalmi konstrukciós elméletek alapján történő vizsgálata nagy segítséget nyújthat a tudományos és pragmatikus igényeknek egyaránt megfelelő hiteles dolgok és eszközök internetes (IoT „Internet of Things" dolgok internete, IoD „Internet of Devices" eszközök internete kifejezések rövidítéseként ismert) hálózatának kialakításában és fenntartásában egyaránt. Gondolok itt például annak a kérdésnek az eldönthetőségére, hogy kit lehet felelősségre vonni, ha egy szállító drón balesetet okoz, vagy két eszköz egymást támadja, és fizikai károkozás következik be.

A társadalmi aspektus másik kiemelt vetülete a digitális megosztottság, amelynek hatása az elektronikus aláírás területén is jelentkezik. A digitális megosztottság mindhárom, Molnár Szilárd által összefoglalt szintjén (hozzáférés, használat, használati minőség) beavatkozás szükséges ahhoz, hogy az elektronikus aláírási technikák jelen lehessenek a hétköznapi életben, különös tekintettel az e-közigazgatási ügyintézésben. Nem hagyhatók figyelmen kívül Csótó Mihály következtetései az információs szegénységről, amely szerint egyrészt a technológiákhoz való hozzáférés vagy annak hiánya jelentős hatást gyakorol a társadalom szereplőire, másrészt az eddigi tapasztalatok alapján a technológia inkább fokozza az egyenlőtlenségeket, nem pedig megszünteti, harmadrészt általában vett információs szegénység nem definiálható, ezt a fogalmat csak egy adott kontextusban van értelme mérni egy adott normarendszer alapján. Ebből adódik, hogy az elektronikus aláírás használata tovább mélyítheti a digitális szakadékot, továbbá az információszegénység az elektronikus aláírás kontextusában is értelmezhető fogalom, a fentebb vázolt dimenziók pedig segíthetnek a kontextusok pontosabb feltérképezésében. A kérdés az, hogy vajon mi szükséges a digitális szakadék negatív felén lévő populáció számosságának és arányának csökkenéséhez a pozitív oldalhoz képest. Ha nem feltételezhető számottevő ismeretanyag a felhasználói körről, akkor a biometrikus aláírások alkalmazása jó választás lehet, mivel a felhasználói oldal részéről nem követel meg sem tudást, sem pedig eszközöket, a digitális világba mégis be tudnak lépni. Távolabbra tekintve felmenő rendszerben a graduális oktatás kiváló eszköz az elektronikus aláírási technológiák bevezetéséhez a digitális szakadék mindkét oldalán. Az elektronikus aláírási ismeretanyag és az e-közigazgatás által megkövetelt elektronikus ügyintézésben szükséges elektronikus aláírási kompetenciák közötti különbség számszerűsítése következtében mérhetővé válik a digitális szakadék is. Ugyanez a metódus alkalmas az ügyfelek pozicionálására és az elmozdulás folyamatos mérésére is. Ezzel az érveléssel belátható, hogy az elektronikus aláírások és bélyegzők értékelése a kidolgozott modell alapján a közigazgatásban is automatizált módon alkalmazható szabályozási, tervezési, implementálási, oktatási és monitorozási célokra egyaránt.

6 A kutatási eredmények gyakorlati felhasználása

6.1 Az elektronikus aláírás mérhetősége

Az elektronikus aláírás mérhetősége hozzájárul a hatékonyság növeléséhez a közhatalom gyakorlásában, az elektronikus véleménynyilvánítási lehetőségek fejlesztésével további empirikus vizsgálatok lefolytatását teszi lehetővé az államtudomány, a közigazgatás, az önkormányzatok, a honvédelem és rendészet területén. Tekintettel arra, hogy a mérhetőség nem korlátozódik csupán a technikai elemekre, hanem érvényes a társadalmi konstrukciókra is, a modell alkalmazható a jogalkotásban (például az adott kontextusban felhasználható elektronikus aláírások minimumszintjének és maximumszintjének numerikus definiálhatósága révén) is. Ezáltal csökkenthető a technológiafüggetlenség jogbiztonságra gyakorolt kedvezőtlen hatása, mivel egy adott érték specifikálása jelentős bizonytalanságot szüntet meg az adott szituációban az adott elektronikus aláírás elfogadhatósága terén. Az elektronikus aláírások mérése azok e-közigazgatási szolgáltatásokba való bevezetését megelőzően már a tervezési szakaszban elvégezhető lenne (pl. a hatásvizsgálat részeként), ami megelőzheti különösen a „gyenge technológia – erős jogi vélelem” kockázatos vagy az „erős technológia – gyenge jogi vélelem” költséges párok kialakulását.

