NEMZETI KÖZSZOLGÁLATI EGYETEM

Közigazgatás-tudományi Doktori Iskola

Erdősi Péter Máté

Az elektronikus aláírás mérése

Doktori (PhD) értekezés

Témavezető:

Dr. Muha Lajos

főiskolai tanár

……..

Budapest, 2019

1. BEVEZETÉS

„Elég egyszerű volt az ügy, barátaim; mikor átvette az első végzést, és aláírta a kézbesítőkönyvet, máris elveszett. A Büro-Krá-Cia nevű csodagépet alkalmaztam; mert amíg a kozmosz kozmosz, senki sem állhat neki ellen.”

Stanislaw Lem: Kiberiáda

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 alkalmas az írásbeliség alaki követelményének kielégítésére. Példának említhetjük erre az Azonosításra Visszavezetett Dokumentum Hitelesítés (AVDH)[1] szolgáltatás által biztosított elektronikus aláírást, amelyről önmagában, további információk begyűjtése nélkül nehezen eldönthető kérdésként vethető fel az, hogy használható-e teljes bizonyító erejű magánokirat létrehozására – hazai vagy országhatáron átnyúló módon – vagy alkalmas-e közokirat elektronikus aláírására, ami alapvető fontosságú a felhasználhatóság tekintetében és egyik oka lehet az penetráció alacsony fokának. Ezek a kérdések kezdetek óta jelen vannak, a terület jeles szakemberei már 2000-ben feltették maguknak azt a kérdést, hogy létezik-e „egyetlen helyes” elektronikus aláírási struktúra [177], illetve a kockázatokat felmérve az a kérdés is megfogalmazódott, hogy „egyáltalán szükséges nekünk ez az infrastruktúra?” [5]. A kérdésre egyértelmű válasz azóta sem született, de az biztosra

[1] A szolgáltatás elektronikus aláírási lehetőséget biztosít a természetes személy felhasználók számára anélkül, hogy saját tanúsítvánnyal rendelkeznének vagy regisztrálniuk kellene a szolgáltatásba. A megfelelő szintű azonosítás és hitelesítés után távolról – akár mobil eszközről – is igényelhető elektronikus aláírás a szolgáltató titkos kulcsának segítségével, ami teljes bizonyító erejű magánokiratok létrehozásának lehetőségét biztosítja a polgárok számára. (Bővebben lásd http://www.nisz.hu/hu/avdh-azonos%C3%ADt%C3%A1sra-visszavezetett-dokumentumhiteles%C3%ADt%C3%A9s)

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[2]. A fogalmi zavart jól jelzi, hogy az elektronikus leveleknél aláírásnak „signature" nevezték már a kezdetek óta a levelek végére automatikusan odaillesztett, előre megírt záradékokat, ami, 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[3] rendelet (a továbbiakban: eIDAS vagy Rendelet) 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[4]. 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[5]. Ennek 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

[2] Bob Thomas (BBN-TENEX): On the Problem of Signature Authentication for Network Mail. Request for Comments: 644, Jul 1974. (https://www.rfc-editor.org/pdfrfc/rfc644.txt.pdf, 2019 február 12.)
[3] eIDAS rendelet alatt a továbbiakban az Európai Parlament és a Tanács 910/2014/EU rendeletét (2014. július 23.) értjük, ami a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szól. OJ L 257, 28.8.2014, p. 73–114
[4] eIDAS Rendelet 3. cikk 10: „elektronikus aláírás": olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ;
[5] eIDAS Rendelet 3. cikk 9: „aláíró": elektronikus aláírást létrehozó természetes személy;

az Európai Unió megkülönbözteti a jogi személyek aláírását a természetes személyek aláírásától és külön szóval is illeti. Ez a fogalom az elektronikus bélyegző[6] (electronic seal), létrehozója pedig kizárólag jogi személy lehet[7]. Az elektronikus aláírás és bélyegző fogalmai közötti erőteljes hasonlóságot mutatja az, hogy egyrészről az eIDAS rendelet megismétli szinte szóról-szóra az elektronikus bélyegzők esetében az elektronikus aláírásra vonatkozó előírásokat, másrészről az elektronikus ügyintézésről szóló törvény (e-ügyintézési tv, a továbbiakban: Eübszt.[8]) kodifikációs fikcióval élve előírja, hogy – eltérő rendelkezés hiányában – bizonyos szabályok vonatkozásában az elektronikus bélyegzőt is elektronikus aláírásnak kell tekinteni[9]. 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 abban az értelemben, ahogyan ezt Henri Poincaré, Dmitrij Fjodorovics Jegorov, Pavel Szamuilovics Uriszon és Luitzen Egbertus Jan Brouwer megalkotta a topológia számára – állapította meg van Dalen 2005 [13], 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 távolság-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

[6] eIDAS Rendelet 3. cikk 25: „elektronikus bélyegző”: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét;
[7] eIDAS Rendelet 3. cikk 24: „bélyegző létrehozója”: elektronikus bélyegzőt létrehozó jogi személy;
[8] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (A törvényt az Országgyűlés a 2015. december 15-i ülésnapján fogadta el. A kihirdetés napja: 2015. december 23.).
[9] Eübszt. 99. § (2) Ahol valamely jogszabály elektronikus aláírást vagy elektronikusan aláírt dokumentumot említ, azon kifejezett eltérő rendelkezés hiányában elektronikus bélyegzőt vagy elektronikus bélyegzővel ellátott dokumentumot is érteni kell.

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. 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 a Rendelet előírásainak vonatkozniuk. A harmadik felek számára is elérhető nyilvános bizalmi szolgáltatásokra nézve viszont kötelezően kell érvényesíteni az európai előírásokat[10]. Mivel Magyarországon az ügyfelet megilleti az elektronikus ügyintézési jog az elektronikus ügyintézést biztosító szerv előtt[11], 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[12], a normativitást biztosítva az elektronikus ügyintézés szabályait a

[10] eIDAS Rendelet Preambulum (21) „E rendeletnek létre kell hoznia a bizalmi szolgáltatások általános jogi keretét is. Nem írhatja azonban elő általános kötelezettségként azok használatát, illetve azt sem, hogy minden, már meglévő bizalmi szolgáltatáshoz elérési pontot kell kialakítani. Különösen nem vonatkozhat olyan szolgáltatások nyújtására, amelyeket kizárólag meghatározott résztvevői körök használnak zárt rendszerekben, és amelyek nem érintenek harmadik feleket."

[11] Eüsztv. 3 § (1) Magyarországon az ügyfelet megilleti a jog, hogy az elektronikus ügyintézést biztosító szerv előtti ügyét – az e törvényben meghatározott módon – elektronikusan intézze.

[12] 2016. évi CL. törvény az általános közigazgatási rendtartásról (Ákr.) 26. § – hatályos 2018. január 1-től:
(1) A hatóság írásban, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvényben (a továbbiakban: Eübszt.) meghatározott elektronikus úton (a továbbiakban együtt: írásban), vagy személyesen, írásbelinek nem minősülő elektronikus úton (a továbbiakban együtt: szóban) tart kapcsolatot az ügyféllel és az eljárásban résztvevőkkel.
(2) Ha törvény másként nem rendelkezik, a kapcsolattartás formáját a hatóság tájékoztatása alapján az ügyfél választja meg. Az ügyfél a választott kapcsolattartási módról más – a hatóságnál rendelkezésre álló – módra áttérhet.

közigazgatás külön rendeletben tette közzé. A 137/2016 (VI. 13.) Kormányrendelet rendelet 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[13]. 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.):** Az e-közigazgatás a közigazgatás-fejlesztés egyik olyan szegmense, amely minden közszolgáltatási ágazatban feltűnik. Ágazatoktól függetlenül az elektronikus közigazgatással szemben támasztott következő három állampolgári igény emelkedik ki, amelyekkel kapcsolatosan az értekezés tartalmaz releváns elemeket:
    - 1. elektronikus – adott esetben hitelesített – ügyintézés,
    - 2. elektronikus adatkikérési és tájékozódási lehetőség,
    - 3. egyablakos rendszerben, kellő felhatalmazással, ellenőrzés mellett átjárható közigazgatási adatbázisok kialakítása.
- **Az adminisztratív terhek csökkentése (3.2.3.2.):** a digitális világ vívmányainak adott korban elfogadott megfelelő műszaki színvonalon

[13] Constitution of the United States, Az Amerikai Egyesült Államok Alkotmánya (4. oldal) https://www.archives.gov/founding-docs/constitution

történő megvalósításának jelentős hatása van az adminisztrációs terhek csökkentésére és az információcsere ciklusának felgyorsítására. Az értekezés kapcsolódik az adminisztratív terhek digitális hitelesítési eszközökkel történő csökkentésének műszaki és jogi hátteréhez, ami a közigazgatási normatívák fejlesztésében alapvető fontosságú.

1.1. AZ ÉRTEKEZÉS MÓDSZERTANA

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. Az elektronikus aláírás térben és időben történő változásait és a változások kölcsönhatásait megvizsgálva eljutottam az elektronikus aláírás ontogenezisének értelmezéséhez.

A kutatás fő módszereként a modellalkotást választottam. A modellben megjelenítettem az elektronikus aláírások mérhető attribútumaként fellelhető elemeket, kategorizáltam ezeket és megvizsgáltam ortogonalitásukat és az egymástól való függőségüket is. A modellt ezt követően alkalmaztam empirikus mintákra és következtetéseket vontam le a modell kimenetének értékeléséből. Állításom szerint minden elektronikus aláírás jellemezhető egyetlen egy helyesen megválasztott modellben, tekintet nélkül annak keletkezési helyére időbeli, földrajzi és társadalmi értelemben egyaránt. A kapott eredményekből kidolgozott klaszterek segítésével a modell eredményeinek alkalmazhatóságára adtam példát.

Külön fejezetben elemzem a kézírásos aláírás és a digitális aláírás emelt biztonsági szintű alkalmazhatóságát, a jogszabályi háttér és következményeinek bemutatásával, ami elvezet a fokozott biztonságú biometrikus elektronikus aláírás fogalmának létrejöttéhez. A fogalom létezésének szükségszerűségét dedukcióval, a fogalom gyakorlati tartalommal való kitölthetőségét pedig egy prototípus empirikus leírásával támasztom alá.

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

1.2. A KUTATÁS HIPOTÉZISEI

Hipotézis 1: Mérhető-e az elektronikus aláírás?

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[14]. Ebből a definícióból automatikusan nem következik az elektronikus aláírások mérhetősége (a triviális mérhetőségen kívül[15]), ezért feltehető az a kérdés, hogy mérhető-e az elektronikus aláírás nemtriviális 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.

Hipotézis 2.: Létrehozható-e fokozott biztonságú elektronikus aláírás biometrikus alapokon?

Az elektronikus aláírás és a digitális aláírás fogalmi és tartalmi szinten is különbözők. 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, aminek az elfogadottsága a polgári társadalom óta nem kérdéses, és kialakultak a vitatható aláírások vizsgálatának módszerei és eljárásrendjei is. Kérdésként merül fel, hogy létezik-e az elektronikus világban olyan elektronikus aláírás, amely egyrészről az aláíró kézi aláírásán

[14] eIDAS Rendelet, 3. cikk. 10. pont.
[15] Triviális mérhetőség alatt az egyes elektronikus aláírások bináris számként történő értelmezését értjük. Mivel minden elektronikus aláírás digitális formában létezik, ezért minden elektronikus aláírás reprezentálható egy 0 és 1 számjegyekből képzett véges hosszúságú kettes számrendszerbeli számként. Ez a mérés azonban korlátozottan enged betekintést az aláírások belső struktúrájába és csak alapszintű összehasonlítást tesz lehetővé, az így előállítható, jellemzően igen nagy bináris számok között.

alapul, másrészről kielégíti a fokozott biztonságú elektronikus aláírással szemben támasztott magasabb szintű követelményeket?

Hipotézis 3: Az elektronikus aláírásnak a hétköznapi felhasználói kultúrába való integrálásához szükséges-e oktatás?

Az elektronikus aláírás használatához komplex informatikai infrastruktúra szükséges. A különböző bizalmi szolgáltatások elérhetősége alapvető fontosságú a komplexebb elektronikus aláírások elkészítéséhez, az aláírás paramétereinek helyes megválasztása pedig szükséges feltétele a jogszabályi feltételek teljesítéséhez. Ha az aláírás során valamely elem nem elérhető vagy a paraméterek rosszul lettek megválasztva, akkor az aláírás nem készíthető el vagy a felhasználó által szándékolt joghatás létrejötte válik megkérdőjelezhetővé. Ha a felhasználóra túl sok teher hárul az elektronikus aláírás használatának előkészítésében, nagy valószínűséggel felbukkanhatnak olyan technológiai problémák, amelyek megoldásához a felhasználó nem rendelkezik elegendő ismeretanyaggal és nem, vagy csak körülményesen érhetők el ezek az információk a világhálón is, következésképpen egy nem működtethető vagy nem felhasználható technológia elterjedése akadályokba ütközhet. Természetesen nem arról van szó, hogy mindenkinek rendszermérnöki szinten kellene az elektronikus aláírásokhoz érteni, hiszen az autóvezetők sem szükségszerűen rendelkeznek a robbanómotorok készítési és javítási ismereteivel, mégis képesek az adott technológia használatára. Ennek alapján kérdésként meg lehet fogalmazni azt, hogy vajon várható-e az elektronikus aláírás használatának elterjedése tudástranszfer nélkül, a társadalom aktuális képzettségi szintjén és oktatási intézményrendszereinek kimeneteire építve Magyarországon, különösen akkor, ha az elektronikus közigazgatásra, mint közműre tekintünk a közeljövőben.

2. AZ ELEKTRONIKUS ALÁÍRÁS TÁRSADALMI BEÁGYAZÓDÁSA

2.1. TECHNOLÓGIA ÉS TÁRSADALOM KAPCSOLATA

A technológiai innovációk társadalomra gyakorolt hatása elvitathatatlan, hiszen az aszimmetrikus kriptográfián alapuló digitális aláírás és az internet együttesen megteremtették az írásbeli levelezés elektronikus formáját, amely globálisan is elérhető és használható. Ez a levélküldésnek ma az egyik lehetséges formája, amelyet a kortárs technológiák tesznek lehetővé és biztosítják ennek elérhetőségét és működését. Nem mellékes körülmény, hogy ez az igény az akkori társadalom szokásrendszeréből volt levezethető, mivel a postai levelek feladásakor a feladó általában személyesen, vagy megbízottja útján adta fel a leveleket a postahivatalban, ahol ismert lehetett mind a feladót, mind a megbízottat, mint a lokális közösség tagjait. Az sem lényegtelen körülmény, hogy a papíralapú küldemények kezelése kb. 1 800 éve ismert volt már, azaz újszerűségről távolról sem beszélhetünk, a kezelés nem okozott problémát az érintettek számára. A postai szolgáltatások a kialakulásuktól számított kb. 6 000 év alatt[16] számos változáson mentek keresztül, példának okáért az amerikai postai szervezet a történeti áttekintésében megemlíti azt, hogy a postai küldemények célba juttatását a korabeli technológiai vívmányok (gőzhajó, vasút, autómobil[17]) nagyban elősegítették és a postai szervezet az innovációkat azonnal kész volt alkalmazni, amennyiben azok a szolgáltatás színvonalát képesek voltak növelni. Ez felveti az innovációk osztályozásának a szükségességét is. De hogyan szervezhető ezeknek a hatásoknak a vizsgálata tudományos rendszerbe?

Az iparosodás korában a termelékenység növekedése a gőzgépek feltalálásának volt köszönhető[18], ami számos társadalmi, gazdasági és technológiai változást idézett elő. Yonei Masuda felismerte [131], hogy a társadalmak evolúciójának sorában az ipari társadalom nem végállomás, azaz szükségszerű egy új kornak beköszöntenie, amit

[16] Postai szolgáltatásokról először i.e.4000-ből találtak utalásokat Kínában (https://www.2-clicks-stamps.com/article/postal-services-history-and-origins.html, 2019. március 3.)
[17] Lásd United States Postal Service (USPS) honlapján, 1775. július 26-án alapították meg az amerikai postai szolgáltatásokat Philadelphiában, https://about.usps.com/publications/pub100/pub100_001.htm, 2019. március 3.)
[18] Lásd James Watt 913. számú szabadalmát 1769-ből, a gőz- és energiafogyasztás csökkentéséről, (https://worldwide.espacenet.com/publicationDetails/originalDocument?CC=GB&NR=176900913A&KC=A&FT=D&ND=1&DB=&locale=en_EP#)

információs társadalomnak nevezett el és ő használta ezt a Japánban az 1960-as évek elején felbukkant fogalmat angolul először[19] 1970-ben, ahogyan ezt Z. Karvalics megmutatta [193], ezzel kezdetét vette az információs társadalom kora (Information Age). Az a kérdés azonban már – többek között – Hegelt és Marxot is foglalkoztatta, hogy vajon létezik-e a társadalmak evolúciója és ez véget fog-e érni valamikor? Hegel a liberális demokráciában, Marx pedig a kommunizmusban látta meg a legfejlettebb társadalmat, azonban Fukuyama szerint a legfejlettebb társadalmi berendezkedés – figyelembe véve az elmúlt évtizedek globális tapasztalatait – csak a liberális demokrácia lehet ([159]: 5), mivel az erősen központosított hatalmak – mindamellett, hogy jólétet tudnak teremteni – arra alkalmatlanok, hogy létrehozzák az úgynevezett „komplex posztindusztriális gazdaságot", amelyben az információ és a technikai újítás sokkal nagyobb szerepet kap ([159]:12). Vajon várható-e, hogy a Föld minden országa a társadalmi evolúció útján eljut a liberális demokráciához, mint legfejlettebb társadalmi berendezkedéshez? Huntington válasza erre kategorikus „nem" [160], mivel úgy látja, hogy a világ a hidegháború után nem a legfejlettebb társadalom elérését tűzte ki célul, mint a globális társadalom megvalósítását, hanem minden civilizáció a fejlődését ugyan folytatja tovább, de saját kulturális bázisán, azaz a világpolitika ma nem kétpólusú, hanem sok (hét vagy nyolc). A konfliktusok létezéséért a kulturális különbségeket teszi felelőssé és megállapítja, hogy „A kultúrák közti háborúban mindig a kultúra a vesztes." ([160]: 465).

Miért lehet fontos egy technológiai innováció esetében az, hogy milyen a társadalmi berendezkedés? Az elektronikus aláírás esetében úgy tűnik, hogy az érdeklődés globális, a jogszabályi rendszerbe való átültetés a DocuSign[20] és Adobe által globálisan vizsgált országok többségében valamilyen módon megtörtént[21] már az új évezred kezdetén [161] – de legkésőbb a végén – az UNCITRAL modelltörvény[22]

[19] A fogalomhasználat tényleges elsőségének a kérdésre Z Karvalics szerint többen is pályázhatnak, ma már nehezen lenne eldönthető, hogy Kisho Kurokawa, Tadao Umesao, Jiro Kamishima, Michiko Igarashi, Yujiro Hayashi, Yoneji Masuda vagy Konichi Kohyma a fogalom szülőatyja. ([193]: 29)
[20] A 63 országra kiterjedő elektronikus aláírásra vonatkozó jogi kitekintést lásd itt: https://www.docusign.com/how-it-works/legality/global (2019. március 9.)
[21] Lásd az Abobe 2016-ban készült globális felmérését: Global Guide to Electronic Signature Law: Country by country summaries of law and enforceability (https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf, 2019 március 4.)
[22] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, Article 2 (a) (http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html)

alapján, illetve az EU-ban az 1999/93/EK[23] irányelv szerint minden tagállamban. A nyugati kultúrától eltérő kultúrával rendelkező országok is élénken érdeklődnek az elektronikus hitelesítési technológiák iránt, több kutatási eredmény is született az e-government és az e-szavazás területén például Dél-Korea [162], Katar [163], Szaúd-Arábia [164], Kuvait [166], Uganda [168] és India [165] e-közigazgatásának a vizsgálata révén. A rendszerek komplexitása és a társadalmi berendezkedés között van összefüggés, ezt bizonyítja az, hogy a fejlett iparra rendelkező régiókban a gazdasági-technikai fejlődés egyik jellemző vonása, hogy rohamosan növekszik az egyre bonyolultabb és összetettebb (komplexebb) műszaki rendszerek létrehozása és működtetése iránti igény [167] és a társadalmaknak képesnek kell lenniük ezt az igényt kielégíteni a komplex rendszerek üzemeltethetősége érdekében, ellenkező esetben a komplex rendszerek fenntarthatósága nem biztosítható – esetleg katasztrofális esemény következik be, így elvész (vagy meg sem születik) a komplex rendszerek használatából származó produktivitási előny. Az érdeklődés a technológiai innovációk iránt azonban úgy tűnik, hogy független a civilizációktól, így érdekes lehet az innovációk elterjedésének törvényszerűségeit a fókuszba helyezni.

Robert M. Solow közgazdaságtani megközelítésben azt vizsgálta, hogy az innovációk hogyan jelennek meg a bruttó hazai termékben (Gross Domestic Product, GDP) különböző intervallumokban. Megvizsgálva az USA adatait az 1909 és 1949 közötti időszakra azt találta, hogy az egy főre jutó bruttó teljesítmény kétszeresére nőtt a vizsgált 40 év alatt, ahol a növekedés 87,5 százaléka a technológiai változásnak, a fennmaradó 12,5 százalék pedig a tőkeemelkedésnek volt köszönhető ([169]: 320). Ha azt a kérdést tesszük fel, hogy vajon a technológia által lehetővé tett változásban lehet-e kiemelt szerepe az infokommunikációs innovációknak a többi innovációval szemben, akkor erre a kérdésre Solow egyrészről azt a választ adja, hogy a technológiai lehetőségeket a termelékenységi függvény magában foglalja ([170]: 66), másrészről minden intelligens innováció – így az ICT innováció is – növeli a termelékenységet. Az ICT innovációk „szuper-profitábilis" hatását azonban nem sikerült kimutatni 1950 és 2000 között az amerikai gazdasági növekedésben, amit a „dotcom-lufi" kipukkadása is alátámaszt, ugyanis, ha egy innovációs terület a többi területtől magasabb profittal kecsegtetne, akkor a tőkebeáramlás (és megtérülés) révén észlelhetővé válna ez az előny

[23] Az Európai Parlament és a Tanács 1999/93/EK irányelve (1999. december 13.) az elektronikus aláírásra vonatkozó közösségi keretfeltételekről, OJ L 13, 19.1.2000, 12–20

[171]. Solow az ICT innovációk hatását vizsgálva – Schumpeter osztályozása alapján [173] –azt is megállapította, hogy a technológiai innovációk önmagukban (felfedezés) nem okoznak jelentős gazdasági hatást mindaddig, amíg az innováció használata el nem terjed (használat). Ezt a jelenséget Solow számítógépes paradoxonjaként ismerjük 1987 óta: „a számítógépes kor mindenhol látható, de leginkább a termelékenységi statisztikákban" ([172]: 166). A paradoxon a nagyfokú ICT innováció megléte és az eredmény GDP-ben való kimutathatatlansága közötti ellentmondásra világított rá. Ennek a paradoxonnak a feloldása további 10 évet vett igénybe, míg más általános felhasználású technológiák (mint például a gőzgép) ettől is hosszabb idő alatt terjedtek el és fejtették ki jelentős hatásukat a gazdaságra – állapította meg Solow.

Az innovációk elterjedéséhez szükséges időfaktor felismerését követően megnyílt az út az innovációk disszeminációjának vizsgálata előtt. Rogers többszáz ilyen irányú kutatási eredményt szintetizálva kidolgozta az innovációk terjedésére vonatkozó elméletét [174], amely szerint az innovációk társadalmi elterjedésében öt társadalmi csoportot lehet megkülönböztetni, amelyeknél az elterjedés görbéje az idő függvényében normáleloszlást mutat:

1. felfedezők (2.5%)
2. korai adaptálók (13.5%)
3. korai többség (34%)
4. késői adaptálók (34%)
5. lemaradók (16%)

Tekintettel arra, hogy Magyarországon 18 év alattiak nem kaphatnak elektronikus aláírási lehetőséget állampolgári jogon, a KSH adatait[24] alapul véve a potenciális felfedezők számossága 201 581 fő, a korai adaptálók száma 1 088 536, a korai többségnek és a késői adaptálóknak 2 741 499 főnek kell lennie és várhatóan 1 290 117 állampolgár sosem fog elektronikus aláírást használni belátható időn belül. Az innovációk elterjedését befolyásoló tényező Hámori és Szabó összefoglaló írása szerint [175] a társadalmi viszonyok komplexitása. A gazdasági fejlődés nem véletlenül alakul ki, hanem a társadalmi viszonyok komplexitásának az eredménye, vagy ugyanezek a viszonyok

[24] Korfa, https://www.ksh.hu/interaktiv/korfak/orszag.html (2019. március 9.), a teljes lakosság létszáma 2018-ban 9 778 371 fő volt, közülük 1 715 140 volt 0-17 év közötti.

szabhatnak gátat a fejlődésnek. Az innováció és a társadalom között kimutatható kapcsolat áll fenn, amelyet számos kutatás bizonyított. Az innovációk kapcsán elegendő arra utalni, hogy ha egy vállalat fennmaradását az államhoz fűződő kapcsolata eredményezi, ami nem függ össze a piaci teljesítményével, akkor a vállalatnak nincs motivációja innovatívnak lenni és új termékek vagy szolgáltatások piaci bevezetésével foglalkozni.

A társadalom intézményi struktúrája határozza meg azt, hogy milyen szervezeteket lehet az adott társadalomban létrehozni és fenntartani – állítja North et. al. [176]. Hozzáteszi, hogy a primitív társadalmak nem képesek támogatni komplex szervezeteket. A korlátozott hozzáférésű társadalmak támogatják ugyan a komplex szervezeteket, de korlátozzák a komplex szervezetek számát és a kölcsönzés intézménye is megjelenik a korlátozott számosságú szervezetek között az igények kielégíthetősége érdekében. Ha a kölcsönzés költségei meghaladják a büdzsé kereteit, akkor az veszteségként jelentkezik a kölcsönzött erőforrás tulajdonosánál. A nyílt hozzáférésű társadalmak támogatják a szervezetek nyílt hozzáférését, ami elősegíti a gazdasági és a politikai versenyt, továbbá számos komplex gazdasági és politikai szervezetet eredményez. Fontos megjegyezni, hogy intézményi struktúra alatt nem kizárólag formalizált és kívülről szabályozott kereteket kell érteni itt, hanem minden olyan szabályt, ami az adott interakció létrejöttéhez – a szereplők viselkedéséhez – hozzájárult. Ebből adódik, hogy pontos definíciót az intézményi struktúrára nehéz megfogalmazni, mivel az adott esetre alkalmazott szabályok közé tartoznak az írott törvények, a formális társadalmi egyezmények, az elfogadott viselkedési formák és a világról való közös meggyőződés.

2.2. A BIZALOM ÉS AZ ELEKTRONIKUS ALÁÍRÁS

A „bizalom” szó definíciója (a Magyar Értelmező Kéziszótár alapján[25]) vagy a körülmények kedvező alakulásába vetett hit, bizakodásm vagy pedig egy olyan személyre irányuló érzésünk, akiben (meg)bízunk. Politikai értelemben bizalmat szavazunk valakinek, vagy valaminek (pártnak, programnak), azaz a választópolgár szavazatával kinyilvánítja, hogy bízik a vezetésben. Ebből a definícióból az derül ki, hogy a bizalom többértelmű fogalom, egyszer egy tevékenység (bizakodás, szavazás), máskor egy érzés.

[25] Magyar Értelmező kéziszótár, harmadik, változatlan kiadás. Budapest, Akadémiai Kiadó, 1978. ISBN 963 05 1588 1. 138. oldal

A bizalom kategóriáit az alábbiakban lehetséges megjelölni (felhasználva McKnight és Chervany interdiszciplináris modelljét ([32]: 33):

1. feltétlen bizalom: bizalom minden és mindenki iránt (ősbizalom),

2. intézményi bizalom: az egyes intézmények irányában megjelenő kapcsolati minőség,

3. interperszonális bizalom: az egyes emberek egymás közötti kapcsolatára utaló fogalom.

Az intézményi bizalmat az előbbiek szerint nem kizárólag a formális struktúrákon lehet értelmezni, hanem az adott szituációban elvárható cselekvések, viselkedések kontextusában is – bízni valamiben vagy valaminek a bekövetkezésében. A bizalom és a biztonság közötti kapcsolat feltárásához a biztonság definícióját kell közelebbről szemügyre venni. Vasvári György szellemes megfogalmazásában ([33]: 11) a biztonság olyan kedvező állapot, amely megváltozása nem valószínű, de nem is lehet kizárni. Ebben az értelmezésben a „biztonság" a „bizalom" tárgyának materializált formája, hiszen míg a „bizalom" egy (emberen belüli) hit, bizakodás, érzés, addig a „biztonság" mérhető (emberen kívüli) valóság, amely tevékenységek révén áll elő és maradhat fenn. Visszahatás is létezhet közöttük, hiszen a „gondolat-érzés-cselekedet" láncolatban a tevékenység későbbi, míg az érzés korábbi eleme az idősornak, és a biztonság megteremtésére és fenntartására irányuló tevékenységek (védelem) megteremtése nélkül a biztonság (mint állapot) mérhető értéke nem változik, de a fenyegetettség, a veszélyérzet (és ezzel kapcsolatosan a bizalmatlanság, vagyis a biztonság megteremtésének képességébe vetet negatív hit) növekedhet.

A biztonság formális modelljei már viszonylag régen ismertek, példának felhozható Landwehr 1981-es cikke [34], amelyben összefoglalja az addig létrejött biztonsági modelleket. Anélkül, hogy belemennénk a formális modellek ismertetésébe, összefoglaló jelleggel annyit mondhatunk, hogy formális szempontból a biztonság egy véges állapotú (Turing) gép azon állapotainak halmaza, amelyek úgy jöhetnek létre, hogy engedélyezett állapotból engedélyezett műveletekkel az adott objektumok tulajdonságait engedélyezett módon megváltoztatják. Amíg ezen belül maradunk, addig biztonságban vagyunk, amint kilépünk, elveszítettük a formális biztonságot. Érdekes itt még az is, hogy az egyes formális modellek között ütközés állhat fenn, például a bizalmasság

kommunikációs modellje teljesen ellentétes a sértetlenség kommunikációs modelljével, amiből következik, hogy más módokon kell a kettőt biztosítani. 2013-ban a Gemalto megszerezte az első Common Criteria EAL7[26] szintű értékelést a Sealys ID Motion eID kártyájára és szoftverére egyaránt[27], ami azt jelzi, hogy az intelligens kártyák világában a biztonság formális bizonyítása gyakorlatilag is lehetségessé vált. Ez a biztonsági szint azonban csak extrém magas kockázati környezetekre ajánlható, ahol a védendő információk értéke arányban áll a formálisan ellenőrzött tervezésen és tesztelésen alapuló biztonság megteremtésének magas költségeivel. Hétköznapi használatra még sokáig nem lesz valószínűleg ilyen eszköz alkalmazva. 2019-ben a minimum követelmény a minősített elektronikus aláírást létrehozó eszközökre EAL4+[28]. A „+" itt azt jelenti, hogy a követelmény-specifikáció teljes mértékben lefedi az EAL4 szintet és kiegészíti azt további elemekkel, a következő szintet még nem lefedve (lehetne akár EAL5- jelölést is alkalmazni ezekre a garanciaszintekre).

Meg kell itt említeni a biztonságnak Muha Lajos informatikai biztonsági rendszertanában [4] alkalmazott definícióját, amely szerint a biztonság a rendszer olyan — az érintett számára kielégítő mértékű — állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Láthatóan tehát a biztonság ebben a rendszerben sem hit, bizakodás eredményeként jön létre, hanem védelem megvalósításával, vagyis konkrét tevékenységek révén.

A kockázatok és a biztonság közötti összefüggés ebből tehát világos. Az arányosság annyit jelent, hogy egy bizonyos kockázattűrő képességi szint alatt biztonságban vagyunk, felette pedig nem. Vagyis a kockázatok értékének kiszámításával és számosságukkal is jellemezhető a biztonság, az incidensek számossága mellett. Az incidensek számossága pedig egyenesen arányos a – statisztikailag kezelhető – kockázatokkal, és fordítottan arányos a biztonsággal. Megemlítjük, de részletezésétől eltekintünk annak, hogy ugrásszerű változások általában akkor következnek be a biztonság érzékelésében, amikor statisztikailag nem kezelhető kockázatok következnek be (pl. 9/11, Csernobil), amelyek egy entrópia-alapú hadviselés következtében is

[26] EAL: Evaluation of Assurance Level: Értékelési garanciaszint, amely értéke 1 és 7 között lehet. A „+" jel azt fejezi ki a szám mögött, hogy az értékelés tárgya kielégíti az adott szint összes garanciális követelményét és a következő szint követelményeiből is egyet vagy többet, de nem az összeset.
[27] Lásd https://www.gemalto.com/brochures-site/download-site/Documents/gov_sealys_ID_motion.pdf (2019. március 5.)
[28] Lásd https://www.commoncriteriaportal.org/files/ppfiles/pp0059b_pdf.pdf (2019. március 5.)

előállhatnak [108].Természetesen ezeket is lehetséges kezelni, de más módon – ezekhez eszközül a logikai [106] és a percepciós [107] kockázatelemzés módszertana szolgálhat.

A bizalom és a kockázat táblázatát Daniel W. Manchala munkásságát felhasználva [36] adjuk meg, ami a múltbéli tranzakciók minősítése és az ellenőrzés szükségességének megítélése közötti összefüggés alapján tesz a bizalom háromszögére javaslatot. Manchala az elektronikus kereskedelembe vetett bizalom kérdését és mérhetőségét vizsgálta meg tulajdonképpen az elmúlt évezred utolsó éveiben – a Xerox Research and Technology kutatójaként – azt a felismerést követve, hogy a hagyományos eladó-vevő bizalmi modell az e-kereskedelemben – megengedve az anonim tranzakciókat – már nem, vagy akár nem úgy működik. Modellje a tranzakciók kockázati értékeit bizalmi változók sajátos függvényeként határozta meg, ezért a bizalom változóinak tételes meghatározása ebben alapvető fontosságú volt. Bizalmi változóként a tranzakciós költséget, a tranzakciós múltat és a kártérítési felelősséget határozta meg, továbbá a költési mintát és a rendszerhasználatot jelölte meg olyan nem állandó változóként, amelyek vizsgálata lehetőséget ad a hamis tranzakciók felderítésére. A bizalom mérésében használt további két paramétert javasolta Manchala a bizalom változóinak finomhangolására felhasználni, amelyek közül az egyik az idő, a másik pedig a helyszín. A tranzakciók frekvenciájának változása, illetve a tranzakciók közvetítése nem megbízható köztes szereplők által, mind a bizalom csökkenésének a jele lehet. A bizalom és a kockázat ezek szerint a döntéshozatal két oldala. Jøsang és Lo Presti elemezte a kockázatok és a bizalom kapcsolatát [35] Manchala munkásságát felhasználva és szerintük a bizalmat a negatív következmények lehetőségei ellenére valakitől, illetve valamitől való függésre vonatkozó hajlandósággal lehet definiálni. Fontos megjegyezni, hogy itt a bizalom formális modelljét keresték műszaki aspektusból, automatizált rendszerek számára.

2.3. A HITELESSÉG ÉS AZ ELEKTRONIKUS ALÁÍRÁS KAPCSOLATA

A hitelesség fogalomrendszerében megkülönböztethetjük a hiteles, hitelesítés és hitelesség fogalmakat, az alábbi módon:

- hitelesítés (folyamat): az állított azonosság megerősítése – azonosság állítható személyről, eszközről és tulajdonságról egyaránt,
- hitelesség (eredmény): a forrás ismert és a tartalom eredeti, illetve

- hiteles (tulajdonság): a forrás és a tartalom eredetisége megerősítetté vált.

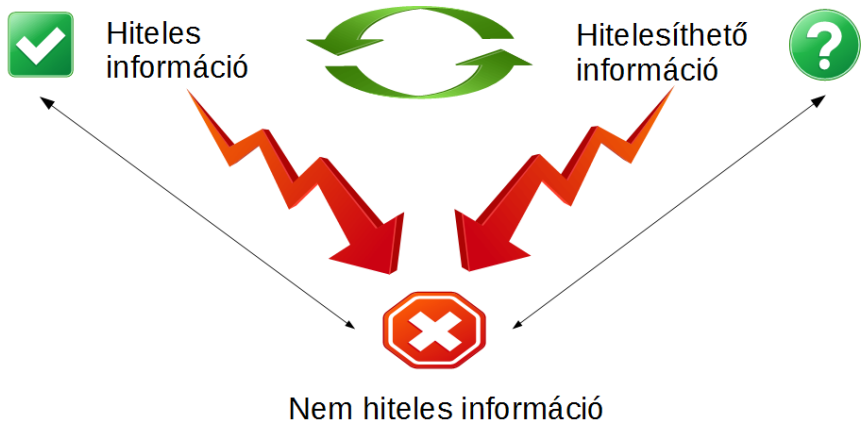
Ezekből a definíciókból az következik, hogy az önmagában megtett állítás sosem számíthat hitelesnek, mert azt a tulajdonságát minden esetben további tevékenység (megerősítés, verifikálás) révén nyerheti csak el. Ezért nem szerencsés az „azonosítás” szóhasználat az „erős azonosítás” jelentéstartalommal, hiszen itt a hitelességet (eredményt) a hitelesítési folyamat végrehajtása eredményezi, nem pedig önmagában a megtett kijelentés. Ebből levezetve elvégezhető az információk osztályozása is hitelességi szempontból:

1. **hiteles információ:** a forrás és a tartalom eredetiségének ellenőrzését elvégezték, aminek az eredménye pozitív és hozzáférhető,

2. **hitelesíthető információ:** a forrás és a tartalom eredetiségének ellenőrzését nem végezték még el, de ennek akadálya nincsen, mivel minden szükséges adat rendelkezésre áll vagy beszerezhető, a hitelesítés elvégezhető, és

3. **nem hiteles információ:** egyrészről a hitelesítés során negatív ellenőrzésre jutott információt (hamis információ), másrészről az érvényesítési adatokkal nem rendelkező (nem hitelesíthető) információt nevezzük nem hiteles információnak.

Ezeket a definíciókat a következő ábrában foglaljuk össze és jelöljük az állapotváltozások dinamikáját is:



1. ábra: A hitelesség dinamikája (forrás: saját ábra)

Tulajdonképpen az információk a hitelességüket csak korlátozott ideig képesek megőrizni, egészen pontosan addig, amíg a hitelesítési folyamat sikeres elvégzéséhez szükséges információk érvényessége fennáll és rendelkezésre is állnak. Amennyiben ez

az idő múlásával megváltozik, akkor az információ hitelessége is megváltozik. Ha a korábbi hitelesítési folyamatban felhasznált adatok érvényessége szűnt meg, de a megismételt hitelesítésnek akadálya nincsen, akkor az információ átkerül a „hitelesíthető” osztályba. Ha azonban a hitelesítéshez szükséges adatok nem állnak rendelkezésre, akkor az információ rögtön a „nem hiteles” osztályba kerül. Ha előkerülnek a hitelesítéshez szükséges adatok, akkor az információ visszakerül a hitelesíthető” osztályba, a sikeres hitelesítési procedúra elvégzését követően pedig a „hiteles” címkét is visszakaphatja. A direkt átmenet a „nem hiteles” osztályból a „hiteles” osztályba nem képzelhető el, mivel a hitelesítési folyamat végrehajtása előtt annak bemeneteit kell meghatározni, amivel az információ már a „hitelesíthető” osztályba lépett, még mielőtt a hitelesítési folyamat végrehajtása megtörténne. Természetesen a hitelesítési folyamat negatív eredménye a „nem hiteles” osztályba kerülést eredményezi azonnali hatállyal.

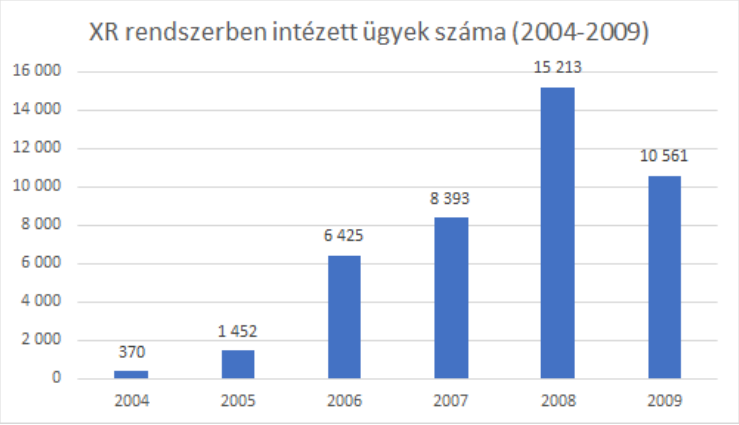
A kapcsolatot a hitelesség és az elektronikus aláírás között az elektronikus aláírás szabványosítási munkacsoport végleges jelentése[29] fogalmazta meg egyértelmű formában. Egyrészről megállapítja, hogy az „aláírás” fogalmat a szabályozás nem kizárólag a kézi aláírás elektronikus alternatívájaként alkalmazza, ha így értelmeznénk, akkor csak korlátozottan lenne használható az elektronikus aláírás a gyakorlatban. Másrészről egyértelművé teszi, hogy az elektronikus aláírás minden esetben valójában elektronikus hitelesítés, mivel az általánosan használt hitelesítési definíciók alapján itt valamilyen állított azonosság megerősítéséről van szó. Tulajdonképpen minden elektronikus hitelesítés elektronikus aláírásnak tekinthető egészen addig, amíg össze van kapcsolva vagy logikailag hozzá van rendelve ahhoz az adathoz, aminek a hitelességét igazolni szándékozik. Ebből adódóan a szabályozás nem zárja ki azt, hogy elektronikus aláírásnak lehessen tekinteni egy szimmetrikus vagy aszimmetrikus kriptográfián alapuló hitelesítési eljárást, vagy egy név odagépelését egy e-mail végére, esetleg egy szkennelt kézi aláírás csatolását valamely dokumentumhoz, illetve egy aláírópadon éppen létrejött

[29] Lásd https://cryptome.org/jya/eessi.htm (2019.02.04.)
„An "electronic signature" without being further qualified, is indeed an electronic authentication. The term " authentication " itself is not defined nor explained in the recitals of the Directive and thus leaves room for a broad interpretation. However, the term is usually defined as "validation of a claimed identity". Every type of electronic authentication will be regarded as an electronic signature, as long as it is attached to or associated in a logical way with other electronic data. Thus, biometric authentication methods, such as Penop or Smartpen, are regarded as electronic signatures, Message Authentication Codes (MAC), which are based on symmetric cryptography, are electronic signatures. Public key authentication schemes, such as digital signatures, are electronic signatures. The definition of an electronic signature in the directive does even not exclude the typed name at the bottom of an email or the attachment of a scanned signature to a document.”

kézi aláírást. A szabályozás különbséget tesz az elektronikus aláírás (electronic signature) és a fejlett elektronikus aláírás (advanced electronic signature) között, de nem kriptográfiai alapon, hanem technológiasemleges módon, értelmezve ezt a relációt minden olyan adat kontextusában, amelyik egy másik adathoz van – fizikailag vagy logikailag – csatolva aláírás céljából.

2.4. AZ ELEKTRONIKUS ALÁÍRÁS A MAGYAR KÖZIGAZGATÁSBAN

Az elektronikus ügyintézés kialakítása a magyar közigazgatásban kezdetben nem igényelte az elektronikus aláírást, példa erre az XR rendszer[30] kezdeti állapota. A rendszer úgy biztosította a lehetőséget az egyes ügyek előkészítésére és az okmányirodai időpontfoglalásra, hogy nem igényelt magas szintű azonosítást és nem foglalkozott a keletkezett dokumentumok hitelességével sem túlzott mértékben (elektronikus aláírást nem követelt meg). Ennek oka az volt, hogy az ügyintézések jelentős hányadában a személyes megjelenés még kötelező volt, így a célkitűzés akkor nem a teljesen elektronikus ügyintézés megvalósítása volt, hanem az ügyfelek személyes megjelenési számosságának felülről való közelítése az egyhez. Ezt bizonyítja a rendszer 2004-es használatának statisztikai adatai, amely szerint a körülbelül 4 000 regisztrált felhasználó 370 ügyet indított (töltött ki űrlapokat) és 1 832 időpontfoglalás történt (űrlapkitöltések nélkül) ([14]: 108).