További fejlesztési lehetőséget kínál a modellnek különböző társadalmakra vagy országokra való kiterjesztése és a kiterjesztések potenciális összegzése is, ami a globális egységes értékelés lehetőségét nyújtja. Egy lehetséges kiterjesztés az időben eltérő állapotok historikus elemzése, ami felveti a modell értékeinek különböző időpontokban való ábrázolásának és ezek összehasonlításának lehetőségét is.

6.2 A biometrikus aláírásokban rejlő globális potenciál

A biometrikus megoldásoknak számos előnye van az üzleti és az e-közigazgatási oldalon is, mivel ezek az ügyfelek részéről nem igényelnek jelentős költségeket, hatékonyak és a biometria alkalmazása nem igényel semmilyen oktatást sem az ügyfelek számára, de a használatuk elterjedése azonban mégis korlátozott lehet, mert az ilyen aláírások határokon átnyúló elfogadása esetében szükséges a nemzeti jogszabályok kiterjesztése. Amíg Magyarországon a minősített elektronikus tanúsítványon alapuló fokozott biztonságú elektronikus aláírásnak teljes bizonyító ereje van attól függetlenül, hogy hol keletkezett az aláírás, más tagállamokban a joghatásról csak akkor lehet bármilyen képet alkotni, ha a nemzeti jogszabályok erről érdemben rendelkeznek. Ha nincs ilyen rendelkezés az adott nemzeti jogban, akkor elképzelhető, hogy ugyanannak az aláírásnak más-más joghatása lesz különböző tagállamokban. Mindezt az teszi lehetővé, hogy a minősített elektronikus aláírás fogalmának kialakításakor a kézi aláírást tették meg referenciapontnak.

Nem kétséges, hogy a biometrikus elektronikus aláírás addig csak nemzeti szinten lesz használható, amíg a fokozott biztonságú biometrikus aláírások létrehozásának és ellenőrzésének módszereit nem szabványosítják és széles körben el nem fogadják. Bi- vagy multilaterális megállapodások alapján elméletileg a határokon átnyúló elfogadás is megvalósítható, a gyakorlatban azonban csak az általánosítás (mint például a „minden minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírásnak teljes bizonyító ereje van Magyarországon") lehet működőképes a rendeleti szintű jogalkotásig. Ehhez szükséges lehet az ügyfél aláírásának újradefiniálása a magyar közigazgatásban, hogy a bankszektor és a közigazgatás versengését és a finn példa negatív következményeit el lehessen kerülni. Jó eszköznek tűnik ehhez a Jon Ølnes és Leif Buene által felvetett validációs hatóságok („validation authority") kialakítása, amelyek a természetes személy aláírók regisztrációs dokumentumait rögzítik, tárolják, és a hozzájuk benyújtott szabványos ellenőrzési kérésekre szabványos válaszokat adnak. Ha ezeket a válaszokat a kérdés érkezési helyének területi korlátozása nélkül meg lehetne valósítani, akkor ez a megoldás globális szinten lehetővé tenné a kézírásos aláírás aláírópadokon történő használatát, hiszen mindegy, hogy a természetes aláíró hol írna alá, az aláírás ellenőrzését minden esetben a személy által erre felhatalmazott validációs hatóság végezné el, így egyrészről nem válik szükségessé minden alkalmazási helyen a regisztrációs dokumentumok másolati példányának tárolása és őrzése, másrészről a helyi validációs hatóságoknak csak a helyi aláírási szokásokkal, személyhitelesítési lehetőségekkel és automatikus aláírás-ellenőrzési problémákkal kellene megküzdeniük, nem pedig a világban felmerülő összes problémával. A validációs hatóságok globális federált láncolata biztosíthatja a biometrikus aláírások globális ellenőrizhetőségét minden regisztrációs dokumentummal rendelkező humán entitás számára, tekintet nélkül az aktuális tartózkodási helyére. Az országok közötti elfogadhatóság érdekében még egy további lépésre is szükség lenne: a nem másolható biometrikus aláírásokat önálló és egyenlő joghatással kellene felruháznia minden csatlakozó országnak, függetlenül a jelenlegi kézíráshoz, minősített elektronikus aláíráshoz vagy digitális aláíráshoz fűződő joghatásoktól. Tekintettel arra, hogy a fokozott biztonságú biometrikus aláírás teljesíti a fokozott biztonságú elektronikus aláírással szembeni európai és a joghatással bíró digitális aláírásokkal szembeni amerikai követelményeket is, ez az elképzelés nem borítaná fel a jelenlegi rendszert, csupán egy új elemet adna hozzá a már meglévő elemekhez, ami megfelel a régi szabályoknak és nem jelennének meg benne a PKI alapú aláírások globális elfogadhatóságának kialakítása során felmerülő problémák.