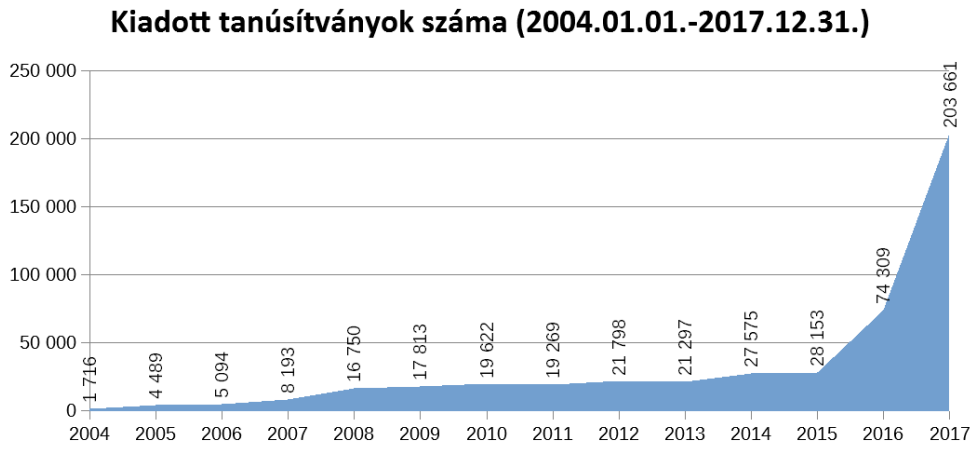


2. ábra: XR rendszerben elintézett ügyek száma (2004-2009) (forrás: [14]: 111)

[30] A kormányzati portálon 2003. október 28-tól elérhetővé vált az Internetes Közigazgatási Szolgáltató Rendszer (a továbbiakban: XR), amely megteremtette az elektronikus ügyintézés alapjait. ([14]: 106)

Az ellenőrzéseket azért nem végezték el előzetesen, mert a tranzakciók hitelesítésére csak a személyes megjelenés során volt lehetőség, java részben függetlenül attól, hogy mi történt előzetesen az elektronikus előkészítés során. Az elektronikus ügyintézés azonban ezzel elindult és egyre növekvő mértékben volt jelen a közigazgatásban.

A Nemzeti Média- és Hírközlési Hatóság statisztikai adatszolgáltatásra kötelezte 2004-től a nyilvánosan működő szolgáltatókat és évente közzéteszi az adatszolgáltatások statisztikai eredményeit. 2016. június 30-ig bezárólag ezek az adatok az elektronikus aláírással kapcsolatos szolgáltatásokra vonatkoznak, 2016. július 1-től pedig a bizalmi szolgáltatásokra. 2004 és 2017 közötti időszakban a kibocsátott tanúsítványok számosságát a következő ábra mutatja be:



3. ábra: Magyar hitelesítésszolgáltatók által kibocsátott tanúsítványok száma (2004-2017) (forrás: NMHH adatai alapján[31])

A kormányzat váltakozó és mérsékelt lelkesedését mutatja az ebben az időszakban a kormányzati szervezeteknek kibocsátott tanúsítványok száma, ez a 422-es minimum és 7 342-es maximum között mozgott, 2 799,14 átlaggal és 2 402-es mediánértékkel.

Az elektronikus cégeljárás megindulását jelző pozitív irányú törés jól kivehető 2008-ban, de az itt megjelen tanúsítványnövekedés mértéke láthatóan elmarad az állampolgári tanúsítványok 2016-os bevezetése utáni növekedéstől. Az elektronikus cégeljárás bevezetése EU irányelvek alapján történt (68/151/EGK irányelvet módosító 2003/58/EK irányelv), amit a tagállamoknak 2007-ig kellett implementálniuk. Nemzeti

[31] Lásd http://nmhh.hu/dokumentum/194375/Bizalmiszolg_statisztika.pdf (2019. március 10.)

szinten ez a 2003. évi LXXXI. törvény hatálybalépésével valósult meg 2005. január 1-én. Az elektronikus ügyintézés lehetősége már 2005 szeptemberétől elérhető volt, de kötelezővé csak 2008. július 1-től vált[32] ([187]: 36). Ennek következtében minden cégeljárásra jogosult jogi képviselőnek rendelkeznie kellett minősített elektronikus aláírási lehetőséggel[33].

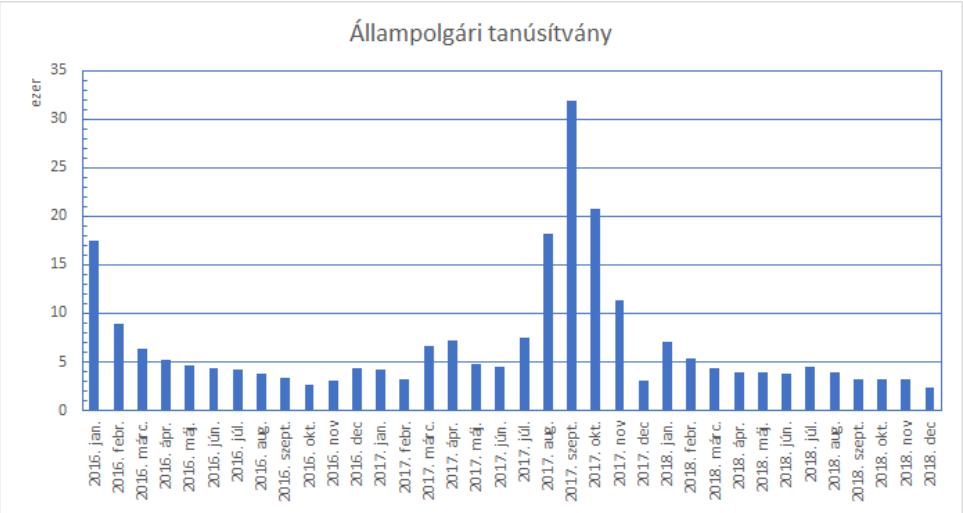
A 2016-os kiugró érték több tényező együttes hatását mutatja, egyrészről 2016. január 1-évl elindult a Kormányzati Hitelesítés Szolgáltató tanúsítványkibocsátási szolgáltatása állampolgárok számára (a kapcsolódó szolgáltatói tanúsítvány[34] 2015. december 18., péntek 12:27:19 UTC+0100 jött létre) és már az első félévben 47 069 állampolgári tanúsítvány lett kibocsátva, ezzel együtt pedig a NISZ GovCA pedig a 2016-os tanúsítványkibocsátás 68,4%-áért felelős, azaz a piacon jelenlévő szolgáltatók ebben az időszakban csupán 22 290 tanúsítványt bocsátottak összesen ki. A növekedés a magánszemélyek számára kibocsátott tanúsítványokban jelentkezett, a 2015-ös 1076-os érték 2016 első félévére 46 837-re nőtt, 2017-re pedig 162 870-re. A másik – ettől lényegesen kisebb jelentőséggel bíró hatást a polgári peres eljárásokban 2016. július 1-től a jogi képviselők által kötelezően alkalmazott elektronikus kommunikáció jelentette.

Az Állampolgári Tanúsítványkiadó által kibocsátott tanúsítványok számosságát 2016 és 2018 között a következő ábrán mutatom be.

[32] Lásd 2007. évi LXI. törvény a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény és egyéb törvények módosításáról, 12. § A Ctv. 35. §-ának (1) bekezdése helyébe a következő rendelkezés lép: „(1) A cégbejegyzésre (változásbejegyzésre) irányuló kérelmet a cég székhelye szerint illetékes cégbíróság részére a cégformának megfelelő, a jogi képviselő által aláírt elektronikus nyomtatványon kell - e törvényben meghatározott módon és a mellékletekkel együtt - előterjeszteni."

[33] Lásd Uo., 13. § (1) A Ctv. 36. §-a (1) bekezdésének első mondata helyébe a következő rendelkezés lép: „A cég bejegyzése (változásbejegyzése) iránti kérelmet elektronikus úton kell benyújtani."
13. § (3) A Ctv. 36. §-ának (5) bekezdése helyébe a következő rendelkezés lép: „(5) Ha törvény a cégirat cégbírósághoz történő benyújtására közvetlenül valamely személyt kötelez, e személy a kötelezettségét elektronikus okiratként készített cégirat esetén, minősített elektronikus aláírás alkalmazásával maga is teljesítheti.

[34] Lásd http://cca.hiteles.gov.hu/cer/GOVCA-CCA.cer (2019. március 10.)



4. ábra: Állampolgári tanúsítványok számának alakulása 2016-2018 között (forrás: NISZ GovCA adatai alapján)

Gellén ([188]: 107) tárgyalja az a kérdést is, amit az elektronikus közigazgatás kérdéskörének felbukkanása vetett fel a közigazgatási reformokkal kapcsolatosan. A kérdés az volt, hogy vajon a technológia fejlődése eldönti-e az NPM[35]-NWS[36] vitát. A technológia korai alkalmazásának időszakában úgy tűnt, hogy az NPM filozófiáját jobban képes támogatni a technológia, ám a problémák előkerülésével felerősödött a centrális problémamegoldás iránti igény. Ez azonban a technológiától független, inkább az ezzel kapcsolatos humán elvárásokat tükrözi, emiatt Gellén megállapítja, hogy „Az elektronikus közigazgatást semleges technológiaként kezelve megállapítható, hogy mindkét irányzatot erősítheti törekvéseiben.” [188] :104). Ezt a gondolatot azzal folytatja, hogy ha minden e-állampolgár döntési helyzetbe kerül az e-közigazgatás által, akkor ez közelebb van az NPM-hez, de ennek ellenpontjaként egy erős állam az e-polgárok véleményét begyűjtve és ignorálva már az NWS szabályozottságához áll közelebb. Itt is megjelenik Neumann állítása a technológia kétarcúságáról [99], a fenti példa is mutatja, hogy nem a technológiai sajátosságok döntik el azok alkalmazási minőségét, hanem az alkalmazást előíró és annak szabályait létrehozó ember.

A technológiától való függőség mindkét oldalt felerősítheti. A társadalmi stabilitás megőrzéséhez, az elektronikus aláírási rendszerek fenntartásához és az aláírt dokumentumok hitelességének hosszú távú biztosításához ma már nélkülözhetetlen

[35] NPM: a New Public Management, Új Közmenedzsment közigazgatási reformirány megnevezése, alapelve, hogy az üzleti világban sikeres technikák közigazgatási átvételével kell elérni a célkitűzéseket.
[36] NWS: a Neo-Weberian State, Új Weberiánus Állam rövidítése, ami Max Weber centrális, hierarchikus és szabályokra épülő államfelfogását egészítette ki a tevékenységek eredményességi kritériumaival

bizalmi szolgáltatók közeledtek az elmúlt időszakban a kritikus infrastruktúrákhoz, ezt bizonyítja Muha [3], amikor a védelem alanyai között felsorolja egyrészről a közigazgatási informatikát és kommunikációt megvalósító rendszereket (például ilyen lehet a Kormányzati Hitelesítés Szolgáltató „GovCA" és a Közigazgatási Gyökér Hitelesítés Szolgáltató „KGYHSZ"), valamint a kritikus infrastruktúrák létfontosságú infokommunikációs rendszereit, illetve javasolja a védelmet kiterjeszteni azokra a szervezetekre is, amelyek az infokommunikációs rendszereket működtetik, vagy ezzel összefüggő szolgáltatásokat nyújtanak (ilyenek például a bizalmi szolgáltatók). Póserné 2011-ben ennél is továbbment és megállapította, hogy a közigazgatási informatikai rendszerek, mint a kormányzati és önkormányzati szféra infokommunikációs rendszereinek részhalmazai, kritikus – létfontosságú – információs infrastruktúrának minősülnek [105].

2.5. AZ ALÁÍRÓ MEGHATÁROZÁSÁNAK PROBLÉMÁJA

Az elektronikus aláírásról szóló 2001-es törvény[37] (Eat.) szabályozási felhatalmazást adott olyan részletszabályok megalkotására, amelyek a ténylegesen elektronikus ügyintézési környezetet specifikálták volna, azonban ez a ráhatás nem volt elég közvetlen ahhoz, hogy jelentős hatást váltson ki, illetve széles körben elfogadott összehangolt fejlesztésekhez vezessen a szigetszerű megoldások helyett. Ezen a helyzeten változtatott a 184/2004. (VI. 3.) Kormányrendelet, ami definiálta az elektronikus közigazgatási ügyintézést és a kapcsolódó szolgáltatásokat, illetve eljárást adott az elektronikus és papíralapú dokumentumok közötti konverzióra és az eljárási cselekmények összekapcsolására. Az alapelv az volt, hogy ha az ügyfél rendelkezik legalább fokozott biztonságú elektronikus aláírási képességgel vagy ügyfélkapus regisztrációval, akkor képes elektronikusan ügyeket intézni joghatályos módon. Ekkor azonban még nem volt lehetőség a papíralapú ügyintézéssel egyenrangú, annak minden aspektusát átfogó elektronikus ügyintézési mód kialakítására, többek között az olyan kérelmek esetében, amelyek csatolmányokkal is rendelkeztek, nem lehetett elektronikus úton azokat az ügyfélnek elindítania. Az elektronikus aláírás szerepe itt csupán a dokumentum változatlanságának és egy előzetesen ismert személy általi ellenőrzés

[37] 2001. évi XXXV. törvény az elektronikus aláírásról. (Eat.) A törvényt az Országgyűlés a 2001. május 29-i ülésnapján fogadta el. A kihirdetés napja: 2001. június 12.

tényének igazolására szolgált, nem pedig az aláíró személyének tanúsítására, állapította meg Szittner ([14]: 128).

Az Eat. által adott felhatalmazás nagyon korlátozott volt, hiszen attól tették függővé az alkalmazását, hogy létezik-e olyan jogszabály, amely az egyes ágazatokhoz tartozó hatóságok által lefolytatott államigazgatási eljárásokban csak elektronikus irat, dokumentum, illetőleg elektronikus aláírás felhasználásával teszi azt végrehajthatóvá. A szabályozás alapja ekkor az volt, hogy csak ott lehetett elektronikusan ügyintézést lefolytatni, ahol ezt jogszabály kifejezetten lehetővé tette. Ilyen jogszabályok azonban 2004-ig nem születtek, ezen a helyzeten változtatott a Ket. és a (184/2004-es Kormányrendeletet felváltó) 193/2005 (IX.22.) Kormányrendelet. Az elektronikus dokumentumoknak az ügyfélhez való hozzárendelése problémás volt, hiszen egy általános célú (például álneves) fokozott biztonságú elektronikus aláírás nem biztosította az aláíró kilétének beazonosítását. A dokumentum ügyfélhez rendelését ezért vagy a hatóság végezte el, vagy az ügyfélnek kellett papíron aláírnia az elektronikusan előkészített dokumentumokat ([15]: 506). A közigazgatási célra használható tanúsítványokra éppen ezért speciális követelmények vonatkoztak, egyrészről csak személyes megjelenés útján voltak igényelhetők, másrészről a szolgáltatóknak garantálniuk kellett az ügyfél nevének személyazonosító okiratban foglaltakkal való teljes egyezőségét a kibocsátott tanúsítványokban. Az elektronikus aláírás közigazgatásban való elterjedésének egyik legfontosabb akadályává vált így az a körülmény, hogy egy szabványos aláíró tanúsítványban az aláíró személy természetes személyazonosító adatai közül adott esetben egyetlen egy sem szerepel, így a hatóság nem képes hitelt érdemlő módon azonosítani az ügyfelet, ha az elektronikus aláírással ellátott dokumentum segítségével szeretett volna ügyeket intézni. Ennek érdekessége az, hogy a hitelesítés szolgáltatók csak az igénylő személyének különböző szintű azonosítását követően adhatták ki ezeket az aláírói tanúsítványokat, vagyis a folyamatban létezik legalább egy szereplő, akinél az aláíró azonosító adatai fellelhetők és akinek ezeket jogszabály általi felhatalmazás alapján a tanúsítvány lejáratát követő 10 évig meg kell azokat őriznie. Ennek a problémának a megoldására a magyar közigazgatás két szinten fogalmazott meg előírásokat, egyrészről ügyfelek csak olyan tanúsítványokat használhattak az elektronikus ügyintézésben, amelyek teljesítették a közigazgatási ügyfél-tanúsítványokra vonatkozó követelményeket (legfontosabb elem az álnév tiltása és a személy nevének igazolványban rögzített módon való feltüntetése volt), másrészről

ilyen tanúsítványokat csak olyan szolgáltatók bocsáthattak ki, amelyek vállalták a viszontazonosítási folyamat bevezetését és működtetését. Tekintettel arra, hogy a tanúsítvány ebben az esetben is csupán az aláíró nevét tartalmazta a természetes azonosító adatok közül, az egyértelmű ügyfélazonosításhoz szükségesnek ítélte a jogalkotó a többi adat egyezőségének a vizsgálatát is, ez volt a viszontazonosítási folyamat, mint információs interoperabilitási folyamat bevezetésének oka. Az interoperabilitás relevanciáját a 2013-as interoperabilitási törvény[38], illetve az Európai Unió határokon átnyúló elektronikus azonosítási kezdeményezései megerősítik (STORK[39], eIDAS[40], PEPPOL[41]), habár az ügyfelek azonosítását a viszontazonosítástól eltérő módon interpretálták (így az megmaradt nem adaptált és alig használt magyar megoldásnak az eID létrejöttéig). Az interoperabilitási törvény a benne foglaltak teljes hatályba lépésére a 2015. január 1-et követő 21. hónapot jelölte meg – vagyis 2016. október 1-ével kellett legkésőbb ezeket az előírásokat teljesíteni.

A közigazgatási hitelesítésszolgáltatók létrejöttétől az elektronikus ügyintézés felfutását várta a jogalkotó. A gyakorlati megvalósítás során azonban számos probléma merült fel (információs, műszaki és értelmezési is), amelyeket meg kellett oldani a hatékony és eredményes működés megvalósításáért. Ismeretes, hogy az ügyfélazonosítás során a hivatalnok minden egyes esetben közhiteles személyazonosító okmányok alapján végzi el az ügyfél hitelesítését (azonosságának megerősítését), amit kezdetben implicit módon elvártak a digitális tanúsítványokat használó rendszerektől is, amelyet azok nem minden esetben tudtak teljesíteni. Erre a problémára egyébként már 2000-ben rávilágított Ellison és Schneier [5], ahol tíz kockázatra hívták fel a szerzők a figyelmet. Ezeknek a kockázatoknak a kiküszöbölése (csökkentése) akkor sem látszott triviálisnak, és közülük néhány ma is létező relevanciával bír. A viszontazonosítás problémakörére vonatkozó kockázatot az alábbiakban látták:

„Risk #4: 'Which John Robinson is he?'" - vagyis „ő melyik Nagy László?"

[38] 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól
[39] STORK: Secure idenTity acrOss boRders linKed – Határokon átnyúló biztonságos azonosítás (https://www.eid-stork.eu/)
[40] eIDAS: Electronic Identification and Signature – elektronikus azonosítás és aláírás (http://certifiedsignature.eu/2014/03/01/eidas-electronic-identification-and-signature-electronic-trust-services-final-draft/)
[41] PEPPOL: Pan-European Public Procurement Online – Pán-európai elektronikus közbeszerzés (http://www.peppol.eu/)

Az X.509v3 tanúsítványban[42] ugyanis a kötelező adatok köre nem, vagy csak részlegesen terjed ki a természetes személyt egyértelműen azonosító adatokra. A korábbi személyazonosító jel használatát felváltó módokról rendelkező 1996. évi XX. törvény[43] az alábbiakat mondja ki:

„4.§ (4) Természetes személyazonosító adat a polgár

a) családi és utóneve, születési családi és utóneve,

b) születési helye,

c) születési ideje és

d) anyja születési családi és utóneve."

A probléma lényegét jól megmutatja, hogy a fentiek közül digitális tanúsítványban kötelezően egyik sem jelenik meg (álneves tanúsítvány esetében még a név sem lesz használható természetes személyazonosító adatként, mindazonáltal opcionális mezőben, a tanúsítvány birtokosának szabad akaratából, bármilyen adat elhelyezhető benne, akár a természetes személyazonosító adatok is, vagy más olyan adatok, amelyekhez ezek egyértelműen kapcsolódnak (például a fényképes személyazonosító okmányok adatai). A Kormányzati Hitelesítés Szolgáltató a személyazonosító okmány adatait az alanynak a szerződésben megadott hozzájárulása alapján helyezi el tanúsítványban és publikálja azt a nyilvánosság számára. A tanúsítvány egyedi sorozatszáma kapcsolja össze jelen esetben a regisztráció során megadott természetes személyazonosító adatokat a tanúsítványban meghatározott adatokkal. A kérdés tehát egy közigazgatási hatósági ügyintéző számára úgy jelentkezik, hogy ha kap egy közigazgatásban használható digitális tanúsítvány segítségével aláírt elektronikus dokumentumot az ügyféltől, akkor vajon hogyan lesz képes az ügyfelet hitelesen beazonosítani annak természetes személyazonosító adataival, az ügyfél személyes jelenléte nélkül, amennyiben az nem tartalmazza az állampolgár igazolványának a számát? Más szóval azt is kérdezhetjük, hogy az ügyfél által használt tanúsítvány

[42] Lásd International Telecommunication Union, Telecommunication Standardization Sector of ITU: ITU-T X.509, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory. Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks. ITU-T Recommendation X.509. 14.10.2016., ami teljesen megegyezik az ISO/IEC 9594-8:2017 nemzetközi szabvánnyal.

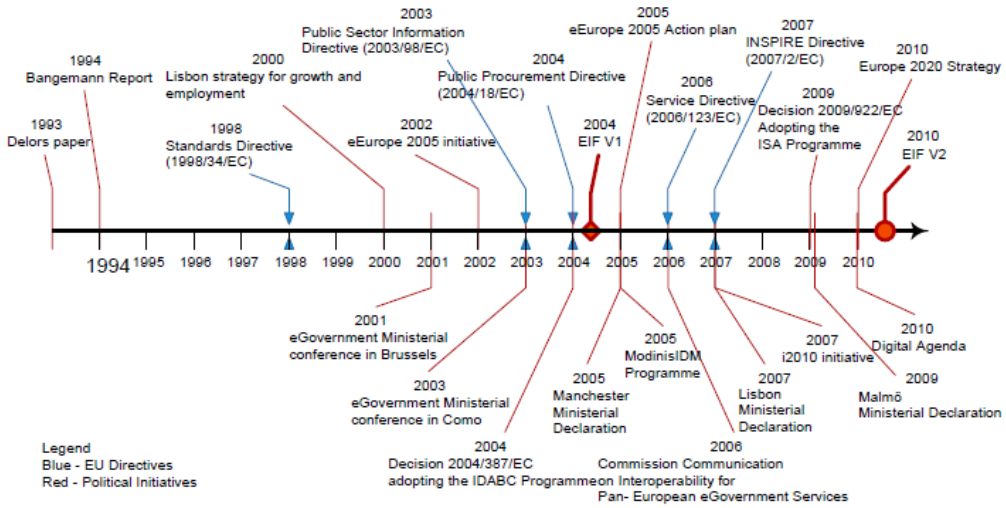
[43] 1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról

sorozatszáma hogyan válhat kapcsolati kóddá a hatóság és a hitelesítés-szolgáltató között, vagyis összekapcsolhatók-e ilyen értelemben a hatósági és a közigazgatásban használható tanúsítványokat kibocsátó hitelesítés-szolgáltatók adatbázisai [6].

Felber Zsófia így ír erről a problémáról 2014-ben [11]: „A közigazgatási eljárás egyik alapelve, hogy a hatóság ne kérjen az ügyféltől olyan adatot, amit már valamelyik állami szerv nyilvántart. Ennek az elvnek az alkalmazása azonban, több esetben akadályba ütközik, mivel az állami nyilvántartások egymástól eltérő struktúrát alkalmaznak, amely megnehezíti a hatóságok közötti kommunikációt és lehetetlenné teszi az eljárások gyors ügyintézését.”

Az együttműködés információbiztonsági szempontból is felmerült Muha megfogalmazásában is a stratégia megalkotásánál ([3]: 214): „Az információs rendszerek védelme részben (...) kiemeli a kormányzati információs rendszerek védelmének fontosságát és felhívja a figyelmet a sikeres védelem érdekében szükséges együttműködésre, az érintett informatikai és távközlési szolgáltatókkal.”

Az interoperabilitás, mint kulcsfogalom, 1993 óta jelen van az Európai Unió kezdeményezései között is:



5. ábra: Az európai interoperabilitás megteremtésének mérföldkövei (forrás: Európai Interoperabilitási Keretrendszer[12])

2.6. A VISZONTAZONOSÍTÁS FELTÉTELEI

A feltett kérdésre a választ annak megvizsgálásával kezdjük, hogy a hiteles azonosításhoz szükséges, a természetes személyt egyértelműen azonosító információk - amelyek a folyamat elindításának alapfeltételei között vannak - hol találhatók meg az ügyintéző-ügyfél-hitelesítésszolgáltató háromszögben?

1. *Információk az Ügyintézőnél:* ebben az esetben feltételezzük, hogy az Ügyfél és az Ügyintéző között egy korábbi interakció eredményeként az Ügyfél természetes személyazonosító információi már megtalálhatók, és egy – rájuk jellemző – kapcsolati kóddal vagy ilyen jellegű azonosítóval veszik fel egymással a kapcsolatot. Ebben az esetben az Ügyintéző képes a viszontazonosítási eljárás segítségével összehasonlítani az elektronikus aláírást készítőjének személyazonosító információit az Ügyfél Ügyintézőnél megtalálható személyazonosító információival, és egyezőség esetén nagy biztonsággal fogadhatja el az Ügyfél által beküldött elektronikus dokumentumot. Különbözőség esetén a dokumentum elfogadását az Ügyintézőnek el kell utasítania és más módszert kell keresnie az ügyfél hiteles azonosítására. Az ügyfél az aláírást HunEID kártyával is készítheti[44].

2. *Információk az Ügyfélnél:* ha az Ügyintéző nem rendelkezik az ügyfél természetes személyazonosító információival vagy kapcsolati kód jellegű információval, be kell azt szereznie valahonnan. Ha az Ügyintéző nem rendelkezik az Ügyfélről semmilyen személyazonosító információval vagy személyazonosító kóddal, akkor nem járható út a másik hatóságtól való adatkapcsolat-szolgáltatás sem, hiszen nem lehetséges megmondani, hogy melyik Ügyfélről kér információt az ügyintéző. Ez az eset azonban igen ritkán fordul elő, ezért a hiányzó információk beszerzésének legegyszerűbb módja az ügyféltől magától elkérni az ügyintézéshez szükséges információkat, vagy az ügyfél valamely azonosító kódjának ismeretében egy másik hatóságtól (például BM közhiteles adatbázisai) elkérni a természetes személyazonosító információkat. Így visszajutottunk az 1. esethez, vagyis a viszontazonosítási eljárás lefolytathatóvá vált.

3. *Információk nem elérhetők:* elképzelhető olyan eset, amikor a hatóságnál nincsen meg a szükséges ügyfél-információ, az ügyfél pedig nincs abban a helyzetben, hogy az elektronikusan aláírt dokumentum beküldését követően prezentálja azt, mert már

[44] Lásd https://docplayer.hu/2061503-Kozigazgatasi-informatikai-bizottsag-21-szamu-ajanlasa-az-ugyfelkapu-es-hivatali-kapu-kapcsolodas-muszaki-specifikacioja-2.html (2019.02.04.)

vagy nincs érvényes azonosítója (esetleg lejárt az igazolványa), vagy fizikailag akadályoztatva van (ideértve a halálesetet, kóros elmeállapot-változást) ez esetben az ügyintézés lefolytatásához szükséges információkat a fenti 1. és 2. esetek szerint nem lehetséges beszerezni. Egyedi megoldásokra lehet itt szükség, amelyek visszavezetnek ebből az esetből az 1. esethez, a viszontazonosítás elvégezhetőségéhez.

2.6.1. A VISZONTAZONOSÍTÁSI ELJÁRÁS

Az eljárás ismertetéséhez felhasználjuk a vonatkozó IHM ajánlást[45] [10]. A viszontazonosítási protokoll az alábbiak szerint működött:

1. lépés: kérés összeállítása: a viszontazonosítást kérő a személy természetes azonosító adatait (viselt név és születési név, anyja neve, születési helye, születési ideje, esetleg állampolgársága) vagy ezek egy részhalmazát felhasználva elkészítette a szabványos kérést XML-ben, ellátta saját digitális aláírásával és elküldte a tanúsítványt kibocsátó hitelesítés-szolgáltató megfelelő interfészére.

2. lépés: ellenőrzés:

    a. küldő jogosultságának ellenőrzése: a hitelesítés-szolgáltató ellenőrizte a küldő jogosultságát, és csak a megfelelő esetben lépett a b) pontra

    b. kérés ellenőrzése: a hitelesítés-szolgáltató feldolgozza a kérést – a megfelelő tolerancia-szint46 mellett, és összehasonlítja a küldő által ismert adatokat a saját adatbázisában tárolt adatokkal

3. válaszolás: a hitelesítés-szolgáltató az összehasonlítás eredményét (IGEN/NEM válasz) eljuttatja a küldő számára megfelelő szabványos XML-formában, saját digitális aláírásával ellátva.

    Egy sikeres válasz például a következő alakban jöhetett létre:

[4545] Az Informatikai és Hírközlési Minisztérium (IHM) ajánlása a közigazgatásban a hitelesítésszolgáltatók által végzett viszontazonosítás protokolljának műszaki specifikációjára (2005. december 6.)
[46] Az alkalmazott tolerancia-szint megegyezik az ügyfélkapun keresztül azonosított felhasználók viszontazonosításánál alkalmazott megoldással

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://www.iop.hu/2004"
xmlns:hszva="http://www.melasz.hu/schema/hszva/hszva1.0">
        <soap-env:Header/>
        <soap-env:Body soap-env:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
                <Valasz>
                        <ValaszFejlec>
                                <Felhasznalo>RendszerAzonosító</Felhasznalo>
                                <UzenetIdopont>2001-12-17T09:30:47-05:00</UzenetIdopont>
                        </ValaszFejlec>
                        <Session>
                                <Property Source="HivatalAzonosító" Name="TranzakciosKod"
                        Value="111111111"/>
                        </Session>
                        <Form>
                                <hszva:Azonositott EID="1">1</hszva:Azonositott>
                        </Form>
                        <Parancs PID="String">
                                <Rendszer>String</Rendszer>
                                <Szolgaltatas Module="String" FormID="String"
                                Muvelet="String">String</Szolgaltatas>
                                <Cimke>String</Cimke>
                        </Parancs>
                </Valasz>
        </soap-env:Body>
</soap-env:Envelope>
```

6. ábra: Viszontazonosítás válasz (forrás: IHM ajánlás [10])

A sikertelen válasz annyiban különbözött az előzőtől, hogy az Azonosított EID változó értéke nem 1, hanem 0 volt. Más érték nem volt megengedve a válaszban.

A viszontazonosítási eljárás könnyen programozható XML-állományokon keresztül kommunikáló protokoll volt 2005. december óra a magyar közigazgatásban. Tekintettel arra, hogy a hitelesítés-szolgáltatók számára (azaz jellemzően a regisztrációs szervezetek) a közigazgatásban használható tanúsítványok kibocsátásakor az ügyfél azonosítása során minden egyes esetben törvényi előírás volt az, hogy az ügyfél által bemutatott igazolványok adatait ellenőrizni kell[47], a közigazgatási szervezet a

[47] Eat. 9. § (3) A hitelesítés-szolgáltató a 12. §-ban foglalt jogosítványaival élve azonosítja az igénylő személyét, majd a saját elektronikus aláírásával aláírt tanúsítvánnyal hitelesíti az igénylő elektronikus aláírását.
Eübszt. 82. § (1) A bizalmi szolgáltató által kibocsátott tanúsítványnak az abban foglalt adatokat a valóságnak megfelelően kell tartalmaznia, kivéve ha magából a tanúsítványból kitűnik, hogy az adat valódiságát a bizalmi szolgáltató nem ellenőrizte (így különösen álnév esetén). Ennek érdekében a bizalmi szolgáltató a tanúsítványba foglalandó adatokat köteles ellenőrizni, így különösen a tanúsítvány tartalmától függően ellenőrzi a tanúsítvány alany személyazonosságát, a személyazonosság megállapításához használt azonosító adatok valódiságát és – ha van ilyen – közhiteles vagy más központi nyilvántartásban foglalt adatokkal való megegyezőségét, a tanúsítvány alany nevében a bizalmi szolgáltató előtt eljáró képviselő képviseleti jogosultságát, a tanúsítványba foglalandó képviseleti jog meglétét, a tanúsítvány által igazolt címtartomány (domain) fölötti rendelkezési jogot, a tanúsítványban feltüntetendő IP-cím fölötti rendelkezési jogot, a tanúsítványba foglalandó szervezeti egység létezését, a tanúsítványba foglalandó szabályozott szakma megnevezése esetén az annak gyakorlására való jogosultságot.

viszontazonosítással gyakorlatilag automatizált ellenőrzést hajtott végre a közhiteles nyilvántartásokkal egy köztes rendszeren (adatbázison) keresztül. A rendszer használatának gyakoriságát egyrészről az határozta meg, hogy a közigazgatás mennyire volt képes digitálisan aláírt dokumentumok befogadására az ügyfeleitől, másrészről az, hogy a közigazgatási szervezetek képesek voltak-e XAdES-aláírásokkal[48] ellátott viszontazonosítási kérések kibocsátására a hitelesítés-szolgáltatók felé, illetve tudták-e a kapott XML-válaszokat fogadni és értelmezni. Meg kell még említeni azt is, hogy a kérések biztonsági követelményeire vonatkozó megoldások nem voltak részei a protokollnak, arról ezen kívüli eljárásokkal gondoskodtak (pl. https-kapcsolat). Mindenesetre ez a megoldás az elektronikus aláírás használatát inkább komplexebbé tette, semmint egyszerűsítette volna. Az igény azonban teljesen érthető és világos, sőt, ma is aktuális. A Rendelet 24. cikkének 1. c) pontja szerint a minősített tanúsítványokat kibocsátó minősített bizalmi szolgáltatóknak azonosítani szükséges és ellenőrizni kell az azonosítási adatokat, mielőtt a minősített tanúsítványt kibocsátják, ehhez felhasználhatják az ügyfél minősített elektronikus aláírását is.

Azon túl, hogy a Pp. szerint a magyar jogrendben a minősített elektronikus aláírással ellátott magánokiratnak teljes bizonyító ereje van[49], a minősített bizalmi szolgáltató a természetes azonosító adatok ismeretében kéréssel fordulhat a minősített aláírás létrehozásához használt minősített tanúsítvány kibocsátójához, hogy a minősített tanúsítvány és a teljes bizonyító erővel állított természetes azonosító adatok valóban összetartoznak-e, mivel a regisztrációkor felvett adatokat a minősített bizalmi szolgáltatóknak legalább 7 évig[50], Magyarországon 10 évig[51] meg kell őrizniük a tanúsítvány lejártát követően. Ilyen kérések teljesítése tehát nem ütközhet az adatok hiányának a problémájába, de természetesen a Rendelet 24. cikkében megadott felhatalmazást a GDPR előírásainak figyelembevételével együtt kell kezelni[52]. Ezt az eljárást azonban az eID azonosítás tagállami és határokon átnyúló alkalmazása

[48] XAdES: XML-based Advanced Electronic Signature, XML-alapú fokozott biztonságú elektronikus aláírás
[49] Pp. 325. § (1) Teljes bizonyító erejű a magánokirat, ha f) az elektronikus okiraton az aláíró a minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírását vagy bélyegzőjét helyezte el, és – amennyiben jogszabály úgy rendelkezik – azon időbélyegzőt helyez el.
[50] Lásd ETSI EN 319 411-1, OVR-6.4.6-01 követelményét.
[51] Lásd 24/2016. (VI.30.) BM rendelet, 35. § (1) bek.
[52] Lásd eIDAS Rendelet, 5. cikk 1. bek. Habár itt a Rendelet még a 95/46/EK irányelvet említi, ezt hatályon kívül helyezte Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről.

szükségtelenné teheti, amennyiben a 4T adatok[53] rendelkezésre állnak, ahol természetes személyazonosító adatok alatt a polgárok következő adatait kell érteni:

a) családi és utóneve, születési családi és utóneve,

b) születési helye,

c) születési ideje és

d) anyja születési családi és utóneve.

2.7. A DIGITÁLIS TANÚSÍTVÁNYOK DISSZEMINÁCIÓS KÉRDÉSEI

Digitális tanúsítványt személyesen odaadni egy-egy ember számára nem jelent problémát, azonban ezek nagy tömegű kiosztása már felvethet kérdéseket. A teljesen elektronikusan intézhető közszolgáltatások végzése (e-közigazgatás) feltételezi az elektronikus hitelesség fennállását is, amelyhez szükséges a digitális tanúsítványon alapuló fejlett digitális aláírás (legalább fokozott biztonságú elektronikus aláírás). Ebből adódóan mind a köztisztviselőnek, mind az ügyfélnek rendelkeznie kell elektronikus aláírási képességekkel. A megválaszolni kívánt kérdés az, hogy milyen paraméterek mentén lehetséges nagy tömegű (ezrestől a milliósig) terjedő számosságú embercsoport ellátása digitális tanúsítványokkal. A vizsgálathoz felvázolok egy egyszerűsített modellt a tanúsítványok kibocsátására, ezt követően meghatározom a mérni kívánt mutatókat, majd elemzem a mutatók értékeinek változásait egy logaritmikus értelmezési skálán.

Az e-kormányzat alapvető szolgáltatásait a CLBPS (Common List of Basic Public Services, alapvető közszolgáltatások listája) meghatározta, amelyek értékelésére az Európai Bizottság a Capgeminivel közösen kidolgozott egy értékelési módszertant, ami módosította az eredetileg négy szintet tartalmazó keretrendszert és Capgemini módszertan néven futott tovább. Tózsa észrevette, hogy az Európai Unió tudatosan hozta létre a CLBPS-t, nem az elektronikus közigazgatás megvalósulásának a képéért, hanem azért, „mert a CLBPS-ben leírt 12+8 ügytípus jelenti azokat a „játékhajókat”, amelyek a jövő mobil-interneten alapuló hármas csatornáján (online PC, mobil és digitális kábel tv) új dimenzióba vezetik a közigazgatást” ([94]: 18). A végrehajtási szintek eredetileg a

[53] 4T adatok alatt az 1996. évi XX. törvény 4. § (4)-ben megfogalmazott természetes személyazonosító adatokat kell érteni.

folyamatok digitalizációjával kapcsolatosan fogalmaztak meg egyre erősebb követelményeket, ismertette Budai ([37]: 197-198):

1. szint: információs szint, elegendő információk elektronikus hozzáférhetőségét biztosítani ezen a szinten.

2. szint: nyomtatvány szint, az információkon túl az ügyek intézéséhez szükséges formanyomtatványok is megjelennek.

3. szint: interaktív szint, az űrlapok kitöltésére online is lehetőség nyílik, de minden tevékenység még nem hajtható végre elektronikusan.

4. szint: tranzakció szint, a folyamatban minden egyes lépés (ideértve a tranzakciós illeték lerovását is) elvégezhető elektronikus formában, személyes megjelenésre nincs szükség (de a személyes megjelenéssel egyenértékű elektronikus azonosítás megjelenhet a folyamat-elemek között).

5. szint: perszonalizációs szint: az ügyfél-élmény fokozása érdekében személyre szabott targetizált ügyintézés valósítható meg, ideértve az ügyfélről már rendelkezésre álló adatok felhasználását újbóli bekérés nélkül[54]. A proaktív személyre szabott elektronikus ügyintézés például egy 3D avatar segítségével is megvalósítható (Tózsa 2013 [8]).

A Capgemini 2017-es e-kormányzati elemzése[55] az EU28+ e-kormányzati felkészültségét mérve az elmúlt öt évben elért előrehaladást mutatta meg négy mutatóra vonatkozóan:

1. felhasználó-központúság
2. átláthatóság
3. határon átnyúló szolgáltatások
4. kulcsfontosságú technológiai ösztönzők

[54] Az Európai Unió az Uniós e-kormányzati cselekvési terv 1.7.1 fejezetében alapelvként fektette le az egyszeri adatszolgáltatás elvét (‘once-only’ principle). (Brüsszel, 2016.4.19. COM(2016) 179 final, Uniós e-kormányzati cselekvési terv 2016–2020. A közigazgatás digitális átalakításának felgyorsítása)
[55] Lásd https://www.capgemini.com/wp-content/uploads/2017/11/2017-egovernment-benchmark_background_v7.pdf (2019. március 5.)

A közigazgatási folyamatok csak hiteles, ellenőrzött információkat használhatnak fel, akár papíralapon, akár elektronikusan történik az ügyintézés. Ehhez ma már nélkülözhetetlennek látszik az elektronikus hitelesség, az elektronikus írásbeliség és elektronikus teljes bizonyító erő, amelyeket különböző elektronikus aláírások segítségével lehet megvalósítani. Az elektronikus aláírások készítéséhez megfelelően biztonságos kriptográfiai módszerek szükségesek, amelyek Muha [4] IT biztonsági rendszertanában védendő elemként szerepelnek – a biztonság az elektronikus aláírási rendszereknek is az egyik kulcsfontosságú tényezője.

Az elektronikus aláírás közösségi alkalmazásáról szóló eIDAS rendelet három aláírás-típust (kettő explicit és egy implicit típust) definiál az elektronikus alírásokon belül:

- (normál) elektronikus aláírás,
- fokozott biztonságú elektronikus aláírás, és
- minősített elektronikus aláírás.

A minősített aláírások kiemelt jelentőségűek, mert egyrészről a jogalkotó teljes bizonyító erőt, másrészről európai szintű feltétel nélküli elfogadási kötelezettséget rendel hozzájuk. Azonban a jogszabály szigorú feltételeket is szab az ilyen aláírások készítési eljárásához:

„eIDAS. 3. cikk 12. ’minősített elektronikus aláírás’: olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás minősített tanúsítványán alapul;”

A két feltétel tehát egy eszköz, és egy minősített tanúsítvány megléte, aminek az aláíró felügyelete alatt kell lennie az aláírás előtt, annak végrehajtásához. Minősített tanúsítványt pedig csak minősített hitelesítés-szolgáltató bocsáthat ki, regisztrációs folyamatain keresztül. Tömeges elektronikus ügyintézéshez ebből következendően nagy mennyiségben szükséges megfelelő, elektronikus ügyintézéshez felhasználható tanúsítványokat kibocsátani.

Ez a fejezet annak a kérdésnek a megválaszolását tűzte ki célul, hogy milyen hatékonysággal lehetséges minősített tanúsítványokat nagy számosságú ügyfélkör számára kibocsátani. Ehhez egy olyan modellt kell megalkotnunk, amely valós

folyamatok adatain alapulva, különböző kiindulási feltételek megfogalmazása mellett lehetővé teszi a hatékonysági mutatók számítását, elemzését, összehasonlítását. A hatékonysági mutatókat két oldalról vizsgáljuk meg, egyrészről a szolgáltató oldaláról, másrészről a felhasználó oldaláról.

A kérdés aktualitását az adja, hogy 2013 év végén elkezdte működését a 83/2012. Kormányrendelet 74. § által leírt hitelesítés-szolgáltatás SZEÜSZ, vagyis elindult a Kormányzati Hitelesítés Szolgáltató Magyarországon és megkezdte az állampolgári jogon járó tanúsítványok kiosztását az új személyazonosító igazolványba integráltan, opcionális jelleggel, azaz kizárólag az állampolgár kérdésére. Kérdés, hogy ha hirtelen nagy számosságú igényléssel találja magát szemben a Kormányzati Hitelesítés Szolgáltató – a kezdeti 10% körüli penetráción túlmenően, akkor milyen lefutású folyamat várható ennek kapcsán.

Az e-közigazgatásban kívánatos lenne, hogy elektronikus ügyintézéssel minden köztisztviselő foglalkozhasson, aminek előfeltétele, hogy legyen elektronikus ügyintézésre feljogosító tanúsítványa. Hogyan lehetséges hatékonyan hozzájuttatni a közszolgálati tisztviselőket digitális tanúsítványhoz? A vonatkozó előírások csupán megengedő felsorolást tartalmaznak ezzel kapcsolatosan, ami azt jelenti, hogy adott esetben több választási lehetőség közül is választat a szervezet. Érdekes lenne megvizsgálni modellezési szinten azt a kérdést is, hogy az egyes megoldási lehetőségek milyen hatékonysági tulajdonságokkal rendelkeznek, vagyis hogyan képzelhető el a nagyságrendileg 350 000 szellemi foglalkozású közszolgálati alkalmazott – vagy a közülük érintettek – ellátása elektronikus aláírásra és kiadmányozásra egyaránt feljogosító digitális tanúsítvánnyal, ha felmerülne ennek szükségessége?

2.7.1. A REGISZTRÁCIÓS FOLYAMAT ÉS OPCIÓI

A hitelesítésszolgáltató a tanúsítványokat csak regisztrált felhasználó számára bocsáthatja ki (Eübszt. 82. § (1), (2)), más szóval az igénylő adatait ellenőrzi, mielőtt a tanúsítványban feltüntetné azokat. Erre az Eübszt. 82. § (3), (4) adja meg a törvényi felhatalmazást. Attól függően lehet megkülönböztetni az egyes regisztrációs szinteket, hogy mennyire erősen győződnek meg az adatok valódiságáról. A regisztrációs szintek definiálásához különösen fontos kérdések a következők:

1. személyes megjelenés kötelező-e vagy lehetséges elektronikusan is regisztrálni,

2. milyen személyes adatok megadása szükséges a regisztrációnál,

3. hol és hogyan ellenőrzik le a megadott adatokat,

4. ki veheti át az elkészült aláírás-létrehozó adatot és tanúsítványt.

#	Regisztrációs szint	Ellenőrzési tevékenység
1.	Fokozott (eIDAS előírásaiból következtetett szint)	Az e-mailben beküldött adatokat a szolgáltató közhiteles adatbázisokban leellenőrzi, kiállítja a tanúsítványt és elküldi a megadott e-mail címre. A felhasználónak nem kötelező személyesen megjelenni a szolgáltató előtt.
2.	Közigazgatási (Eübszt. által lehetővé tett, 137/2016. Korm.R. által definiált szint)	A személyesen megjelent felhasználó által bemutatott igazolvány adatait a regisztrációs tisztviselő szemrevételezéssel és közhiteles adatbázisokban leellenőrzi, aláírásával igazolja az ellenőrzés meglétét, kiállítja a tanúsítványt a felhasználó nevére – álnév használata kizárt és a felhasználó saját kezébe adhatja csak oda.
3.	**Minősített (eIDAS által definiált szint)**	**A személyesen megjelent felhasználó által bemutatott igazolvány adatait a regisztrációs tisztviselő közhiteles adatbázisokban leellenőrzi, kiállítja a tanúsítványt a felhasználó nevére vagy álnevére, és a felhasználónak személyesen adhatja át – képviselő általi átvétel is kizárt.**

7. ábra: Regisztrációs szintek (forrás: saját ábra)

A modell megalkotásában kizárólag a minősített és közigazgatási tanúsítványokra vonatkozó regisztrációs folyamat elemeit használom fel, amelyek személyes megjelenéshez kötöttek. A vizsgálat kiterjeszthető a személyes megjelenéshez nem kötött tanúsítványok kiosztásának vizsgálatára is, ekkor nyilvánvaló módon a személyes kontaktusok ideje nem fog megjelenni a modellben, azonban az az adatok feldolgozási ideje és a kommunikáció előkészítéséhez szükséges idő ekkor is számítható és része a modellnek.

A regisztrációs folyamatot elemeire bontva a következő részfolyamatokat lehetséges megkülönböztetni:

1. az igénylés benyújtása

2. benyújtott adatok ellenőrzése

3. az aláírás-létrehozó és ellenőrző adatok legenerálása

4. a tanúsítvány kiállítása

5. a kiállított tanúsítvány és az aláírás-létrehozó adat igénylő általi átvétele

A regisztrációt végző szereplők vonatkozásában a 83/2012. Kormányrendelet a Kormányzati Hitelesítés-szolgáltató számára egyrészről előírja azt, hogy „A tanúsítvány

kibocsátásához szükséges regisztrációt természetes személyre a szolgáltató kizárólag a közigazgatás központi humánpolitikai szerve, vagy ha a személy tekintetében az nem illetékes, a hatóság bevonásával végzi.”, másrészről „A szervezeti tanúsítványokkal kapcsolatos regisztrációt és kulcsátadást a hatóság szervezeti és működési szabályzatában kijelölt, vagy a hatóság vezetője által közokiratban meghatalmazott szervezeti egységének bevonásával végzi.”

A fentiek tükrében tehát az egyes részfolyamatok végzésére az alábbi opciók lehetségesek:

#	Folyamatelem	Potenciális lebonyolítók
1.	az igénylés fogadása	REG1 / REG2 / REG3
2.	benyújtott adatok ellenőrzése	REG1 / REG2 / REG3
3.	az aláírás-létrehozó és ellenőrző adatok legenerálása	REG1
4.	a tanúsítvány kiállítása	REG1
5.	a kiállított tanúsítvány és az aláírás-létrehozó adat igénylő általi átvétele	REG1 / REG2 / REG3

8. ábra: Regisztrációs opciók (forrás: saját ábra)

A modellalkotásban ki kell térni arra, hogy milyen hatékonyságú lesz a regisztráció akkor, ha a fenti folyamat-elemeket a Szolgáltató (REG1) vagy a HR szervezet (REG2) vagy az Okmányiroda (REG3) végzi. Mindhárom esetben a modell kimenetét befolyásoló fontos feltételezés, hogy hogyan alakul az ügyintézők száma és mennyien képesek foglalkozni egyidőben a regisztrációs tevékenységekkel.

2.7.2. A REGISZTRÁCIÓS MODELL (R.M.) ELEMEI ÉS LEÍRÁSA

A modell kimeneteinek számításához meg kell határozni az egyes folyamatelemekre vonatkozó alapadatokat. Az alapadatok meghatározásánál a rendelkezésre állás megváltozásait (pl. üzemszünetek, leállások) nem vettem figyelembe, folyamatos rendelkezésre állást feltételeztem a regisztráció ügyintézési idejében. A modell alapadatait ennek megfelelően így rögzítettem:

#	Folyamatelem	Szükséges időtartam		
		REG1	REG2	REG3
1.	az igénylés befogadása	10 perc	10 perc	10 perc
2.	benyújtott adatok ellenőrzése	5 perc	5 perc	5 perc
3.	az aláírás-létrehozó és ellenőrző adatok legenerálása	5 perc		
4.	a tanúsítvány kiállítása	5 perc		
5.	a kiállított tanúsítvány és az aláírás-létrehozó adat igénylő általi átvétele	10 perc	10 perc	10 perc

9. ábra: A tanúsítvány-kiosztási folyamat elemei (forrás: saját ábra)

A modellben az eltérő opciók által végzett részfolyamatok időszükségletének alapadatait azonosnak tekintettem és nem tekintettem ennek részeként az igénylő általi további időigényes ráfordításokat (pl. utazás, sorban állás, várakozás). Elviekben lehetséges különböző opciókhoz különböző időtartamok hozzárendelése is. A modell kiszámítja a meghatározott alapadatok alapján a vizsgálandó igénylések számosságához tartozó időszükségletet. Az időt munkanapokban (munkaévekben) határozom meg, 8 órás nettó munkaidőt feltételezve az év 200 munkanapján. A modell úgy tekinti az igényléseket, hogy egyszerre, egy adott időpillanatban megjelennek, nem számol az igénylések esetleges időbeli eloszlásával.

A modell a tanúsítványok és aláírás-létrehozó adatok előállításának végzésére szekvenciális módot feltételez, párhuzamosítást nem enged meg ezekben a lépésekben. Az ügyintézők által végezhető lépések párhuzamosíthatók, azzal a feltételezéssel, hogy a közhiteles adatbázisokban történő ellenőrzéshez szükséges rendelkezésre állást és kapacitást a rendszerek üzemeltetői biztosítják. Az igénylések és az ügyintézők feltételezett számát előre rögzítettem, mégpedig az igénylések számosságát négy szintben (ezer, tízezer, százezer, egymillió), míg a feltételezett ügyintézők számát három szintben (REG1: 5, REG2: 500, REG3: 5 000).

A modellt jelentősen le kellett egyszerűsíteni ahhoz, hogy működőképessé lehessen tenni, több olyan implicit feltételezést be kellett építeni, ami csupán távolról közelíti a valóságot, de a használhatóságot növeli:

- a tanúsítványok kibocsátására szolgáló humán erőforrás a vizsgált esetekben nem változik,
- a tanúsítványok kiállításánál minden igénylőnek meg kell várnia az összes tanúsítvány előállítását, valamint

- az igénylés befogadását a kijelölt szervezetek (REG2, REG3) ügyintézői is el tudják párhuzamosítva végezni.

Az R.M modellnek arra a kérdésre kell választ adnia, hogy milyenek lesznek a regisztrációs folyamatok nettó időszükségletei, a meghatározott opciók választása esetén.

2.7.3. HATÉKONYSÁGI MÉRŐSZÁMOK

Az informatikai projektek sikerességi kritériumai jó kiindulási alapot szolgáltatnak hatékonysági mutatók deriválásához is. Ezt az is alátámasztja, hogy DeLone és McLean a D&M IS Success Model [7] leírásában is a sikeresség és a hatékonyság fogalmakat egymás szinonimájaként használja információs rendszerek esetében. A D&M modell három szintű sikerességet és annak mérési koncepcióját definiálja:

1. technológiai sikeresség: az IT rendszerek minősége jellemzi;

2. szemantikai sikeresség: az információ minősége jellemzi;

3. hatékonyság sikeressége: használhatóság, felhasználói elégedettség, személyes hatás, szervezeti hatás jellemzi.

A modell frissítése bevezet új fogalmakat is, legfontosabb a „net benefits”, a nettó előnyök mérése – ezt fogom felhasználni én is ebben a modellben a 3. sikerességen túl.

A regisztrációs folyamat előnye az, hogy minden jogosult igénylő a lehető legrövidebb időn belül megkaphassa a tanúsítványát. Ebben a mondatban három mérési lehetőség is benne foglaltatik, ami a sikerességet mérhetővé teszi:

A. jogosult igénylések téves elutasításának a száma nulla,

B. a felhasználók átlagos várakozási időfüggvényének minimum-pontja az igénylések és ügyintézők számának függvényében megfelel az elvárásoknak,

C. minden igénylés feldolgozása befejeződik, a várakozó kérelmek száma nulla.

A szolgáltató számára a legfontosabb hatékonysági mutató az, hogy milyen rövid idő alatt képes kiállítani az igényelt tanúsítványokat a benyújtástól az átadásig számítva. A párhuzamosítható lépésekben az ügyintézők számától függően fog ez az érték változni. Ha az egyes részfolyamatokat nem a szolgáltató végzi, akkor úgy tekinti, hogy egyszerre kapja meg és adja át csomagként a bejövő és a kimenő adatokat, eszközöket. A

szolgáltatói oldal hatékonyságát az igénylések teljesítéséhez szükséges nettó időtartammal kívánom reprezentálni.

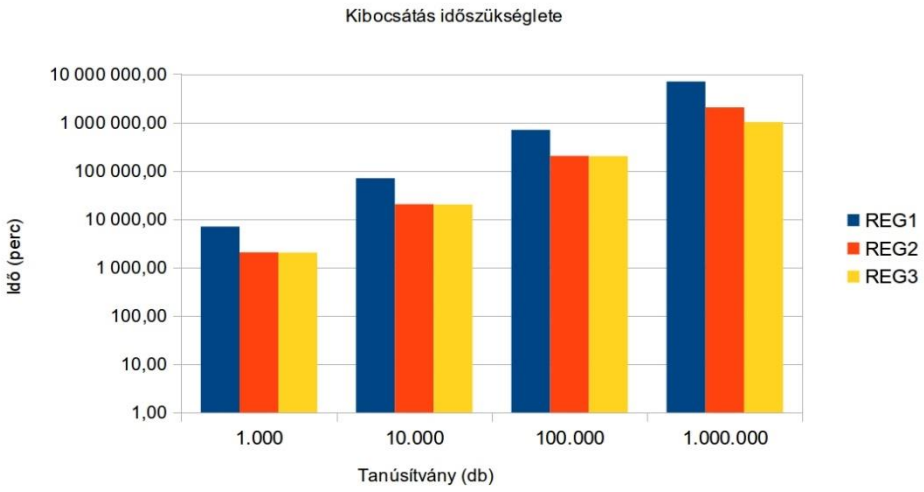
Az igénylő elégedettségét az első találkozás során kapott impulzusok jelentős mértékben befolyásolják. Az igénylésének befogadása, a várakozási idő és a megkapott tanúsítvány felhasználhatósága mind-mind olyan tényezők, amelyek részt vesznek az elégedettség vagy elégedetlenség megjelenésében. A regisztráció hatékonyságát vizsgáló modellben a várakozási idő függ össze legjobban a folyamat nettó időszükségletével, ezt a B. sikeresség-jelző statisztikai paraméter (átlagos várakozási idő) változásai jelzik leginkább, ezért ezt vizsgálom meg az ügyintézők és igénylések számának változása tükrében. Ez lesz a felhasználó-oldali hatékonyság mérőszáma.

2.7.4. Az R.M. modell kimenetei

A modell eredményeit látva két megállapítás olvasható le a grafikonról a kibocsátás időszükséglete tekintetében:

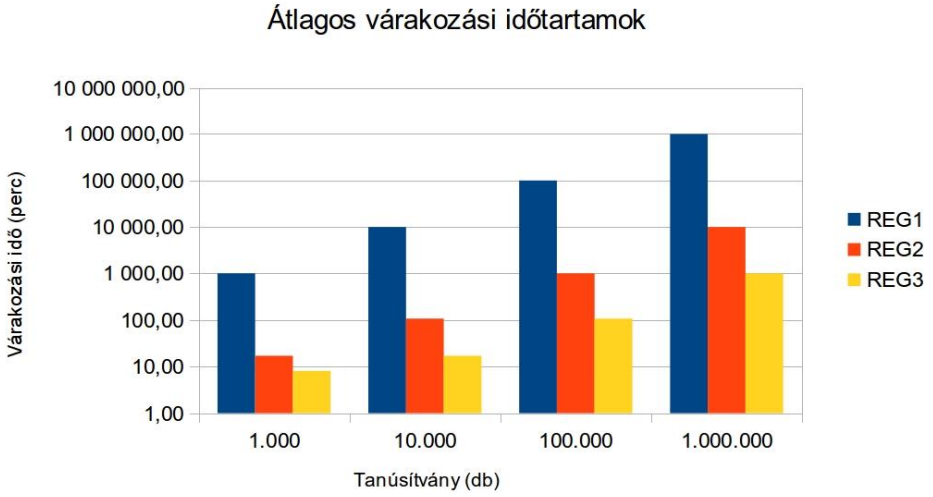
a) a REG2 és REG3 minden esetben minimum fél nagyságrenddel gyorsabban el tudja végezni ezt a feladatot,

b) az REG3 kapacitásainak látható, kézzelfogható előnyei a REG2 erőforrásaihoz képest csupán 1 000 000 tanúsítvány-nagyságrend körül jelentkeznek.



10. ábra: Tömeges minősített tanúsítvány-kibocsátás időszükséglete (forrás: saját ábra)

A felhasználók számára a hatékonyság egyik fő mérőszáma az volt, hogy mennyit kell várniuk az igénylés benyújtásától számítva addig, amíg a tanúsítvánnyal el nem kezdhetnek dolgozni.



11. ábra: Tömeges kibocsátás átlagos várakozási időtartamai (forrás: saját ábra)

A logaritmikus skálázású grafikonról jól leolvasható, hogy a várakozási idők a hitelesítés-szolgáltatói kibocsátáshoz képest minden esetben meghaladják az egy nagyságrendet, az ügyintézői létszámok pontosan tükröződnek a grafikonon. Kérdés, hogy egy esetleges további párhuzamosítás (a lépések közötti várakozási ciklusok lerövidítése) mekkora további csökkenést képes előidézni. Megjegyzésre kívánkozik, hogy 1 000 perc kicsit több, mint két munkanap, 10 000 perc az majdnem 21 munkanap – ez nagyjából a lélektani felső várakozási időt jelenti (egy hónap). Az ettől magasabb várakozási időszükséglettel rendelkező megoldásokat e-kormányzati viszonylatban is nyugodtan tarthatjuk – a teljes eljárások kivételével – alkalmazhatatlannak, hivatkozva az Ákr. 50. §-ában megfogalmazott ügyintézési határidőkre[56].

Nagyon fontos eredménynek gondolom azt, hogy már ez a – korlátosan szofisztikált – modell is rávilágított a regisztrációs kapacitások lényegességére. Tömeges tanúsítvány-kibocsátást a fentiek szerint csak olyan kapacitású szervezetek közreműködésével lehetséges hatékonyan végrehajtani, amelyek képesek az IT sikerkritériumokat a felhasználói elégedettség megfelelő szintjén tartani, ilyen például Magyarországon az okmányiroda. Ettől eltérni mindaddig nem célszerű, amíg a közhiteles azonosítás másként nem lehetséges. Megvizsgálva az elektronikus azonosítás (eID) előfeltételeit, az ügyfél személyes megjelenése az első eID megszerzéséhez

[56] Ákr. 50. § [Az ügyintézési határidő] Ha törvény eltérően nem rendelkezik, az ügyintézési határidő az eljárás megindulásának napján kezdődik. Az ügyintézési határidő automatikus döntéshozatal esetén huszonnégy óra, sommás eljárásban nyolc nap és teljes eljárásban hatvan nap.
Korábban a Ket. 33. paragrafusa által rögzített általános közigazgatási ügyintézési határidőt 21 napban határozta meg a jogalkotó.

továbbra is szükséges, habár a továbbiakban használható a már megszerzett elektronikus jogosultság a tanúsítványok igénylési folyamatában, ahogyan ezt a Rendelet 24. cikkének (1) b) pontja megfogalmazza[57]. Jelentősen redukálhatja azonban az azonosítási eseményeket, ha a személyes megjelenést mindaddig nem szükséges megismételni, amíg az első eID eszköz érvényessége és a kapcsolódó adatok változatlansága fennáll. A magyar Kormányzati Hitelesítés Szolgáltató minősített állampolgári tanúsítványt kérelemre bocsát ki, a kérelmet az eljáró hatóságnál[58] kell benyújtani minden egyes esetben. Habár az igénylés és a szerződés megkötése elektronikus úton is megvalósítható[59], az igénylőnek minden esetben kötelező személyesen is megjelenni[60] a személyazonosságának megállapítása céljából[61], a 2019-ben hatályos magyar szabályozás szerint, továbbá az 51. § (4) bekezdésében említett online felület műszaki és technikai feltételei 2019 februárjában még nem voltak adottak.

2.8. KÖZIGAZGATÁSI KIEGÉSZÍTÉSEK

2.8.1. A MAGYAR KÖZIGAZGATÁSBAN HASZNÁLHATÓ TANÚSÍTVÁNYOK

Az elektronikus aláírások általános leírására alkalmas dimenziók nem használhatók kiegészítések nélkül a magyar közigazgatásban, így van értelme megkülönböztetni az elektronikus aláírások általános és közigazgatási célú felhasználását. Az eIDAS rendelet szerint nem kell a közigazgatási belső eljárások lebonyolítására szolgáló és ehhez bizalmi szolgáltatásokat igénybe vevő rendszerekre a Rendelet előírásainak vonatkozniuk, de a harmadik felek számára is elérhető nyilvános bizalmi szolgáltatásokra nézve viszont ezeket kötelezően érvényesíteni kell. Az érvényesítés során azonban a közigazgatási szervek által nyújtott online szolgáltatások határokon átnyúló igénybevétele tekintetében a tagállamok nem követelhetnek meg a

[57] eIDAS rendelet 24. cikk (1): Bizalmi szolgáltatásra vonatkozó minősített tanúsítvány kibocsátásakor a minősített bizalmi szolgáltató megfelelő eszközökkel és a nemzeti jogszabályokkal összhangban ellenőrzi annak a természetes vagy jogi személynek az azonosságát, és – adott esetben – egyedi jellemzőit, akinek vagy amelynek a részére a minősített tanúsítványt kibocsátották.
Az első albekezdésben említett adatokat a minősített bizalmi szolgáltató a nemzeti jogszabályokkal összhangban közvetlenül vagy harmadik fél révén ellenőrzi: (…)
b) távolról, olyan elektronikus azonosító eszköz használatával, amely tekintetében a minősített tanúsítvány kibocsátása előtt biztosították a természetes személynek vagy a jogi személy képviseletre jogosult képviselőjének személyes jelenlétét, és amely megfelel a 8. cikkben a „jelentős”, illetve a „magas” biztonsági szintre vonatkozóan meghatározott követelményeknek
[58] Az „eljáró hatóság” értelmezését a 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól adja meg 11. § (1) pontjában.
[59] Lásd 414/2015. (XII. 23.) Korm. rendelet 51. § (4) bekezdését.
[60] Lásd 414/2015. (XII. 23.) Korm. rendelet 52. § (1) bekezdését.
[61] Lásd 414/2015. (XII. 23.) Korm. rendelet 52. § (2) bekezdését.

minősített elektronikus aláírásnál vagy bélyegzőnél magasabb biztonsági szintű elektronikus aláírást (Rendelet 27. cikk (3) és 37. cikk (3)). Ez azt jelenti, hogy a közigazgatás számára a minősített elektronikus aláírás és bélyegző lehet a legmagasabb szint, amit előírhat és amit befogadhat, azok minden követelményével együtt. Azaz megkérdőjelezhető ennek révén az a hazai gyakorlat, hogy az állampolgári tanúsítvány igénylésekor minden esetben személyesen kell megjelenni az azonosításhoz, hiszen ez ellentmondhat a Rendelet 24. cikkében foglaltaknak és abból csak az egyik lehetőséget (a személyes megjelenést) ragadja ki, a többit (eID, minősített tanúsítvány, nemzeti egyenértékű tanúsított azonosítási módszer) pedig nem, vagy csak részben alkalmazza. A feltételes mód indokolt, mivel jelenleg nincs olyan eID eszköz, amely a 24. cikk (1) b. pontja szerint alkalmazható lenne, viszont az (1) c. pont alkalmazását (az ügyfél minősített elektronikus aláírásával is kérheti a minősített tanúsítványának megújítását) nem lehet megtiltani. Ez a kérdés csak abban az esetben érdekes, ha a személyazonosító igazolvány más adata nem változik, csupán a rajta tárolt minősített tanúsítvány megújítását igényli az állampolgár. A 2019. február 12-én érvényes magyar szabályozás szerint egyrészről a személyazonosító igazolvány kiadása csak személyes jelenlét útján valósítható meg (néhány kivétellel, pl. kiskorú igazolványa)[62], másrészről a Kormányzati Hitelesítés Szolgáltató nem nyújt megújítási szolgáltatást, csupán a még érvényes tanúsítványát használva az állampolgár jelezheti egy új tanúsítványra vonatkozó igényét, amelyet személyesen kell ezt követően a kijelölt regisztrációs helyeken átvennie egy új személyazonosító igazolványon[63].

A fokozott biztonságú elektronikus aláírások és bélyegzők elismerésénél szintén van kötelem, ugyanis ha egy tagállam egy közigazgatási szerv által nyújtott online szolgáltatás használatához fokozott biztonságú elektronikus aláírás alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie minden olyan fokozott biztonságú elektronikus aláírást, amely a végrehajtási aktusokban meghatározott, ideértve a nem minősített vagy minősített tanúsítványon alapuló és a minősített elektronikus aláírásokat is (Rendelet 27. cikk (1) és 37. cikk (1)). Amennyiben csak a minősített tanúsítványon alapuló elektronikus aláírásokat vagy bélyegzőket kíván egy tagállam elfogadni, akkor

[62] Lásd 414/2015. (XII. 23.) Korm. rendelet 12. § (1) bekezdését.
[63] Lásd NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Bizalmi Szolgáltatási Szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (BSZ-ESZIG), v1.6, 2017.06.29., „4.6 Tanúsítványok megújítása” fejezetében leírtakat. (http://hiteles.gov.hu/letoltes/228/BSZ-ESZIG_v1.6_signed.pdf, 2019. február 12.)

mentességet kap az ettől alacsonyabb szintű, nem minősített tanúsítványon alapuló fokozott biztonságú aláírások elfogadása alól, de a magasabb szintű minősített aláírásokat ebben az esetben is el kell fogadnia függetlenül a kibocsátó tagállamtól (Rendelet 27. cikk (2) pont és 37. cikk (2) pont).

Magyarországon a közigazgatás saját nyilvános kulcsú infrastruktúrát működtet annak érdekében, hogy elkülönítse az általános célra használható és csak a közigazgatás által felhasználható elektronikus aláírásokat. A közigazgatás számára a közigazgatási gyökér-hitelesítésszolgáltató elektronikus bélyegzőjével hitelesíti az elektronikus ügyintézést biztosító állami szervek által használt bizalmi szolgáltatáshoz tartozó tanúsítvánnyal szemben meghatározott követelményeknek megfelelő tanúsítványt kibocsátó bizalmi szolgáltató nyilvános kulcsát[64]. A szolgáltató működtetését a Nemzeti Média- és Hírközlési Hatóság (NMHH) látja el, köztisztviselők által. Egyszerűbben szólva az NMHH által működtetett Közigazgatási Gyökér Hitelesítés-Szolgáltató[65] (KGyHSz) hitelesíti felül minden olyan tanúsítványkibocsátó szolgáltatói tanúsítványát, amelyekkel a közigazgatásban használható tanúsítványokat szeretnének kibocsátani, akár piaci, akár kormányzati szolgáltatóról van szó. Ennek következménye, hogy ha egy szolgáltató tanúsítványa szerepel a böngészők megbízható legfelső szintű tanúsítványtárolójában, a közigazgatási célú szolgáltatói tanúsítványa nem fog ott megjelenni mindaddig, míg a KGYHSZ tanúsítványa be nem kerül oda, azaz az ügyfelek felé a közigazgatási aláírások nem látszanak automatikusan hitelesnek. Ennek oka az, hogy az adott végfelhasználói tanúsítványlánc nem lesz megbízható gyökértanúsítványra visszavezethető[66], így a megbízhatóságáról a böngészők és az aláírás-megjelenítő szoftverek nem tudnak pozitív megállapítást tenni.

[64] Lásd 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről, 3. § (1).
[65] Bővebben lásd http://www.kgyhsz.gov.hu/ (2019. január 30.). A KGYHSZ szerepéről itt lehet további információkat kapni: http://www.kgyhsz.gov.hu/kgyhsz_ismerteto.pdf. (2019. január 30.) A KGYHSZ működését szabályozó hitelesítési rend elérhető a következő linken: http://www.kgyhsz.gov.hu/KGYHSZ_HR_v1.0.pdf. Tekintettel arra, hogy a szabályzatot 2006 március 3-án bocsátották ki, felülvizsgálata indokoltnak látszik, több módosítás bekövetkezett a szabályozás kiadása óta, amely nem itt, hanem a jogszabályokban és végrehajtási rendeletekben tükröződik. Kérdéses ennek a dokumentumnak a szerepe és jelentősége a jogi szabályozás kibővülését követően. Adott esetben elképzelhető a hitelesítési rend integrálása valamely végrehajtási rendeletbe is mellékletként.
[66] A gyakorlatban ezt jelenti a „nem megbízható” üzenete a böngészőknek, ami nem feltétlenül a szolgáltatás minőségére vonatkozik, hanem a szolgáltatásnak az adott programban való szerepeltetésére.

Az EüszR. az alábbi részterületeken fogalmaz meg előírásokat:

- Az elektronikus ügyintézési célra, illetve közigazgatási célra használható elektronikus aláírással, elektronikus bélyegzővel és tanúsítványokkal szembeni követelmények
- A kiadmányozásra nem jogosult személy (ügyintéző) által használt aláíráshoz tartozó tanúsítvánnyal szembeni követelmények
- A kiadmányozásra feljogosított személy (ügyintéző) által használt aláíráshoz tartozó tanúsítvánnyal szembeni követelmények
- Az ügyintézési célú elektronikus bélyegző létrehozásához használt tanúsítvánnyal szembeni követelmények

A korábbi szabályozások[67] az ügyfelek által használható tanúsítványokra nézve is tettek korlátozó kitételeket a közigazgatásban való felhasználás érdekében, ezek a részletek 2016. július 1-ével kikerültek a módosított szabályozásból.

A közigazgatásban használható elektronikus aláírások terén meg kell említeni a kormányablakokban lehetővé tett biometrikus aláírások használatát is, amelyet a fővárosi és megyei kormányhivatal ügyfélszolgálatain, a járási (fővárosi kerületi) hivatal kormányablakaiban, illetve a települési ügysegédnél az elektronikus dokumentumok ügyfél általi hitelesítésére lehet alkalmazni az aláírás képi, dinamikai és íráserősségi adatainak elektronikus felvételezésére képes hitelesítő eszköz rendszeresítésével a 2016. évi CIV. törvény 88. § (11) bekezdése alapján[68]. A rendszeresített eszközön történő aláírásnál az aláíró és a tárolt minták közötti egyezés vizsgálatának eredményéről tanúsított, zárt rendszer által kiállított, a dokumentumazonosítót tartalmazó, de az aláíró biometrikus jellemzőit már nem tartalmazó elektronikus igazolást a dokumentumhoz kell csatolni. Az ilyen elektronikus igazolással ellátott dokumentum teljes bizonyító erejű magánokiratnak minősül. Ez a fajta aláírás ebben a formában kizárólag a magyar közigazgatásban használható, így elfogadottsága is csak a magyar közigazgatásra

[67] Lásd 194/2005. (IX. 22.) Kormányrendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről, illetve a 78/2010. (III. 25.) Kormányrendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól

[68] Lásd 2010. évi CXXVI. törvény a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról, 20/J. § (1)

korlátozódik. Ilyen korlátozott aláírási rendszert azonban bármelyik csoport számára létre lehet hozni, azonban annak ismeretében, hogy az általános célú biometrikus aláírás nem biztonságos[69], javasolható további védelem is ezekhez az aláírásokhoz, hogy teljesíthessék a fokozott biztonságú elektronikus aláírással szemben támasztott követelményeket és ne csak egy magyar hatósági záradék szolgáljon a bizalom alapjául hanem technológiai intézkedések is alátámaszthassák azt. A rendszer egyébként fel van készítve a biometrikus adatok tárolására, azonban azt az ügyfél hozzájárulásához és szándékához köti, a hatályos adatvédelmi szabályozásnak megfelelően.

2.8.2. Ügyintézési csatornák a magyar közigazgatásban

A Nemzeti Közigazgatási Egyetem 2015-től minden évben elkészíti a „Jó Állam Jelentés" dokumentumot ([147], [148], [149], [150]), amely reprezentatív kutatáson alapul, és több témát is felölel, köztük a magyar lakosság által előnyben részesített ügyintézési csatornákat (H.5.3 A közigazgatási ügyintézési csatornák igénybevételének megoszlása). Tekintettel arra, hogy a felmérés sokváltozós, országosan reprezentatív nemi és életkori megoszlásra is, illetve 2 500 fős mintán végzett adatgyűjtésen alapul, a lakossági ügyintézési szokások lényeges megváltozása nem feltételezhető banki ügyek intézése során sem egy olyan bankban, amelyiknek a legtöbb bankfiókja van Magyarországon és tradicionálisan elérhető minden településen. A közigazgatási ügyek intézésében mindazonáltal a magyar lakosság inkább a személyes ügyintézést részesíti évek óta előnyben a többi rendelkezésre álló csatornához képest, amint azt az alábbi táblázat is mutatja – a felmérés során megengedett volt, hogy egy válaszadó több csatornát is bejelöljön:

Év / Csatorna	személyes	postai szolgáltatások	telefonos ügyfél-szolgálat	online, internetes
2016 (populációhoz viszonyítva) [149]	58,1% 5.692,3e	20,8% 2.037,9e	4,1% 401,7e	18,3% 1.793,0e
2017 (populációhoz	61,8% 6.043,0e	5,8% 567,1e	17,8% 1.740,5e	14,7% 1.437,4e

[69] MELASZ Állásfoglalás a biometrikus aláírásokról. http://www.melasz.hu/lang-hu/remository?func=fileinfo&id=186 (2019. január 30.)

Év / Csatorna	személyes	postai szolgáltatások	telefonos ügyfél-szolgálat	online, internetes
viszonyítva) [148]				
2017 (csatorna-használók számosságához viszonyítva) [152]	89,6%	8,5%	11,0%	12,0%
2018 (csatorna-használók számosságához viszonyítva) [147]	86,5%	5,0%	11,3%	19,1%

1. táblázat: Előnyben részesített csatornák a magyar közigazgatásban (készült: [147]: 170, [148]: 169 és [149]: 140 és KSH[70] alapján)

Az ügyfelek számosságát a háttéradatok megadott Venn-diagramjából határoztam meg. A táblázat rávilágít arra, hogy az e-közigazgatás fejlesztése és számos elektronikus ügyintézési szolgáltatás bevezetése ellenére a polgárok ügyeket intézni személyesen szeretnek, ez a preferenciájuk annak ellenére, hogy az internetes ügyintézés volumene jelentékeny mértékben növekedett az elmúlt évhez képest. Ez továbbra is indokolja a papíralapú használathoz közelálló elektronikus megoldások bevezetését és jelenlétét az e-közigazgatás során. A személyes ügyintézés preferenciáját magyarázó tényezők feltárása érdekes kérdés lehet, azonban messze túlmutat ennek a dolgozatnak a keretein. A Jó Állam Jelentés háttérváltozói azonban rámutattak arra, hogy az alternatív csatornák használatával együtt a személyes ügyintézést preferálók számossága csökken[71], vagyis az alternatív csatornák nem versengenek egymással, hanem kiegészítő és továbblépési formaként vannak jelen a személyes ügyintézés mellett, illetve a személyes ügyintézést hagyják el az ügyfelek, ha már képesek alternatív csatornákon is az ügyeiket elintézni.

[70] KSH Népesség, összesen (2007–2018)
https://www.ksh.hu/docs/hun/eurostat_tablak/tabl/tps00001.html (2019. február 26.)
[71] Lásd [152] 115. ábra

Ezt a trendet erősíti a kötelező elektronikus ügyintézés egyre szélesebb körre való kiterjesztése.

2.9. BIZTONSÁGI KÉRDÉSEK

2.9.1. A MAGYAR KÖZIGAZGATÁS INFORMATIKAI FENYEGETETTSÉGE

A közigazgatás digitalizálódásával és az elektronikus információs rendszerek térnyerésével megjelentek a biztonságuk ellen ható informatikai tényezők is, amelyek a papíralapú közigazgatásban java részben ismeretlenek voltak. Az e-közigazgatás mellett azonban ma már nincsenek reális – ugyanilyen hatékonysággal és eredményességgel működő – alternatívák, a közigazgatással szemben támasztott elvárásokat csak magas szintű számítógépesítéssel és információfeldolgozással lehetséges teljesíteni. Ezt az álláspontot fogalmazza meg Budai, amikor a „közigazgatási informatika” kifejezést alapfogalomként használja az e-közigazgatás elméletében és rendszertanában, illetve amellett érvel, hogy az informatikát közműnek kell tekinteni a XXI. században [37]. Az informatikától való függőség felveti az eredményesség elérését célzó fejlesztési, innovációs kérdések vizsgálata mellett a rosszindulatú károkozó programok hatásának vizsgálatát is, annak eldöntési igénye nélkül, hogy ez rossz vagy jó. Neumann János szavaival élve annyit lehetséges mondani, nem valamilyen különleges felfedezés különlegesen romboló mivolta okozza a veszélyt, mert a technikai hatékonyság olyan kétarcú vívmány, amelynek a veszélye a lényegéből fakad. A technikai rendszerek ugyanakkor hallatlan életerőt rejtenek magukban, így a visszaszorításukra irányuló tanácsok már Neumann János idejében sem látszottak elfogadhatónak [99].

Az informatikafüggés azonnal feltételezi az energiafüggést is, hiszen a szilíciumalapú számítástechnikai eszközök állandó működéséhez az energia folyamatos külső betáplálása szükséges (ha nincs állandó saját energiaforrása az eszköznek). A magyar közigazgatás számára ez azt jelenti, hogy az elektronikus információs rendszerek rendelkezésre állása előbb-utóbb szorosan összekapcsolódik a villamosenergia-ellátó rendszerek állapotával is (mivel a szünetmentes áramforrások egy idő után kimerülnek és a generátorok üzemanyag-ellátási lánca is megszakadhat). A magyar villamosenergia-ellátó rendszer állapotáról Bárdos Zoltán így írt 2009-ben:

„A villamosenergia-piaci kereskedelem révén a határkeresztező szállítások mennyisége és távolsága megnőtt; továbbá, a pontosan előre nem jelezhető, időszakosan

működő villamos energiatermelés (szélerőmű, kiserőművek) gyors térhódítása figyelhető meg. Ezek az Európát átszelő, egyre növekvő nagyságú áramlásokat idéznek elő, melyeket a rendszer kezdeti tervezésénél nem vettek figyelembe. A megváltozott körülmények miatt a rendszert a biztonsági határokhoz közel üzemeltetik, ami miatt a napi hálózatüzemeltetés sokkal kihívóbb feladattá vált." ([100]: 79)

A villamosenergia-ellátó rendszer biztonsági határokhoz közelebbi üzemeltetése miatt az incidensek valószínűsége természetes következményként megnövekszik, mivel kisebb lehetőségei vannak a rendszernek a jövőbeli kiugró helyzetek elviselésére. Az energia-ellátásnak a számítógépes biztonsághoz való kapcsolódását a SCADA[72] rendszerek teremtik meg, amelyekkel az energia-ellátási folyamatokat vezérlik. Ennek távoli (logikai) támadásával közvetlenül lehet hatást gyakorolni az energia-ellátó rendszerekre az informatikai rendszereken keresztül, a vezetékek és elosztóközpontok (fizikai) támadásán túl, ahogyan erre Kovács László és Krasznay Csaba is rávilágított 2010-es elhíresült Digitális Mohács tanulmányukban [75]. Az üzemeltetési szempontok változása és a szakértelem centralizálódása miatt szükségessé vált az irányítási rendszerek távoli elérhetőségének kialakítása, ami újabb veszélyforrásokat teremtett a rendszerek számára és ezzel ez a terület is összekapcsolódott az internetes fenyegetésekkel.

Resperger a közép- vagy hosszú távon bekövetkező kibertámadás valószínűségét magasként értékeli, az országra gyakorolt közepes hatás mellett ([74]: 89, 10. táblázat). Kovács és Krasznay [75] arra hívják fel a figyelmet, hogy ezek a támadások egyszer nagyon magas valószínűséggel (szinte teljes bizonyossággal) bekövetkeznek, és egy összehangolt támadás során előálló több közműszolgáltatást párhuzamosan érintő események hatása már katasztrofális is lehet, ami ellen csak koordinált módon lehetséges a védelem megvalósítása. A holland DigiNotar esetében[73] az üzemeltetők csak a kontrollt veszítették el részlegesen a tanúsítványok kibocsátása felett, a szolgáltatói titkos kulcsok