A technológia otthoni és mobil használata szintén elképzelhető, különösen az okosvárosokban, ha egy távoli azonosító eljárással (pl. videóazonosítással) kombinálva van, és ha az aláíró környezet biztonsága, valamint a szoftver integritása az aláírást rögzítő eszközön biztosított. Ehhez azonban – a fejlesztés ilyen irányú igényeinek

elmozdulása esetében – további innovációra lesz vélhetően szükség annak felhasználásával, hogy bizalmi listák létesítése és kezelése meglehetősen intézményesült technológiának tekinthető a fejlett világ információbiztonságának megteremtésében (pl. EU Trust List, Root CA programok).

6.3 Az oktatás fejlesztése

Oktatási szempontból megállapítottuk, hogy az elektronikus aláírási technológiák elterjedése tudásfüggő, a hozzá kapcsolódó tudás társadalmi ismerete nélkül csupán a technológiai rétegekben tud elterjedni, a technológiában jártas programozók és informatikusok révén, innen pedig a technológiai ismeretek társadalmi transzferálása nem valószínűsíthető, a tudás szerteágazó mivolta és bonyolultsága miatt. Három, nem teljesen ekvivalens megoldási mód kínálkozik arra az esetre, ha az elektronikus aláírás felhasználásához szükséges tudás elterjedése prioritássá válna Magyarországon:

1. alap- és középfokú graduális képzésbe való integrálása,

2. nem graduális, de széles társadalmi támogatottságot élvező oktatási rendszerből származó tanúsítvány preferálása (a már létező példákhoz hasonlóan) vagy

3. minimálisan invazív oktatás lehetővé tétele.

A 3. változat létjogosultságát erősíti, hogy a graduális oktatásba a Nemzeti Alaptanterv hitelességre vonatkozó elemein kívül 2020 januárjáig nem került be a terület. Az további vizsgálatot igényelhet, hogy létezik-e az átadható tudás komplexitásának felső korlátja minimálisan invazív módszerek esetében, ideértve az elsajátítani szükséges tudás mértékét vagy az ehhez szükséges időtartamot is, valamint kérdés, hogy kidolgozható-e felnőttek számára is ilyen konstrukció.

Az ECDL modul 2010 óta elérhető, de lényeges számosságot nem sikerült elérni (az NJSZT ECDL Iroda adatai szerint 205 fő szerzett bizonyítványt 2011.01. – 2019.01. között), így lehetséges, hogy új módszerek felé kell nézni a terjedés elősegítéséhez, mivel az oktatás kulcsszerepét Vrabie is megerősítette.

Vrabie rávilágított arra is, hogy a jó e-közigazgatás és az informatikai oktatás között erős korreláció áll fenn, ami azt jelenti, hogy az új innovatív megoldások *mellett* az „intelligens polgárok” létezése *is* szükséges feltétele a minőségi e-közigazgatás létezésének. Az elektronikus aláírás dimenziómodell alkalmas az oktatásban való felhasználásra is, mivel az adott területen használt elektronikus aláírások és a mindenütt nulla értékű aláírás (nullvektor) Hamming-távolságai pontosan az adott elektronikus aláírás használatához szükséges tudáselemeket jelölik meg, amelyekből olyan oktatási anyag képezhető, amelyik az eddig esetleg rejtve maradt összefüggéseket is explicit módon képes tárgyalni.

7 A jelentősebb publikációk jegyzéke

1. ERDŐSI Péter Máté: *Fokozott biztonságú biometrikus aláírások alkalmazhatósági és szabályozási kérdései a közigazgatásban*.
   - In. dr. POLGÁR Miklós tű. százados (szerk.): A társadalom szolgálatában – felkészülés és felkészítés a katasztrófavédelmi kihívások tükrében. - Pécs: Baranya Megyei Katasztrófavédelmi Igazgatóság, 2019. - p. 63-68.

2. ERDŐSI Péter Máté: *Az elektronikus aláírás fogalmának megjelenése és változása.*
   - In. Információs Társadalom. Társadalomtudományi Folyóirat, 2019. XIX. évf. 1. szám. - p. 66-91.