[72] SCADA: Supervisory Control And Data Aquisition, felügyeleti ellenőrző és adatbegyűjtő számítógép által vezérelt/felügyelt ipari vezérlő rendszer

[73] A támadás eredményeként a támadók számos weboldal hitelesítő tanúsítványt generáltak (például a *.google.com, *.microsoft.com és a *.aol.com wildcard domain nevekre is), amelyet minősített európai bizalmi szolgáltató érvényes legfelső szintű tanúsítványára lehetett visszavezetni a támadás ideje alatt. Ezeket a hamis tanúsítványokat heteken át felhasználták közbeékelődéses támadás végrehajtására (MITM), amelyben közel 300 000 olyan felhasználó volt érintett, akik az Iráni Iszlám Köztársaságból használták az internetet. A Google szervereinek szánt forgalmat valószínűleg lehallgatták vagy átirányították a támadás során, ezzel valószínűleg sikerült hozzáférni a lehallgatott tartalomhoz, valamint az érintett felhasználók Google hitelesítő adataihoz. Az esetről készített részletes jelentés letölthető a következő URL-ről: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf

bizalmassága fennmaradt, a hatás mégis katasztrofális volt a holland e-közigazgatásra, van der Meulen egyenes a „digitális katasztrófa” (digital disaster) kifejezést használta erre az esetre a részletes elemzésében [93], ami az első ilyen esemény volt Hollandiában. Az események következményei rávilágítottak arra, hogy az egyes országok szolgáltatásainak megtámadása mögött olyan érdek is állhat, amely nagyon távol van földrajzilag az adott országtól – esetleg egy másik kontinensen realizálódik a támadás eredménye.

Az interneten a mindennapos szolgáltatások (böngészés, web2 alkalmazások, e-mail, csevegő szobák, közösségi oldalak, játékok stb.) mellett ma már folyamatosan jelen vannak a rosszindulatú támadások is. Kezdetben a CERT közzétette a bejelentett incidensek számát, amely 1997-2003 között lényegében exponenciális növekedést mutatott, de ezt egy idő után abbahagyta azzal az indoklással, hogy az incidensek számának növekedése már nem jelent hozzáadott értéket, gyakorlatilag majdnem mindegy, hogy százezer, egymillió, tízmillió vagy százmillió incidens következik-e be egy adott hónapban a világban. Ezzel implicit módon ekkor kimondták azt, hogy a fenyegetettség folyamatos, a sérülékenységek kihasználására nap mint nap számtalan próbálkozás történik az internetes világban. Más szóval a 2010-es évektől kezdődően elérkeztünk a folyamatos fenyegetettség korszakába, amelyet a szakirodalom Advanced Persistent Threat (APT) fogalommal illetett, Gyebrovszki találó magyar definíciójában ez lett a Folyamatosan Fennálló Fejlett Fenyegetés (4F):

„Informatikai rendszerekbe észrevétlenül, célzott módon, adatszerzés és/vagy rombolás céljából bejuttatott különleges képességű folyamatok, melyek külső kapcsolat segítségével, távolról kiadott vezérlőparancsok végrehajtásával folyamatosan működve fejtik ki jogszerűtlen tevékenységüket.” ([101]:149)

Figyelemre méltó – és Neumann Jánosnak a kétarcú technikai veszélyekről szóló álláspontját támasztja alá Bransfield [104] a 2003-ban felfedezett féreg (worm) kód elemzésével (Welchia [Nachi]), amely a rosszindulatú és nagy károkat okozó Blaster féreg által kihasznált sérülékenységet megpróbálta kijavítani, a Blaster férget törölte, majd önmagát is megsemmisítette időzített módon, 2004. január 1-én. Vagyis ezzel bebizonyosodott, hogy lehetséges a féreg terjedési mechanizmusát a féreg számítógépes irtására felhasználni, természetesen a megfelelő óvintézkedéssel (önmegsemmisítés). Ez a mechanizmus a vírusok Adleman által megadott absztrakt elmélete [103] alapján a patogén és fertőző osztályba tartozik, habár már Adlemannál is megjelenik a segítő

(„helpful”) vírusok létezésének lehetősége. A Welchia féreg írója valószínűleg nem gondolt arra, hogy a segítőkészségével óriási hálózati forgalmat fog generálni, ami jelentős fennakadásokat okozott a hálózati szolgáltatásokban és leállásokat is eredményezett.

A világban zajló események hatására Magyarországon is érdemi lépések történtek a közigazgatásban az információbiztonság terén. 1994-ben megjelent az Informatikai Tárcaközi Bizottság 8. számú ajánlása[74], 1996-ban elkészült az Informatikai Tárcaközi Bizottság 12. számú ajánlása az informatikai rendszerek biztonsági követelményeiről a Miniszterelnöki Hivatal Informatikai Koordinációs Iroda megbízásából[75]. Az ajánlások sorát a Közigazgatási Informatikai Bizottság által kibocsátott dokumentumok folytatták 2008-2009-ben[76]. A magyar Országgyűlés 2013. április 15-én elfogadta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényt, amelynek hatóköre a teljes közigazgatásra és minden olyan szereplőre is kiterjed, akik a közigazgatás számára adatkezelést végeznek. Habár az információbiztonsági szabályozása több évtizedre visszamenőleg jelen volt már Magyarországon, ez a törvény teremtette meg a jogalapot a közigazgatás és a kritikusnak minősíthető infrastruktúrák, a létfontosságú rendszerelemek egyenszilárdságú védelmének kialakításához és fenntartásához. A törvény hatályba lépését követő első öt évben kialakultak azok az intézmények, amelyek a biztonság fenntarthatóságát célozzák és elindult az érintett szervezetek felelőseinek folyamatos információbiztonsági oktatása, képzése is, ami a biztonságtudatosság megteremtésében az első építőkockának tekinthető [102].

2.9.2. BIZTONSÁGI KÉRDÉSEK AZ ELEKTRONIKUS ALÁÍRÁSOKHOZ

A legfontosabb biztonsági kérdés az elektronikus aláírások esetében az, hogy vajon lehetséges-e olyan aláírást készíteni, amely az aláíró szándéka ellenére és tudta nélkül készül, mégis elfogadhatónak látszik. Legrosszabb eset az, ha ennek a hamis aláírásnak az érvénytelenségét be sem lehet bizonyítani, mert ebben az esetben a látszólagos aláíróra olyan kötelezettségek terhelődnek, amelyek alól az érvényes szabályok szerint nem tud mentesülni. Ennek elkerülése tehát kívánatos lenne minden társadalomban, az elektronikus aláírások széles körű használatát feltételezve. De miért is

[74] Lásd https://web.archive.org/web/20120823032129/http://www.itb.hu/ajanlasok/a8 (2019. február 18.)
[75] Lásd https://web.archive.org/web/20120822212331/http://www.itb.hu/ajanlasok/a12/ (2019. február 18.)
[76] Lásd https://segitseg.magyarorszag.hu/segitseg/kibajanlasok.html (2019. február 19.)

ennyire fontos az elektronikus aláírások biztonsága? Kik akarhatnak csalni az aláírásokkal?

Szabó és Hámori [110] játékelméleti megközelítésben vizsgálja meg az eladó és a vevő kontextusában a csalás-korrektség és ellenőrzés-nem ellenőrzés párok alakulását, a kifizetések és egyensúlyok kiszámításával. Azt találták, hogy mindkét fél kifizetése akkor maximális, ha a csalások értéke és az ellenőrzés költsége egyaránt minimális. Rövid távon talán működhet a kisebb értékű csalások költségeinek beárazása, mint védelmi intézkedés, ha az esetek számát azonban nem korlátozzák, akkor a magas esetszám előbb-utóbb megkérdőjelezheti az intézkedés költséghatékonyságát. Ez azt is jelenti más szóval, hogy ebben a kontextusban is a kockázatok csökkentése a biztonság növelését jelenti. A kockázatcsökkentésre négy alapvető mechanizmust definiálnak:

1. tranzakciók technikai biztonságának növelése

2. tranzakciók korrektségét garantáló, a tisztességtelenségből adódó károkat ellensúlyozó és szankcionáló jogintézmények kiépítése

3. társadalmi mechanizmusok kifejlesztése, amelyek elviselhető mértékűre csökkentik a kockázatot, a személyes bizalmat támogatva, és

4. a partnerek közötti személyes bizalom (interpersonal trust) kialakítása és fenntartása.

Ha ezt a szemléletmódot át szeretnénk ültetni a közigazgatásba, akkor rögtön szembetűnik néhány sajátos körülmény. Egyrészről a hatósági ügyek intézésekor az ügyfél azonosítása és hitelesítése nem kerülhető meg és nem engedhető el költségtakarékossági okokból, másrészről az ügyintéző és ügyfél között esetleg fennálló interperszonális bizalom nem feltétlenül transzferálódik az ügyfél és intézmény viszonylatára is. Ha például rendőr a szomszédom, akivel jó viszonyt ápolok, ebből nem következik automatikusan az, hogy a Rendőrségben is, mint intézményben feltétlenül meg fogok bízni. Z. Karvalics ezt úgy fejtette ki az univerzális és egzisztenciális kvantorok használatra vonatkozó írásában [111], hogy ha létezik legalább egy olyan rendőr, akiben megbízok, ebből nem következik az, hogy minden rendőrben megbízok, ez egy hibás következtetés, amely a kvantorok helytelen használatán, de esetleg valódi

érzelmeken alapul. A kettő között (senki és mindenki[77]) széles skálán mozoghat a bizalmi index. Azt is nyilvánvaló módon túlzás lenne állítani, hogy nincs semmilyen hatása az intézménnyel szembeni bizalomra az intézmény tagjaival (képviselőivel) szemben fennálló interperszonális bizalom mértéke, a mindennapokban tapasztalható tranzakcionális biztonság szintje is képes befolyásolni a fenti említett bizalmi viszonyok kialakulását és fennmaradását.

A tranzakciók biztonsága tehát fontos tényező a kockázatok csökkentésében. Az elektronikus aláírások tekintetében a biztonságnak több aspektusa is felmerült a téma tárgyalása során. A kezdeti időkben az algoritmusok biztonsága állt a fókuszban, majd a termék, a hitelesítésszolgáltatás megfelelő nyújtása volt a fontos. Az internet növekedésével az aláírások elkészítési környezetének a biztonsága is jelentős tényezővé lépett elő. Az RSA Security Inc. (Ron Rivest) által kifejlesztett Mailsafe e-mail titkosító alkalmazás piacra dobása Bidgoli szerint [113] 11 évvel a Microsoft megalapítása után, a 386-os processzor megjelenését követő évben, 1986-ban történt. Ebben az évben jelent meg az MS-DOS 3.2 és 3.25, illetve a Microsoft Windows a kibocsátását követő két hónapban 35 000 példányban kelt el, Polsson [114] adatgyűjtését felhasználva. Diffie is megerősíti, hogy az RSA Security Inc. a Mailsafe terméket az 1980-as évek közepén jelentette meg a piacon [115].

Az aláírás létrehozásában fontos szerepe van az aláírásban közreműködő informatikai rendszerelemek, szoftveres környezetek védelmi szintjének. Azonban a biztonság önmagában egy olyan fogalom, aminek az értelmezése nagyon nehéz, ha nem tudjuk, hogy kik ellen kell védekezni és milyen időtávra kell a védelmet biztosítani, ahogyan erre Schneier rámutatott az üzleti világban szerzett érdekes tapasztalatait követően [118]. A biztonság megteremtésének azonban csak egyenszilárd módon van értelme, ami Vasvári megfogalmazásában azt jelenti, hogy a védelem minden ponton elér egy minimális értéket [52]. Felmerül a kérdés, hogyan deríthető ki az, hogy milyen pontokon kell egyáltalán védekezni. Howard 1997-ben kidolgozta az addig bekövetkezett internetes támadások analizálása segítségével az internetes fenyegetések taxonómiáját [121], amit mind a mai napig használnak az információbiztonsági eseménykezelő központok és Howard-séma néven hivatkoznak rá [122]. Ezt követően Schneier bevezette a támadási fa fogalmát [118], [119] egy adott biztonsági eseményhez vezető események

[77] A gyakorlatban ez nyílt halmazként jelenik meg, mivel a bizalomra való képtelenség (senki) és a bizalmatlanságra való képtelenség (mindenki) elvi lehetőségek lehetnek csupán.

és az eseményeket kiváltó okok logikai ábrázolásával konjunktív és diszjunktív formulák segítségével. A módszer hasonló alapelveket alkalmaz, mint a hibafaelemzés nemzetközi szabványa[78]. Az egyes kiváltó okokat értékelni is szükséges, ezért Schneier gyakorlatilag alkalmazza a támadási fa elemeire a Common Evaluation Methodology (CEM)[79] támadási potenciál kiszámítási metódusát, benne a támadáshoz szükséges idő, szakértelem, eszköz figyelembevételét.

Az elektronikus aláírások készítésére használt terminálok biztonságának tárgyalásához Berta specifikál egy másik személy aláírásának egy tetszőleges dokumentumon való megszerzéséhez vezető támadási fát [109] és megállapítja, hogy nem biztonságos terminálon (például egy meghackelt számítógépen) az emberi felhasználó nem tudja kiszámítani a titkosítási ellenőrző összeget egy olyan biztonsági szinten, amelyet a terminál nem tud könnyen megsérteni, illetve nem képes titkosítani egy üzenetet olyan biztonsági szinten, amelyet a terminál nem tud könnyen megsérteni (és nem is oldhatja meg a titkosított üzenetet ilyen biztonsággal). Vagyis ha egy támadó mindenhez hozzáférhet az aláíró környezetében, akkor képes lehet lecserélni az aláírni kívánt üzenet kivonatát egy másik kivonatra az aláírási folyamatban, megszerezni az aláírás-létrehozó eszköz PIN-kódját lehallgatással, lecserélni az aláírás-ellenőrzés pozitív eredményét negatív eredményre és azt megjeleníteni a felhasználó számára, vagy megmódosítani a tartalmat úgy, hogy az eredeti hitelesség látszólag érvényes legyen a módosított – de nem hiteles – tartalomra is, manipulatív szándékkal[80], egyszóval bizonyítottan nem lehetséges biztonságos aláírást készíteni, ha azt feltételezzük, hogy az aláírási környezet nem biztonságos. Ebben az esetben az itt készült aláírások hitelességében sem lehetne megbízni. Erre a problémára született meg többek között a PACE[81] protokoll, ami a terminál és az aláírás-létrehozó eszköz között biztosít védett

[78] Lásd IEC 61025:1990 Fault tree analysis (FTA). A szabvány 2006-ban frissült.
[79] Lásd CEM v1.0, Annex B, B.8 fejezet (https://www.commoncriteriaportal.org/files/ccfiles/cemv10.pdf, 2019. február 19.). Az első verzió 1999. augusztusban jelent meg, a kézirat lezárását megelőzően pedig a 2017. áprilisában kiadott Version 3.1 Revision 5 dokumentumváltozat volt az érvényes.
[80] 2014. novemberében a SERACH-LAB Kft. (Rad Imre) felfedezett egy XML-injection típusú támadási formát, ami látszólag megváltoztatta az már aláírt XML-dossziék tartalmát és azt jelenítette meg a felhasználó felé, nem pedig az eredeti tartalmat. Mivel az aláírt tartalmat a támadás nem változtatta meg – nem is lett volna értelme, csupán erre ráültetett egy plusz réteget, az aláírás ellenőrzése pozitív eredményt adott – mivel nem vizsgálta a ráültetett réteg hitelességét. A veszélyt az jelentette, hogy a felhasználó nem az eredeti tartalmat látta a megjelenítő szoftverben, hanem a módosítottat, így könnyen juthatott volna téves következtetésre a dokumentum hitelességét illetően (https://nvd.nist.gov/vuln/detail/CVE-2015-3931, https://nvd.nist.gov/vuln/detail/CVE-2015-3932, 2019. február 20.)
[81] A PACE rövidítés a „Password Authenticated Connection Establishment” (Jelszóval hitelesített kapcsolat létesítés) kifejezést takarja, amit az aláírás-létrehozó eszközök (érintésmentes kártyák) és az

kommunikációt [178]. Az aláírásban résztvevő többi elem biztonságáról továbbra is szükséges gondoskodni.

Amennyiben feltételezzük, hogy az e-közigazgatás kötelező és egyeduralkodó egy adott ország irányításában, akkor a kibertérben bekövetkező negatív események potenciális veszélyét is vizsgálni szükséges és védelmi intézkedéseket kell definiálni ellenük a polgárok védelmében, ahogy erre Krasznay rámutatott [123]. Véleménye szerint a kiberhadviselés egyre növekvő lehetőség, amellyel már napjainkban is számolni kell, a fegyveres konfliktusok kísérőjeként. Az okos városok terjedésével felmerült az a kérdés is, hogy a kibertér felől mennyire lesznek védettek vagy védtelenek. Orbók megmutatta, hogy a kezdeti funkcionális lelkesedés ellenére a kibertér biztonsági kérdéseinek kezelését sikertelennek kell tekinteni, a hiányosságok növekedési üteme gyorsabb volt a 2010-es években, mint a veszélyforrások eliminálása a megfelelő biztonsági szint elérése érdekében [200]. Példának okáért az előbb említett támadási forma annak ellenére komoly zavart tud kelteni egy e-közigazgatásra épülő ország működésében, hogy a tárolt információk hitelessége ténylegesen nem sérül. Amennyiben az összes dokumentum hitelességébe vetett bizalom megkérdőjelezhetővé válik és minden egyes archivált dokumentum ismételt hitelesítését el kellene végezni mielőtt az adott folyamat felhasználhatná, az jelentős mértékben akadályozná a folyamatok működőképességét, hatékonyságát. Hatványozottan jelentkezik ez a probléma akkor, ha az információ hitelessége sérül (például az okoseszköz elfogad utasítást arra nem jogosult személytől). A feladat sikeres teljesítését a rendszerek komplexitása sem segíti. Komplex rendszerek esetében a biztonság dekompozíciója nem egyszerű feladat, mutat rá Munk, javaslata szerint az egyes biztonsági kérdések dekompozíciójához a vizsgálat tárgyát képező objektumra vonatkozó összes biztonsági kérdést le kell bontani az összetevők biztonsági kérdéseire és meg kell határozni a közöttük fennálló összefüggéseket [124].

A digitális aláírás terjedésével a kriptográfiai biztonság mellett a PKI[82] rendszerek biztonságával is elkezdtek foglalkozni a kutatók, így ért össze az algoritmikus és a szolgáltatási biztonság kutatása. A PKI szolgáltatásokkal kapcsolatosan a szükséges mértékű transzparencia folyamatos elvárás volt a szolgáltatások nyújtásának szabványosításával együtt. Habár a PKI rendszerek variabilitása magas, a teljes rendszer

aláíró terminál közötti kapcsolat biztonsága érdekében fejlesztett ki a német BSI (Bundesamt für Sicherheit in der Informationstechnik) a német eID kártyák vezeték nélküli kapcsolatához.

[82] PKI: Public Key Infrastructure, Nyilvános Kulcsú Infrastruktúra

szabályozhatósága mégis lehetséges, előre definiált tartalommal bíró szabályzatok (hitelesítési rendek, szolgáltatási szabályzatok, aláírási politikák) nyilvánosságra hozásával[83]. Az ügyfelek és érintett felek ezekből tájékozódhatnak a szolgáltatások paramétereiről, biztonságosságáról és a felhasználás érvényességéről. Az egyes szabályzatok formális kódolásának lehetőségét a 2000. januárjában kiadott elektronikus aláírási formátumokat leíró ETSI szabványtervezet[84] veti fel az elektronikus aláírásokkal kapcsolatosan. A formalizált szabályzatok összehasonlítása könnyebben megvalósíthatónak tűnik, ezt állapítja meg Grill is 2004-ben [116], amikor a leíró logikát (description logic, DL) javasolja a szabályzatok összehasonlításának eszközéül, egy alkalmasan megválasztott formális tudásleíró nyelvvel. Megemlíti a CLASSIC [117] mellett a W3C Consortium által javasolt Resource Description Framework (RDF[85]) keretrendszert is, mint lehetőséget. Az ilyen típusú leíró nyelvek objektum-orientált módon formalizálják a természetes nyelvi szövegekben általánosságban előforduló kifejezéseket, megnevezéseket, tulajdonságokat és műveleteket. Az eszköz választását indokolja, hogy a hitelesítési rendek és a szolgáltatási szabályzatok megszövegezése igen távol van egy szabadabb formátumú szépirodalmi mű szókincsétől és stílusától, követelményeket, utasításokat és folyamatleírásokat tartalmaz általában különböző megfogalmazásokban, de azonos struktúrában – kötöttebb formában – megjelenítve. Ez a struktúra 1999. március óta az RFC 2527 5. fejezete által – később az RFC 3647 6. fejezete által[86] „de facto" szabványként szabadon hozzáférhető – valamint a Mozilla és gyakorlatilag a Microsoft által is kötelezően előírt – minden érintett szereplő számára. Az RFC-ben a különböző szolgáltatók különböző szabályzatainak összehasonlíthatósága hangsúlyos célkitűzésként jelenik meg, különösen egy kereszttanúsítás megvalósíthatóságának kiértékelésében. Casola et. al. [112] felvetik 2007-ben a PKI infrastruktúrák biztonsági szintjei összehasonlításának lehetőségét egy biztonsági szabályzatokra kidolgozott generikus formális modell adaptálásával és egy alkalmas

[83] A szabályzatok egységességét szabványos előírások segítik, lásd például az RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) vagy RFC 7382 (Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)) dokumentumokat.
[84] Lásd Draft ETSI ES 201 733 V1.1.2 (2000-01), ETSI Standard, Electronic Signature Formats, 12. oldal: „A signature policy may be written using a formal notation like ASN.1 or in an informal free text form provided the rules of the policy are clearly identified. However, for a given signature policy there shall be one definitive form which has a unique binary encoded value."
[85] Lásd https://www.w3.org/TR/rdf-schema/ (2019. február 19.)
[86] Lásd RFC 2527 Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, 5. fejezet (https://www.ietf.org/rfc/rfc2527.txt, 2019 február 19.), amelyet 2003. novemberében felváltott az RFC 3647, 6. fejezete (https://www.ietf.org/rfc/rfc3647.txt, 2019. február 19.), amely átstrukturálta és kiegészítette az addigi előírásokat.

metrika felhasználásával. A javasolt módszer szerint minden szabályzatot egy olyan mátrix segítségével lehetne reprezentálni, amely egyrészről négyszintű (a nullát is értelmezve ötelemű) biztonsági skálán értékeli az egyes követelmények teljesülését, majd a mátrixok euklideszi távolságával értelmezi az egyes szabályzatok egymástól való távolságát, különbözőségét, illetve a mátrixok nullmátrixtól való különbségével pedig a szabályzatok sajátértékét definiálja. A referenciaértékek definiálását követően (nulla, alacsony, közepes, magas, nagyon magas biztonsági szintet képviselő szabályzatok sajátértékei) minden szabályzat besorolható az öt numerikus érték által meghatározott négy intervallum (biztonsági osztály) valamelyikébe. Ez a módszer azért jelent többet az algoritmusok biztonságának értékelésénél vagy a fizikai védelem erősségének meghatározásánál, mert a technológiai biztonságon túlmenően reflektál a szervezeti és a működési folyamatok biztonságára is, ezek is megjelennek a végső értékelésben.

3. AZ ELEKTRONIKUS ALÁÍRÁS FEJLŐDÉSTÖRTÉNETE

3.1. A DOKUMENTUMHITELESÍTÉS PROBLÉMAKÖRE

Hitelességre minden korszakban szükség volt, és – nem meglepő módon – minden írásos korszakban fel is merülhetett az iratok hamisításának igénye, ezzel együtt a hamisított iratok felismerésének, azaz a hitelesség biztosításának követelménye is. Az írásbeliség kialakulása azonban korábbra tehető, mint a hozzákapcsolódó törvényi szabályozás kialakulása, az intézményesülés követte a királyok adományainak írásos rögzítésének igényét. A gyakorlatban a szokásjog, a valamelyest kialakult gyakorlat lett később a törvények által szabályozva.

Kálmán király 1110-ben elrendelte a pecsét használatát a közéletben, ami megalapozta a közhitelesség írásbeli formáját, és maga után vonta az intézményi keretek – a hiteles helyek – kialakulását és fejlődését. Ekkorra már szokássá vált bizonyos iratok (végrendeletek, ajándékozások, adásvételi szerződések) írásba foglalása, azonban az írástudók ebben a korban szinte kizárólag papi személyek voltak. Erre példa Arha veszprémi jobbágy végrendelete 1114 körül, melyet a győri kanonok szerkesztett tanúk és a királyi bíró jelenlétében. Az egymással háborúskodó birtokosok a királyi adományleveleiket gyakran papi személyek őrizetére bízták és szükség esetén hiteles másolatokat készíttettek róluk.

Bogdán István [76] a következő módon idézte III. Béla király 1181-ben kiállított birtokeladási oklevelének bevezető passzusát: „Én, Béla, Magyarország nagyságos királya, megfontolván és királyi méltóságunkat a jövendőre megőrizni akarván, nehogy bármely a mi jelenlétünkben megtárgyalt és eldöntött dolog felforgattattassék, szükségesnek láttam elrendelni, hogy a mi felséges kihallgatásunkon megtárgyalt minden ügy írott bizonysággal megerősítessék.”[87] III. Béla idejében az írástudás oktatása és a római jog felé fordulás megerősödött, a tudomány és művészetek művelése iránti igény külföldről begyűrűző hatásának következtében, és ez vezetett a gyakorlat élet megváltozásához is.

[87] Lásd „8. Írott bizonyság...” fejezet első bekezdése.

A hiteleshelyekről alkotott első törvénynek II. Endre 1231. évi XXI. törvénycikkét tekinthetjük, amelyik kimondta, hogy csak a hiteleshelyek tanúsága alapján lehessen bárkit is perbe hívni[88], a megszaporodó hamis idézések visszaszorítása érdekében. Ezt a rendelkezést meg kellett erősítenie a jogbiztonság fenntarthatósága érdekében 1291-ben[89], majd részletszabályok – napidíjak, oklevelekért járó díjak – követték ezt 1298-ban[90]. Falus Orsolya értekezésében [77] megvizsgálta a hiteleshelyek által kiállított iratok hitelességét biztosító eljárásokat, és azt találta, hogy az általánosan használt pecsét mellett más eljárásokat is alkalmaztak az iratok eredetiségének védelmében. Ilyen eljárás volt a jogügylet tanúinak felsorolása az oklevélben, vagy ha ugyanazt a szöveget egyetlen hártyára – többnyire egymás alá – kétszer vagy háromszor leírták, majd közéjük a szabadon hagyott helyre kalligrafikus jeleket írtak, majd ezeken át lehetőleg nem egyenes vonalban több darabra vágták a hártyát. Az irat akkor volt hitelesnek tekinthető, ha a darabok és a jelek összeillettek és minden egyes darabon ugyanaz a szöveg volt található.

A hiteleshelyek gyakran megőrzési (archiválási) szerepet is betöltöttek az egyik példány tárolásával és védelmével, ezt a tevékenységét később kiterjesztette más kiállítók okleveleire is. Az 1200-as évek elejétől pecsételést is alkalmaztak, amivel már háromféle hitelesítési eszköz is rendelkezésre állt az okirat jogosságának biztosítására: két vagy több tanú aláírása a kiállító mellett, kézírásos elemek elhelyezése és szétvágása (chirographum), illetve a pecsét[91]. A szétválasztási célú chirographumot a pecsét a későbbiekben kiszorította. Használták ugyan a XV. századi okleveleken is, azonban a XIII. század közepétől a díszítő szerepe erősebb, mint a hitelesítő szerepe.

---

[88] 1231. évi XXI. törvénycikk a poroszlókról és az egyházak hiteleshelyi működéséről (https://net.jogtar.hu/ezer-ev-torveny?docid=23100021.TV&searchUrl=/, 2019. március 5.).
a) És mivel az országban sokan szenvednek sérelmet a hamis poroszlók miatt, ezek idézései vagy tanúbizonyságai ne legyenek érvényesek, csak a megyés püspök vagy a káptalan tanúbizonysága által (támogatva);
b) s a meggyanúsított poroszló is csak ezek tanúbizonysága által tisztázhassa magát;
c) kisebb ügyekben pedig a szomszédos konventek vagy kolostorok tanúbizonysága legyen érvényes.

[89] 1291. évi V. törvénycikk a megyei ispánok bíráskodásáról (https://net.jogtar.hu/ezer-ev-torveny?docid=29100005.TV&searchUrl=/, 2019. március 5.)
Úgyszintén a megyei ispánok vagy alispánok jelenléte elé senkit se lehessen a káptalanok vagy konventek tanúbizonysága nélkül idézni, s a (megyei) ispán ne merészeljen ítéletet hozni vagy bíráskodni a négy választott nemes nélkül.

[90] Lásd 1298. évi LXXV. törvénycikk a hiteleshelyi kiküldöttek napidíja peres ügyekben, 1298. évi LXXVII. törvénycikk a királyi kancellária díjainak szabályozása: mennyi jár az ünnepélyes oklevelekért, 1298. évi LXXVI. törvénycikk az erről szóló oklevelek díja, illetve 1298. évi LXXIX. törvénycikk mennyi jár a kisebbekért

[91] A módszereket összefoglalja például a Nottinghami Egyetem weboldala is, korabeli példákkal. (https://www.nottingham.ac.uk/manuscriptsandspecialcollections/researchguidance/medievaldocuments/authentication.aspx, 2019. február 11.)

Nem nehéz felfedezni a hasonlóságot a chirographum átvágása-összeillesztése és a számadórovás között, amelyről Réthy Lászlót [79] idézi Tubay [78], aki szerint az erdélyi pásztorok, favágók, tutajosok és napszámosok a rovás-féle írással és két egymásba illesztett pálcára írt jegyekkel egész számadásokat voltak képesek nagy pontossággal végrehajtani. Ezt a formát is írásbelinek tekinthetjük, habár kétségkívül nem lesz még elektronikus.

Történetileg a közjegyzőség első fellépésének tekinthető esemény Róbert Károly királyhoz kapcsolódik, akit 1308. november 27-én az országgyűlés királlyá koronázott és erről – Érdújhelyi megállapítása szerint egy közjogi botlással – Gentilis pápai követ, Pontecurvo János és Sanguineto Vilmos apostoli és császári közjegyzők készítettek hiteles okiratot, amelyet a jelenlévő főpapok és főnemesek pecsétjeikkel megerősítettek ([201]: 105). A közhitelesség már a szóban között szerződéseknél is megjelent igényként, kezdetben a pristáldok (pristaldusok jelenlévők) tanúsították ezek hitelességét a XIII. század végéig. 1231-től 1874-ig a hiteleshelyek voltak a hiteles okiratok kiállításával megbízva, azonban a XII. századtól tartó létezésük eddigre elavulttá vált, helyüket ekkor vette át a közjegyzőség intézménye az 1874. évi XXXV. törvénycikk életbe lépésével[92].

A középkorban számos okirathamisítási eset látott napvilágot, amelyeknek két ismertetőjele volt, egyrészről a legfontosabb motiváció a jogtalan haszonszerzés, másrészről az elkövetők többnyire papi személyek voltak. A büntetési tételek a hűtlenség, a teljes vagyonelkobzás, tüzes vassal történő megbélyegzés, esetleg fejvesztés voltak, a hamisítók ennek ellenére számos dokumentált esetben próbálkoztak a hamisítással. Habár II: Endre 1298-ban elrendelte a periratok levéltári elhelyezését is[93], ennek ellenére viszonylag kevés ilyen tárgyú irat maradt fenn az utókor számára. Ezek közül az alábbi felsorolás mutat be néhány esetet:

- 1259-ben Pál Borics bán fia hamisított királyi okleveleket használt fel Fülöp zágrábi püspök elleni birtokperében

[92] Lásd 1874. évi XXXV. törvénycikk a királyi közjegyzőkről (https://net.jogtar.hu/ezer-ev-torveny?docid=87400035.TV&searchUrl=/, 2019. március 5.)
[93] Lásd 1298. évi XLVII. törvénycikk a bűnpereket a rendes bíráknak az illetékes megye levéltárában kell elhelyezniök
A bűnügyekben a királyi kúriában a nádor úr, vagy az országbíró, vagy más rendes bíró által ítélendő perek iratait a mondott tizenkét esküdt nemes előtt az alispán székén le kell tenni.
(https://net.jogtar.hu/ezer-ev-torveny?docid=29800047.TV&searchUrl=/, 2019. március 5.)

- 1268-ban Beriszláv Julcsok és társait ítélték el, mert hamis iratokkal akarták megszerezni egy várjobbágy földjét,
- 1296-ban Gógán zágrábi őrkanonok az általa őrzött káptalani pecsétet hamis oklevelek készítésére használta fel,
- 1391-ben Bodrogasszonyzakai Chuchkách István papot hamis pecsétek és oklevelek készítése miatt elítélik (távollétében, és megölését bárki számára engedélyezik),
- 1436-ban a Matucsinai család veszítette el birtokait hamis oklevelek gyártása miatt,
- 1448-ban Zömlényi Gábort hamisítás miatt halálra ítélték,
- 1450-ben Hunyadi János Hercegh Ráfael elleni perében Gábor deákot hamisításon kapják,
- 1467-ben az egri káptalantól vették el a hiteles pecsétjét hamisítás miatt.

A korabeli hamisítások feltárásához számos támpont állt a vizsgálók rendelkezésére. Megvizsgálták az oklevelek külsejét, az alkalmazott betűk típusát, az oklevelek hártyáit, az időrendiséget – anakronizmust keresve, az alkalmazott nyelvezet és stílus az előbbiekkel együtt szintén alkalmas volt a hamisítások kiszűrésére.

A papíralapú világ korabeli hamisításai a jogosulatlan használaton vagy hamis tanúsításon alapultak, az utólagos hamisítások előtt számos akadály tornyosul, például a korabeli papír megszerzése, festékanyag, bélyegző, toll, esetleg írógép vagy nyomdagép megszerzése és működtetése mind akadálya lehet egy megtévesztő hamisítvány elkészítésének. A digitális világ eredet- és tartalomhamisításai ellen a digitális aláírás és az időbélyegzés nyújtja a legnagyobb védelmet, habár ma már a korabeli adathordozók használata is meglehetősen problémás lehet (pl. CD, DVD, merevlemez, szalagok, lyukkártyák). A maradandó értékű iratok hamisításának megakadályozására vagy felismerésére tehát számos technológiai módszer létezik ma már. A valódiság felismerése azonban a technológián túl a kapcsolódó egyéb adatok elemzését is szükségessé teheti (pl. adott iktatószámon megjelenő irat tartalma, kapcsolódó előkészítő iratok tartalma, fellelhető példányok konzisztenciája).

3.2. AZ ELEKTRONIKUS ALÁÍRÁS FOGALMÁNAK KIALAKULÁSA

Ha megvizsgáljuk az elektronikus aláírás tudományos szakirodalmát, azt találjuk, hogy számos publikáció foglalkozik az elektronikus aláírás valamely aspektusával (leggyakrabban a jogi és a biztonsági-kriptográfiai vetületek kerülnek előtérbe), de olyan rendszerező összefoglalásra, amely a technológiai és a társadalmi kereteket integrálta volna, nem igazán találhatunk példát. Leginkább Jos Dumortier és munkatársai által 2003-ban elkészített kutatási anyagot (Leuven-jelentés) lehetne megemlíteni átfogó elemzésként, azonban a fókusz a közös piaci hasznosíthatóság és a problémák beazonosítása volt, mivel a munka az Európai Bizottság számára készült [92]. A ScienceDirect keresőjében a 2018. december 17-én lefuttatott keresés az „electronic signature” kulcsszóra 1959 darab cikket adott eredményül az alábbi éves bontásban:

Év	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Cikkek száma	21	39	25	41	85	112	96	99	68	81	78	68	88
Év	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Cikkek száma	92	72	62	75	71	116	112	108	104	103	124	19	?

2. táblázat: Elektronikus aláírás témájú cikkek a ScienceDirect keresőben 2018. december 17-én (forrás: saját táblázat)

A Springer kiadó 2004 és 2013 között minden évben közzétette az EuroPKI konferencián elhangzott előadások anyagát – 186 cikk, amelyek szintén széleskörű támpontot nyújtanak a területet vizsgálni kívánok számára[94]. A cikkek között számos esettanulmány és új felvetés is található. Érdemes megemlíteni például De Cock D. et. al. cikkét a belga EID kártyáról [80], Lopez et. al. cikkét [81] a tanúsítványok osztályozásáról – amely négy általam is használt dimenziót említ, Ølnes és Buene cikkét [82] a Validációs Hatóságról, mint hatékony kockázatcsökkentő eszközről, a Zeng [83] által kidolgozott univerzálisnak szánt álneves PKI rendszerről szóló felvetést, Pala és Smith cikkét [84] az AutoPKI-ről, ami egy automatizált verifikációs protokollt definiált a tanúsítványokhoz, Montana és Reynolds írását az internetes hálózatok forgalomirányítását a lehetséges útvonalak validálásával biztonságosan megvalósító RPKI-ról [85], Dent cikkét a tanúsítvány nélküli aszimmetrikus titkosításról [86], továbbá

[94] Lásd https://link.springer.com/conference/europki (2019. február 11.)

Pala et. al. írt először a PorPKI-ról (proxy tanúsítványok által hordozhatóvá tett – portable – PKI) [87], Van Damme et. al. új típusú leírása a PKI-alapú mobilbankolásról [88] szintén érdekes lehetőségeket feszegetett, Vigil et. al. gondolatai a közjegyző által aláírt, hosszú távon hiteles, érvényességi idő nélküli tanúsítvány-alapú PKI-ról [89] újszerűek, Kim et. al. felvetése a földrajzi elhelyezkedést is tanúsító GeoPKI-ról [90] vagy akár Werlang et. al. cikke [91] a felhasználó-központú digitális aláírási sémáról további potenciális dimenzionális elemekre is ráirányította a figyelmemet.

Az elektronikus aláírás fogalmának tárgyalásakor természetesen nem lehet elkerülni a kriptográfiai kitekintést, hiszen az elektronikus aláírások jelentős része alkalmaz valamilyen kriptográfiai megoldást – ahogyan a digitális aláírás NIST által[95], ISO által[96] és az ETSI által szabványosított definíciója[97] is mutatja, de nem lehetséges a tisztán matematikai-műszaki megfontolásokra sem szorítkozni, a technológia intézményesülésének számos kérdése megmutatta ennek relevanciáját is. A technológiának a jogrendszerbe illesztésekor olyan kérdések is napirendre kerültek, amelyek túlmutatnak az elektronikus aláírás technológiáján, például az e-kereskedelem [18], a jogi vélelem [19], valamint az elektronikus írásbeliség [2] kérdéseit lehet itt említeni. A nem koordinált használat számos különböző implementációt eredményezett, ami szintén nem az általános elterjedés irányába ható tényezőként hatott a múltban. Mindezek következtében be kellett avatkozni az elektronikus aláírás fogalmi rendszerébe. Az elektronikus aláírás evolúciója ebből következően értelmezhető fogalom, erre bizonyíték, hogy már 2000-ben is globális koordinációs – és nem technológiai – problémaként tartotta számon Coglianese az együttműködés hiányát az elektronikus aláírások széles körű elfogadásában [17]. Az Európai Unió az elektronikus aláírási irányelv végrehajtását folyamatosan értékelni kívánta, az értékelés kötelmét bele is foglalta a jogi szövegbe[98] és ennek eredményeként az 1999. decemberében megjelent elektronikus aláírási irányelv tapasztalatait 2014-ben a Rendeletben korrigálták.

[95] Lásd NIST FIPS PUB 186-4, 2.1 Digital signature: The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation.
[96] Lásd ISO 7498-2:1989(en), 3.3.26: digital signature: Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.
[97] Lásd ETSI EN 319 411-1, 3.1 Definitions: *digital signature:* data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient
[98] Lásd az Európai Parlament és a Tanács 1999/93/EK irányelve (1999. december 13.), 12. cikkét és a Rendelet 49. cikkét.

Az elektronikus levelezés hitelességének a problémáját Bob Thomas a BBN Inc. munkatársa már 1974 júliusában az RFC 644 dokumentumban megfogalmazta: hogyan lehet egy hálózati levél fogadója bizonyos abban, hogy a levél valóban attól a küldőtől jött, aki a levében szerepel (állított küldő)? A probléma akkori elméleti és gyakorlati jelentőségének érzékeltetéséhez idézném az internetes csomópontok számát 1981-1991 között rögzítő RFC 1296[99] dokumentum által megadott adatot, amely szerint 1981 augusztusában az egész interneten összesen 243 csomópont volt, azaz 12 év alatt keletkezett legfeljebb 239 új internetes csomópont. A BBN Inc. megjelenése a probléma megfogalmazásában nem véletlen, mivel az 1960-as évek végén a Bolt, Beranek és Newman (BBN) nyerte meg az internet megépítésére kiírt pályázatot. A hálózat felépítésének és tesztelésének tervét az RFC 4[100] írja le. Az eredmény az USA három kaliforniai és egy utahi egyetemén üzembe helyezett távolsági kommunikációs hálózat, amelyen 1969. október 29-én jelent meg az első éles üzenet, egy távoli bejelentkezési kísérlet (LO)[101]. 1973. június 1-én publikálták az első levelezési protokoll-javaslatot RFC 524 névvel[102], amit 1973. szeptember 5-én követett a levélfejléc szabványosítása (RFC 561[103]). A kommunikációs protokoll karakteres átvitelt valósított meg telefonvonalakon, az autentikációt a felhasználói név és jelszó párok alkalmazása jelentette ekkor. A fentiek alapján megállapíthatjuk, hogy a hitelesség problémája már az internet elindulását követő öt éven belül markánsan jelentkezett.

A kézírással egyenértékű digitális aláírás fogalmának legelső felbukkanásakor a kézi aláírást szerették volna kiváltani a szerződő felek között és a számlázásban, egy számítógépes hitelesítési probléma megoldásának eredményeként. Szemléletes, és pontosan beleillik Wiebe E. Bijker [16] elmélete változási és stabilitási követelményének szükségességébe az, ahogyan a körvonalazódó és egyre inkább felmerülő igényt Diffie

[99] Mark K. Lottor (SRI International): Internet Growth (1981-1991), Request for Coments: 1296, January 1992. (https://tools.ietf.org/html/rfc1296, 2019 február 12.)
[100] Elmer B. Shapiro (Stanford Research Institute): Network Timetable. Request for Comments: 4, 24 March 1969. (https://tools.ietf.org/html/rfc4, 2019. február 22.)
[101] Az ARPANET születésének és első eseményeinek részleteit a Live Science foglalja kronologikus sorrendben össze (https://www.livescience.com/20727-internet-history.html, 2019. február 12.). A BBN fejlesztette ki a mai routerek elődjét, az Interface Message Processort (IMP) és az első elektronikus levelek formátum-specifikációjának a kidolgozásában is részt vett.
[102] Jim White (SRI-ARC): A Proposed Mail Protocol, Request for Comments: 524, 13 June 1973. (https://tools.ietf.org/html/rfc524, 2019. február 12.)
[103] Abhay Bhushan (MIT-DMCG), Ken Pogran (MIT-MULTICS), Ray Tomlinson (BBN-TENEX), Jim White (SRI-ARC): Standardizing Network Mail Headers, RFC 561, 5 September 1973. (https://tools.ietf.org/html/rfc561, 2019. február 12.)

Whitfield és Martin Hellman 1976-ban megfogalmazták korszakalkotó cikkükben aszimmetrikus kriptográfiai alapokat feltételezve ([20]: 649):

„Current electronic authentication systems cannot meet the need for a purely digital, unforgeable, message dependent signature."

Vagyis az akkori elektronikus hitelesítési rendszerek nem feleltek meg a tisztán digitális, hamisíthatatlan, az üzenettől függő aláírás létrehozási igényének, amelyeket a digitális világban a papíralapú aláírások helyett lehetett volna alkalmazni, és ami nélkül az üzleti folyamatokat nem látták működőképesnek. A hitelesség (authenticity), mint igény a magyar polgári eljárásjogban is megjelenik, Kemény Miklós az okirati bizonyítás tárgykörében szintén megfogalmazza az okirat valódiságának a szükségességét. Hamis okiratnak nevezi azt, amelyet nem a feltüntetett kiállítója írt alá, továbbá hamisított okiratnak nevezi azt, amelyek ugyan a kiállítója írt alá, de időközben a tartalma megváltozott [21]. Ez a dichotómia az információbiztonság témakörében is megjelenik.

Auguste Kerckhoffs 1883-ban [22] hat követelményt fogalmazott meg a kriptográfiai rendszerek számára, aminek a hatása a későbbi korok kriptográfusaira elvitathatatlan volt. A második követelményét Kerckhoffs-elvnek is szokták nevezni, ami kimondja, hogy egy kriptográfiai rendszer nem követelheti meg a titokban maradását feltételként, és hogy a rendszer minden nehézség nélkül az ellenség kezébe kerülhet. Kerckhoffs harmadik követelménye szerint a kulcsnak könnyen megjegyezhetőnek kell lennie, de ne igényeljen feljegyzést, illetőleg a szereplők a kulcsokat tetszés szerint tudják lecserélni vagy megváltoztatni. Claude Elwood Shannon (1949) már 1946-ban kidolgozta a titkosítási rendszerek értékelési követelményeit [23], amit azonban nem hozhatott nyilvánosságra, csak a későbbiek folyamán oldották fel az anyag titkosítását. Ebben az öt legfontosabb követelmény között felsorolta a kulcs hosszát is. Véleménye szerint a jó kriptográfiai rendszerek egyik ismérve az, hogy a lehető legrövidebb kulcsokat alkalmazzák benne. Egy rövid és fejben tartható kulcs igen előnyös lehet tehát egy kriptográfia rendszer használhatósági értékelésében.

A digitális aláírás elvének Diffie és Hellman által történő lefektetését [20] követően három matematikus elkezdett dolgozni az addig csak elméletileg lehetséges problémán, és 1977 áprilisában megírtak egy kutatási jelentést [97] – amely akkor nem volt nyilvános a várható szabadalmaztatási eljárás miatt, de a szerzők terjesztésében – válaszborítékért cserébe – korlátozott módon hozzá lehetett férni. A módszer megjelent a

Scientific American 1977 augusztusi számában [95] matematikai játékként részletes leírás nélkül, egy játékos kódfejtésre invitálva az olvasót[104]. Az algoritmus szabadalmát 1977. december 14-én nyújtották be és 1983. szeptember 20-án adták ki, ez volt annak az oka, hogy a szabadalom 2000. szeptemberében járt le[105], onnantól kezdve bárki az egész világon szabadon felhasználhatta az algoritmust (US Patent 4,405,829[106]). 1978-ban – jelent meg az első, gyakorlatban is használható nyilvános kulcsú kriptográfiai algoritmus leírása [24], a szerzők nevének kezdőbetűiből (Rivest, Shamir, Adleman) elnevezve ezt az algoritmust RSA néven ismerte meg a világ. A leírás kiegészítette a digitális aláírás követelményeit az üzenetfüggőség mellett az aláírófüggőséggel is, ellenkező esetben az aláírásokat nem lehetne aláíró entitáshoz kötni. Ha a digitális aláírás elkészítéséhez szükséges titkos kulcs létrehozását és birtoklását nem kötjük senkihez, akkor az aláírás létrehozható, de nem adhat információt az aláíró kilétéről. A dokumentum hitelessége is megkérdőjelezhető, ha tetszőleges titkos kulcsot fel lehet használni az aláírás készítéséhez, hiszen így az aláírás következmények nélkül lecserélhetővé válik. Ha az aláírás viszont csak és kizárólag az aláírótól függene és az üzenethez nem lenne köze, akkor az a helyzet állna elő, hogy csak egyetlen egy aláírást (kódot) lehetne használni a különböző dokumentumok aláírásához, és egy digitális állomány másolatait megkülönböztetni egymástól és a legelső állománytól nem lehetséges a példányok tökéletes egyezősége miatt. Erre a problémára Shamir [133] ötvözte az aláíró azonosítását a nyilvános kulcsú kriptográfiával a CRYPT0'84 konferencián tartott előadásában. A gyakorlatban ezt az elvet mind a mai napig használják, ha nem is teljesen az itt leírt formájában.

Az RSA-publikáció leírta az algoritmus matematikai működését, definiált egy számítási eljárást és biztonsági megfontolásokat is megfogalmazott az új algoritmushoz. A kriptoanalízissel (cryptanalysis) foglalkozók széles tábora próbált az algoritmusban gyengeséget találni, tekintettel arra, hogy az algoritmus elméleti biztonságát nem sikerült bebizonyítani. A próbálkozások első 20 évét Dan Boneh foglalta össze 1999-ben [25]. Már itt szétváltak az RSA matematikai hátterére és az implementációra vonatkozó támadási formák. A következő 10 évre – valójában összesen 33 évre – pedig Jingjing

[104] Ezt a feladatot tizenhét év múlva sikerült megoldani, 1994. április 26-án hatszáz önkéntesből álló csoport határozta meg a feladvány prímtényezős alakját. Lásd [96] 329. old.
[105] Az 1975 előtt benyújtott szabadalmak védettségi időtartama 20 év volt a benyújtástól vagy 17 év a publikálástól, a kettő közül a hosszabb volt érvényes.
[106] A szabadalom teljes szövege elérhető itt: http://www.freepatentsonline.com/4405829.pdf (2019. január 30.)

Wang [26] 2011-ben megismételte a Boneh által megtalált támadási módszereket, egyetlen egy új módszert hozzátéve az addig felfedezettekhez, ami azonban döntő fontosságúnak bizonyult 2017-ben az észt állampolgári tanúsítványok kompromittálódásában. Az RSA algoritmus gyakorlati felhasználása az első 10-15 évben vontatottan haladt, a 90-es évek elejére azonban tömeges méretekben hozzáférhetővé vált a piacon [27] és a civil szektorban is (RFC 1991) – ez utóbbiról egy 2014-ben a titkosítás alól feloldott amerikai dokumentum, ami vélhetően az ezredforduló előtt készült [28], lábjegyzetben annyit jegyez meg, hogy a Pretty Good Privacy (PGP) programcsomag ***még mindig*** (kiemelés tőlem) hozzáférhető a Massachusetts Institue of Technology (MIT) weboldalán[107]. Az információs sztráda tengerentúli fejlődésének két ösztönző tényezőjét (Rózsa 1997 [29]) a hidegháború végében és a termelékenység fokozásának eredményeként felfejlődő, a GDP 50%-át meghaladó szolgáltatási szektorban látta, amiből következhet, hogy az elektronikus szolgáltatások fejlődése szintén ennek lehetett a következménye. Az Egyesült Államokban az aláírás útja 1994-ben a szabványosításba (DSS 1994 [58]), 1994. december 21-én Utah államban az első elektronikus aláírási helyi törvénybe[108], majd az elektronikus aláírási törvénybe (Electronic Signatures in Global and National Commerce Act 2000[109]) torkollott.

Európában Martin Bangemann a munkacsoportjával 1994-ben lefektette az Európai Információs Társadalom alapelveit a Bangemann Report[110] néven ismertté vált dokumentumban, amelynek „Electronic protection (encryption), legal protection and security", azaz az elektronikus védelem (titkosítás), jogi védelem és biztonság fejezete foglalkozott az elektronikus biztonság kialakításával [30]. A nyilvános kulcsú infrastruktúra ismert volt a csoport előtt, ez teljes bizonyossággal állítható, hiszen az akkori európai infokommunikációs (ICT) cégek döntéshozói jelentős számban vettek részt ebben a munkában. Érdekességként megemlíthető, hogy Romano Prodi, aki 1999 és 2004 között az Európai Bizottság tizedik elnöke lett, szintén tagja volt ennek a munkacsoportnak. Mindezek ellenére a munkaanyagba a digitális aláírás technológiája

[107] Az anyag Phil Zimmermann és az RSA közötti indult szabadalmi vitára utalt, amelyet vádemelés nélkül lezártak. Sokat segített ebben, hogy a vitában az MIT Zimmermann mellé állt ([115]: 230) és megjelentette a PGP leírását egy 933 oldalas könyvben 1995-ben [134].
[108] Utah Digital Signature Act. Utah Code §§ 46-3-101 to 46-3-504. Enacted by L. 1995, ch. 61
[109] ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT. 106th Congress Public Law 229. https://www.govinfo.gov/content/pkg/PLAW-106publ229/html/PLAW-106publ229.htm (2019.01.24.)
[110] Europe and the global information society. Recommendations of the high-level group on the information society to the Corfu European Council http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf (2019.01.24.)

nevesítve mégsem került bele. Az ICT ipar képviselőinek döntő többségű bevonása valószínűleg jelentős hatást gyakorolt arra, hogy a változás motorját a jelentés az ICT iparban és az ICT piac szereplőiben látta. Felismerte a titkosítás egyre növekvő szerepét a fizetési szolgáltatásokban (pay services) és fontosságát az elektronikus kereskedelemben (telecommerce). Ez utóbbiban szükségesnek ítélte meg abszolút garanciák létezését az aláírások és aláírt szövegek sértetlensége, visszavonhatatlan idő- és dátumbélyegzők, illetve a nemzetközi jogi elfogadhatóság területén. Ezekben a garanciákban már fellelhető a digitális aláírások tulajdonságainak követelmény-szintű absztrahálása.

Az európai közösségben használható elektronikus aláírásról szóló gondolkodás ezt követően indult el egy olyan szakértői csoport által, akik kidolgozták az új európai szabályozás jogi hátterét és elkezdtek dolgozni a szabványosítási háttéren is. A szabványosítási munka első körét 2003-ban fejezték be, ennek eredményeként jöttek létre az első európai elektronikus aláírással kapcsolatos elektronikus aláírási[111] és technikai[112] szabványok.

1998. június 6-án az Európai Bizottság hivatalosan is elküldte az Európai Parlamentnek és Tanácsnak az elektronikus aláírás közösségi keretrendszeréről szóló javaslatát (COM(1998) 297 final [31]), amelyet 1999. decemberében ki is hirdettek (EU irányelv). Ezt követően viszonylag gyorsan minden tagállam kidolgozta a saját elektronikus aláírással kapcsolatos nemzeti szabályozását, ami Magyarországon a 2001. évi XXXV. törvény (Eat.) és végrehajtási rendeletei által lett szabályozva.

Az irányelvben a működés felügyelete előírásként is megjelent, két év elteltével meg kellett vizsgálni az irányelvben lefektetettek működését. Ehhez a felügyeleti eljáráshoz már 2003-ban a felügyeleti hatóságok önkéntes és nem hivatalos szervezete (FESA: Forum of European Supervisory Authorities for Electronic Signatures) feltárt számos olyan pontot, ahol az irányelv módosítását látta szükségesnek, ami azóta több jelentésben tovább finomodott. 2010-ben az EU megállapította, hogy a digitális piac szétaprózottsága, az interoperabilitás hiánya és a számítógépes bűnözés terjedése jelenti

[111] Az ETSI az elektronikus aláírással kapcsolatos szabványait a következő weboldalon publikálja: http://www.etsi.org/deliver/etsi_es/
[112] Az ETSI a technológiai szabványai (köztük az elektronikus aláírással kapcsolatosak is) a következő weboldalon érhetők el: http://www.etsi.org/deliver/etsi_ts/

a digitális gazdaság önmagát működtető folyamatának legfőbb akadályát[113], amelyek meggátolják az uniós polgárokat abban, hogy kihasználják az egységes digitális piac és a határokon átnyúló digitális szolgáltatások nyújtotta előnyöket. Az irányelv az elektronikus aláírásra vonatkozott, és nem hozott létre átfogó, határokon átnyúló és ágazatközi uniós keretet az elektronikus tranzakciók biztonságának, megbízhatóságának és könnyű használhatóságának érdekében. Elindult tehát az irányelv és a vonatkozó szabványok átalakításának folyamata (M460 Mandate[114]) 2009. december 22-én. Az új szabályozás formája már nem irányelv, hanem az egész Európai Unió területén azonnal, külön nemzeti jogi aktus nélkül hatályosuló parlamenti és tanácsi rendelet lett, hogy az együttműködést még jobban elősegítse, kikényszerítse – vagy ahogy a rendelet záró pontja fogalmaz: „a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban”[115]. A szabályozás és az újragondolás eredménye öltött testet a 2012-es előkészítő javaslatban[116], majd a végleges eIDAS Rendeletben 2014-ben, amit Magyarország kiegészített az Eübszt. előírásaival 2015-ben, ezzel együtt az 1999/93-as irányelven alapuló Eat. 2017. július 1-én hatálytalanná is vált.

3.3. ÍRÁSBELISÉG A MAGYAR JOGBAN

A papíralapú világ dokumentumkezelési folyamatai az elmúlt 1 000 év alatt letisztultak, kialakultak és közismertté váltak a hitelesítési technikák, eljárások, és a jogalkotó is pontosan és világosan megfogalmazta az egyes dokumentumokra vonatkozó alaki kellékek teljesítésére vonatkozó elképzeléseit. Az elektronikus világ megjelenésével és elterjedésével egyre kevésbé látszott megfelelő megoldásnak az, hogy minden folyamat eleje papíralapú dokumentummal indul és minden folyamat vége papíralapú dokumentummal zárul, más szóval megjelent az igény az elektronikus írásbeliségre is. Három fogalom vált kiemelkedően fontossá az elektronikus világban: az egyik az

[113] Brüsszel, 2010.5.19. COM(2010)245 végleges, A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK. Az európai digitális menetrend

[114] EUROPEAN COMMISSION, ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL, Innovation policy ICT for Competitiveness and Innovation, Brussels, 22nd December 2009, M/460 EN, STANDARDISATION MANDATE TO THE EUROPEAN STANDARDISATION ORGANISATIONS CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES APPLIED TO ELECTRONIC SIGNATURES

[115] eIDAS Rendelet, 52. cikk: Hatálybalépés

[116] Az Európai Bizottság javaslata,(Brüsszel, 2012.6.4. COM(2012) 238 final 2012/0146 (COD)), AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és megbízható szolgáltatásokról

írásbeliség (written form), a másik a kézírással egyenértékű joghatással bíró elektronikus aláírás (handwritten signature), a harmadik pedig a teljes bizonyító erejű dokumentum (full probative force). A jogalkotóra várt az a feladat, hogy meghatározza az elektronikus írásbeliség megvalósítására alkalmas formákat, valamint rögzítse a kézírással egyenértékű elektronikus aláírás pontos, minden kétséget kizáróan teljesíthető tulajdonságait, továbbá meghatározza, hogy mely dokumentumokhoz fűződik teljes bizonyító erő s melyekhez nem.

Az 1999/93/EK Irányelv kimondta az 5. cikkében, amelyik az elektronikus aláírások joghatását definiálta, hogy:

„(1) A tagállamok biztosítják, hogy a minősített tanúsítványon alapuló és biztonságos aláírás-létrehozó eszközzel létrehozott, fokozott biztonságú elektronikus aláírások:

a) ugyanúgy megfeleljenek az elektronikus adathoz kapcsolódó aláírásra vonatkozó jogi követelményeknek, ahogy a saját kezű aláírás megfelel a papíron megjelenő adatokra vonatkozó ilyen követelményeknek; és

b) bírósági eljárásokban bizonyítékként elfogadhatók legyenek.

(2) A tagállamok biztosítják, hogy az elektronikus aláírás joghatását és bírósági eljárásokban bizonyítékként való elfogadhatóságát ne tagadják meg kizárólag amiatt, hogy:

- az aláírás elektronikus formában létezik, vagy

- nem minősített tanúsítványon alapul, vagy

- nem akkreditált hitelesítésszolgáltató által kibocsátott minősített tanúsítványon alapul, vagy

- nem biztonságos aláírás-létrehozó eszközzel hozták létre.”

Az erre a kérdésre adott választ tovább finomította az Európai Parlament és a Tanács COM/2012/0238 final - 2012/0146 (COD) rendeletére tett javaslata a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és

megbízható szolgáltatásokról[117]. A javaslat 6. szakaszának Elektronikus dokumentumokra vonatkozó 34. cikkében ez volt olvasható:

„Az elektronikus dokumentumok joghatása és elfogadása

(1) Az elektronikus dokumentumot a papíralapú dokumentummal egyenértékűnek és a bírósági eljárásokban bizonyítékként elfogadhatónak kell tekinteni, figyelembe véve hitelességének és sértetlenségének biztonsági szintjét."

Ebből következik, hogy nem minden elektronikus dokumentum lesz egyenértékű egy ugyanolyan tartalommal bíró papíralapú dokumentummal, mert a hitelesség és sértetlenség biztonsági szintje további osztályozásra ad lehetőséget. Felmerülhet tehát kérdésként, hogy a magyar jogrend tulajdonképpen milyen választ ad az elektronikus írásbeliségre, hol és hogyan van lehetőség joghatást kiváltó elektronikus dokumentumok létrehozására és felhasználására a magyar jogrend által támogatott módokon? A feltett kérdésnek a megválaszolásához először az „írásbeliség" fogalmát vizsgáljuk meg, ezután rövid elemzést készítünk az „írásban" kifejezés előfordulásairól a különböző jogszabályhelyek szövegeiben, majd kitekintünk az elektronikus aláírások típusaira és ezt követően megkíséreljük megfogalmazni a választ a fenti kérdésre.

Az írásbeliség kialakulására a polgárosodást követően volt szükség, amikor a városban a polgárok már nem tudtak az ismertségre támaszkodni, amikor egymással szemben valamilyen kötelezettséget akartak felvállalni. Komjáthy Miklós így fogalmazza ezt meg, kiindulva a Magyar Királyság első két évszázadából:

„Annak azonban, hogy az emberi viszonylatok alakításában az irásbeliségnek alig volt szerepe, a magyar társadalmi és gazdasági élet akkori fejlettsége is magyarázatául szolgál. Az emberek tulnyomó része ügyes-bajos dolgát el tudta intézni, az élete fenntartásához szükséges dolgokat be tudta szerezni egynapi járóföldön belül. Az emberek ismerték egymást, a függőben levő ügyekre vonatkozó nézeteiket szóban cserélték ki. Szavuknak hitelt nem irás, nem pecsét, hanem az őket ismerő emberek tanubizonysága adott.

Az igények növekedtével, amikor már a szomszéd megyébe, idegen országba, esetleg még távolabb is elmentek, ahol már senki sem ismerte őket, a természeti gazdálkodás apró társadalmi-gazdasági sejtjei falának áttörésével, az élőszó már nem

[117] Lásd https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0238:FIN

bizonyult elégnek, az ügyek intézése, az emberi együttélésből származó ügyek maradandó rögzítése más segédeszközt kivánt, az irást. Az uj technika, az ügyek intézésének uj módja csak lassan, akadozva tört utat magának.” ([1]: 151-152)

3.3.1. EAT. IDŐSZAK

Rátai Balázs – aki aktívan közreműködött az elektronikus aláírás hazai szabályozásában – leírja az Eat. kidolgozási folyamatának közepén [2] – az Irányelv három joghatás-típusát:

1. elfogadását nem lehet megtagadni elektronikus formája miatt,

2. amennyiben olyan fokozott biztonságú aláírás, amihez minősített tanúsítvány létezik, és biztonságos aláírás-létrehozó eszközzel készítették – magyar terminológiában ez a minősített elektronikus aláírás, akkor a kézírással egyenértékű joghatást kell számára biztosítani, valamint

3. a közszférán belüli aláírásokhoz olyan követelményeket fogalmazhatnak meg a tagállamok, amelyek objektívek, arányosak, és előre megismerhetők, valamint nem vezethetnek a piaci szereplők hátrányos megkülönböztetéséhez.

A 2016. évi CXXX. törvény a polgári perrendtartásról (továbbiakban: Pp.) 196. § a 2. vélelmet kiegészíti még egy aláírás-típussal. Ha az elektronikus okiraton kiállítója minősített elektronikus aláírást vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást helyezett el, akkor a magánokirat az ellenkező bebizonyításáig teljes bizonyítékul szolgál arra, hogy kiállítója az abban foglalt nyilatkozatot megtette, illetőleg elfogadta, vagy magára kötelezőnek ismerte el. A két aláírás-típus közötti lényeges különbség az, hogy az első aláírás készítéséhez szükséges biztonságos aláírás-létrehozó eszköz, míg a másodikhoz nem.

Az írásbeliség alaki formáira az 1960. évi 11. törvényerejű rendelet a Polgári Törvénykönyv hatálybalépéséről és végrehajtásáról (PTKÉ.) ad részletes útmutatást a szerződések vonatkozásában, amelyet érvényesnek lehetett tekinteni minden más dokumentum esetében is:

„38. § (1) Ha az okiratot több példányban állítják ki, a szerződés akkor is érvényes, ha mindegyik fél csak a másik félnek szánt példányt írja alá.

(2) Ha jogszabály a szerződés érvényességéhez írásbeli alakot rendel, jogszabály eltérő rendelkezése hiányában írásbeli alakban létrejött szerződésnek kell tekinteni a levélváltás, a táviratváltás, valamint a távgépírón és telefax útján történt üzenetváltás, továbbá a külön törvényben meghatározott maradandó eszközzel tett nyilatkozatváltás – így különösen fokozott biztonságú elektronikus aláírással aláírt okirat – útján létrejött megegyezést."

Az Eat. a törvény szintjén rendelkezett az elektronikusan aláírt dokumentumok viszonyáról az írásbeliséghez az elektronikusan aláírt elektronikus dokumentum, illetve az elektronikus aláírással kapcsolatos szolgáltatások jogkövetkezményei szakaszában:

„4. § (1) Ha jogszabály a 3. § (2)-(4) bekezdésében foglaltakon kívüli jogviszonyban[118] írásba foglalást ír elő, e követelménynek eleget tesz az elektronikusan aláírt elektronikus dokumentumba foglalás is, ha az elektronikusan aláírt elektronikus dokumentumot fokozott biztonságú elektronikus aláírással írják alá."

3.3.2. eIDAS IDŐSZAK

Az eIDAS legfontosabb vívmánya a kézírással egyenértékű minősített elektronikus alírás és a minősített elektronikus bélyegző egységes elfogadásának előírása az Európai Unióban:

1. eIDAS 25. cikk: Az elektronikus aláírás joghatása

(1) Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

(2) A minősített elektronikus aláírás a saját kezű aláírással azonos joghatású.

118 A Polgári Törvénykönyvről szóló 1959. évi IV. törvény (Ptk.) 598-684. §-ában szereplő, illetve a házasságról, a családról és a gyámságról szóló 1952. évi IV. törvény szerinti jogviszonyokban nem lehet az elektronikus formán kívüli dokumentumokat mellőzve, csak elektronikus aláírást felhasználni, illetve elektronikusan aláírt elektronikus dokumentumot készíteni. A bírósági eljárások különböző típusaiban - a bizonyítási eszközkénti felhasználáson túlmenően - eljárási cselekményeket akkor lehet az elektronikus formán kívüli dokumentumokat mellőzve, csak elektronikusan aláírt elektronikus dokumentum, illetve elektronikus aláírás használatával foganatosítani, ha ezt az eljárástípusra vonatkozó jogszabály kifejezetten lehetővé teszi.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus aláírást az összes többi tagállamban el kell ismerni minősített elektronikus aláírásként.

2. eIDAS 35. cikk: Az elektronikus bélyegző joghatása

(1) Az elektronikus bélyegző joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formában létezik, illetve nem felel meg a minősített elektronikus bélyegzőkre vonatkozó követelményeknek.

(2) A minősített elektronikus bélyegzők esetében vélelmezni kell a hozzájuk kapcsolódó adatok sértetlenségét és a bélyegzőnek megfelelő eredetét.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus bélyegzőt valamennyi tagállamban el kell ismerni minősített elektronikus bélyegzőként.

A kézírással történő aláírás az írásbeliség alaki kelléke. Az Alaptörvény az írásbeliséget, mint alaki kelléket, két esetben nevesíti:

1. 21. cikk: (1) Az országgyűlési képviselők egyötöde a miniszterelnökkel szemben írásban - a miniszterelnöki tisztségre javasolt személy megjelölésével – bizalmatlansági indítványt nyújthat be.

2. XXV. cikk: Mindenkinek joga van ahhoz, hogy egyedül vagy másokkal együtt, írásban kérelemmel, panasszal vagy javaslattal forduljon bármely közhatalmat gyakorló szervhez.

Mindez megtehető az eIDAS szerint elektronikus aláírással is, feltéve, hogy az országgyűlési képviselők vagy a közhatalmat gyakorló szervek képesek fogadni az ilyen típusú aláírással ellátott dokumentumokat. Az eEurope 2020 erre is fel kívánja készíteni Európát, az alapvető közszolgáltatások legmagasabb, proaktív szintű és határon átnyúló működésének támogatásával.

Ha a jogszabályi hierarchiában az Alaptörvény szintje alá tekintünk be, közel ötezer helyen szerepel az alsóbb szintű jogszabályainkban az „írásban” kifejezés, ahol – ha feltételezhetjük az aláírás meglétét az írásbeli formák esetében – az eIDAS általános

érvényű elfogadási kötelezettsége alapján minősített elektronikus aláírást biztosan lehetséges használni a folyamatok felkészültségi szintjétől függően.

3.4. MAGYAR KRONOLÓGIA

A magyar jogalkotás és szolgáltatói piac fejlődésének jelentősebb lépcsőfokait érdemes feleleveníteni annak érdekében, hogy a Kormányzati Hitelesítés Szolgáltató 2013. év végén történt elindulását megelőző erőfeszítésekről és előzetes tevékenységekről megfelelő képet lehessen alkotni. A felsorolás a teljesség igénye nélkül készült azzal a céllal, hogy au EU irányelv és az eIDAS rendelet közötti időintervallum elektronikus aláírással kapcsolatos főbb eseményeinek kronologikus sorrendjéből a történések evolúciós ívét valamelyest specifikálja.

- 1997. megjelent egy kormányhatározat tervezet az elektronikus aláírás kormányzati bevezetéséről, de a végrehajtás kormányváltás miatt akkor megakadt
- 1999. június 14-én megalakult a Közlekedési, Hírközlési és Vízügyi Minisztérium (KHVM) elektronikus aláírás munkacsoportja[119]
- 1999. a NetLock Kft. elindítja nem minősített hitelesítés-szolgáltatását, elsőként Magyarországon, Rózsahegyi Zsolt vezetésével
- 2000. augusztus 29-én elfogadták az 1075/2000. (IX.13.) Korm. határozatot az elektronikus aláírásról szóló törvény szabályozási alapelveiről és az ezzel kapcsolatban szükséges intézkedésekről
- 2001. májusában megjelent az elektronikus aláírásról szóló 2001. évi XXXV törvény, itt még csak három szolgáltatással, amelyek rendben az elektronikus aláírás hitelesítés-szolgáltatás, időbélyegzés és aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése voltak.
- 2001. az APEH KAIG[120] (mai nevén NAV) megkezdte a tízezer kiemelt adózó számára az aláíró eszközök és tanúsítványok kibocsátását, csak adóbevallási célzattal

[119] A minisztériumot 1998 júliusától 2000 májusának végéig Katona Kálmán vezette, aki 1995 és 1998 között a Hírközlési Főfelügyelet elnökhelyettesi pozícióját is betöltötte. 1994 és 1998 között a Közlekedési, Hírközlési és Vízügyi Minisztérium politikai államtitkára Kovács Kálmán volt, aki 2002-2006 között informatikai és hírközlési miniszter volt.

[120] KAIG: Kiemelt Adózók Igazgatósága, 1996-ban alakult meg a legnagyobb adózókra specializálódott szervezeti egység, hogy a közvetlenebb kapcsolatnak köszönhetően koncentráltan legyen biztosítható az

– később a jogszabály úgy rendelkezik, hogy a szolgáltatást az első minősített szolgáltató piacra lépésétől számított 60 napon belül be kell fejezni, amit nem tett meg időben

- 2001. a Hírközlési Felügyelet (mai nevén Nemzeti Média- és Hírközlési Hatóság) 2001. október 27-én vette nyilvántartásba a NetLock nem minősített szolgáltatásait (NHH regisztrációs szám: FA 6133-5/2001)

- 2001. december 21-én a Matáv (mai nevén Magyar Telekom) szintén elindította a nem minősített szolgáltatásait, a Deutsche Telekomra építve

- 2001. december 23-án a GIRO Elszámolásforgalmi Zrt. megindította nem minősített hitelesítés-szolgáltatásait tanúsítvány és eszköz kibocsátására – ezek az Eat. szerinti első és harmadik szolgáltatások voltak (NHH regisztrációs szám: FA 7717-1/2001)

- 2002. április 26-án megjelent a 2/2002 MeHVM irányelv a minősített szolgáltatókra és a biztonsági követelményekre vonatkozó követelményekről, ami egyedülálló eszközként vonult be a magyar jogrendszer technológiát szabályozó részébe, mint az első irányelv az informatikai szabályzásban

- 2002. A Microsec Kft. 2002. május 30. óta szerepelt a Hatóság nyilvántartásában nem minősített szolgáltatóként (NHH regisztrációs szám: MH 6834 1/2002)

- 2002. november 6-án a MÁV INFORMATIKA is csatlakozott a nem minősített szolgáltatókhoz

- 2002. márciusában kormányhatározat született arról, hogy az államigazgatásban meg kell születnie egy nem minősített hitelesítés-szolgáltatónak, majd egy minősített hitelesítés-szolgáltatónak is, 2003. december 31-ig (1026/2002. (III. 26.) Korm. határozat)[121]

adóigazgatási feladatok hatékony ellátása.
(http://nav.gov.hu/data/cms221302/kaig_prospektus_magyar_k.pdf)

[121] A feladat akkor nem teljesült: „A 1026/2002. számú kormányhatározat előírta a Belügyminisztérium számára, hogy 2002. szeptember 30-ig egy fokozott biztonságú hitelesítés-szolgáltató rendszert alakítson ki (KEAR - Közigazgatási Elektronikus Aláíró Rendszer). A projekt előkészítése és a megvalósíthatósági tanulmány elkészítése megtörtént, azonban a projekthez szükséges források hiányában, az eredeti tervektől eltérően egy Entrust alapú pilot hitelesítés-szolgáltató rendszert állított fel a Belügyminisztérium, ami azonban nem felelt meg az előírtaknak, így az eredeti, kormányhatározatban rögzített feladat nem teljesült.” (http://nmhh.hu/dokumentum/4018/e_alair2004gki_nhh.pdf p.12.)

- 2003. Az NHH március 19-én nyilvántartásba vette a Netlock Kft.-t minősített szolgáltatóként (NHH regisztrációs szám: MH-1372-12/2003), de az archiválás-szolgáltatás nem lett még ekkor elindítva
- 2003 április 3-án a MÁV INFORMATIKA Zrt. elindította minősített hitelesítés-szolgáltatásait – a négyből az első hármat (NHH regisztrációs szám: MH-2460-8/2003)
- 2003. szeptember 4-én megjelent a 2205/2003. (IX. 4.) Korm. határozat a közigazgatási szervek egységes iratkezelési szabályozásának koncepciójáról, amely már tartalmazta a papírmentes ügyintézés biztosításának elvét
- 2003. december 3-án megalakult Almási János vezetésével a Magyar Elektronikus Aláírás Szövetség (MELASZ), amely a hazai szakemberekre és technológiai cégekre építve az elektronikus aláírás és annak rokon, kapcsolódó és származékos technológiáinak a népszerűsítését, a széleskörű hazai bevezetés támogatását, illetve az elterjedés elősegítését tűzte ki célul
- 2004. június 14-én az Országgyűlés elfogadta a 2004. évi LV. törvényt[122], ami számos módosítást eszközölt az Eat-n, többek között beillesztette az archiválás-szolgáltatást negyedik szolgáltatásként
- 2004. júliusában a Nemzeti Szakképzési és Felnőttképzési Intézet a 20/2004. (VII. 27.) OM rendelkezésének megfelelően bevezette és kötelezővé tette a vizsgaszervezők számára az elektronikus vizsgabejelentési rendszer használatát
- 2004. október 1-én a Matáv is elindította a minősített hitelesítés-szolgáltatásait, az immáron négy Eat-szolgáltatásból az első hármat
- 2005. március 11-én megjelent a 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

[122] 2004. évi LV. törvény az elektronikus aláírásról szóló 2001. évi XXXV. törvény módosításáról, 3. § (1)

- 2005. március 18-án megjelent a 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 2005. május 15. óta minősített szolgáltatóként működik a Microsec Kft. (a hatósági nyilvántartásban 2005. május 30 szerepel kezdeti dátumként), mind a négy Eat-ben felsorolt szolgáltatással
- 2005. október 27. megjelent a 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól
- 2006. március 1-én hatályba lépett a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) hitelesítési rendje és a KGYHSZ megkezdte a közigazgatásban használható végfelhasználói tanúsítványok kibocsátására jogosult szolgáltatói tanúsítványok felülhitelesítését
- 2006. március 15-én az EU Bizottság jelentést készített az 1999/93/EK Irányelv működéséről, annak végrehajtásáról[123]
- 2006. október 30-án megjelent az 1103/2006. (X. 30.) Korm. határozat az Új Magyarország Fejlesztési Terv elfogadásáról, ami különösen nagy problémaként írta le az elektronikus közigazgatási szolgáltatások és közszolgáltatások körében a kétoldali interakciós és tranzakciós szintű szolgáltatások szerény kínálatát
- 2007. február 1. óta minősített elektronikus archiválás szolgáltatást is nyújt a Microsec Kft. (NHH regisztrációs szám: HL-3549-2/2007) a világon elsőként
- 2007. augusztus 6-án az Educatio Társadalmi Szolgáltató Nonprofit Kft. kibocsátotta első hitelesítési rendjét, zárt körben
- 2007. december 29-én megjelent a 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól
- 2008. július 1. óta kötelező a cégeljárásban az elektronikusan aláírt dokumentumok használata
- 2008. október 29-én a GIRO Zrt. befejezte a nyilvános hitelesítés-szolgáltatásait

[123] https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52006DC0120&from=HU

- 2008. december 20. Kormányhatározat írja elő az e-taj kártyákra azt, hogy a megvalósítás alkalmas legyen az állampolgár kérésére az Okmányirodában közigazgatásban használható tanúsítványok elhelyezésére, és elindul a Kopint-Datorg Zrt-nél egy új kormányzati szolgáltató kialakítása
- 2009. A SIEMENS Zrt. úgy döntött, hogy február 5-én elindítja minősített archiválás-szolgáltatását a közjegyzői digitális levéltári érintettsége miatt, de az érintettség megszűnését követően a hatósági nyilvántartásból való törlését is kérte 2011. június 7-én, a szolgáltatás nem vált élővé egy pillanatra sem
- 2009. július 1-ével az Educatio Társadalmi Szolgáltató Nonprofit Kft. nyilvános szolgáltatóvá vált
- 2010. március 15-én a Kormány kibocsátja a 78/2010. (III. 25.) Korm. rendeletet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól
- 2010. május 14-én a Magyar Telekom befejezte – a minősített időbélyeg-szolgáltatását kivéve – az Eat. szerinti szolgáltatásainak nyújtását
- 2010. szeptember 15-én a hatóság bejegyezte a Netlock Kft. minősített archiválás-szolgáltatását, a hatósági nyilvántartás december 15-i dátumot rögzített (NMHH regisztrációs szám: HL/18188-4/2010)
- 2011. augusztus 5-én a Digitoll Kft. elindította nem minősített tanúsítvány-, eszköz- és időbélyeg-szolgáltatásait
- 2012. április 21-én megjelennek a SZEÜSZ-rendeletek (83/2012, 84/2012 és 85/2012 Korm. rendeletek)
- 2012. december 21-én az Educatio Társadalmi Szolgáltató Nonprofit Kft. befejezte a szolgáltatását
- 2013. november 23-án az NMHH bejegyzi a Kormányzati Hitelesítés Szolgáltatót mind a minősített, mind a nem minősített szolgáltatásaival (tanúsítvány-kibocsátás, időbélyegzés-szolgáltatás és aláírás-létrehozó eszköz szolgáltatás, mint első három Eat-szolgáltatás)

- 2013. december 30-án elindulnak a kormányablakok az 515/2013. (XII. 30.) Korm. rendelet alapján
- 2014. július 23-án megjelenik az Európai Parlament és a Tanács 910/2014/EU rendelete (eIDAS) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről
- 2014. június 2-án a MÁV Szolgáltató Központ Zrt. (korábbi nevén MÁV INFORMATIKA Zrt.) hivatalosan bejelentette a Nemzeti Média- és Hírközlési Hatóságnak, hogy az elektronikus aláírással kapcsolatos szolgáltatói tevékenységét 2014. július 31-i dátummal befejezi
- 2015. december 16-án megjelent a 2015. évi CCXII. törvény az egyes törvényeknek a gazdasági növekedéssel összefüggésben történő módosításáról, amely kötelezővé tette az elektronikus kapcsolattartást a bírósági eljárásokban
- 2015. december 23-án kihirdetik a 2015. évi CCXXII. törvényt az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, ami hatályon kívül helyezi az Eat-t és amely kötelezővé teszi az elektronikus ügyintézést számos szervezet számára
- 2016. június 13-án megjelenik a 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről
- 2016. a változás előtti utolsó pillanatban megjelenik a 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről, ami lecseréli a 3/2005. IHM rendeletet
- 2016. december 19-én a Kormány kibocsátja a 451/2016. (XII. 19.) Korm. rendeletet az elektronikus ügyintézés részletszabályairól
- 2017. május 25-én megjelent a 2017. évi L. törvény az általános közigazgatási rendtartásról szóló törvény és a közigazgatási perrendtartásról szóló törvény hatálybalépésével összefüggő egyes törvények módosításáról, amely 2018. január 1-i hatállyal pontosít számos törvényt, köztük az Eübszt-t is

- 2018. január 1-én hatályba lépett a 2016. évi CL. törvény az általános közigazgatási rendtartásról, amely a KET lecserélésével újonnan szabályozta a közigazgatási kapcsolattartást, továbbra is biztosítva az elektronikus kapcsolattartás lehetőségét

Az elektronikus aláírás technológiai és jogi hátteréről Balogh írt részletes összefoglaló tanulmányt 2014-ben [192].

3.5. JOGSZABÁLYI HÁTTÉR

Az elektronikus aláírásokra és bélyegzőkre vonatkozó európai jogszabályhelyeket a függelékben soroltam fel (12.2). A legfontosabb vonatkozó magyar jogszabály az Eübszt. A törvény részletezi az elektronikus ügyintézésre vonatkozó előírások mellett a bizalmi szolgáltatókra vonatkozó követelményeket is.

A törvény szövegezésének és hangsúlyainak a vizualizálására elkészítettem a törvény szófelhőjét az Eübszt. 2019. március 5-i állapotának megfelelően. Az ábra elkészítése előtt a szöveget előkészítettem, a numerikus hivatkozásokat és a kötőszavakat töröltem, a szavak toldalékolását megszüntettem és a szótőre koncentráltan egységesítettem az előforduló szavakat. A lábjegyzetek nem voltak bevonva a szófelhő korpuszába. Ennek eredménye látható az alábbi ábrán (12. ábra):

12. ábra: Az Eübszt. szavaiból képzett felhő (forrás: saját ábra)

Az első rész bevezető rendelkezései definiálják a fogalmakat, sokszor visszautalnak az eIDAS rendelet definícióira (pl. 1. § 2., 7., 10., 13., 20) biztosítva a két törvényi szintű jogszabály közötti konzisztenciát. A második rész az elektronikus ügyintézést biztosító szervezetek és az ügyfelek elektronikus kapcsolatának általános

szabályait rögzíti. A VI. fejezet írja le a szabályozott elektronikus ügyintézési szolgáltatások (SZEÜSZ) nyújtásának szabályait, ideértve a Kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatásokat, a VII. fejezet pedig a központi szabályozott elektronikus ügyintézési szolgáltatásokat (KEÜSZ) részletezi. Az elektronikus ügyintézés felügyeletéről a IX. fejezet tartalmaz előírásokat. A harmadik részben az informatikai együttműködés alapelveit és követelményeit fekteti le a jogalkotó. Az 55. § alapján csak olyan informatikai fejlesztés valósulhat meg, amelyik képes a szabályozott és központi elektronikus ügyintézési szolgáltatásokkal való együttműködésre. A papíralapú dokumentumok teljes kiküszöbölését segíti, hogy az együttműködő szerv a csak papíralapon létező dokumentumokról elektronikus másolatot készíthet vagy készíttethet (59. § (3)). A XII. fejezetben az elsődleges információforrások kizárólagos használatának igénye jelenik meg. Ha közhiteles – vagy a törvény által elsődlegesnek tekinthető – adatforrás tartalmazza az ügyintézéshez szükséges adatokat, akkor azokat az elektronikusan együttműködő szerv köteles elektronikus úton ezekből az adatforrásokból azokat beszerezni, amivel az egyszeri adatszolgáltatás elve (’once-only’ principle) automatizált eszközökkel teljesíthető.

A törvény a bizalmi szolgáltatások nyújtásának feltételeit tárgyalja a XVI. fejezettől kezdődően. A szolgáltatókra, a tanúsítványokra és az ellenőrzésre vonatkozó szabályok között alapvető fontosságú jogi vélelmeket is megfogalmaz az elektronikus dokumentumokkal kapcsolatosan:

- minősített aláírással, bélyegzővel vagy időbélyegzővel ellátott dokumentum tartalmát változatlannak kell vélelmezni, amennyiben az aláírások ellenőrzése pozitív (97. § (1)),
- minősített bizalmi szolgáltató által megőrzött dokumentumok esetében vélelmezni kell (az ellenkező bebizonyosodásáig) azt, hogy az aláírás időpontjában az aláírás, bélyegző vagy időbélyegző érvényes volt (100. §).

Ezt ki kell egészíteni a papíralapú és az elektronikus dokumentumok átjárhatóságát biztosító vélelmekkel, amely szerint amennyiben az eredeti dokumentumról készült vagy készíttetett hiteles másolat bizonyító ereje megegyezik az eredeti dokumentum bizonyító erejével (12. §).

A törvény végrehajtásához és az itt definiált szolgáltatások működtetéséhez számos további részletszabály jelent meg, amelyeket az Elektronikus Ügyintézési Felügyelet a honlapján összegyűjtött és hozzáférhetővé tett a nyilvánosság számára[124]. Az elektronikus ügyintézésre vonatkozó legfontosabb szabályokat kiadásuk időrendi sorrendjében a következő jogszabályhelyek tartalmazzák[125]:

- 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól
- 137/2016. (VI.13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről
- 41/2016. (X. 13.) BM rendelet a minősített elektronikus aláírást és minősített elektronikus bélyegzőt létrehozó eszközök megfelelőségét tanúsító szervezetekről és a kijelölésükre vonatkozó szabályokról
- 451/2016. (XII.19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről

A kiadások dátumából nem lehet azt a következtetést levonni, hogy nincs újabb jogszabályi előírás, mivel az egyes jogszabályok időközben változhatnak más módosító jogszabályok kiadásával, például a 470/2017. Kormányrendelet 3. melléklete – az önhibájukon kívül elektronikus ügyintézés megvalósításában akadályozott szervezetek

[124] Lásd https://euf.gov.hu/kapcsolodo-jogszabalyok-szeusz (2019. március 5.)
[125] Az NMHH E-szolgáltatás-felügyeleti osztálya folyamatosan közzéteszi az aktuális jogszabályok listáját (http://nmhh.hu/szakmai-erdekeltek/jogforras?HNDTYPE=SEARCH&name=doc&page=1&fac_provider_theme=elektronikus, 2019. március 5.)

listája – a 290/2018. (XII. 21.) Korm. rendelet 3. §-a szerint módosított szöveg. A jogszabályok folyamatos követése ajánlható tevékenység az érintettek számára.

3.6. SZANKCIÓK A BIZALMI SZOLGÁLTATÁSOK VÉDELMÉBEN

Az eIDAS szerinti és a nemzeti bizalmi szolgáltatások nyújtásában van egy közös tényező, az intézményi bizalom. Minden érintett szereplőnek meg kell bíznia abban, hogy a szolgáltató megfelelően nyújtja a szolgáltatását – még egy kiberkonfliktus esetén is, különben nem működhetnek az erre alapozott társadalmi folyamatok. A bizalmat a szabályozott működés és a rendszeres ellenőrzés segítheti elő (a technológiai szint erősítésével). Tekintettel arra, hogy ezek a szolgáltatások Muha [4] szerint is alapvető fontosságúak az informatikai biztonság rendszertanának hét alcsoportja közül az ötödikben: „Kommunikáció és hálózat", érdekes kérdés lehet közép- és hosszú távon az, hogy vajon az egyes bizalmi szolgáltatások felügyelete mutat-e hasonlóságot egymás iránt, összefügg-e a bizalmi szint és a felügyelet erőssége, illetve mekkora elrettentő erő jelenik meg a jogszabályokban az esetleges támadások kivitelezői számára? Ezeknek a kérdéseknek a megválaszolásához két bizalmi szolgáltatás felügyeletét hasonlítom össze a következő részben. Az egyik egy eIDAS szerinti minősített bizalmi szolgáltatás, a másik pedig nemzeti minősített adatok kezelésének a megvalósítása, előre rögzített szempontok alapján. A kérdések kiterjednek a felügyeletet végzők kijelölésére, a felügyeletet végzők feladatainak rögzítettségére, az ellenőrzések tulajdonságaira és a hibás működés esetén követendő eljárásokra is. Ezeken túl fontos lehet annak a vizsgálata is, hogy miként kapcsolódnak az egyes felügyeleti eljárások az európai rendszerekhez, hiszen ma már nem kizárólag magyar bizalomról beszélhetünk, a bizalomnak lehetnek kontinentális és globális vetületei is. A bizalom megteremtésének emiatt olyannak kell lennie, hogy képes legyen támogatni a magyar, az európai és a globális intézményekbe vetett bizalmat egyaránt. Az egyes összehasonlítási szempontok részletesen az alábbiak lesznek:

I. a felügyeleti szerv kijelölési módszere: megvizsgálom, hogyan történik a felügyeletre jogosult szervezet kijelölése, milyen követelményeknek kell megfelelnie a kijelölt szervezeteknek ahhoz, hogy egyáltalán ezt a tevékenységet végezhessék.

II. a felügyeleti szerv feladatköre és hatásköre: fontos kérdés, hogy a felügyeletet végzőknek milyen előírt tevékenységeik vannak és az meddig terjed, vagyis hol vannak a tevékenységek korlátjai

III. az ellenőrzések rendszere: meg kell vizsgálni az ellenőrzési tevékenységeknél azt, hogy melyiket milyen rendszerességgel végzik, és van-e bármilyen követelmény előírva az ellenőrzések lefolytatására

IV. az ellenőrzött követelmények rögzítettsége: az ellenőrzés megfelelőségét növelő tényező, ha előre megadott elemeknek való megfelelőséget és megvalósulást kell ellenőrizni. Kérdésként merül tehát fel, hogy vannak-e előre rögzített és elvárt követelmények a felügyeleti eljárásokhoz.

V. szankcionálás: a bizalomerősítést befolyásoló tényező a büntetéstől való félelem is, emiatt fontos összehasonlítani az előírások megsértésekor foganatosítható intézkedéseket is.

VI. a felügyeletek európai kapcsolódása: a bizalmi szolgáltatások területi hatálya nem korlátozódik csak Magyarország területére és populációjára, emiatt szükséges a bizalom kiterjesztése Európára is, azaz fontos kérdés lehet, hogy milyen európai vonatkozásai vannak az egyes felügyeleteknek.

Szempontok / Terület	**Bizalmi-szolgáltatások felügyelete**	**Nemzeti titokvédelem felügyelete**	**Értékelés**
I. Kijelölési módszer	A Nemzeti Média- és Hírközlési Hatóságot (NMHH) a 2015. évi CCXXII. törvény nevezi ki[126].	A Nemzeti Biztonsági Felügyeletet (NBF) a 2009. évi CLV. törvény nevezi ki[127].	Törvény nevezi ki mindkét szereplőt a felügyeleti tevékenységre.
II. Feladat- és hatáskör	2015. évi CCXXII. törvény rögzíti, 470/2017. (XII. 28.) Korm.R. részletezi, a díjakat a 25/2016. (VI. 30.) BM.R. tartalmazza.	2009. évi CLV. törvény rögzíti, 90/2010. (III. 26.) Korm.R. részletezi, kiegészítve a 92/2010. (III. 31.) Korm.R. és a 418/2016. (XII. 14.) Korm.R. előírásaival.	Törvény írja le és végrehajtási rendeletek részletezik mindkét területen a feladatokat és hatásköröket.
III. Ellenőrzések rendszere	A bizalmi felügyelet a szolgáltatás nyújtásának megkezdését követő harminc napon belül felügyeleti ellenőrzést végez a minősített bizalmi szolgáltatást bejelentő szolgáltatóknál az előírt követelmények betartása tárgyában. A bizalmi felügyelet évente legalább egyszer átfogó helyszíni ellenőrzést tart a minősített	Tevékenység megkezdését megelőző tanúsítványok beszerzése, nemzetbiztonsági szolgálat bevonásával, bejelentés vagy incidens esetén újból végrehajtva, ötéves megújítással. A szervezet biztonsági vezetője évente köteles ellenőrzéseket lefolytatni és jelentéseket készíteni.	A hitelesítés-szolgáltatásoknál bejelentést követő szemle és éves rendszeres ellenőrzés van az NMHH szá-mára előírva, a titokvédelemnél előzetes vizsgálat, tanúsítás kiállítása és ennek ötévenkénti megújítása az előírás az NBF számára.

[126] 2015. évi CCXXII. törvény, 91. § (1)
[127] 2009. évi CLV. törvény, a minősített adat védelméről (Mavtv.) 20. § (1) – (4)

Szempontok / Terület	Bizalmi-szolgáltatások felügyelete	Nemzeti titokvédelem felügyelete	Értékelés
	bizalmi szolgáltatást nyújtó bizalmi szolgáltatóknál.		
IV. Műszaki követelmények az ellenőrzött alanyokra	24/2016. (VI. 30.) BM.R. részletesen tartalmazza	418/2016. (XII. 14.) Korm.R. és a 92/2010. (III. 31.) Korm.R. részletesen tartalmazza	Végrehajtási rendeletek által részletesen szabályozottak az ellenőrzési követelmények
V. Szankcionálás	Figyelmeztetés, felhívás, pénzbírság, szolgáltatás megszüntetése (hatósági jogkörben). A bírság mértéke: szolgáltató: 20e – 20M Ft vezető: 50e – 2M Ft[128] 2012. évi C. törvény (Btk.) tényállások megvalósulása esetén szabadságvesztés • vétség: 2 év, • bűntett: 3 év, • közérdek elleni: 2-10 év)	Külső elkövető[129]: • elzárás (5-90 nap), • szabadságvesztés (1 év, 3 év, 1-5 év minősítéstől függően) Belső elkövető[130]: • szabadságvesztés (1 év, 2 év, 1-5 év, 2-8 év) függően a minősítéstől Biztonsági tanúsítványok módosítása, visszavonása	A büntetés mértéke a minősített adattal történő visszaélés esetén elzárás vagy szabadságvesztés, a hitelesítés-szolgáltatásnál pénzbírság, és a Btk. alkalmazása esetében elzárás vagy szabadságvesztés. A szolgáltatás megszüntetése, mint következmény, mindkét esetben fennállhat.
VI. Európai kapcsolódás	Az NMHH felelős a bizalmi lista magyar részének a működtetéséért[131] és tagja a hitelesítés-szolgáltatókat felügyelő önkéntes európai fórumnak (FESA[132])	1. A Mavtv. leképezi az európai és NATO titkok minősítését nemzeti szintre. 2. A Nemzeti Kibervédelmi Intézet (NBF-CDMA) kapcsolódik az európai és NATO kibervédelmi szervezetekhez	A szolgáltatások nemzeti jellegének biztosításán túl mindkét felügyeleti szerv kapcsolódik nemzetközi szervezethez, együttműködési jelleggel.

3. táblázat: Bizalmi felügyelet és titokvédelmi felügyelet összehasonlítása (forrás: saját táblázat)

A szankcionálási eltérések figyelmet érdemelnek, főként egy kormányzati hitelesítés-szolgáltatás megindításakor, hiszen a kormányzati hitelesítésszolgáltatói aláíró kulcsok illetéktelen kezekbe kerülése vagy az állampolgári aláírások könnyű hamisíthatósága esetén olyan tanúsítványok, időbélyegek kiállítására nyílik lehetőség, amelyek felett Magyarországnak nincs közvetlen kontrollja, de kihasználja a korábban Magyarország neve alatt felépített bizalmat, amelyet az Európai Bizalmi Szolgáltatók

[128] Eübszt. 57. A bizalmi felügyelet által kiszabható bírság mértéke, 96. §
[129] Btk. 265. § (1) és (2)
[130] Btk. 265. § (3)
[131] Eübszt. 91. § (1). A bizalmi listáról bővebben: http://www.kgyhsz.gov.hu/bizalmilista_tajekoztato.pdf
[132] FESA. Forum of European Supervisory Authorities for Electronic Signatures. A tagok a következő weboldalon találhatók: http://www.fesa.eu/members.html

Listájában (EU Trusted List[133]) szereplő szolgáltatások élveznek, ahogyan ez első példánk, a holland DigiNotar esetében 2011-ben történt. A DigiNotar által kibocsátott tanúsítványok különböző elektronikus közigazgatási szolgáltatásokban is felhasználhatók voltak. Az eset nyilvánossá válását követően a DigiNotar beszüntette a működését és az általa kibocsátott tanúsítványok érvényessége pedig megszűnt. Ez jelentősen visszavetette a holland e-közigazgatást és a hozzákapcsolódó bizalmat is erodálta. Másik példaként említhető, hogy Észtország 2017-ben úgy döntött, hogy egy cseh kutatócsoport által felfedezett aláírás-létrehozó eszközt érintő technológiai hiba[134] miatt [54] minden állampolgári tanúsítványt azonnali hatállyal visszavon és az érintett kártyák forgalmazását megállítja.

Ezért az elektronikus közigazgatást támogató kormányzati hitelesítés-szolgáltató aláíró kulcsainak érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele – ahogyan a holland példa is megmutatta – alkalmas állami vagy közfeladatot ellátó szervek rendeltetésszerű működésének ellehetetlenítésére vagy lényeges akadályozására, és ez közvetlenül Magyarország törvényben meghatározott érdekeit sérti, hiszen az állampolgárok biztonságának és alkotmányos jogainak komoly sérelmével járhat együtt. A számítógépes bűnözés jellegét megvizsgálva és összefoglalva Balogh megállapította, hogy az elkövetők általában magas intellektussal rendelkeznek, nem feltétlenül lesznek a megtámadott állam polgárai, és a rövid idő alatt kivitelezhető támadások java része nem derül ki azonnal, esetleg később sem. A bűncselekmények helyes osztályozásához különbséget kell tenni a számítógépes bűnözés és a számítógéppel kapcsolatos bűnözés között is ([191]: 177). Ennek értelmében a szolgáltatói magánkulcsokkal való visszaélést – diszjunktálva a halmazokat – tekinthetjük számítógéppel kapcsolatos számítógépes bűnözésnek, amit a két halmaz közötti tartalmazási relációt visszaállítva nevezhetünk egyszerűen számítógépes bűnözésnek. Tekintettel arra, hogy egy idegen állam névtelen polgára elleni büntetőper kilátásai számítástechnikai bűntett miatt alacsony hatásfokúnak

[133] EU Trusted List Browser, EU Bizalmi Lista Böngésző a https://webgate.ec.europa.eu/tl-browser/#/ URL-en érhető el (2019. január 26-i állapot szerint)

[134] A hiba súlyosságát annak leírásából lehetséges kikövetkeztetni: „A remote attacker can compute an RSA private key from the value of a public key. The private key can be misused for impersonation of a legitimate owner, decryption of sensitive messages, forgery of signatures (such as for software releases) and other related attacks.” A távoli támadó elő tudja állítani a titkos kulcsot a nyilvános kulcs ismeretében, így gyakorlatilag bármilyen műveletet végre tud hajtani a kulcsbirtokos nevében annak tudta nélkül.

bizonyultak az elmúlt időszakban, indokoltnak tűnhet a kormányzati hitelesítésszolgáltatásban alkalmazott védendő elemek védelmét a területre vonatkozó védelmi intézkedéseken túlmenően nemzeti titokvédelmi minősítési eljárás segítségével növelni. Ezt – tekintettel a nemzetbiztonsági ellenőrzés alá eső személyek körének meghatározására[135] – csak abban az esetben lehetséges a 2018-ban hatályos titokvédelmi előírásoknak megfelelő módon megvalósítani, ha a minősítő a védendő elemeket (szolgáltatói titkos kulcsok) „Bizalmas!", „Titkos!" vagy „Szigorúan titkos!" minősítési szintre emeli. Ennek eredményeként egyrészről tovább növelhető a bizalmi szolgáltatások biztonságkritikus elemeinek a védelme, másrészről erőteljesebben szankcionálható egy nem kívánt esemény bekövetkezésekor az ismert elkövető tette is, mivel súlyos bűncselekmény mellett minősített adattal való visszaélés is szankcionálható lenne, ami magasabb elrettentő hatást jelenthet legalább a potenciális elkövetők egy része számára. A Btk. 423. § szerint