3. ERDŐSI Péter Máté: Elektronikus aláírás e-közigazgatási használatához kapcsolódó tudás szétosztási megoldásainak összehasonlító elemzése biztonsági aspektusból.
   - In. Társadalom és Honvédelem, 2018. 2016. évf. 2. szám. p. 31-40.

4. Dr. HORVÁTH Attila, ERDŐSI Péter Máté: *Rosszindulatú számítógépes fertőződés vizsgálatának lehetséges kérdései és indokai a közigazgatásban.*
   - In. KISS Ferenc, HORVÁTH Attila (szerk.): IT és hálózati sérülékenységek társadalmi-gazdasági hatásai. - Budapest: Információs Társadalomért Alapítvány, 2016. - p. 31-48.

5. ERDŐSI Péter Máté: *A 2013. évi L. törvény végrehajtásának tapasztalatai kettes szintű közös önkormányzati hivatalok esetében.*
   - In. KERESZTES Gábor (szerk.): Tavaszi Szél 2016 = Spring Wind 2016. Tanulmánykötet. III. kötet. - Budapest: Doktoranduszok Országos Szövetsége, 2016. - p. 34-40.

6. ERDŐSI Péter Máté: *Elektronikus aláírások ortogonális dimenzionálása*.
   - In. KISS Natália, NAGY Bálint, NÉMETH István Péter (szerk.): Tudományos terek, Dunaújváros, Magyarország: DUF Press, 2014. - p. 57-64.

7. ERDŐSI Péter Máté: *Magyar bizalmi szolgáltatások felügyeletének összehasonlító elemzése.*
   - In. Műszaki Katonai Közlöny, 2014. 2014. évf. 1. szám. - p. 200-212.

8. ERDŐSI Péter Máté: *Elektronikus írásbeliség a magyar jogban.*
   - In. Társadalom és Honvédelem, 2013. 2013. évf. 3-4 szám. - p. 589-595.

9. ERDŐSI Péter Máté: *Az információ hitelessége.*
   - In. KALOTAY Balázs, KOVÁCS Zoltán, ERDŐSI Péter Máté, KOVÁCS Árpád, OZSVÁR Ferenc, KANCSÁR Attila (szerk.): E-Government Tanulmányok

V. Elektronikus rendszerek a közigazgatásban. - Budapest: E-government Alapítvány, 2011. - p. 37-47.

10. EGERSZEGI Krisztián, ERDŐSI Péter: *Problems in the Implementation of the Electronic Signature.*
- In. Periodica Polytechnica - Social And Management Sciences, 2003. Volume 11. Issue 1. - p. 67-82.

11. ERDŐSI Péter: *Az elektronikus aláírás alkalmazásának háttere.*
- In. Híradástechnika: Hírközlés-Informatika, 2002. LVII. évf. 9 szám. - p. 41-44.

12. ERDŐSI Péter: *A hazai informatikai biztonsági helyzet és az elektronikus aláírás.*
- In. EGERSZEGI Krisztián, KISS Ferenc, GELLÉRI Péter, RÁCZ Csaba (szerk.): Intelligens rendszerek, hatékony alkalmazások. - Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem, 2001. - p. 119-131.

7.1 Fontosabb konferencia cikkek

13. ERDŐSI Péter Máté: Comparative Analysis and Measurement of Electronic Signatures Created by Notaries In Europe.
- In. From Policy Design to Policy Practice. e-Proceedings of the 27th NISPAcee Annual Conference. May 24-26, 2019 Prague, Czech Republic. - NISPAcee Press, 2019. - ISBN 978-80-89013-99-9

14. ERDŐSI Péter Máté: Advanced Biometric Electronic Signature in Practice: Lessons for the Public Administration from a Hungarian Case Study.
In. HANSEN, Hendrik, MÜLLER-TÖRÖK, Robert, NEMESLAKI András, PROSSER, Alexander, SCOLA, Dona, SZÁDECZKY Tamás (eds.): Central and Eastern European e|Dem¸and e|Gov Days 2018. Conference proceedings. - Wien, Ausztria: Facultas Verlags- und Buchhandels AG, 2018. - p. 407-418.

15. ERDŐSI Péter Máté: Digitális tanúsítvány kiosztási modelljének elemzése különböző regisztrációs feltételek mentén.
- In. CSISZÁR Imre, KŐMÍVES Péter Miklós (szerk.): Tavaszi Szél 2014 / Spring Wind 2014: I. kötet Közgazdaságtudomány, Debrecen: Doktoranduszok Országos Szövetsége, 2014. - p. 141-150.