A Btk. 265. § szerint, aki minősített adatot jogosulatlanul megszerez vagy felhasznál, illetve jogosulatlan személy részére hozzáférhetővé, vagy jogosult személy részére hozzáférhetetlenné tesz, mindenképpen minősített adattal való visszaélést követ el. A jogszabály büntetni rendeli a visszaélésre irányuló előkészületet is, ami azért fontos jelen esetben, mivel az informatikai rendszerek vagy adat megsértése miatt szankció csak a negatív esemény bekövetkezését követően szabható ki, míg az erősen védendő adat szabályoktól való eltérő kezelése – gondatlanság vagy szándékosság esetében egyaránt – szankcionálható lenne az előkészületre való hivatkozással. A szolgáltatói titkos kulcsok helytelen kezelése ugyanis már eredményezheti azok illetéktelen kezekbe kerülését, azaz kompromittálódását, de nem szükséges a titkos kulcsoknak valóban kikerülnie ahhoz, hogy a szankció életbe léphessen, ha az előkészületek monitorozása már megfelelő információkkal látja el a biztonságért felelős szerepköröket és az esemény felderíthetőségét növeli, a feltáráshoz szükséges időtartamot pedig lecsökkenti.

[135] A nemzetbiztonsági ellenőrzés alá eső személyek körét az 1995. évi CXXV. törvény (Nbtv.) 74. § i) pontja határozza meg. A felvázolt esetben az ip) pont lenne alkalmazható.

4. AZ ELEKTRONIKUS ALÁÍRÁS DIMENZIONÁLÁSA

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. Sok esetben nehezen eldönthető kérdésként vethető fel az, hogy az adott elektronikus aláírás – mint alaki jogi kellék – használható-e teljes bizonyító erejű magánokirat létrehozására vagy alkalmas-e közokirat elektronikus aláírására? Számos további kérdést fel lehet még vetni a tárgyban, elegendő csak a konténerekre vagy az aszimmetrikus kriptográfián túlmutató, vagy éppen ezzel ötvözhető megoldásokra (például biometrikus aláírások[136] [49]) gondolni. Ezek a kérdések ugyanabba az irányba mutatnak, az elektronikus aláírások mérhetőségének igénye irányába. Érvelésem szerint az egyértelmű elhelyezhetőség teremti meg a mérhetőség és az összehasonlíthatóság alapjait az elektronikus aláírások tekintetében is.

Az elektronikus aláírás fogalmát 2014 óta az eIDAS rendelet definiálja az Európai Unióban olyan elektronikus adatként, amelyet egy másik elektronikus adathoz csatolnak, és amelyet az aláíró (signatory) aláírásra használ[137]. Az aláíró kizárólag természetes személy (natural person) lehet, aki éppen aláír[138]. Az aláírásnak ebből adódóan három implicit jellemzője létezik:

1. a természetes személy aláíró
2. az aláírás csatolása valamely más adathoz
3. az aláírt elektronikus adatok

Az eIDAS rendelet hatályba lépését követően az Európai Unió megkülönbözteti a jogi személyek (legal person) aláírását a természetes személyek aláírásától és elektronikus bélyegzőnek[139] (electronic seal) nevezi[140]. Az elektronikus aláírás és bélyegző tulajdonságai között azonban erőteljes hasonlóságot lehet felfedezni, mivel

[136] Ez a kutatási irány például a nem egzakt bemenetű privát kulcs generálási módszerek kialakítására vonatkozott, ami biometrikus bemenő adatok feldolgozását tűzte ki célul, összhangban az azonosítás-alapú kriptorendszerek és aláírási sémák Shamir által javasolt elvével [133].
[137] eIDAS Rendelet 3. cikk 10.
[138] eIDAS Rendelet 3. cikk 9.
[139] eIDAS Rendelet 3. cikk 25.
[140] eIDAS Rendelet 3. cikk 24.

egyrészről az eIDAS rendelet megismétli szinte szóról-szóra az elektronikus bélyegzők esetében az elektronikus aláírásra vonatkozó előírásokat, másrészről az elektronikus ügyintézésről szóló törvény kodifikációs fikciót alkalmazva azt mondja ki, hogy – eltérő rendelkezés hiányában – az elektronikus bélyegzőt is elektronikus aláírásnak kell tekinteni[141].

Tekintettel arra, hogy a fentiek szerint az elektronikus aláírásokhoz számos további jellemző csatlakozik, felmerül a kérdés, hogy lehetséges-e az elektronikus aláírás jellemzőit dimenzionálni? Kutatásaim szerint igen, meg lehet határozni azokat a dimenziókat, amelyekben az elektronikus aláírások elhelyezhetővé válnak és lehetővé válik az így létrejött térben metrika vagy metrikák definiálása is. Egy metrikus térben – amelynek a fogalmát Maurice Fréchet alapozta meg 1906-os PhD disszertációjával [50] – elméletileg számos távolságfüggvény felírható. A Hamming-metrika [53] alkalmazásával megkaphatjuk az egyes aláírások leírásában szereplő különbözőségek számát, míg az euklideszi távolság értelmezésével az egyes aláírások (azaz az ugyanolyan tulajdonságokkal rendelkező aláírások alkotta kategóriák) egymástól való távolságait tudjuk megmérni és szemléletesebbé tenni. Ezeket a metrikákat alkalmazva két elektronikus aláírás-kategória távolsága kizárólag nemnegatív lehet, továbbá akkor és csak akkor nulla, ha a leírásukban ugyanazok a tulajdonságok szerepelnek, a dimenziók sorrendjére való tekintet nélkül. Matematikai nyelven kifejezve, két binárisan nem identikus elektronikus aláírás euklideszi távolsága akkor és csak akkor lesz pozitív, ha a Hamming-távolságuk is pozitív, egyébként távolságuk ebben a modellben zéró. A dimenziók tehát absztrakciós szintet hoztak létre és az ugyanolyan tulajdonságokkal leírható elektronikus aláírásokat tartalmazzák, azaz jelen esetben nem az egyes aláírások bináris reprezentánsai hordozzák az aláírás elhelyezhetőségéhez szükséges információkat, hanem az egyes bitsorozatok jelentései. Vagyis két különböző elektronikus aláírás akkor lesz ebben a leíró térben ugyanazon a helyen, ha absztrahált tartalmuk azonos. Szemléletesen szólva, két különböző dokumentumon elhelyezett különböző elektronikus aláírás Hamming-távolsága akkor lesz zéró, ha minden tulajdonságuk rendre megegyezik, holott a két aláírás műszaki és bináris értelemben teljesen különböző is lehet. Tekintettel arra, hogy az egyes dimenziók értékkészlete nem izomorf a valós számok halmazával, így ez a tér nem lesz euklideszi és a vektortér-axiómák sem fognak teljesülni benne, de a távolság fogalma értelmezhető, mivel a

[141] Eübszt. 99. § (2)

dimenziók értékkészletének leképezése a valós számok körére azt eredményezte, hogy a leíró tér valódi részhalmaza egy ugyanolyan dimenziós euklideszi térnek. Ez a matematikai alapokon nyugvó, de társadalmi beágyazódást is mérni képes metrika teszi lehetővé az elektronikus aláírás átfogó tárgyalását elméletben (in thesi) és gyakorlatban (in praxi) a közigazgatásban és a közigazgatási jogban egyaránt, amelyek különböznek egymástól, ahogyan azt Tamás András megállapította [51], ezért a fókusz mind a négy területre kiterjeszthető.

Kérdésként felvethető továbbá az is, hogy az elektronikus aláírások általános leírására alkalmas dimenziókat meg kell-e különböztetni vagy ki kell-e egészíteni a magyar, európai vagy egy esetleges jövőbeli globális közigazgatás számára. 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 a felhasználói közösség minden tagja számára, akár nemzeteken vagy kontinenseken átívelő módon. Az eIDAS rendelet az Európai Unióban 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 a Rendelet előírásainak vonatkozniuk. A harmadik felek számára is elérhető nyilvános bizalmi szolgáltatásokra nézve viszont kötelezően kell érvényesíteni az európai előírásokat[142]. Az eIDAS rendeleten túl az elektronikus ügyintézés szabályait a magyar jogalkotó külön törvényben és rendeletben tette közzé. Ez a rendelet az elektronikus ügyintézést nyújtó szervezetekre, az ügyfélre, az alkalmazható bizalmi szolgáltatásokra és a felügyeleti szervre terjed ki[143]. A magyar állam tehát élt a külön előírások definiálásának jogával a közigazgatási ügyek elektronikus intézése vonatkozásában, ami indokolttá teszi az általános célú vizsgálatok kiterjesztését a közigazgatásra vonatkozó speciális előírásokra is.

Az elektronikus aláírást az 1999/93/EK Irányelv definiálta először jogi szabályozási környezetben az EU-ban 1999-ben, az itt megfogalmazott definíciója szerint egy elektronikus aláírás a következőt jelenti:

[142] eIDAS Rendelet Preambulum (21)
[143] Lásd a 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről című jogszabály hatályát.

„olyan elektronikus adat, amely más elektronikus adathoz van csatolva, illetve logikailag hozzárendelve, és amely hitelesítésre szolgál;”[144]

A 2001-ben hatályba lépett elektronikus aláírási törvény (Eat.) úgy fogalmaz, hogy az elektronikus aláírás az „elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.” A két definíció látszólagos ellentmondásban van, hiszen az azonosítás nem lehet egyenlő a hitelesítéssel. A kontraindikatív kapcsolatot a két definíció között a hitelesség Vasvári György általi meghatározása képes megszüntetni [52], amely szerint általánosságban véve a hitelesség az állított azonosság megerősítése, így az elektronikus hitelesség az elektronikusan állított azonosság megerősítése. Azonosságot pedig – a korábban felismert dichotómiát alkalmazva – lehet állítani a forrásról (signatory) és a tartalomról (content). Egy aláírt adat esetében ennek az azonosságnak a megerősítése két vizsgálat – azaz az aláíró és a tartalom hitelesítésének eredményét jelenti – összhangban a NIST FIPS 800-53 amerikai szabványban[145] a hitelesítésről megfogalmazottakkal[146]:

1. az adat látszólagos aláírója megegyezik az adat tényleges aláírójával,
2. az adat látszólagos tartalma megegyezik az aláíró által aláírt tartalommal.

Ez azonban nem technológiafüggő megfogalmazás, ezért az eIDAS rendelet definíciója még jobban általánosította az elektronikus aláírás definícióját 2014-ben. Elektronikus aláírás az, amit az aláíró aláírásra használ – ennek következtében az aláírási gyakorlatban számos megvalósítás jött létre teljesen különböző paraméterekkel. Az elektronikus aláírási rendszerek implementálásakor ezek közül választ a bevezető paramétert az előre megfogalmazott kritériumok alapján, illetve a megvalósítás során rögzíti az előre nem definiált paramétereket előre nem megfogalmazott módon. Az előre nem definiált paraméterek számossága a fejlesztési metódusban nyilvánvaló módon negatív hatással van az interoperabilitásra.

[144] Az angol nyelvű definícó így szólt: „"electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”.
[145] NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. April 2013, includes updates as of 01-22-2015.
[146] NIST Special Publication 800-53 Revision 4: „Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.” p.B-2

Az elektronikus aláírások dimenzionálásának az a legfontosabb célkitűzése, hogy rögzítve legyenek azok a dimenziók, amelyek az elektronikus aláírásokkal kapcsolatosan felmerülhetnek, valamint meg is legyenek határozva az egyes dimenziók értékkészletei. Tekintettel arra, hogy az egyes értékek között vannak nyilvánvaló és lehetnek rejtett összefüggések is, ezek feltárása alapvető fontosságú az egyértelmű dimenzionáláshoz. Matematikai nyelven megfogalmazva, az egyértelmű dimenzionáláshoz az elektronikus aláírások dimenzióiból összeálló elektronikus aláírási térhez tartozó generátor-rendszert is meg kell határozni.

Az Európai Unió az elektronikus aláírásra vonatkozó szabályozás kidolgozását az infokommunikációs szabványosítási testületek (ICTSB) égisze alatt kezdte el, ennek érdekében első lépésként az európai ipar és a szabványosítási testületek elindították az Európai Elektronikus Aláírás Szabványosítási Kezdeményezést (EESSI) 1998 novemberében. Az EESSI célja, hogy az elektronikus aláírásokról szóló európai irányelv támogatására irányuló szabványosítási tevékenységek igényeit koherens módon elemezze, különösen az üzleti környezetben. Az EESSI által kijelölt szakértői csoport 1999 júliusában elkészítette azt a riportot, amely az első európai elektronikus aláírási irányelv alapjául szolgált és amelyben – kicsit szabadabb fordításban – a következő magyarázatot tették közzé:

Az ’elektronikus aláírás’ minden további minősítés nélkül valójában elektronikus hitelesítés. A ’hitelesítés’ fogalmát az Irányelv nem határozta még meg, de az "állított azonosság validálása" interpretáció a leggyakoribb. Az elektronikus hitelesítés minden típusát elektronikus aláírásnak kell tekinteni mindaddig, amíg azt más elektronikus adatokhoz hozzákapcsolják vagy logikusan hozzákapcsolják (azaz amíg a kapcsolat fennáll). Így a biometrikus hitelesítési módszerek (aláírópados megoldások) elektronikus aláírásnak minősülnek, a szimmetrikus kriptográfián alapuló Message Authentication Codes (MAC) szintén elektronikus aláírás. A nyilvános kulcsú hitelesítési rendszerek, mint például a digitális aláírások, ugyancsak elektronikus aláírások. Az elektronikus aláírás definíciója az Irányelvben nem zárja ki aláírásként a gépelt nevet az e-mail alján, vagy a beolvasott aláírás képének csatolását a dokumentumhoz.

A szabványok kidolgozásakor az irányelvben lefektetett fogalmi definíciókon túl megjelent az aláírás társadalomban betöltött szerepe is, más szóval az aláírás célhoz

kötöttsége. A legelső szabványdokumentum tervezete 2000. januárjában ezt így fogalmazta meg:

„An electronic signature produced in accordance with the present document provides evidence that can be processed to get confidence that some commitment has been explicitly endorsed under a Signature policy, at a given time, by a signer under an identifier, e.g. a name or a pseudonym, and optionally a role."[147] (Egy elektronikus aláírás egy adott dokumentummal kapcsolatban feldolgozható bizonyítékot nyújt arra a bizonyosságra nézve, hogy valamely kötelezettséget valamely aláírási szabályozás alapján egy adott időben explicit módon felvállalt egy adott azonosítóval meghatározott aláíró (pl. név, álnév vagy opcionálisan egy szerepkör.)

Az aláírás szerepe tehát itt az arról való bizonyosság megszerzése volt, hogy egy név, álnév vagy opcionálisan egy szerepkör által azonosított aláíró valamely kötelezettséget egy adott szabály szerint egy adott időben felvállalt, ami 2014-re az aláírásra, mint szándékra egyszerűsödött le az Európai Unióban.

Az Amerikai Egyesült Államokban az elektronikus aláírási törvény a következőképpen definiálta az elektronikus aláírást 2000. június 30-án:

„Electronic signature. -- The term „electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[148] (Elektronikus aláírás: az elektronikus aláírás fogalma egy olyan elektronikus hangot, szimbólumot vagy eljárást jelent, amelyik fizikailag vagy logikailag kapcsolódik egy szerződéshez vagy más adathoz, és amely olyan személy által keletkeztetett, akinek szándékában állt aláírni az adott adatot.)

Lényeges különbségnek látszik, hogy amíg a digitális aláírás csak kriptográfiailag transzformált adat lehet, addig az elektronikus aláírás lehet hang, szimbólum vagy eljárás, amelyet az aláírást megtenni szándékozó – a szó legtágabb értelmében vett – személy hajt végre vagy fogad el.

Az ENSZ Nemzetközi Kereskedelmi Jogok Bizottsága (UNCITRAL) által kiadott modellben az aláírástól elvárt, hogy azonosítani is lehessen az aláírót kimondottan az

[147] ETSI Standard: Draft ETSI ES 201 733 V1.1.2 (2000-01) Electronic Signature Formats. p.8.
[148] Lásd US Electronic Signatures in Global and National Commerce Act 2000, SEC. 106 (5).

aláírni kívánt adatokkal kapcsolatban és az aláíró jóváhagyását is kifejezze az aláírni kívánt üzenetben foglalt információk vonatkozásában:

„"Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message"[149]. („Elektronikus aláírás" alatt olyan elektronikus formában létező adatot kell érteni, amelyik hozzá van csatolva vagy logikailag hozzá van rendelve egy elektronikus üzenethez, amelyik felhasználható az aláíró azonosítására az elektronikus üzenettel kapcsolatosan, és jelzi azt, hogy az aláíró elfogadta az elektronikus üzenetben lévő információt.)

Ehhez teljesen hasonló módon definiálta a Kínai Népköztársaság az elektronikus aláírást, de kiegészítve a fokozott biztonságú elektronikus aláírás azonosítási követelményével és az aláírónak az üzenetre vonatkozó megismerési vélelmével: „electronic signature means the data in electronic form contained in and attached to a data message to be used for identifying the identity of the signatory and for showing that the signatory recognizes what is in the message"[150].

India a digitális aláírás útján indult el[151], amit 2008-ban habozás nélkül felcserélt az elektronikus aláírásra[152], azaz a jogszabályban a módosítás által a táblázatban foglalt helyeken a „digitális aláírás" szövegrészt egész egyszerűen ki kellett cserélni az „elektronikus aláírás" szövegrésszel, ami a következőket eredményezte: „(d) "affixing ~~digital~~ electronic signature" with its grammatical variations and cognate expressions

---

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, Article 2 (a) (http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html)

[150] Lásd Article 2, Electronic Signature Law of the People's Republic of China (Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress on August 28, 2004 and promulgated by Order No.18 of the President of the People's Republic of China on August 28, 2004)

[151] Lásd Section 2. d), MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department) New Delhi, the 9th June, 2000/Jyaistha 19, 1922 (Saka)The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information: — THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000): „(d) "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;"

[152] Lásd the Table in the Part II Section 2 of MINISTRY OF LAW AND JUSTICE (Legislative Department) New Delhi, the 5th February, 2009/Magha 16, 1930 (Saka) The following Act of Parliament received the assent of the President on the 5th February, 2009, and is hereby published for general information: — THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008 (No. 10 OF 2009): „2. In the Informatin Technology Act (…), for the words „digital signature" occurring in the Chapter, section, subsection and clause referred to in the Table below, the words „electronic signature" shall be substituted.

means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of ~~digital~~ electronic signature;".

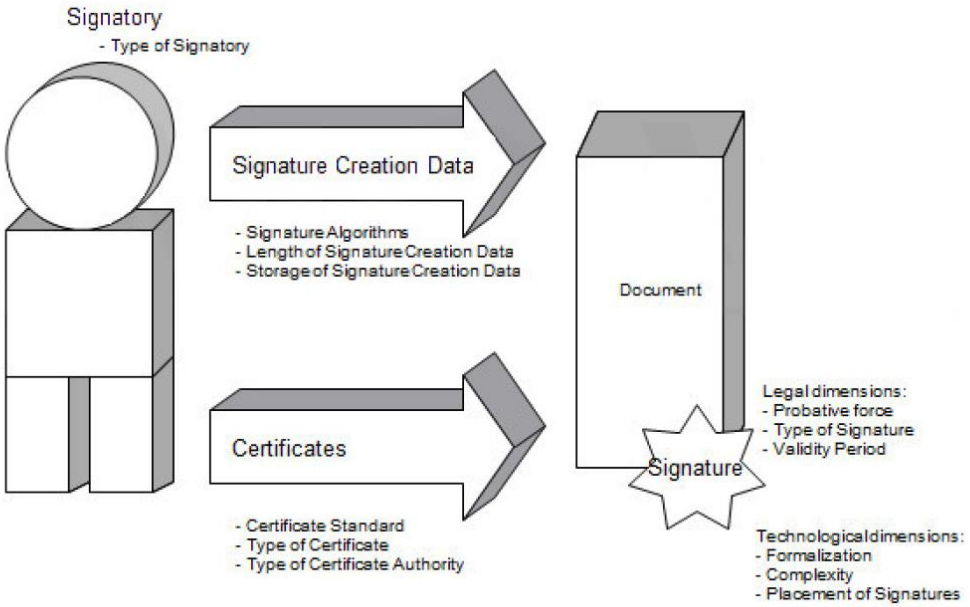
4.1. A DIMENZIÓK SPECIFIKÁLÁSA

Ebben a fejezetben megkísérlem összegyűjteni és felsorolni az elektronikus aláírásokkal és bélyegzőkkel kapcsolatosan fellelhető összes olyan potenciálisan releváns tulajdonságot, amelyek elméleti vagy gyakorlati aspektusban felmerültek idáig a szakirodalomban. A tulajdonságok elé első megközelítésben jogosnak látszik a „potenciális" jelző, hiszen „valódi" dimenziók esetében elvárt a közöttük lévő függetlenség, ami további vizsgálatokat is feltételez. Elméletileg (matematikai értelemben) végtelen sok generátor-rendszere létezhet egy adott térnek, amelyben minden eleme reprezentálható, de a dimenziók függetlensége csak a bázis-rendszerek esetében jelenik meg követelményként. Az elektronikus aláírások és bélyegzők tere különbözik a valós vagy komplex számokon értelmezett matematikai absztrakt tértől abban az értelemben, hogy a dimenziók értékkészletei nem feltétlenül skaláris tulajdonságúak, lehetnek kategoriális elemek is az egyes dimenziókban. Ortogonalitási vizsgálatot azonban csak a már ismert és definiált dimenziókon lehetséges elvégezni, ennek eredményeként állítható elő az a legszűkebb dimenzió-halmaz (bázis-rendszer), amelyben egyrészről minden elektronikus aláírás vagy bélyegző egyértelműen felírható, másrészről további dimenziók felvételét csak úgy lehetséges megtenni, hogy valamely már létező dimenziótól való függés nem áll fenn. A dimenziók elnevezése saját tapasztalataimat tükrözi, megválasztásuk során az alkotói szabadság és a létező fogalom-használat optimális konkatenációja volt az alapvető célkitűzés. Természetesen az egyes dimenziók elnevezésekor más fogalmakat is lehetett volna használni, bízom abban, hogy ezek a fogalmak is teljesíteni fogják céljukat és használható alapot jelentenek a modell számára.

Az elektronikus aláírások dimenzióinak meghatározásakor először az elektronikus aláírás értelmezési keretét definiáljuk, vagyis az aláírás kontextusából, valamit annak jogi és technológiai környezetéből indulunk ki. A kontextus felveti az aláíró entitás, az aláírás-létrehozó adat és az aláírás-ellenőrző adat, illetve az aláírás osztályozását és az egyes osztályok kapcsolati hálóinak elemzését, ideértve a technológiai és jogi környezet elemeinek hozzákapcsolását az aláírások különböző osztályaihoz. Ez nagyon fontos megállapításnak tűnik abból a szempontból nézve, hogy az eddig létező technológiai

szabványok kizárólag műszaki oldalról közelítették meg az aláírásokat, a jogalkotók kizárólag a jogszabályokban való alkalmazhatóságot tűzték ki célul, és eközben nem sikerült az egyes aláírásfajták társadalomban betöltött szerepét megragadni, egyértelműsíteni vagy mérhetővé tenni. Ennek eredményeként a jogalkotó Magyarországon olyan elektronikus aláírással ellátott magánokiratokhoz rendelt teljes bizonyító erőt, amelyek biztonsági tulajdonságai nem egyenszilárdságúak[153], így az alkalmazásukban a költséghatékonyság – ideértve az implementációt és a fenntartást is – lényeges szerepet játszhat, mellyel végeredményben a kevésbé biztonságos aláírási formák elterjedését ösztönzi a jogalkotó a biztonságosabbakkal szemben, ha ugyanolyan társadalmi alkalmazhatóságot rendel hozzájuk.

A fenti eszmefuttatás világossá tette, hogy az elektronikus aláírásokat nem lehet kizárólag műszaki aspektusból tárgyalni, szükséges a társadalmi vetületét is valamilyen formában megragadni és explicitté tenni. Az aláírások kontextusában az alábbi elemek különíthetők el:



13. ábra: Az elektronikus aláírási környezet szereplői és elemei (forrás: saját ábra)

Az egyes elemek egymáshoz való viszonya vagy további tulajdonságai határozzák meg a lényeges különbségeket az egyes aláírások között.

[153] Lásd Pp. 325. § (1) a) – h)

Az értelmezési keretet az alábbi táblázat foglalja össze:

Kontextus	Aláíró	Aláírás-létrehozó adat	Tanú-sítvány	Aláírás
Osztályozási alapelv	típus	hossz tároló generálás	szabvány típus kibocsátó	megjelenítés típus alaki bizonyító erő komplexitás érvényességi idő algoritmus elhelyezkedés szerkeszthetőség implementáció

4. táblázat: Elektronikus aláírások értelmezési kerete (forrás: saját táblázat)

4.1.1. A MEGJELENÍTÉS

Az informatikai leíró nyelvek, dokumentumok formátumainak a fejlődésével egyre több helyről jelent meg az igény az elektronikus aláírások beillesztésére. A szabványosítás követte ezeket az igényeket és három különböző megjelenítésű elektronikus aláírás-típus létrehozására és használatára alakultak ki szabványok. Közös jellemzőjük, hogy mindegyik aláírás kielégíti a fokozott biztonságú elektronikus aláírásokra vonatkozó követelményeket (illetőleg a PDF szabvány fogalmazása szerint „képes kielégíteni azokat"), ebből adódóan a Rendelet ilyen irányú követelményeit is. Ennek jelentősége abban áll, hogy ahol a jogszabály „fokozott biztonságú elektronikus aláírás" létezését követeli meg, ott ezek szerint használható CAdES (CMS based Advanced Electronic Signature)[154], XAdES (XML-based based Advanced Electronic Signature)[155] és PAdES (PDF-based based Advanced Electronic Signature)[156] kódolású aláírás is. A megjelenítés tehát a kódolással szinonim fogalom ebben a kontextusban.

[154] ETSI EN 319 122-1 V1.1.1 (2016-04) és ETSI EN 319 122-2 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); Electronic Signatures and Infrastructures (ESI); CAdES digital signatures. A CMS rövidítés itt a „Cryptographic Message Syntax", kriptografikus üzenet szintaxis fogalmat jelenti, amelynek első specifikációját 1999 júniusában jelentette meg az IETF (Internet Engineering Task Force) az RFC (Request for Comments) 2630 dokumentumban.

[155] ETSI EN 319 132-1 V1.1.1 (2016-04) és ETSI EN 319 132-2 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); XAdES digital signatures. Az XML leíró nyelv első verzióját 1998 február 10-én adta ki a World Wide Web Consortium.

[156] ETSI EN 319 142-1 V1.1.1 (2016-04) és ETSI EN 319 142-2 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); PAdES digital signatures. A PDF (Portable Document Format) formátum

A PAdES szabvány a PDF dokumentumok elektronikus aláírására vonatkozóan valójában nem ad meg új eljárásokat, hanem a már ismert CMS és XML alapú megoldásokat alkalmazza PDF formátumra is, azaz egyszerűen beilleszti a már ismert formátumokat a PDF belső struktúrájába. A szabványos megjelenítés előnye az, hogy a szabvány követése esetén az aláírások teljesítik a fokozott biztonságú aláírásokkal szemben támasztott követelményeket, ennek hiányában csupán CMS, XML és PDF aláírásokról lehet szó, szemben a CAdES, XAdES és PAdES aláírásokkal.

A megjelenítés kérdéskörébe tartozhatna a konténerek[157] jellemzőinek ismertetése is, azonban ezek a képződmények olyan bonyolultságúak, amelyekre önmagában is alkalmazható a modell, ezért ezeket nem tekintjük első körben a modell részének. Más szóval a konténerben vagy a konténeren elhelyezett aláírásra értelmezhető a megjelenítési, avagy kódolási kérdés önmagában is, ezért külön értelmezhető értékkészletet nem jelent egyik potenciális dimenzió számára sem. A kérdés szemléltetéséhez egy lezárható aláírókönyben szereplő aláírt papírlapok elképzelését javasoljuk.

4.1.2. AZ ALÁÍRÁS TÍPUSA

A Rendelet az aláírásokat három típusba sorolja be: normál, fokozott biztonságú és minősített. A normál elektronikus aláírás (Rendelet 3. cikk 10. szerint) elektronikusan aláírt elektronikus dokumentumhoz aláírás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat. A fokozott biztonságú elektronikus aláírás (Rendelet 3. cikk 11. alapján) olyan elektronikus aláírás, amely alkalmas az aláíró azonosítására, egyedülállóan az aláíróhoz köthető, olyan eszközökkel hozták létre, amelyek nagy megbízhatósággal az aláíró befolyása alatt állnak, és a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhetővé válik. A minősített elektronikus aláírás (Rendelet 3. cikk 12.) pedig olyan fokozott biztonságú elektronikus aláírás, amelyet az aláíró minősített elektronikus aláírás-létrehozó eszközzel hozott létre és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

megszületését az Adobe Inc. jelentette be 1992 novemberében, az első program, amely kezelte a formátumot, 1993-ban jelent meg.

[157] ETSI EN 319 162-1 V1.1.1 (2016-04) és ETSI EN 319 162-2 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI);Associated Signature Containers (ASiC). Az aláírás-konténerek specifikációja.

Az aláírások egymás valódi részhalmazai, más szóval a legszűkebb halmaz lesz a minősített aláírások halmaza, ez valódi részhalmaza a fokozott biztonságú aláírások halmazának, amit teljes egészében tartalmaz – és még sok mást is – a normál elektronikus aláírások halmaza. Nagyon fontos következménye a definícióknak az, hogy olyan minősített tanúsítvánnyal, amelyet nem biztonságos aláírás-létrehozó eszközzel hoztak létre, nem lehetséges minősített elektronikus aláírást létrehozni. Ez azonban nem akadálya a teljes bizonyító erőnek, mint azt később látni fogjuk.

Esetenként erre a tulajdonságra az aláírás biztonságaként is szoktak utalni, amely hétköznapi értelemben helytálló lehet és a besorolások magyar fordítása is elősegítette ezt a vélekedést. A „fokozott biztonságú" angol megfelelője azonban itt az „advanced", ami információbiztonsági értelemben már nem feltétlenül utal biztonságosabb aláírásra, mivel a fejlett elektronikus aláírás tulajdonságai egyrészről az aláíró fizikai személlyel való erősebb összekapcsolhatóságra, másrészt a dokumentum sértetlenségével való összefüggésére vonatkoznak – azaz az aláíró és a tartalom hitelességére. A hitelesség azonban csak az egyik biztonsági követelmény és a minősített aláírásnál is létezhet magasabb szintű biztonsággal létrehozható aláírás. Ugyanis elképzelhető olyan aláírás, amelynek a biztonsági szintje magasabb (biztonságosabb környezetben és biztonságosabb eljárással hozták létre), de betű szerinti értelemben mégsem lehet például minősített ez az elektronikus aláírás, mert nem teljesíti a minősített aláírás követelményeit (például nem egy tanúsított eszközön hozták létre vagy nem nyilvános szolgáltató által kibocsátott tanúsítványon alapul). Kérdésként vetődik fel továbbá a nyílt forráskóddal készített PGP-alapú elektronikus aláírások[158] besorolhatósága a fokozott biztonságú elektronikus aláírások körébe, amelyeknél az aláírás készítésének a biztonsága és algoritmus-készlete teljes mértékben azonos lehet a nyilvános szolgáltatók által kibocsátott tanúsítványokon alapuló aláírásokéval, eltérés a tanúsítvány és az aláíró közötti kapcsolat hitelességében van csupán. Észrevehető a párhuzam a III. Béla király idejében – 13. században – megerősödő – és a 19. században megszűnő – hiteleshelyek[55] és a nyilvános bizalmi szolgáltatók funkcionalitása között, mindkettőt azért hozta létre a társadalom, hogy a széles körben elfogadni kívánt dokumentumokat egy olyan központi hatalom ellenőrizze, amelyben – illetve a tevékenysége eredményének felhasználhatóságában – minden szereplő megbízik. Mivel a minősített aláírásnak két olyan feltétele van, amelyek megjelennek más dimenziókban is (tanúsított

[158] http://openpgp.org/

aláírás- vagy bélyegző-létrehozó eszköz, illetve minősített aláíró vagy bélyegző tanúsítvány), meg kell fontolni ezek szerepeltetésének a helyét, hiszen a definícióból adódóan a következő két fogalom ekvivalens:

1. „olyan fokozott biztonságú elektronikus aláírás/bélyegző, amelyet minősített aláírás/bélyegző-létrehozó eszközön hoztak létre és amelynek az aláírás/bélyegző-létrehozó adatához minősített tanúsítvány kapcsolódik”

2. „minősített elektronikus aláírás/bélyegző”

4.1.3. ALAKI BIZONYÍTÓ ERŐ

Az elektronikus aláírások bizonyító erejét tekintve kizárólag az alaki bizonyító erővel lehetséges az aláírások tulajdonságainál foglalkozni, hiszen az anyagi bizonyító erőről az aláírás információt általánosságban nem tartalmazhat[159]. Egy elektronikus aláírás elkészítésének nem kötelező előfeltétele az aláírni kívánt dokumentum megnyitása, elolvasása, ezért vizsgálatomnak az alaki bizonyító erőre való korlátozását indokoltnak véltem. Az alaki bizonyító erőre általános szabályt a Rendelet fogalmaz meg, két esetben. Egyrészről az elfogadás meg nem tagadhatósága elv miatt minden egyes elektronikus aláírást megillet a bizonyítékként való felhasználás vélelme (Rendelet 25. cikk (1) bek.), másrészről a minősített elektronikus aláírás kézírással való egyenértékű elfogadása vált kötelezővé (Rendelet 25. cikk (2) bek.) az Európai Unióban (Rendelet 25. cikk (3) bek.).

Az írásbeliség tekintetében az Eat. korábban megfogalmazta, hogy írásbelinek kell tekinteni egy elektronikus dokumentumot, ha azt legalább fokozott biztonságú aláírással látták el (Eat. 4. § (1)), ez a vélelem azonban az Eat. hatályvesztésével expressis verbis kikerült a magyar jogrendből és máshol sem jelent meg. A Polgári Törvénykönyv (Ptk.)[160] írásbeliségre vonatkozó szabályait értelmezve (6:7. §) azt kapjuk, hogy írásbelinek azt kell tekinteni általánosságban, amit a felek aláírtak, azaz aláírásukkal láttak el. Ezt összevetve a Rendelet elektronikus aláírás definíciójával (aláírás az, amit a természetes személy aláíró aláírásra használ), azt kapjuk, hogy elektronikus írásbeliség feltétele az elektronikus aláírás megléte minden érintett fél részéről, az aláírásra nézve

[159] Az Új Polgári Perrendtartás Koncepciója. A Kormány 2015. január 14. napján megtartott ülésén elfogadott Koncepció. 2015. 92-93.old.
[160] 2013. évi V. törvény a Polgári Törvénykönyvről. A törvényt az Országgyűlés a 2013. február 11-i ülésnapján fogadta el. A kihirdetés napja: 2013. február 26. A hatálybalépésével összefüggő átmeneti és felhatalmazó rendelkezésekről lásd a 2013. évi CLXXVII. törvényt.

minden további korlátozás nélkül. Ez túl tág teret biztosítana az írásbeli formáknak és a velük szembeni visszaéléseknek, mivel egy normál elektronikus aláírás nem biztosít elegendő védelmet a hamisíthatóság ellen. Egy normál elektronikus aláírás (példának okáért egy szkennelt aláírás képe vagy egy e-mail végére gépelt név) nagyon könnyen lemásolható vagy teljes egyezőséggel reprodukálható, és felhasználható az érintett tudta nélkül olyan dokumentumokon, amelyeket az érintett nem is látott, emiatt a Ptk. 6:7. (3) bekezdésére vonatkozó kommentár szerint az itt megfogalmazott elvárásoknak minden kétséget kizáróan csak a legalább fokozott biztonságú (illetve a fokozott biztonságú aláírással szemben támasztott követelményeket teljesítő) elektronikus aláírás képes megfelelni. Az írásbeliség vélelmét minden normál elektronikus aláíráshoz hozzáfűzni jogi szempontból logikailag rendben lévőnek tűnik, ha társadalmi szempontból problémás is lenne, hiszen teljes bizonyító erő hiányában az aláírás létrejöttét állító félnek kellene igazolnia vitás esetekben azt, hogy az aláírás minden érintett fél részéről valóban megtörtént, ellenkező esetben az aláíráshoz fűződő kötelmi vélelem megdöntése valószínűsíthető. Mivel a gyakorlatban az ilyen esetek száma idáig meglehetősen alacsony volt, nem lehet előrejelzést adni arra nézve, hogy a normál elektronikus aláírással ellátott dokumentumok írásbeliségének hamis vélelmezéséből adódó peres ügyek mekkora terhet jelentenek majd az ítélkezésben, ez nyilvánvaló módon függ majd a hamisítások mértékétől. Egyes jogszabályhelyek külön nevesítik a fokozott biztonságú elektronikus aláírás szükségességét, mint alaki kelléket[161], ebből azonban nem következik, hogy csak a fokozott biztonságú elektronikus aláírással ellátott dokumentum lehet írásbeli [129]: 200.

Az okiratiság fontos szerepet tölt be a bírósági eljárásokban, két okból. Egyrészről az 1952. évi III. törvény a polgári perrendtartásról (Pp1952.)[162] – illetve 2018. január 1-től a 2016. évi CXXX. törvény a polgári perrendtartásról (Pp2018.)[163] kimondja, hogy ha a tényállás okirattal bizonyítható, akkor a bíróság az egyéb bizonyítást mellőzheti (Pp1952. 192. §, Pp2018. 320. § (5)), másrészről a bizonyítási teher alól mentesül az a fél, aki – az ellenkező bebizonyításáig – teljes bizonyító erejű magán- (Pp1952. 196. §

[161] 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (Hpt.) 279. § (1)
[162] 1952. évi III. törvény a polgári perrendtartásról. A kihirdetés napja: 1952. június 6. A hatálybalépés napja: 1953. január 1. A Magyar Közlöny 1952. évi december 28-i számában közzétett helyesbítésnek megfelelő szöveget tartalmazta ez a változat. A törvényt a 2016. CXXX. törvény 633. §-a hatályon kívül helyezte 2018. január 1. napjával.
[163] 2016. évi CXXX. törvény a polgári perrendtartásról. A törvényt az Országgyűlés a 2016. november 22-i ülésnapján fogadta el. A kihirdetés napja: 2016. december 2.

(1), Pp2018. 325. § (3)) vagy közokirattal (Pp1952. 195. § (7), Pp2018. 323. § (2)) tudja igazolni a tényállást. A teljes bizonyító erő vélelmezésében tehát az elektronikus aláírások fontos szerepet kaptak, magánokiratok vonatkozásában a Pp1952. 196. §, illetve a Pp2018. 325. §, a közokiratok terén pedig a Pp1952.195. §, illetve a Pp2018. 323. § rendelkezik azokról az alaki követelményekről, amelyeket ezeknek az okiratoknak teljesíteniük kell.

4.1.4. A KOMPLEXITÁS

Az egyes aláírások komplexitásának belső szerkezetét a vonatkozó szabványok pontosan specifikálják. Az alap aláírások (AdES-BES[164], AdES-EPES[165]) létrehozása nagyon könnyű, viszont a hosszú távú érvényességükkel probléma van, mivel hiteles időbélyeg hiányában az ellenőrzés mindig csak az aktuális pillanatra vonatkozóan végezhető el, nem pedig az aláírás pillanatára. Az időbélyegzett aláírások (AdES-T[166]) alkalmazása hiteles idő beépítésével és a hitelesség megváltozásának detektálhatóságával már lehetővé teszi az aláírás ellenőrzését bármelyik későbbi időpontban az aláírás létrehozásának idejére, de ha az érvényességi adatok időközben elérhetetlenné váltak (vagy felülíródtak), az ellenőrzés nem végezhető el, vagy igen körülményessé válhat. A komplex aláírások (AdES-C[167]) alkalmazása – akár az aláíró, akár az ellenőrző készíti azt el – megoldja a „hol vannak az akkori érvényességi adatok most” kérdését, azonban a letölthetőségtől függhet az ellenőrzés elvégezhetősége. Ezen a problémán segít a kiterjesztett aláírások (AdES-X, AdES-X-Long[168]) alkalmazása, amelyek az érvényességi adatokat hozzácsatolják az aláírásokhoz. Az archív aláírások (AdES-A[169]) létrejötte megteremtette az aláírások érvényességének hosszú ideig történő fenntarthatóságát – bizonyos korlátokkal, de a többszörös archív aláírások kezelését még nem biztosította. A hosszú távon érvényes aláírások (AdES-LT, AdES-LTV[170]) létjogosultságát az adja, hogy

[164] AdES-BES: Advanced Electronic Signature: Basic Electronic Signature (Fokozott biztonságú elektronikus aláírás: alap elektronikus aláírás)
[165] AdES-EPES: Advanced Electronic Signature: Extended Policy based Electronic Signature (Fokozott biztonságú elektronikus aláírás: kifejezett hitelesítési rend alapú elektronikus aláírás)
[166] AdES-T: Advanced Electronic Signature: Timestamped Electronic Signature (Fokozott biztonságú elektronikus aláírás: időbélyegzett elektronikus aláírás)
[167] AdES-C: Advanced Electronic Signature: Complex Electronic Signature (Fokozott biztonságú elektronikus aláírás: komplex elektronikus aláírás)
[168] AdES-X(-Long): Advanced Electronic Signature: Extended (Long) Electronic Signature (Fokozott biztonságú elektronikus aláírás: kiterjesztett (hosszú) elektronikus aláírás)
[169] AdES-A: Advanced Electronic Signature: Archive Electronic Signature (Fokozott biztonságú elektronikus aláírás: archív elektronikus aláírás)
[170] AdES-LT(V): Advanced Electronic Signature: Electronic Signature with Long Term (Validity) (Fokozott biztonságú elektronikus aláírás: hosszú távú (-on érvényes) elektronikus aláírás)

bármilyen korábbi aláírást – az érvényességi adatok rendelkezésre állása esetén – képesek folyamatosan hitelessé tenni sok-sok éven keresztül is[171].

Az egyes aláírások részletes leírását – tekintettel arra, hogy ezek implementációja függ a megjelenítéstől, a már említett szabványok (CAdES, XAdES, PAdES) részletezik, alap (B) és kiterjesztett (E) szinten[172].

4.1.5. AZ ÉRVÉNYESSÉGI IDŐ

Az aláírások érvényességi ideje alatt azt az időtartamot értjük, amely alatt az aláírásban megtett kötelezettség felvállalásáról az aláírás ellenőrzésével kell meggyőződni, más szóval eddig kell biztosítani az aláírás hitelesíthetőségét, hitelességét. Valójában itt a hiteles archiválás kérdéskörét kell figyelembe venni, ami kicsit több, mint egy egyszerű lemásolás és megőrzés. Ugyanis megőrzés közben a meg nem változás folyamatos detektálhatóságát is biztosítani kell egy hiteles archiválás során. Ezért – felhasználva a digitális archiválásról szóló rendeletben (ITM.R)[173] foglaltakat, az aláírásokat ebből a szempontból három csoportra oszthatjuk fel: azonnali, rövid távú és hosszú távú érvényességi időt megkövetelő aláírások. Az ITM.R nem terjedt ki az állami vagy helyi önkormányzati feladatot, vagy jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy által végzett elektronikus archiválásra (ITM.R 1. § (2)), az ilyen szerveknek az Eübszt-ben foglaltak alapján kell eljárniuk (pl. minősített archiválás-szolgáltatás vagy elektronikus dokumentumtárolás szolgáltatás igénybevételével). Az egyes aláírás-csoportok főbb jellemzői az alábbiak:

1. Az azonnali felhasználásra készített aláírások esetében az aláírást a létrehozásához képest közeli időpontban (percek, esetleg néhány óra múlva) használják fel, vagyis ellenőrzik a megfelelőségét az aláírt tartalom feldolgozása előtt, és a folyamatban többé nem lesz szükség az aláírás újbóli ellenőrzésére. Kétség vagy biztonsági kérdés esetén az ellenőrzéskor megőrzött audit-nyomokat használhatják fel bizonyítékként. Ez a megoldás implicit módon biztosítja a hitelesség megőrzését. Tipikusan ilyen aláírások lehetnek az „egyszer használatos” kriptográfiai magánkulccsal

[171] A hosszú távon érvényes aláírások első specifikációját 2000. decemberében adta meg az ETSI TS 101 733, amelyet 2001. szeptemberében követett az RFC 3126 is, technikailag ekvivalens specifikációval.
[172] Lásd az EU tematikus weboldalát: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-Signature+standards (2019. március 7).
[173] A digitális archiválásra vonatkozó előírásokat 2007-ben fektette le a 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól, amelyet 2018. július 1-től felváltott az 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól.

készített aláírások, amelyek az aláírás elkészítését és azonnali felhasználását követően rögtön elveszítik az érvényességüket.

2. A rövid távú érvényességnek az a tulajdonsága, hogy az aláírást elkészítik, felhasználják, de a felhasználás alapjául szolgáló bizonylatot itt már meg kell őrizni egy bizonyos, előre meghatározott ideig (pl. pár napig, hétig, hónapig, vagy évig). Hét év Magyarországon a legtöbb számviteli bizonylatra elegendő időintervallum, ami meghosszabbítható az utolsó évben megindított külső vizsgálat esetében is. Különbség az előző ponthoz képest, hogy itt az aláírás hitelességét (sértetlenségét és az aláíró tanúsítvány adatait) a megőrzési idő végéig lehetséges ellenőrizni, mert az aláírás érvényességi időtartamán belüli ellenőrzéshez minden szükséges adat hitelesen a rendelkezésre áll az aláírás részeként. Ez a megoldás passzív módon biztosítja a hitelesség megőrizhetőségét.

3. A hosszú távon érvényes aláírásokat több évtizedig meg kell tudni hitelesen őrizni, függetlenül a készítés eszközeitől és technológiájától. Ilyen lehet például egy elektronikus anyakönyvi kivonat vagy halotti bizonyítvány, egy közjegyzői közokirat, esetleg egy banki folyószámla- vagy hitelszerződés is. A megőrzési idő lehet előre definiált (például 20 év, 35 év, 50 év, 60, 100 év), de lehet előre meg nem határozott is (folyószámla megszűnését követő 10 év, elhalálozást követő 25 év). Különbség a rövid távú érvényességhez képest, hogy az őrzés során aktív tevékenységekkel biztosítják a hitelességet, ezért ez a módszer egy esetleges algoritmus-kompromittálódás esetén is alkalmas a hitelesség fenntartására és folyamatos megőrzésére.

Lehetséges gazdálkodó szervezetek számára, hogy a rövid távú érvényességgel rendelkező aláírásaikat és kapcsolódó dokumentumaikat több éven át egyszerűen megőrizzék. Ezt az időtartamot a GKM rendelet 4. § (3) és (4) pontjai 11 évben határozták meg, 11 évnél rövidebb időre a minősített időbélyegzőt is elégségesnek definiálta a rendelet, míg az ettől hosszabb ideig hitelesen megőrizni kívánt elektronikus aláírásokhoz be kell szerezni minden érvényességi adatot és minősített időbélyegzőt kell elhelyezni ezeken az adatokon – azaz egy archív aláírássá egészíti ki a dokumentumon lévő tetszőleges aláírást. A legutolsó műveletet itt meg kellett ismételni minden olyan eset előtt, amikor az archív időbélyegző algoritmusa kompromittálódik. Tekintettel arra, hogy Magyarországon a gyakorlatban használt algoritmusok nagy része (RSA, ECC) nem kvantumbiztos (quantum-safe) algoritmus [56], a jogszabályban rögzített 11 év

technológiai szempontból alátámaszthatatlanná vált a legtöbb akkor használt algoritmus esetében[174], így ki is került a frissített rendeletből. A megőrzés követelményeinek általánosítása természetesen megmaradt, a megőrzés során olyan módszereket kell továbbra is alkalmazni, amely védi az elektronikus dokumentumot a törlés, a megsemmisítés, a véletlen megsemmisülés, az utólagos módosítás és sérülés, valamint a jogosulatlan hozzáférés ellen[175]. Ebből adódik, hogy az algoritmusok jelenkori megfelelőségéből nem következik automatikusan azok jövőbeli megfelelősége és a hosszú távú használat biztosításához aktív tevékenységek lehetnek szükségesek az érvényességi időn belül, annak hosszától függően.

4.1.6. A TANÚSÍTVÁNY SZABVÁNYA

Elektronikus aláírás tanúsítványa alatt a Rendelet olyan elektronikus igazolást ért, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez (név vagy álnév) kapcsolja. Az aszimmetrikus kriptográfián alapuló digitális aláírás[176] területén két technológia terjedt el a világon, az egyik a PGP (Pretty Good Privacy), a másik az X.509, a korán felismert problémák ellenére[177]. Egy PGP „tanúsítványt" az alábbiakról lehet felismerni – az idézőjelet indokolja, hogy itt más értelemben beszélhetünk tanúsítványról, mint az X.509 világban, inkább csak nyilvános kulcsok tartójáról érdemes beszélni, hiszen más elemekkel nem igazán rendelkezik egy PGP nyilvános kulcsfájl:

14. ábra: PGP nyilvános kulcs blokkja (forrás: saját ábra)

[174] ETSI TS 119 312 V1.1.1 (2014-11); Technical Specification, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, Table 12.
[175] ITM.R 3.§ (1)
[176] Az aláírás létezését megalapozó cikket 1976-ban publikálta Bailey Whitfield Diffie és Martin Edward Hellman [20].
[177] A problémák megfogalmazását lásd Carl Ellison és Bruce Schneier méltán elhíresült cikkében [5], amelyben tíz olyan kockázatát fejtik ki a nyilvános kulcsú infrastruktúráknak, amelyre kevés figyelmet fordítottak vagy túlzott elvárások öveztek abban az időben.

A PGP kulcsokhoz is tartozik vagy tartozhat számos attribútum, mint például az alany neve, a nyilvános kulcs numerikus értéke, a kulcshasználat megjelölése (leggyakrabban aláírás, titkosítás vagy hitelesítés), a kulcsgeneráláshoz felhasznált algoritmus (például RSA, ECC, El Gamal DSA) és a lejárat dátuma. Ezeket a tulajdonságokat a kulcs létrehozója állítja be a generálás folyamán, ezért ezeket nem tanúsítja külső független harmadik fél, minden érintett fél vagy megbízik vagy nem bízik meg az adatok megfelelőségében, a digitális aláírás technológiai ellenőrzésén túl.

```
$ pgp -kvc epm@idoertek.eu
pub   2048R/6CEA0830 2016-05-09 [expires: 2026-05-04]
      Key fingerprint = 94DA DBDA 66F4 EB01 578F  F070 0EC1 274B 6CEA 0830
uid                  Péter Máté, Erdősi CISA (managing director) <epm@idoertek.eu>
sub   2048R/BF6803E7 2016-05-09

$ pgp -ke epm@idoertek.eu
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

pub  2048R/6CEA0830  created: 2016-05-09  expires: 2026-05-04  usage: SC
                     trust: ultimate      validity: unknown
sub  2048R/BF6803E7  created: 2016-05-09  expires: never       usage: E
[ unknown] (1). Péter Máté, Erdősi CISA (managing director) <epm@idoertek.eu>
```

15. ábra: PGP nyilvános kulcs attribútumai konzolon (forrás: saját ábra)

A fenti példából azt lehet kiolvasni, hogy ez egy nyilvános kulcs („pub”), a kulcs hossza 2048 bit („2048”), a használt algoritmus az RSA („R”), a kulcsot egyedileg azonosító számsor a „6CEA0830” és az ujjlenyomata („fingerprint”), a kulcsot 2016 május 9-én generálták és elfogadták teljes mértékben megbízható kulcsnak („ultimate”), a kulcs lejár 2026 május 4-én, a tulajdonos azonosító adatai („uid”) a név, a beosztás és az e-mail cím, továbbá egy alkulcs tartozik hozzá, amit ugyanazon a napon generáltak, szintén RSA algoritmussal és 2048 bites hosszúsággal hozták létre. A kulcshasználat az első kulcs esetében aláírás („S”) és a tulajdonos tanúsítása („C”), a második kulcs a titkosító kulcs („E”).

Stallings az alábbi négy szolgáltatást írta le a PGP vonatkozásában[57]:

- digitális aláírás
- üzenet titkosítása
- tömörítés

- e-mail kompatibilitás (bináris adatok radix-64 konverziója ASCII karakterekre)

Itt sem találhatunk olyan értelemben vett tanúsítvány-kibocsátást, mint az X.509 világban, azaz a PGP kulcsok attribútumait nem hitelesíti erre akkreditált harmadik fél, a bizalom mértéke az adott kulcs elfogadóinak számosságával függ össze. Mivel a PGP kulcsok és tulajdonságaik (mint PGP-tanúsítvány) és az X.509 tanúsítványok mezői között (mint X.509 tanúsítvány) meglehetősen nagy átfedés mutatkozik, indokolt ezt a két formát, mint tanúsítványformátumot külön-külön is kiemelni. Az ezekhez tartozó tanúsítványok tartalmát a vonatkozó szabványok részletezik:

1. RFC 2440 OpenPGP Message Format[178]
2. ITU-T X.509 Recommendation[179]

Ezeken túlmenően nem szabványos megoldások is létrejöhetnek a technológia-semlegesség miatt, nem törvényszerű, hogy csak aszimmetrikus kriptográfián alapuló digitális aláírásokhoz létezhet tanúsítvány. Létezik attribútum-tanúsítvány is, amely nem egy nyilvános kulcsot kapcsol valamely entitáshoz, hanem egy tulajdonságot (pl. közjegyző, ügyvéd, oktatási alkalmazott, aláírásra jogosult, kiadmányozásra jogosult). Ennek tisztázása segíthet az esetenként zavaros helyzetet egységesítő állásfoglalások elkerülésében vagy annak értelmezésében is[180]. Az attribútum-tanúsítványok kapcsolhatók a fizikai entitáshoz és annak aláíró vagy bélyegző tanúsítványához is.

Lehetségesnek látszik például biometrikus aláíráshoz is tanúsítványt generálni vagy az is megengedett, hogy egy-egy aláíráshoz, akár fokozott biztonságú aláíráshoz, ne is létezzen tanúsítvány. Azaz eltérően a hétköznapi gyakorlattól, elméletileg nem következik a Rendelet definíciójából, hogy minden egyes aláírás-létrehozó adathoz tartozó aláírás-ellenőrző adatot tanúsítványba kellene foglalni. A technológiai biztonságra alapozott bizalom azonban erősíti a bizalmi szolgáltatók pozícióját, hiszen

[178] Jon Callas, Lutz Donnerhacke, Hal Finney, Rodney Thayer: Request for Comments: OpenPGP Message Format, RFC 2440, November 1998.
[179] International Telecommunication Union, Telecommunication Standardization Sector of ITU: ITU-T X.509, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory. Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks. ITU-T Recommendation X.509. 10/2016.
[180] A Kúria (KMPJE) 1/2019. számon adott ki egy jogegységi határozatot az „aláírás-gate” ügy kapcsán (https://kuria-birosag.hu/hu/print/joghat/12019-szamu-kmpje-hatarozat).

megbízható harmadik félként kötelesek ellenőrizni az alany minden olyan tulajdonságát – az álnév kivételével, amit a tanúsítványba belefoglalnak.

4.1.7. A TANÚSÍTVÁNY TÍPUSA

A tanúsítványok típusait az eIDAS Rendelet két kategóriába sorolja (minősített és nem minősített), ezen kívül lehetőség van tanúsítvány nélkül is aláírást készíteni, hiszen az elektronikus aláírás készítésének a tanúsítvány létezése nem nélkülözhetetlen előfeltétele. Az elektronikus aláírás minősített tanúsítványa (Rendelet 3. cikk 15. definíció szerint) a Rendelet I. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített szolgáltató bocsátott ki. Az elektronikus aláírás nem minősített tanúsítványa (Rendelet 3. cikk 14. definíció alapján) olyan elektronikus igazolás, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja, és igazolja legalább az érintett személy nevét vagy álnevét. Ahogyan említettük, a Rendelet megkülönbözteti a magánszemély aláírókat a jogi személy bélyegzőktől, ezért ez a megkülönböztetés a definíciókban is megjelent. Az elektronikus bélyegző tanúsítványa olyan elektronikus tanúsítvány, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét (Rendelet 3. cikk 29. definíció szerint), illetve az elektronikus bélyegző minősített tanúsítványa alatt elektronikus bélyegző olyan tanúsítványát kell érteni, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a Rendelet III. mellékletében megállapított követelményeknek (Rendelet 3. cikk 30. definíció alapján).

Továbbá az is lehetséges, hogy nincs tanúsítvány, mivel az aláírás-ellenőrző adatot nem foglalják semmilyen tanúsítványba (ettől függetlenül továbbítható formában létrejöhet, ahogyan azt a PGP kulcsblokknál is láthattuk), vagy pedig nincs is olyan értelemben vett aláírás-létrehozó adat, mint egy aszimmetrikus kriptográfiai kulcs.

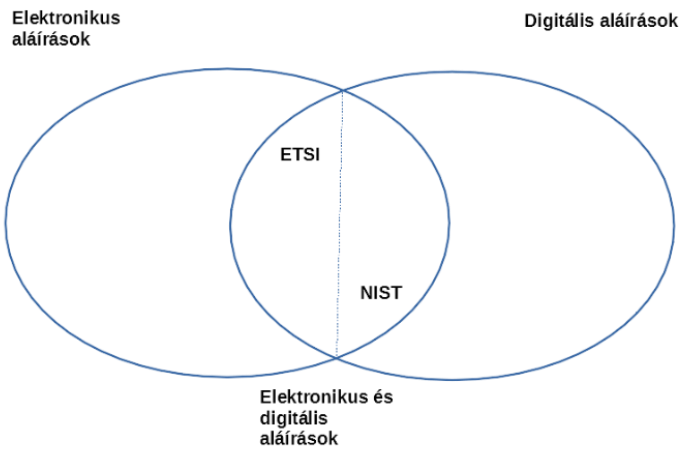
Itt altípusként – vagy különálló dimenziókánt – létrejöhet a magyar közigazgatási tanúsítvány is, amelyből szintén lehetséges minősített és nem minősített aláírás és bélyegző tanúsítványok kibocsátása is, amennyiben a kibocsátó megfelel a vonatkozó előírásoknak.

4.1.8. AZ ALÁÍRÓ KILÉTE

Amennyiben az „aláírás” fogalmát a Rendelet szerint értelmezzük, az „aláíró” fogalmát is ennek megfelelően kell definiálni, a közöttük lévő konzisztencia megtartása

miatt. Itt is megjelenik az, hogy a digitális aláírás elkészítői nem feltétlenül lesznek az elektronikus dokumentum aláírói, különösen az Európai Unióban. Hozzá kell tennem, hogy az aláírók kilétének differenciált megjelenítése nem fogja befolyásolni a modell használhatóságát azokban az országokban, ahol ez nem válik szét ennyire élesen, mint az EU-ban, azonban a differenciálatlanság a modell használhatatlanságát eredményezné ott, ahol ezek szétválasztása jogszabályban rögzített követelmény.

Az aláíróknál egyrészről különbséget kell tenni a végfelhasználói és a szolgáltatói aláírók között, mivel más-más követelmények vonatkoznak az aláírás-létrehozó adatok védelmére, tulajdonságaira és felhasználhatóságukra. A végfelhasználók típusaihoz a személyek aláíró tanúsítványait lehet hozzárendelni, mint például természetes személy, jogi személy természetes személy képviselője, kód-aláírást vagy gépi aláírást elrendelő személy. A szolgáltatói aláírók kapcsán lehetséges beszélni gyökér hitelesítés-szolgáltatóról, köztes hitelesítés-szolgáltatóról, időbélyeg-szolgáltatóról, archiválás-szolgáltatóról és online tanúsítvány állapot szolgáltatóról egyaránt, mind különböző kulcsokat használhatnak a digitális aláírásaik elkészítéséhez. A Rendelet értelmezésében azonban a szolgáltatói digitális aláírások nem lesznek egyben elektronikus aláírások is, hiszen nem természetes személy készítette el az adott digitális aláírást. Ez átrendezte definíciós szinten az aláírásokat az addigi helyzethez képest. Korábban ugyanis minden digitális aláírás egyben elektronikus aláírás is volt, azonban a bélyegzők bevezetésével ez a helyzet megváltozott. A változást a következő ábra szemlélteti.



16. ábra: Elektronikus és digitális aláírások viszonyrendszere (forrás: saját ábra)

Elektronikus aláírás tehát csak a természetes személy által készített aláírás lehet az Európai Unióban, míg digitális aláírás alatt csak kriptográfiai transzformációval létrejött adatsorozatot értenek a NIST szabvány alapján, függetlenül az aláíró kilététől. A metszetben sem egyeznek meg a szabványok, míg az ETSI szabvány megenged kriptográfiai transzformáció nélküli digitális aláírást is, addig ez a tengerentúlon elképzelhetetlen. Ráadásul a két ellipszisen kívül is létezhetnek aláírások teoretikusan, például amelyeket jogi személyek hoznának létre, kriptográfiai transzformációt nem felhasználva. A jogi személyek digitális aláírásai pedig nem lesznek elektronikus aláírások innentől kezdve a Rendelet szerint. Az Egyesült Államokban a személy (person) értelmezése sokkalta tágabb, bele kell érteni a természetes személyeket, a jogi személyeket, a kormányzati szervezeteket, társulásokat, egyszóval minden olyan entitást, amely képes akaratot kifejezni aláírási célból[181]. Az európai definíciónak meg lehet azonban feleltetni minden entitást, hiszen a Rendelet a „jogi személy" terminust használja, de a preambulum (68) szakaszában kifejti, hogy *„„jogi személynek" minősül jogi formájától függetlenül minden olyan szervezet, amelyet valamely tagállam jogszabályai alapján hoztak létre, vagy amelynek tekintetében valamely tagállam joga az irányadó."*

A végfelhasználói aláírásokat meg kell különböztetni tehát aszerint, hogy magánszemély vagy jogi személy az aláíró, a Rendelet szellemének megfelelően, ha olyan modellt szeretnénk definiálni, amely használható az Európai Unióban is. A bélyegzők és aláírások közötti különbséget ebben a dimenzióban fogjuk megjeleníteni.

4.1.9. AZ ALÁÍRÓ ALGORITMUS

Az aláíró algoritmusok tekintetében Európában mértékadó szabványnak az aláíró algoritmus-készletekre vonatkozó ETSI TS 119 312 szabványt[182] kell tekinteni. Elméletileg lehetséges választani szimmetrikus kriptográfiát is (pl. Advanced Encryption Standard – AES, Triple-DES Encryption Algorithm – TDEA, Escrowed Encryption Standard – EES, Secure Hash Standard – SHS illetve Hashed Message Authentication

[181] Lásd General Services Administration (GSA)and Federal Chief Information Officers (CIO) Council: USE OF ELECTRONIC SIGNATURES IN FEDERAL ORGANIZATION TRANSACTIONS, Version 1.0, January 25, 2013. 47. old.
[182] ETSI TS 119 312 V1.2.2 (2018-09). Technical Specification. Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

Code – HMAC), vagy aszimmetrikus kriptográfiát (például RSA[183], DSS[184] és ECDSA különböző változatait)[185]. Az aláíró-algoritmus készletek minden olyan algoritmust tartalmaznak, ami az aláírás létrehozásához a gyakorlatban szükséges, ideértve az üzenet kódolásához használt algoritmust vagy hash-függvényt és magát az aláíró algoritmust. Az aláírás-készleteket meg kell különböztetni az aláírási sémáktól, mert a sémák kizárólag az aláírás-oldali algoritmusokkal foglalkoznak – kulcsgenerálás, aláírás-létrehozás és aláírás-ellenőrzés – és nem érintik az aláírandó dokumentumokat. Az aláíró algoritmus bemenete a gyakorlatban nem a dokumentum lesz, hanem a dokumentumból képzett rövid kivonat (hash), amelynek a bemenete a tényleges dokumentum. A hash-függvény köti tehát össze a dokumentumot és az aláírást[186]. A specifikált algoritmusok a kor adott műszaki fejlettségének megfelelően változhatnak, a digitális aláírásoknak létezhet kvantumkriptográfiai verziójuk is[187]. A kvantum-kriptográfia első elméleti megjelenését Bennett és Brassard az 1970-es évekre teszi és Wiesner 1983-ig nem publikált szemináriumi jegyzetét értik alatta [120]. A témában az első érdemi beszámolók megjelenését Bennett és Brassard a második CRYPTO konferenciára, 1983-ra tették, ezzel az elméleti kutatások elkezdődtek. Körülbelül két évtizeddel később a kvantum-kriptográfia gyakorlatban történő megjelenése után a terület első nemzetközi konferenciáját a Leuveni Katolikus Egyetemen rendezték 2006-ban, ezt követően elindultak olyan kutatások is, amelyek a megfelelően biztonságos algoritmusok megtalálását és specifikálását tűzték ki célul a kvantumszámítógépek megjelenését követő időszakban [61]. A munkát az Európai Unió [63] és az európai szabványosító testület is élénk figyelemmel és jelentős aktivitással kíséri [62], illetve természetesen a az amerikai szabványosító hivatal is foglalkozik részleteiben a problémakörrel [64].

[183] Az első ilyen algoritmusról szóló elméleti jelentőségű cikk 1976-ban [20], míg az első gyakorlati jelentőséggel is bíró publikáció 1978-ban jelent meg [24].
[184] Az első digitális aláírásról szóló NIST FIPS 186 szabványt 1994. május 19-én publikálták.
[185] Az algoritmusok közötti különbségeket Bruce Schneier tematikusan foglalta össze a használat és a matematikai háttér aspektusaiból a kriptográfiáról szóló monográfiájában, a 10. és 11. fejezetben ([59]).
[186] Elméletileg végtelen sok olyan bitsorozat létezhet, amelynek ugyanaz a hash-értéke (mivel a kivonat függvénynek az értelmezési tartománya a bináris számok megszámlálhatóan végtelen halmaza, értékkészlete pedig egy véges számtartomány, következésképpen szükségszerűnek kell lennie, hogy egy vagy több hash-érték végtelen sokszor szerepeljen, ha a szigorú lavina- és bit függetlenségi kritériumok teljesülnek [98], mivel ekkor nem várható kitüntetett hash-osztály létezése. Az összes bitsorozat értelmezhetősége tehát nem feltétele az aláírás matematikai megfelelőségének, de a hétköznapi alkalmazások során nem tudunk mit kezdeni egy értelmezhetetlen bitsorozattal („ákombákom”), hiába lesz helyes az aláírás rajta emiatt lesz használható a gyakorlatban mégis a kivonatolás.
[187] Lásd Gottesman és Chuang preprint cikkét, amelyben elsőként adtak meg egy digitális aláírási protokollt kvantumkriptográfiai alapokon [60].

4.1.10. AZ ALÁÍRÁS-LÉTREHOZÓ ADAT HOSSZA

Az aláírás-létrehozó adatok hossza és a biztonság között esetenként jelentős összefüggés található – de ez nem automatikus, ami az algoritmusok matematikai hátteréből adódik. A gyakorlatban olyan algoritmusok terjedtek el, amelyek biztonsága jellemzően a faktorizáció nehézségétől (vagyis egy megfelelően nagy szám szorzótényezőkre bontásának gyakorlati műveleti igényétől) függ, amennyiben az implementáció korrekt. Ha a műveletek alapjául szolgáló számokat megfelelően – például valódi véletlen prímként – választják meg és azok további követelményeknek is megfelelnek (pl. megfelelő távolság), akkor az algoritmus biztonsága gyakorlatilag megfelelőnek mondható Ez azt jelenti, hogy ezeknek az algoritmusoknak a törhetetlenségét elméletben nem sikerült idáig bebizonyítani, mégis azért lettek alkalmazva széles körben, mert idáig sikerült meggyőzni az alkalmazói kört arról, hogy a feltörés műveletigénye meghaladja a rendelkezésre álló kapacitásainkat. Ezek a megfelelőségek a számítási kapacitások fejlődésével (Moore tapasztalati törvényét idézhetnénk erre [65]) természetszerűleg folyamatosan avulnak, mivel mindig más számít „nehéz” problémának a gyakorlatban attól függően, hogy mekkora a hozzáférhető elvi és gyakorlati számítási kapacitás. A széles körben használható kvantumszámítógép megjelenésével az algoritmusok megbízhatósága lényegesen át fog alakulni, ahogyan ezt az alábbi táblázat is szemlélteti:

Algoritmus	**Kriptográfia típusa**	**Hatás**
AES	szimmetrikus	növelni szükséges a kulcsméretet
RSA	aszimmetrikus	többé nem biztonságos
ECDSA, ECDH	aszimmetrikus	többé nem biztonságos
DSA	aszimmetrikus	többé nem biztonságos

17. ábra: Algoritmusok megbízhatósága kvantumszámítógépen (készült: [63] 2.1 ábrája alapján)

A kvantumszámítógépek azonban nem fogják teljesen megváltoztatni a jelenlegi kriptográfiát, lévén ma sem csupán elméletileg bizonyítottan biztonságos algoritmusokat használunk, hanem a gyakorlatban feltörhetetlennek vélt módszerek is jelen vannak a mindennapjainkban. A mai algoritmusokkal szemben sem elvárás az, hogy elméletileg

biztonságosak legyenek, hanem csupán annyi, hogy a gyakorlatban megfelelő biztonsággal alkalmazható eljárásokat adjanak a kezünkbe. Buchanan és Woodward ezt a kérdést úgy teszik fel, hogy vajon képesek leszünk-e kvantumszámítógépeknek ellenálló algoritmusokat használni addigra, mire a mostani algoritmusaink elméleti fenyegetettsége a gyakorlatban is realizálható lesz [66].

Az észt problémára visszautalva látható, hogy a felhasználás biztonsága nem kizárólagosan az algoritmus matematikai tulajdonságain múlik, mivel a megvalósítás során elkövetett tervezési vagy programozási hibák jelentős mértékben befolyásolhatják a biztonságot. Az implementáció problémáját ennek ellenére ebben a dimenzióban nem érintjük, az aláírás-létrehozó adatok esetében csak azok hosszát jelenítjük meg. A kulcsok hosszait minden esetben bitekben határozzák meg (pl. 128 bit, 256 bit, …, 1024 bit, 2048 bit, 3072 bit, 4096 bit stb.). Elméletileg a hossz tetszőleges nemnegatív egész szám lehet, a gyakorlatban a számítógépek bináris működése miatt kettő hatványaiként fordulnak elő a leggyakrabban. A szakirodalomban az RSA és az ECC kulcsok között 8-as arány van meghatározva biztonsági szempontból, azaz egy adott hosszúságú ECC kulccsal ekvivalens biztonságot 8-szor olyan hosszú RSA kulcs tud biztosítani.

Amennyiben az aláírás-létrehozó adat nem egy kriptográfiai algoritmushoz tartozó kriptográfiai kulcsot jelent, abban az esetben az aláírás-létrehozó adat hossza annak bitben kifejezett értéke lesz. Ebben az esetben a hossz felhasználása a tárolókapacitás biztosításához lesz szükséges, algoritmikus biztonságról itt nem beszélhetünk.

Biometrikus aláírás esetében előfordulhat, hogy nincs olyan adat előre eltárolva, amelyet aláírás-létrehozó adatnak nevezhetnénk, mivel a humán entitás agyi motorikus programja által létrejövő kézmozgás adatait rögzítheti csupán egy erre képes digitális eszköz, ahol nem a rögzített adatot használjuk az aláírás létrehozására, hanem a rögzítés teljes folyamatát. Ebben az esetben vagy nulla lesz az aláírás-létrehozó adat hossza, vagy a rögzített aláírások átlagos hossza jelenik itt meg. A nulla érték azért is indokoltabb, mert az így rögzített bináris adat mérete semmilyen értelemben nem lesz összehasonlítható egy kriptográfiai kulcs hosszával, viszont mivel tartozik hozzá aláírás-ellenőrző adat, ezért a hossz szerepeltetése mégis indokolható. Az a kérdés ebben az esetben felvethető, hogy az agyi motorikus programok módosulásával létrejövő kézi aláírásokhoz tartozó

biometrikus adatok egymásból előállíthatók-e matematikai transzformációk segítségével, de ennek vizsgálata túlmutat a jelenlegi vizsgálati kereteken.

Biztosan nem lesz aláírás-létrehozó adat a kulcsnélküli aláíró rendszereknél (Keyless Signature Infrastructure, KSI), amelyek az aláírni kívánt adatok kivonatából képezik a teljes adathalmazra egyedi kivonatot és ezt tekintik aláírásnak (például a root hash érték egy Merkle-fa [156] csúcsán[188]). Az aláírások PDF dokumentumokba is konvertálhatók [157]. A hash-függvények és a blokklánc (blockchain) technológia között szoros összefüggés van, mivel a blockchain technológiailag a kivonatolásra épít. Ezzel az üzenet tartalma hitelesíthető, de a beküldő (eredet) azonban nem, amit egyébként a BitCoin egyik nagy előnyeként feltüntetett anonimitás is mutat. A lánc ellenőrzéséhez szükséges adatok rendelkezésre állása szintén kihívásként jelentkezik – enélkül használhatatlan a technológia, emiatt is javasolja Budai et. al. ([196]: 377), hogy kizárólag egy jól szabályozott és kontrollált körülmények között működő privát blokklánc jöhet létre a magyar közigazgatáson belül.

4.1.11. AZ ALÁÍRÁS-LÉTREHOZÓ ADAT TÁROLÓJA

Az aláírás-létrehozó adat biztonsága szempontjából létfontosságú annak tárolása. Nyílt adatként sehol sem célszerű megjelennie, ezért különböző kriptográfiai védelemmel ellátott szoftveres tárolókban (pl. Microsoft: certmgr.msc, Mozilla: keyx.db, PGP: Private Key Block) vagy hardveres kulcstároló eszközökben, úgynevezett Hardver Security Modulokban (HSM) vagy Minősített Aláírás Létrehozó Eszközökben (MALE) – angolul Qualified Signature Creation Device, QSCD) szokták ezeket létrehozni és eltárolni. Különbséget jelent az is a tárolók között, hogy a tárolási mód megengedi-e az aláíró kulcs exportálását, tárolóból való kimásolását, vagy sem – a MALE jellemzően ezt meg tudja tiltani, míg a nem ennyire biztonságos Aláírás Létrehozó Eszközök (ALE) lehetővé tehetik ezt. Az eszközök lehetnek hardveres intelligens kártyák, USB (Universal Serial Bus) tokenek, SIM kártyák vagy szoftveres konténerfájlok (pl. pfx, p7b, p12) is. A szoftveres konténerfájlok bármelyik infokommunikációs (ICT) eszközön megjelenhetnek.

[188] A Merkle-fa használható hitelesítési eljárásokban is, de az adatok hosszának ismerete a támadási potenciál növekedéséhez vezethet, így a szivárgásálló változat használatát javasolta Koo et.al. [158]

4.1.12. AZ ALÁÍRÁSOK ELHELYEZKEDÉSE

Az aláírások elhelyezkedésekor meg lehet különböztetni az egyszeres és a többszörös aláírást tartalmazó dokumentumokat, illetve a rajtuk elhelyezett aláírások egymáshoz viszonyított helyzetét, dokumentum-aláírás és aláírás-aláírás viszonylatban. Egyetlen egy aláírásnál csak az a kérdés, hogy hogyan viszonyul az elhelyezkedése az aláírt tartalomhoz, míg többes aláírás esetén ezen túlmenően az aláírások egymáshoz képesti elhelyezkedése is vizsgálható elem. Az egyszerű (single) és a párhuzamos (paralel) digitális aláírások mellett létrehozhatók szekvenciális (sequential) aláírások is, amikor az aláírások egymás után, mintegy egymásba becsomagolva helyezkednek el és ellenőrzésüknél is csak kívülről befelé lehet haladni. A párhuzamos aláírások elkészítésénél akár egyszerre több ember is aláírhatja ugyanazt a dokumentumot, de ezzel az aláírások nem épülnek egymásba, az aláírások egymás mellett léteznek és kezelhetők, létrehozásuk és ellenőrzésük tetszőleges sorrendben elvégezhető, hiszen csak az adott tartalomra vonatkoznak, az aláírt tartalmak hatókörébe a másik aláírás nem tartozik bele. Vegyes aláírásra példa lehet például a különböző szerződések ellenjegyzése (countersigned[189]), ami a szerződő felek párhuzamos aláírásaira rakódó szekvenciális aláírást jelenti, ami a gyakorlatban lehet egy ügyvédi vagy egy közjegyzői ellenjegyzés. Az ellenjegyzés hatóköre kiterjed a dokumentumra és mind a két aláírásra egyaránt. Az aláírások a dokumentumhoz viszonyítottan felvehetnek beágyazott (enveloped[190]), beágyazódó (enveloping) vagy elkülönült (detached) pozíciót is ([179]: 55). Kérdésként merült fel, hogy az elhelyezkedési dimenziónak két aldimenzióját célszerű-e felvenni (aláírt tartalomhoz és más aláírásokhoz való viszony) vagy érdemes külön dimenzióként tárgyalni ezt a két esetet. Tekintettel arra, hogy az aláírások elhelyezkedése nem biztonsági attribútum, hanem felhasználási különbözőség, tárgyalása kisebb súllyal lenne indokolt, ha a biztonsági szempontok dominálnának az értékelésben, azonban az elektronikus aláírás társadalmi konstrukciós hatását is be szeretném mutatni, ezért ez a dimenzió sem nélkülözhető a modellben. Lehetséges, hogy az egyes és a többes aláírások tárgyalásában az elhelyezkedést és a relációt külön célszerű választani, mivel minden aláírás elhelyezkedik valahol a dokumentumhoz képest, de csak a többes aláírásoknál lesz

[189] Az ellenjegyző aláírást a XAdES szabványba is beépítették (lásd ETSI EN 319 132-1 V1.1.1, 5.2.7)
[190] A beágyazódó és elkülönült aláírások mellé a beágyazott aláírást a W3C XML szabványa definiálta. A beágyazott aláírások esetében az aláírt tartalom tartalmazza magát az aláírást is – természetesen nem aláírt tartalomként. A beágyazódó aláírásokban az aláírt tartalom benne foglaltatik. Kezdetben az XML aláírások csak az „embedded” és a „detached” formákat értelmezték (XML-Signature Core Syntax, W3C (first) Working Draft 1999-September-02), 2000-ben ez megváltozott és kialakult a ma használatos fogalomrendszer (XML-Signature Core Syntax and Processing, W3C Working Draft 04-January-2000)

értelmezhető a másik aláíráshoz való viszonya, de lehetséges a többes aláírások értékét nullától különbözőnek beállítani, amivel az egyes aláírás (zéró érték) is azonosítottá vált.

4.1.13. A TANÚSÍTVÁNYOK KIÁLLÍTÓJA

A tanúsítványokat általában hitelesítés-szolgáltatók (certificate authority, CA) bocsátják ki, mint olyan megbízható harmadik felek, akikben a felhasználói közösség megbízik. Nyilvánosan használható tanúsítványokat az eIDAS rendelet hatályba lépését követően csak hatóságilag regisztrált és felügyelt nyilvános bizalmi szolgáltató bocsáthat ki az Európai Unióban. A nyilvántartást Európai Bizalmi Listának hívják (European Trusted List, EUTL), amely a gyakorlatban egy olyan lista, amelyik tartalmazza a tagországok listáira való hivatkozást, azaz listák listája. Az EU biztosítja a szabad és nyilvános böngészési lehetőséget ebben a listában, így le lehet ellenőrizni azt, hogy egy kibocsátó valóban jogosult-e olyan tanúsítványok kibocsátására (például minősített web hitelesítő tanúsítványok QWAC), mint amit állít magáról. Például Magyarországon csak olyan bizalmi szolgáltató működhet nyilvánosan, aki szerepel az európai bizalmi szolgáltatók magyarországi listájában[191]. Lehetséges zártkörű szolgáltatót igénybe venni, aminek a működése nem tartozik a Rendelet hatálya alá, így nem is kell teljesítenie a nyilvános szolgáltatásokra vonatkozó – esetenként igen szigorú – követelményeket. Ennek az a következménye, hogy a zárt körben létrejött szolgáltatásokhoz korlátozott jogi vélelem fűződik, de a felek egymás közötti megállapodásait a Rendelet nem kívánta korlátozni, azokat ettől függetlenül érvényesnek kell tekinteni. Ki lehet bocsátani tanúsítványokat otthoni felhasználásra is például egy nyílt forráskódú szoftver segítségével, nyilvánvaló módon ehhez teljes bizonyító erőt fűzni nem célszerű, de bizonyítékként való megtagadása is ugyanilyen célszerűtlen lehet. A zárt körben működő bizalmi szolgáltatók megítélésénél a zárt kör meghatározása nagyon fontos[192]. Egy holland meghatározás szerint egy csoport zártnak minősül akkor, ha az alábbi négy követelmény teljesül:

1. A kibocsátott tanúsítvány kizárólag a csoporton belül használható fel. A tanúsítványban ezt jelezni is szükséges.

[191] A lista közhiteles verziója itt található: http://www.nmhh.hu/tl/pub/HU_TL.pdf
[192] Forum of European Supervisory Authorities for Electronic Signatures (FESA): Working Paper on „to the public" (Art. 3.3) and on closed systems (REC. 16). April 7, 2003.

2. A tanúsítvány csoporton kívüli felhasználásáért a felelősség erősen korlátozott.

3. A tanúsítvány használatát szerződésben korlátozzák.

4. A tanúsítványt kibocsátó szolgáltatónak aktívan közre kell működnie a csoporton kívüli használat megakadályozásában (pl. technikai intézkedések vagy szerződésben foglalt szankciók bevezetésével).

4.1.14. AZ ALÁÍRÁSOK SZERKESZTHETŐSÉGE

Egy szerkesztőségi rendszerben a hatékonyság növelése érdekben vetette fel Qian és Xu a szerkeszthető elektronikus aláírás fogalmát [67]. Gyakorlatilag arról van szó, hogy a szerző több opciót előzetesen hitelesít, amelyek közül a szerkesztő a későbbi történések függvényében kiválasztja az alkalmas opciót és azzal dolgozik a továbbiakban. A szerkeszthetőség dimenzióként való kezelését negligálja az a tény, hogy a szerkeszthető aláírásokon önmagában lehetséges alkalmazni ezt a modellt. A dimenzióként való tárgyalást azonban a társadalmi hatások miatt fel is lehet vetni és el is lehet vetni, mindkettő mellett szólnak érvek és ellenérvek. Jelen modellben ezt a tulajdonságot nem szerepeltetjük dimenzióként.

4.1.15. AZ ALÁÍRÁSOK IMPLEMENTÁCIÓS KÖRNYEZETE (PROGRAMOZÁSI KÖNYVTÁRAI)

Az aláírás biztonságára az algoritmusok matematikai tulajdonságai mellett azok gyakorlati tulajdonságai is hatással vannak, ahogyan ezt az elmúlt időszak negatív példái megmutatták. Az elméleti jó tulajdonságok mit sem érnek, ha a gyakorlati implementáció gyengíti le az algoritmusokat. Két példa kívánkozik ide, az egyik a Heartbleed probléma[193] , a másik a már korábban is tárgyalt észt kártyaprobléma[194].

A Heartbleed problémát 2014 április elején tette közzé az amerikai számítógépes vészhelyzeti központ, amely szerint az érintett programverziók rosszul megírt memóriakezelési eljárásai miatt egy támadónak lehetősége van a felhasználó azonosítási

[193] Az általánosan használt OpenSSL programcsomag olyan hibája vált ismertté 2014 áprilisában, aminek a kihasználásával a támadó hozzáférhetett a memóriában tárolt titkos kulcsokhoz (https://www.us-cert.gov/ncas/alerts/TA14-098A)
[194] Az észt kormány megszüntette 750.000 észt állampolgári tanúsítvány érvényességét, mivel olyan sérülékenység vált ismertté 2017 szeptemberében, aminek a kihasználásával a támadó a nyilvános kulcs ismeretében ki tudta számítani a titkos kulcsot (https://www.schneier.com/blog/archives/2017/09/security_flaw_i.html)

adatait – ideértve a titkos kulcsait is – megismerni. A probléma nagyságát az okozta, hogy habár a hiba egy szűk és speciális területet, illetve néhány programverziót érintett (OpenSSL 1.0.1 – 1.0.1f, OpenSSL 1.0.2-beta), azonban ezeket a programverziókat számos alkalmazás és szervezet használta fel világszerte a saját szolgáltatásainak a megvalósításában, mivel a forráskódot szabadon fel lehetett használni üzleti és nem üzleti célra az „OpenSSL License" és az eredeti „SSLeay License" szerint[195] (forráskód-módosítás és újralicencelés nélkül). A termék igen népszerű volt, így nem meglepő, hogy az érintettségi adatok alapján a hiba számos nagy unix-alapú biztonsági termékgyártót és ezek felhasználóit érintette[196], például az Amazon, az Aruba Networks, a CA Technologies, a Cisco Systems, a Debian GNU/Linux, az Extreme Networks, a Fedora Project, a Fortinet, a FreeBSD Project és a Gentoo Linux is érintett volt itt.

2017. augusztus 30-án egy nemzetközi kutatócsoport olyan sérülékenységre bukkant az észt állampolgári kártya hardverében és szoftverében, amely lehetővé tette a támadó számára, hogy csupán a nyilvános kulcs ismeretében kiszámítsa a titkos kulcsot. A kutatócsoport nem megbízható elemek felhasználását kutatja megbízható infrastruktúrák kiépítésében [68]. A kérdés a technológia-függés fennállásáig folyamatos relevanciával bír, hasonlóan ahhoz, hogy milyen társadalmi intézményeket érinthet egy-egy kiterjedt technológiai probléma[197]. A probléma felmerülését követően az észt kormány az összes tanúsítványt felfüggesztette (kb. 750.000 tanúsítványról van szó) és felszólította az észt polgárokat, hogy a mobil ID megoldást használják a probléma megoldásáig.

A fentiek rávilágítottak arra, hogy ha egy termék egyik komponense súlyosan kompromittálódik, minden érintett és erre a komponensre épülő megoldás kompromittálódása várható, így annak ismerete, hogy a megoldások milyen komponensekre épülnek, alapvető fontosságú a biztonsági események kezelhetősége szempontjából[198]. Annak a kérdésnek a vizsgálata a metrika kialakításában megkerülhetetlennek látszik, hogy a programkönyvtár használata dimenzionális probléma vagy információbiztonsági kérdés. Az információbiztonsági vetületet erősíti

[195] A licencek pontos leírását lásd itt: https://www.openssl.org/source/license-openssl-ssleay.txt
[196] Az érintett és nem érintett, illetve kérdéses érintettségű vállalatok listáját a következő weboldal sorolja fel: https://www.kb.cert.org/vuls/id/720951
[197] A technológiai konstrukciók és a társadalmi konstruktivizmus kapcsolódásáról részletesen ír Nemeslaki András [9]
[198] Az RSA kriptorendszer ellen 1979-1999 között kidolgozott támadásokat összefoglalóan ismerteti Dan Boneh [25].

Muha Lajos [3], mikor a kritikus infrastruktúrák tárgyalásában felveti egyrészről a közigazgatási informatikát és kommunikációt megvalósító rendszereket (például ilyen a Kormányzati Hitelesítés Szolgáltató[199]) és a kritikus infrastruktúrák létfontosságú infokommunikációs rendszereit, illetve javasolja a védelmet kiterjeszteni azokra a szervezetekre is, amelyek az infokommunikációs rendszereket működtetik, vagy ezzel összefüggő szolgáltatásokat nyújtanak (ilyenek például a bizalmi szolgáltatók és a szabályozott elektronikus ügyintézési szolgáltatók is). Az észt probléma azonban arra is rávilágított, hogy egy információbiztonsági eseménynek az egész társadalomra kiterjedő hatását nem lehet az esemény információbiztonsági menedzselésével megszüntetni, hiszen a társadalom nem fogja elfogadni az esemény áthidalására kifundált helyettesítő megoldást az előre meghatározott sebezhetőségi ablakon (vulnerability windows) belül, mivel ez egy új technológia azonnali társadalmi integrálódását jelenti, aminek a valószínűsége csekély. Emiatt más olyan, már intézményesült elemekre is szükség lehet, amelyek technológiailag megalapozottan teszik lehetővé technológiával támogatott alternatív társadalmi folyamatok kiépülését és zökkenőmentes működését.

Az egyes szoftvermegoldások programozási könyvtárait, illetve szoftveres környezetét nem tekintem a modell elemének, mivel a sérülékenységek ismertté válását követően az érintett ICT elemek listáját a lefolytatott információbiztonsági hatáselemzés után a fejlett biztonságtudattal rendelkező szervezetek elkészítik vagy el kell készíteniük.

4.2. A DIMENZIÓK ORTOGONALITÁSA

A dimenziók definiálása után meg kell vizsgálnunk a közöttük fennálló esetleges függéseket, hiszen a távolságmérés akkor képes megmutatni meg az egyes aláírások közötti tényleges távolságokat, ha rejtett belső függések nem torzítják el az eredményt. Önmagával minden dimenzió identikus definíciónk szerint, emiatt csak két különböző dimenzió között keresünk összekapcsolódási pontokat.

[199] Lásd http://hiteles.gov.hu honlapot a Kormányzat Hitelesítés Szolgáltató működéséről.