16. ERDŐSI Péter Máté: The Integration of Electronic Signature into the Information Society in Hungary.
In. TARGAMADZÉ Aleksandras, BUTLERIS, Rimantas, BUTKIENÉ, Rita (eds.): Conference Proceedings of 14th International Conference on Information and Software Technologies. - Kaunas, Lithuania: Kaunas University of Technology, 2008. - p. 241-248.

8 Szakmai önéletrajz

Név: ERDŐSI Péter Máté

Születési idő: 1969. június 19.

Végzettség

2013/09 – 2016/07 Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi Doktori Iskola

doktori képzés

1988/09 – 1994/07 Kossuth Lajos Tudományegyetem, Természettudományi Kar

matematika-informatika szakos okleveles tanár

Nyelvismeret angol (C1), német (B1), magyar (anyanyelv)

Erdősi Péter Máté 1988 és 1994 között a debreceni Kossuth Lajos Tudományegyetemen végezte felsőfokú tanulmányait, amely során négy tudományterületen (matematika, fizika, informatika és általános nyelvészet) összesen 28 szemesztert abszolvált. 1994-ben a XXII. OTDK konferencián a társadalomtudományi szekcióban IV. helyezést ért el „A természetes nyelv egy fragmentumának ábrázolása intenzionális logikai keretben” című munkájával. Ugyanebben az évben megszerezte a matematika-informatika szakos tanári képesítését is.

Diplomájának megszerzését követően a debreceni Kossuth Lajos Tudományegyetem Informatikai és Számító Központjában kezdett el dolgozni tudományos segédmunkatársként. 2000-ben kezdett el intenzíven foglalkozni az elektronikus aláírás problémáival és oktatási kérdéseivel, ebben az időszakban született 24 publikációjának a zöme ezekkel a területekkel foglalkozott. 2001-ben csatlakozott a Budapesti Műszaki Egyetem Információ- és Tudásmenedzsment Tanszékén létrejött Biztonságmenedzsment Kutatócsoporthoz, ahol aktívan részt vett a csoport munkájában és több kutatási eredményt is publikált. A tanszék megszűnését követően a kutatási feladatokat az Információs Társadalomért Alapítvány vette át, ahol 2005 május és 2006 októbere között kutatói státuszban is dolgozott.

Szakmai tapasztalatait államilag nyilvántartott elektronikus aláírással kapcsolatos szolgáltatási szakértőként szerezte meg 2002 július 3-tól kezdődően a magyar minősített és nem minősített hitelesítésszolgáltatók éves felülvizsgálatához kapcsolódó szakvéleményei révén. 2016 július 1. óta a német TÜViT és TÜV TRUST IT külső eIDAS auditora, valamint irányítja a Crowe nemzetközi könyvvizsgáló céghálózat WebTrust auditokkal kapcsolatos munkáját is. 2019 októberétől részmunkaidőben segíti a Budapest Főváros Kormányhivatalában folyó digitalizációs munkát e-közigazgatási szakértőként.

2013-ban jelentkezett a Nemzeti Közszolgálati Egyetemnek az országban elsőként elindított Közigazgatás-tudományi Doktori Iskolájába, az elektronikus közigazgatási rendszerek biztonsága témakörrel kívánt részleteiben is foglalkozni. A doktori iskola követelményeinek sikeres teljesítését követően 2016. július 6-án abszolutóriumot szerzett. Doktori tanulmányai alatt 28 tudományos publikációja született meg, emellett egy egyetemi jegyzet szerzőjeként és egy ECDL modultankönyv társszerzőjeként elősegítette az oktatási terület fejlődését is. A 2016. évben a Tavaszi Szél országos tudományos konferencián közigazgatási szekcióban megtartott előadása megosztott első helyezést ért el. Doktorandusz hallgatóként részt vett a PD 109740 szám alatt végzett „IT és hálózati sérülékenységek tovagyűrűző társadalmi-gazdasági hatásai" című OTKA kutatásban is, amelynek eredménye hét tudományos publikáció és egy tudományos adatbázis létrejöttében érhető tetten.

A XXXIV. OTDK Had- és Rendészettudományi Szekciójában bíráló bizottsági tagként működött közre a konferencia sikerességének érdekében. A Doktoranduszok Országos Önkormányzata Közigazgatás-tudományi Szekciójának tagjaként ötleteivel, gondolataival a kezdetektől segítette a szekció munkáját.