Az aláírás-típus részlegesen függ az aláírások megjelenítésétől, mivel nem minden CMS[200], XML[201] vagy PDF alapú elektronikus aláírás teljesíti a CAdES, XAdES vagy PAdES szabvány előírásait, így nem lehetnek fokozott biztonságúak. Amelyek azonban igen, azoknál az aláírástípus automatikusan fokozott biztonságú lesz. Ennek kezelésére érdemes lehet csak a CMS, XML és PDF elemeket meghagyni az aláírások megjelenítésében, mivel CAdES = CMS ∩ „fokozott biztonságú aláírás" összefüggés fennáll, ahogyan a XAdES és PAdES esetében is hasonló képletet lehet felírni.

Az aláírások megjelenítése részleges függést mutathat az algoritmusokkal, mivel szimmetrikus kulcsú aláíró algoritmus implementálása CMS-ben látszik lehetségesnek, az XML-séma a digitális aláírást engedi csupán[202] meg (aszimmetrikus kulcs használatával). Ez alapvetően nem okoz problémát, a modell automatizálásakor azonban az érvénytelen értékkombinációkat érdemes lesz listában tárolni és ennek alapján is ellenőrzést lefolytatni.

Az aláírástípusok és a bizonyító erő között szintén részleges függés értelmezhető, mivel minden magánokiraton elhelyezett minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírásnak teljes bizonyító ereje lesz[203], továbbá a fokozott biztonságú aláírások egyenértékűek lesznek az írásbeli formákkal bizonyos esetekben explicit módon[204], általában véve pedig implicit módon a magyar jogszabályi háttér alapján. Biometrikus aláírással is lehetővé válhat lehet teljes bizonyító erejű okiratot létrehozni[205], ha az aláírás előtt a hatóság azonosítja az ügyfelet és képes az ügyfél korábban tárolt biometrikus adataival összevetni az aláírást, továbbá záradékolja is az így aláírt dokumentumot. A záradékolás teremti meg az aláírt dokumentum és az aláírás között azt a kapcsolatot, amely minden fokozott biztonságú aláírásnak a

[200] A Cryptographic Message Syntax (CMS) kriptográfiai üzenetformátumot a PKCS #7 általános kriptográfiai üzenetszabvány 1.5 verziója alapján készítették tetszőleges üzenet digitális aláírásához, kivonatolásához, hitelesítéséhez vagy titkosításához, 2019-ben érvényes leírását az RFC 3370 tartalmazza, kiegészítve az RFC 5754-tel. A PKCS a „Public Key Cryptography Standard" (nyilvános kulcsú kriptográfiai szabvány) kifejezés rövidítését jelenti. A PKCS szabványokat az RSA Laboratory készítette és publikálta.
[201] Az XML (eXtensible Markup Language, kiterjesztett jelölőnyelv) a Standard Generalized Markup Language, szabványos általánosjelölőnyelv (SGML) részhalmaza, először a World Wide Web Consortium (W3C) ajánlásként 1998 februárjában és folyamatosan fejlesztik
[202] . A digitális aláírások XML-specifikációját a W3C konzorcium ebben a leírásban teszi közzé: https://www.w3.org/TR/2015/NOTE-xmldsig-core2-20150723/ (2019. február 12.)
[203] Lásd Pp. 325. § 1) f.
[204] Lásd Hpt. 279. § 1)
[205] Lásd 2010. évi CXXVI. törvénya fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról, 20/J. § (6).

szükséges, de nem elégséges tulajdonsága. Tekintettel arra, hogy itt a teljes bizonyító erőt a jogalkotó tehát nem önmagában az aláíráshoz, hanem az aláírás és a záradék együtteséhez fűzte, ebből az következik, hogy ennek a biometrikus aláírásnak csak a záradékolással együtt van teljes bizonyító ereje.

Az aláírástípusok és a tanúsítványszabványok között részleges függés áll fenn, mivel PGP kulcsfájl használatával automatikusan nem lehetséges teljesíteni a fokozott biztonságú elektronikus aláírással szemben támasztott követelményeket, a garanciális követelmények alacsony szintje miatt. Ha azonban egy nyilvános szolgáltató X.509 tanúsítványba foglalja a PGP által – és egyébként a mértékadó algoritmuslistának és kulcshosszaknak megfelelő eljárásokkal – generált nyilvános kulcsot, akkor ez az aláírás már fokozott biztonságúnak tekinthető. Ebből is látszik, hogy a technológia csak az egyik része az elektronikus aláírás elfogadhatóságának, a másik része az, hogy milyen intézményesült eljárásokat vesz igénybe az aláíró az aláírás elkészítéséhez. Továbbá létezik tanúsítvány nélkül létrehozható biometrikus aláírás, ami teljesíti a fokozott biztonságú aláírással szemben támasztott követelményeket is, vagyis a tanúsítvány hiánya nem feltétlenül akadálya fejlettebb aláírások létrehozásának. Itt is igaz azonban, hogy önmagában az aláírás nem lesz fokozott biztonságú a követelmények teljesítéséig, vagyis az aláíró azonosításáig és az aláírásnak a dokumentumhoz való biztonságos hozzákapcsolásáig.

Az aláírások érvényességi idejét egyrészről a praktikum (meddig szükséges megőrizni az aláírt dokumentumot), másrészről a mértékadó szabványok (meg lehet-e őrizni a szükséges ideig az adott algoritmusokkal) határozzák meg a gyakorlatban. Az algoritmusválasztás hátulütője, hogy nem elfogadható algoritmusokkal készített aláírásokhoz nem fűződik jogi vélelem (a bizonyítékként való elfogadhatóságon kívül), továbbá nyilvános szolgáltatók hatósági döntés alapján nem is alkalmazhatják a szolgáltatásaik nyújtása során az elavult algoritmusokat[206].

[206] Lásd például a Nemzeti Média- és Hírközlési Hatóság 2012. december 29-én hozott határozatát, amely szerint az Educatio Kht. a sha1-with-rsa kriptográfiai algoritmuskészletet 2012. jún. 30-ig alkalmazhatja. http://nmhh.hu/dokumentum/4046/algo_hatarozat_kiegeszit_26838_20_educatio_11_111229.pdf

Dimenziók	Aláírás megjelenítés	Aláírástípus	Bizonyító erő	Komplexitás	Aláírás érvényességi idő	Tanúsítvány szabvány	Tanúsítvány típusa	Aláíró típusa	Algoritmus	Kulcshossz	Kulcstároló	Elhelyezkedés	Tanúsítvány kibocsátó
Aláírás megjelenítés	X	R	R						R				
Aláírás típus	R	X	R			R	R		R	R			R
Bizonyító erő	R	R	X			R	R				R		R
Komplexitás				X									
Aláírás érvényességi idő					X				R	R			
Tanúsítvány szabvány		R	R			X							R
Tanúsítvány típusa		R	R				X	R	R	R			R
Aláíró típusa							R	X					
Algoritmus	R	R			R		R		X	R			
Kulcshossz		R			R		R		R	X			
Kulcstároló		R	R								X		
Elhelyezkedés												X	
Tanúsítvány kibocsátó		R	R			R	R						X

5. táblázat: A dimenziók függései (forrás: saját táblázat)

A táblázatban nem szerepel a specialitásokat magában foglaló dimenzió (pl. magyar közigazgatásban használható tanúsítvány), mivel ez a dimenzió minden előzőtől függetlenül, azok egy részhalmazát kiválasztva jelöli meg azt a saját területén használhatónak. A magyar közigazgatási tanúsítvány segítségével létrehozható aláírások egyetlen eltérő tulajdonsága az, hogy a tanúsítványláncot vissza kell tudni vezetni a KGYHSZ legfelső szintű kibocsátóra.

4.3. AZ ELEKTRONIKUS ALÁÍRÁS DIMENZIÓ MODELL

A dimenziók fenti tárgyalását követően az Elektronikus Aláírás Dimenzió Modell megalkotása a következő lépés. Tekintettel arra, hogy a modell időben változhat, az egyes verziókat érdemes verziókezelés alá vetni, így legyen a következőkben tárgyalt modell verziószáma az 1.0. 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, D_x pedig az aláíráshoz tartozó 14 dimenzió, $D_i(ES)$ pedig az ES aláírás 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 dimenziók értékkészletét és az értékek magyarázatát az alábbi táblázat rögzíti.

D_i	Dimenzió	Leírás	Értékkészlet
D_1	Megjelenítés	Az aláírás kódolási szabványát jelöli	CMS 100 XML 200 PDF 300
D_2	Aláírástípus	Az aláírás biztonsági szintjét jelöli (gyakorlatilag I/N módon)	Normál 100 Fokozott biztonságú 1000
D_3	Alaki bizonyító erő	Az aláíráshoz fűzött jogi vélelem	Nincs 0 Bizonyíték 100 Írásbeli 1000 Teljes 10000
D_4	Komplexitás	Az aláírás részleteinek jelölése, ideértve a szabályzatok, időjel, érvényesítési adatok és időbélyegek aláírásba kerülésének jelzését	B 50 BES 100 EPES 500 T 1000 C 2000 X 3000 X-Long 3500 LT 4000

D_i	Dimenzió	Leírás	Értékkészlet
			LTA 4500 LTV 5000
D_5	Érvényességi idő (nap)	Azt az időtartamot jelöli napban kifejezve, ameddig az aláírás ellenőrzését bármikor el kell tudni végezni	napok száma 1, 2, …, 365, …
D_6	Tanúsítvány szabvány	Az aláíráshoz tartozó tanúsítvány létrehozási formátumát adja meg	nincs 0 PGP key block 50 Biometrikus aláíró 100 X.509v2 attribútum 500 X.509v3 PKI 1000
D_7	Aláíró entitás	Az aláíró entitás kategóriáját jelöli	természetes személy 100 jogi személy 150 kormányzati szerv 200 jogi személyiséggel nem rendelkező társulás 250 egyéb szervezet 300
D_8	Aláíró algoritmus[207]	Az ismert és elterjedten használt kriptográfiai aláíró algoritmusokat sorolja fel	Nincs 0 Schnorr 25 DES 50 3DES 75 GHOST 100 ElGamal 200

[207] Az algoritmusok (sémák) listáját várhatóan bővíteni kell majd a kvantum-ellenálló algoritmusokkal (pl. qTESLA [181], vagy NTRUSign [182], a használatuk elterjedését követően).

D_i	Dimenzió	Leírás	Értékkészlet
			Blowfish 300 DH 950 RSA 1000 ECDSA 7600 DSA 8000
D_9	Aláírás-létrehozó adat hossza	Az aláírás-létrehozó adat hossza bitben meghatározva	bit 0, 64, 256, 384, 512, …, 1024, 2048, … 4096 stb.
D_{10}	Aláírás-létrehozó adat tárolója	Az aláíráshoz használt adat tárolási helyét és módját specifikálja	Nincs 0 Fájl 100 Személyes tároló 500 ALE / SCD 5000 HSM 15000 MALE / QSCD 20000
D_{11}	Aláírás relációja	Az aláírás relatív pozícióját írja le több aláírás esetében	egyetlen aláírás 0 szekvenciális 100 párhuzamos 200 ellenjegyző 300
D_{12}	Aláírás elhelyezkedése	Az aláírások helyét rögzíti az aláírt adatokhoz viszonyítva	beágyazott 100 beágyazódó 150 elkülönült 200
D_{13}	Tanúsítvány kiállítója	a tanúsítvány kibocsátójának típusa	nincs 0 öntanúsított privát 50 zártkörű kibocsátó 100 nyilvános nem minősített 500 nyilvános minősített 1000

D_i	Dimenzió	Leírás	Értékkészlet
D_{14}	Speciális attribútumok	további jellemzők (pl. magyar állampolgári, a magyar közigazgatásban használható)	nincs specialitás 0 magyar állampolgári 1 magyar közigazgatási 2

6. táblázat: Az Elektronikus Aláírás Dimenzió Modell értékkészlete (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 meghatározásánál objektív és szubjektív szempontok is felmerültek. Például annak értékelése, hogy az aláírás elhelyezkedése milyen, tetszőleges sorrendet követhet, az adott alkalmazó preferenciái alapján. Az egyes algoritmusokhoz rendelt értéknek azonban tükröznie kell az algoritmussal szembeni bizalmat, azok matematikai tulajdonságaira alapozva (ehhez felhasználtam többek között Lenstra et.al. tréfás[208], de valós adatokon[209] nyugvó elemzését [180] és Schneier összehasonlító táblázatait ([59]: Table 7.1-7.6) is). Az értékadás alapja egyrészről a feltárt biztonsági szint, másrészről a feltöréshez elméletileg szükséges műveletigény volt. Tekintettel arra, hogy az egyes aláírások tulajdonságai nem minden esetben lehetnek nyilvánvalók a felhasználók számára és a legritkább esetben derülnek ki az aláírások látható részeiből, a

[208] A szerzők a kriptoanalízishez használt energia által felforralható víz mennyiségével definiálták a kriptográfiai algoritmusok biztonsági szintjét, például „teáskanál-biztonság”, „uszoda-biztonság”, „tavi biztonság”, „globális biztonság” (a Föld minden tengervizének elforralása) vagy már csak a begyűjthető energiát alapul véve: „Naprendszer-biztonság”. Az RSA algoritmus érdekességei közé tartozik, hogy az algoritmus „teáskanál-biztonsága” és a „globális biztonsága” között csupán 2138 bitnyi különség van.
[209] Az RSA és DES algoritmusok biztonságának követésére az RSA Laboratories Inc. az RSA Factoring Challenge, a Secret Key Challenge és a DES Challenge III programokat alapította meg. Lenstra számos faktorizációs probléma megoldásában vett részt (pl. RSA-140 [183], RSA-155 [184] és RSA-768 [185]). A DES Challenge III kihívást 22 és egynegyed óra alatt oldotta meg a speciálisan erre a célra épített Deep Crack és majdnem 100 000 internetre kötött személyi számítógép 1999. január 18-án.

modell megfelelő alkalmazásához számottevő szakértelem feltételezett (ebben csatlakozom Casola et.al. eredményéhez ([112]: 199), az értékelési szakértelem vonatkozásában). A szakértői értékelés szükségessége gyakorlatilag bizonyos szubjektivitást hoz be a rendszerbe, ugyanis távolról sem biztos, hogy különböző szakértők azonos szinten értékelik az egyes védelmi intézkedések erősségét iparági gyakorlat vagy szabványosítási háttér nélkül annak ellenére, hogy az aláírások biztonságára vonatkozó követelményeket és kontrollokat már 1999-ben összefoglalták az informatikai szakemberek számára [189] és számos szabvány létezik az elektronikus aláírások válfajaira. Természetesen meg lehet konstruálni a modellből azt a részmodellt, amelyik csupán a frekventált attribútumokat tartalmazza, ezzel azonban elvész a modellnek az az előnye, hogy minden elektronikus aláírás elhelyezhető benne és különböző típusú aláírásokhoz különböző értékek fognak tartozni.

A modell egyes dimenzióinak az értékkészletét úgy próbáltam meghatározni, hogy minden későbbi módosítás – a fenti alapelvek betarthatóságával együtt – végrehajtható legyen. Az értékkészletekbe számos elem beszúrható, az egyes dimenziók belső struktúrájaként belső tartományok is kijelölhetők, torlódás esetén a negatív tartományok is felhasználhatók – vektoriálisan ez nem jelent különbséget, azaz a modell maximálisan rugalmas és skálázhatónak tűnik a jövőbeli előrelátható és előre nem látható igényeknek megfelelően egyaránt.

Demonstrálva a modell működését, négy aláírás-típust választottam ki a szemléltetéshez:

1. ES: PGP-aláírás a felhasználó által generált RSA-1024 kulcspárral és időbélyeg nélkül,
2. ES: nem minősített személyes tanúsítványon alapuló XML aláírás, fokozott biztonságú időbélyeggel, RSA 3072 kulcspárral,
3. ES: magyar közigazgatásban használható minősített szervezeti bélyegző ECDSA 256 kulcspárral, XML dokumentumon minősített időbélyegzővel, és
4. ES: minősített állampolgári aláírás RSA 2048 kulcspárral PDF dokumentumon minősített archív időbélyegzővel együtt.

Az időbélyegeknek az aláírásban konkrétan nincsen szerepük – azon túlmenően, hogy az időbélyegen szereplő elektronikus aláírásra az Elektronikus Aláírás Dimenzió Modellt természetesen lehet alkalmazni és az aláíráshoz tartozó érték biztosan különbözne a fenti három aláírás értékétől, az aláírás értékelésében viszont feltevésként elfogadva, hogy az időbélyegzés célja a hosszabb távú ellenőrzési igény volt, az időbélyegzettség fennállását az aláírás érvényességi idejének meghatározásához használom fel. Ha nincs időbélyegzés, akkor az érvényességi időt nullának tekintem, minősített időbélyeggel pedig 5 évnek (1 826 napnak) veszem, egy szökőnapot is belefoglalva az intervallumba.

Ezekkel együtt a fenti négy aláírás értéke rendre a következő lesz:

$V(ES_1)$ = {100; 100; 100; 50; 1826; 50; 100; 1000; 1024; 100; 0; 100; 0; 0},

$V(ES_2)$ = {200; 1000; 1000; 1000; 365; 1000; 100; 1000; 3072; 100; 0; 150; 500; 0},

$V(ES_3)$ = {200; 1000; 10000; 1000; 1826; 1000; 250; 7600; 256; 20000; 0; 150; 1000; 2}, illetve

$V(ES_4)$ = {300; 1000; 10000; 5000; 1826; 1000; 100; 1000; 2048; 20000; 0; 150; 1000; 1}.

Jól látható, hogy az egyes aláírások (számhalmazok) értékei több helyen különböznek, mindamellett egyezőségek is felfedezhetők közöttük. A továbbiakban azt a kérdést vizsgálom meg, hogy a modellben megjelenített aláírások mérhetősége mit jelent és milyen következtetéseket lehet levonni abból, hogy az elektronikus aláírásokat ebben a formában ábrázoltuk.

5. AZ ELEKTRONIKUS ALÁÍRÁS MÉRÉSE

5.1. AZ ELEKTRONIKUS ALÁÍRÁS METRIKÁJA

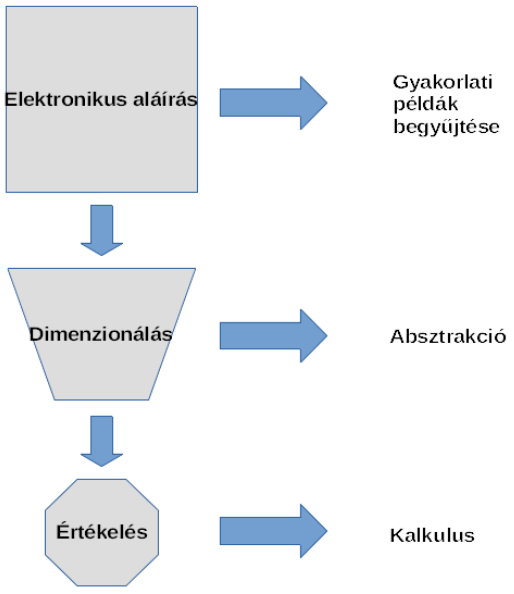
5.1.1. ELMÉLETI MEGFONTOLÁSOK

Az elektronikus aláírások globálisan értelmezett definícióját megalkotva az amerikai UETA és ESIGN, az UNCITRAL modelltörvény és az eIDAS közös nevezőre hozásával – az elektronikus aláírás egy olyan elektronikus adat, amelyik egy másik adathoz van csatolva és amelyet az aláíró aláírásra használ. Ez az adat származhat kriptográfiai transzformációból, de származhat eljárásból, lehet dinamikus biometrikus adat is, vagy bármilyen struktúrájú és hosszúságú információ, amely az aláírási szándékot és tényt képes hitelt érdemlően bizonyítani az ellenőrzés időtartama alatt. Az aláírás alapszintű jogi vélelmekkel rendelkezik, leginkább az elektronikus volta miatti elutasíthatatlanság és a bizonyítékként történő felhasználás területén, de az emelt szintű vélelmekhez további tulajdonságokkal is rendelkeznie kell, amit úgy lehetne összefoglalni, hogy az aláírásnak képesnek kell lennie mind az aláíró, mind az üzenet hitelesítésére (ahogyan ezeket a követelményeket Diffie és Hellmann [20] az üzenetre, illetve Rivest, Shamir és Adleman [97] az aláíróra először felvetette). Ehhez két eszközt kínál, az egyik az aláírás-létrehozó adat és az aláíró kapcsolata, a másik pedig a már létrehozott aláírás és az aláírt adat összekapcsolódási módja.

Mivel az elektronikus aláírás valójában tehát egy elektronikus adat, amelyik számítógépen ábrázolható, ezért bináris reprezentánsa minden esetben egyértelműen azonosítja az adott aláírást, ez – mint minden kettes számrendszerbeli szám – mérésre triviálisan alkalmas. Ezt nevezhetjük az elektronikus aláírás triviális mérhetőségének. A triviális mérhetőség arról ad felvilágosítást, hogy az adott aláírás milyen hosszúságú, azaz hány bitből áll. Ha egy aláírás hosszabb, mint egy másik, akkor vagy az aláíró algoritmus által generált kimenet hosszabb, vagy az aláírás komplexitása magasabb és emiatt van benne több információ. Ettől több adatot azonban nem nyerünk a triviális mérhetőséggel, hiszen abból nagy valószínűséggel semmilyen plusz információ nem nyerhető ki a konkrét aláírásra vonatkozóan, hogy az egyik aláírás 287 bájt (2 296 bit), míg a másik 40 960 bájt (327 680 bit) hosszú, csak sejtésünk lehet arról, hogy az első aláírás RSA-2 048 aláíró algoritmust és kulcsot használt, míg a második egy komplex aláírás lehet, de a belső struktúrájáról az aláírás hossza nem árul el sokat. Felhasználható attribútum, hogy

a gyakorlatban kialakult aláírások vagy aláírási konténer-fájlok mérete fix, csak a belső tartalmuk változik, emiatt esetleg annyi többletinformációt tartalmazhat az aláírások hossza, amivel elegendően sok aláírás tanulmányozása után megtehetők olyan megállapítások, hogy a 287 bájt hosszúsággal rendelkező aláírás valószínűleg PGP aláírás a fájl méretéhez lefelé legközelebb eső kulcsmérettel, valamint a 167 389 bájtot tartalmazó aláírás vélhetően PDF aláírás, de ettől többet az aláírásról a mérete nem képes elárulni, így ha az aláírás belső struktúráját is fel kívánjuk tárni, más metódust kell választanunk.

Következő elgondolásként az egydimenziós lineáris tömb lehetett volna alkalmas a metrika megvalósítására, amelyben véges szakaszokat definiálhatunk az aláírások megjelenési struktúráiból absztrahált dimenziók értékeinek a formális reprezentálására. Ez az eszköz már képes lett volna az aláírások belső struktúráját felfedni, azonban a skálázhatósága korlátozottnak tűnt. Amennyiben a véges szakaszok értékei betelnek, akkor a bővítésre csak három módszer kínálkozik, vagy az egész értékeken túli racionális (vagy irracionális) törteket kell alkalmazni, vagy a tömb végére lehet hozzáfűzni az új értékeket, vagy az adott szakasz határának kitolásával (törtbitek létezésének hiányában) – és egyben az összes további szakasz határainak az átdefiniálásával – oldható meg a bővítés ebben az esetben, a két utóbbi inkompatibilitást eredményezhet a korábbi modellverziókkal, az első pedig a számábrázolási metódust változtatná meg. A modellalkotás során elvégzett feladatokat az alább ábra foglalja össze:



18. ábra: A modellalkotás során elvégzett feladatok (forrás: saját ábra)

Casola et. al. munkáját figyelembevéve [112], akik a szabályozások biztonsági szintjeinek az összehasonlítására a vektoros ábrázolást javasolták a különböző hitelesítésszolgáltatók (CA) kereszttanúsításának a félautomata támogatásához, az ott javasolt lépések (strukturálás, formalizálás, értékelés) elvégzése szükségesnek látszik az elektronikus aláírások ábrázolásához is, mivel az egyes specialitások vagy a jogi vélelmek értékei alapesetben nem numerikusak, hanem szövegesek, amelyek formalizálása nélkül nem lehetséges kvantitatív mérés definiálása az aláírások halmazán. Ilyen értelemben az Elektronikus Aláírás Dimenzió Modellt nevezhetjük a Casola et.al. által kidolgozott szabályozás-alapú Biztonsági Metrika általánosításának az elektronikus aláírásokra. A dimenzió modell nem nevezhető a Biztonsági Metrika kiterjesztésének, mivel az Elektronikus Aláírás Dimenzió Modell explicit módon nem foglalkozik a bizalmi szolgáltatók szabályozásával, implicit módon azonban a minősített és nem minősített szolgáltatások kimenetét felhasználja, ami távoli kapcsolatot jelent a szabályzat, a szolgáltató, a szolgáltatás és a szolgáltatás tárgya vagy eredménye között.

A formalizálást követően minden dimenzió értékkészletében kizárólag numerikus értékeket szerepeltetve az Elektronikus Aláírás Dimenzió Modell számszerűsíteni tudja az egyes elektronikus aláírások sajátértékét és az egymástól való távolságukat is, egy 14-dimenziós elektronikus aláírási vektortérben. Tekintettel arra, hogy az egyes dimenziókban nincs minden számhoz jelentés rendelve, ezért matematikai értelemben meg lehet különböztetni a valós számokon értelmezett 14-dimenziós vektorteret a 14-dimenziós Elektronikus Aláírás Dimenzió Modell vektorértől, a megkülönböztetés alapja az Elektronikus Aláírás Dimenzió Modell által jelentéssel felruházott vektorok véges halma lesz. Az Elektronikus Aláírás Dimenzió Modell matematikai értelemben izomorf a 14-dimenziós euklideszi tér egy adott részhalmazával, így annak minden tulajdonsága elvileg értelmezhető benne attól függően, hogy az értékkészletek halmazában van-e találat vagy nincs. Szemléletesen fogalmazva, a 14-dimenziós euklideszi vektortérben bármelyik két vektornak létezik különbségvektora, de az Elektronikus Aláírás Dimenzió Modellben ez a különbség csak akkor létezik, ha a művelet alapjául szolgáló két vektor is létezik. Tekintettel arra, hogy az Elektronikus Aláírás Dimenzió Modell értékkészletei végesek, a 14-dimenziós euklideszi vektortér koordinátái pedig végtelenek, végtelen sok 14-dimenziós vektornak nem lesz jelentése az Elektronikus Aláírás Dimenzió Modellben, habár ez utóbbi az előbbinek valódi részhalmaza. A vektoros ábrázolás mellett szólt a klaszterezés lehetősége is, hiszen kérdésként felmerült, hogy vajon meghatározható-e egy

olyan tartomány a modellben, amelyik az az összes minősített elektronikus aláírást tartalmazza. Vektoros ábrázolás esetében ez a kérdés átfogalmazható például egy 14-dimenziós gömb, kocka, esetleg ellipszoid tartalmazási relációjának vizsgálatára, azaz az aláírási vektoroknak az alakzat geometriai középpontjától való abszolút (irányfüggetlen) távolságának a meghatározására.

5.1.2. MÉRT EREDMÉNYEK

A 4.3 Az Elektronikus Aláírás Dimenzió Modell fejezetben bemutatott négy aláírást ábrázoló vektoroknak az abszolútértékét az alábbi táblázat részletezi:

Aláírás	Abszolútérték
V(ES1)	2 334,06
V(ES2)	3 860,43
V(ES3)	23 775,72
V(ES4)	23 165,73

7. táblázat: A példaként bemutatott aláírások értéke az Elektronikus Aláírás Dimenzió Modellben (forrás: saját táblázat)

A táblázat eredményét szemléletesen is meg lehet fogalmazni. Az eredmények azt mutatják, hogy a PGP aláírás értéke – hiába használná ugyanazokat a kriptográfiai algoritmusokat, mint egy minősített aláírás – tizedrésze a minősített állampolgári aláírásnak, ellenben a minősített állampolgári aláírás nagyon közel van egy minősített szervezeti bélyegzőhöz még akkor is, ha más algoritmust használ. Továbbá a fokozott biztonságú aláírások értéke valóban sokkal kisebb, mint a minősített aláírások értéke, hiába használna hosszabb titkos kulcsot az aláíró algoritmusához, de azért jól elkülöníthető a csak alapvető jogi vélelemmel rendelkező aláírásoktól.

5.2. A MÉRÉS EREDMÉNYEINEK FELHASZNÁLÁSA

A modellben elméletben létrehozható az összes létező (és nem létező) típusú aláírás, kiszámolhatóvá válnak az aláírásokhoz rendelt vektorok hosszaként értelmezett aláírások értékei és ezeket össze is lehet hasonlítani numerikus módszerekkel. Elvi korlátok felállítására is alkalmas a modell, például a legkisebb, gyakorlatban még elfogadható fokozott biztonságú aláírástípushoz rendelt érték V(min.fok) = 2 738,03 ahol ES(min.fok) = {100; 1000; 100; 50; 0; 1000; 100; 1000; 2048; 100; 0; 100; 500; 0}, a fokozott biztonságú dimenzióértékek középértékei alapján a fokozott biztonságú aláírások vektorjainak a csúcspontja az ES(átl.fok) = {200; 1000; 1000; 1000, 0; 1000;

150; 1000; 2560; 100; 0; 150; 500; 0} körül fognak elhelyezkedni, V(átl.fok) = 3 449,43, így felállítható egy olyan kritérium, hogy az adott aláírási rendszerben csak azokat a fokozott biztonságú aláírásokat lehetséges elfogadni, amelyeknek a modellben számított értéke a 3449,43 értéktől legfeljebb 725-tel tér el.

A modellben nemcsak a teljes vektor hosszára fogalmazható meg állítás, hanem az egyes dimenziókban felvenni kívánt értékek választása is kiköthető rögzített feltételként. Például lehetséges olyan követelményt is megfogalmazni, hogy „az adott aláírás D_8 dimenzióban felvett értékének minimum 1 000-nek kell lennie”. Ez azt jelenti, hogy az adott aláírás aláíró algoritmusa csak a tudomány mai álláspontjának megfelelő, biztonságosnak tartott algoritmus lehet (pl. RSA, ECDSA, DSA, qTESLA, NTRUSign).

Bármelyik elektronikus aláírási rendszerben alkalmazott elektronikus aláírások és bélyegzők típusai megjeleníthetők a modellben, amivel a rendszer használatát biztosító informatikai csapat (fejlesztők, programozók, üzemeltetők) számára egyértelmű információ biztosítható ahhoz, hogy pontosan azt és csak azt implementálják a rendszerben, amire feltétlenül szükség van, mivel rendelkezésre áll a feltételrendszer teljeskörű megfogalmazása programozható alapokon.

5.3. AZ ELEKTRONIKUS ALÁÍRÁSOK TÁVOLSÁGA ÉS KÜLÖNBSÉGE

A vektoros ábrázolás előnyeként tartható számon, hogy az egyes aláírások között távolságfüggvény numerikus módon értelmezhető, az egyes elektronikus aláírás-vektorok távolságaiként. Két elektronikus aláírás *távolsága* a következő érték:

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

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:

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

és $K(V(ES_1);V(ES_2))$-vel jelöljük.

Az elektronikus aláírások csoportosításához a vektorok hosszának értékei mellett a vektorok különbségvektorainak a hossza is felhasználható, mivel valamivel finomabb felbontásban mutatja meg az egyes aláírásokhoz tartozó vektorokból látható hasonlóságokat és különbségeket. Az előbbi példában szereplő ES(min.fok) és ES(átl.fok) vektorok különbségvektorának a hossza

$$T((V(ES(min.fok));V(ES(átl.fok))) = 1\,410{,}55,$$

szemben a vektorok hosszának a különbségével, ami

$$K((V(ES(min.fok));V(ES(átl.fok))) = 711{,}4$$

értéket mutat. Ezt felhasználva az előbbi kritérium átfogalmazható úgy, hogy csak azok a fokozott biztonságú aláírások használhatók az adott aláírási rendszerben, amelyekhez rendelt vektorok távolsága az átlagvektortól legfeljebb 1 500. A kritérium szöveges változatának megfogalmazáshoz az egyes értékek visszafordíthatók a dimenziók értékkészletei segítségével, intervallumok vagy felsorolás alkalmazásával, így a modell a háttérben támogató eszközként funkcionálva képes segíteni az elektronikus aláírások egységes alkalmazását.

A teljesség igénye nélkül, de az összehasonlíthatóság és csoportosíthatóság maximális igényével mutatom be az egyes aláírástípusok értékeit a modellemben. Felhasználtam magyar állampolgári, közigazgatási, SZEÜSZ (AVDH) által készített és piaci, minősített és nem minősített, magyar közjegyzői és román közjegyzői, PGP és bizalmi szolgáltatáson alapuló, lengyel állampolgári, továbbá RSA és ECC algoritmusokon alapuló aláírásokat is, amelyek közötti hasonlóságokat az alábbi táblázat segítségével az egyes értékek (aláírásvektorok) nagyságával (hosszával) ábrázoltam:

#	Aláírás típusa (rövid leírás)	HOSSZ
1	PGP-aláírás a felhasználó által generált RSA-1024 kulcspárral és időbélyeg nélkül	1 508,9072
2	nem minősített személyes tanúsítványon alapuló XML aláírás, RSA 4096 kulcspárral, rövid távú érvényességgel	4 637,9350
3	magyar közigazgatásban használható minősített szervezeti bélyegző	13 582,6605
4a	minősített magyar állampolgári aláírás	24 381,5102

#	Aláírás típusa (rövid leírás)	HOSSZ
4b	minősített magyar állampolgári aláírás	24 479,7475
5	magyar közjegyzői minősített elektronikus aláírás	22 992,3907
6	romániai közjegyzői minősített elektronikus aláírás	23 096,5372
7	lengyel minősített állampolgári aláírás	22 552,6058
8	vállalati belső használatú fokozott biztonságú elektronikus aláírása	2 896,9862
9	minősített bizalmi szolgáltató hitelesítési rendjének aláírása	22 861,3058
10	mobilszolgáltatói e-számla aláírása üzleti ügyfél számára	8 065,8124
11	biztosítói e-számla aláírása üzleti ügyfél számára	8 068,9113
12	mobilszolgáltatói e-számla magánszemély ügyfél számára	7 711,1950
13	gázszolgáltatói e-számla magánszemély ügyfél számra	7 662,4101
14	AVDH aláírás magánszemély számára ügyfélkapus hitelesítéssel	12 588,1901
15	Állampolgári Tanúsítványkiadó aláírása az állampolgári tanúsítványokon	15 691,5723
16	NAV aláírása egy meghiúsulási igazoláson	7 662,4101
17	helyi adóiroda aláírása helyi adóról szóló elektronikus tájékoztatáson	23 234,5612
18	Magyar Közlöny 2019. évfolyam 14. szám elektronikus aláírása	23 096,5372
19	közüzemi (csatorna) számla	7 662,4101
20	nemzeti közműszolgáltatói e-számla	7 662,4101
21	biometrikus aláírással ellátott bizonylaton[210]	1 508,5506

8. táblázat: Elektronikus aláírások értékei (forrás: saját táblázat)

A táblázatban négy csoport azonosítható be. Az első és legnagyobb számosságú csoportot a G_1={7, 9, 5, 6, 18, 17, 4a, 4b} aláírások képezik, 23 338,8994 átlaggal, a

[210] Az aláírás-létrehozó adat hosszát nullának tekintve.

második csoportot a G_2={14, 3, 15} aláírásokból lehet megképezni 13 954,1409-es átlaggal, a következő csoportot a G_3={2, 13, 16, 19, 20, 12, 10, 11} aláírások alkotják 7 391,6868-as átlaggal és az utolsó csoport a G_4={21, 1, 8} aláírásokból áll 1 971,4813 átlaggal. A G_1 csoportba a megbízható aláírás-létrehozó eszköz (MALE, QSCD) segítségével készített aláírások kerültek be, a G_2 csoportban a teljes bizonyító erővel rendelkező végfelhasználói, illetve a biztonságos kulcstárolással rendelkező bizalmi szolgáltatói aláírások találhatók, a G_3 csoport a nem minősített aláírásokat és a minősített tanúsítványon alapuló szoftveres bélyegzőket tartalmazza, végül a G_4 csoport a PGP és belső használatra szánt vállalati aláírásokat foglalta magában, a biometrikus aláírással együtt. Itt meg kell jegyezni, hogy a biometrikus aláírás csak addig fog ebbe a csoportba tartozni, amíg az aláírás-létrehozó adat hosszát nullának vesszük, egyébként attól függően fog átkerülni másik csoportba, hogy milyen érzékenységgel rögzíti a biometrikus aláírás képét, azaz mekkora lesz az aláírás-létrehozó adat hossza. 20 000 bittel számolva az aláírás már a G_1 csoport értékeinek fog megfelelni, 10 000 bitnél pedig a G_2 csoport lesz számára a releváns csoport.

A csoportokban lévő elektronikus aláírások különbségeit és távolságait a korábban megadott definíciók szerint kiszámítva az alábbiakat kapjuk:

K(G_1)	**7**	**9**	**5**	**6**	**18**	**17**	**4a**	**4b**
7	X	308,70	439,78	543,93	543,93	681,96	1828,90	1927,14
9	308,70	X	131,08	235,23	235,23	373,26	1520,20	1618,44
5	439,78	131,08	X	104,15	104,15	242,17	1389,12	1487,36
6	543,93	235,23	104,15	X	0,00	138,02	1284,97	1383,21
18	543,93	235,23	104,15	0,00	X	138,02	1284,97	1383,21
17	681,96	373,26	242,17	138,02	138,02	X	1146,95	1245,19
4a	1828,90	1520,20	1389,12	1284,97	1284,97	1146,95	X	98,24
4b	1927,14	1618,44	1487,36	1383,21	1383,21	1245,19	98,24	X

9. táblázat: A G_1 csoport elektronikus aláírásainak különbségei (forrás: saját táblázat)

Jól látható, hogy az ES(18) és az ES(6) értéke megegyezik, ami azt jelenti, hogy a két aláírás ugyanabba a kategóriába sorolható. Tekintettel arra, hogy az egyik egy romániai közjegyzői aláírás, a másik pedig a Magyar Közlönyön elhelyezett elektronikus

aláírás, a két aláírás bináris értéke biztosan különbözni fog, azonban a modellben elfoglalt helyük – a megegyező dimenzionális értékekből adódóan – mégis ugyanaz lett. A nulla különbség kijelölte a legkisebb különbségi értéket is, a maximális különbség két G_1-beli aláírás között pedig 1 927,14. Összehasonlításként egy PGP és egy magyar minősített állampolgári aláírás közötti különbség:

$$K(ES(4b),ES(21)) = 22\,971{,}20.$$

Vizsgáljuk meg a G1 csoport aláírásainak távolságát is, az alábbi táblázat értékei alapján:

$T(G_1)$	**7**	**9**	**5**	**6**	**18**	**17**	**4a**	**4b**
7	X	3328,85	4001,25	4504,44	4504,44	5008,60	8577,59	8823,55
9	3328,85	X	4801,17	5176,02	5176,02	4147,17	7683,34	7922,99
5	4001,25	4801,17	X	509,90	509,90	2248,58	7587,16	7604,27
6	4504,44	5176,02	509,90	X	0,00	2190,00	7604,27	7587,16
18	4504,44	5176,02	509,90	0	X	2190,00	7604,27	7587,16
17	5008,60	4147,17	2248,58	2190,00	2190,00	X	6944,98	6926,24
4a	8577,59	7683,34	7587,16	7604,27	7604,27	6944,98	X	509,90
4b	8823,55	7922,99	7604,27	7587,16	7587,16	6926,24	509,90	X

10. táblázat: A G_1 csoport elektronikus aláírásainak távolságai (forrás: saját táblázat)

A táblázatból leolvashatóan az egyes aláírásvektorok távolságai jobban mutatják az egymástól való eltéréseket, mint a vektorok hosszainak különbségei, az értékek sokkal nagyobbak, mint az előző különbségtáblázatban, ami a vektorok széttartására utal. Természetesen ha két aláírásvektor azonos hosszúságú és irányultságú, a távolságvektoruk is nullvektor lesz. Ezek a tulajdonságok alkalmasan felhasználhatók aláírás-csoportok képzésére, illetve a különböző aláírások tulajdonságainak összehasonlítására. Ebben a csoportban a távolságok maximális értéke 8 823,547473 lett.

Vizsgálódásunkat folytatva a G_2 csoporttal, az alábbi értékeket kapjuk:

$K(G_2)$	**14**	**3**	**15**
14	X	994,47	3103,38

$K(G_{2})$	14	3	15
3	994,47	X	2108,91
15	3103,38	2108,91	X

11. táblázat: A G_2 csoport elektronikus aláírásainak különbségei (forrás: saját táblázat)

A vizsgálatba bevont G_2 csoportbeli aláírások maximális különbsége 3 103,382232 volt, minimálisan pedig 994,4703932 értékben különböztek egymástól.

A távolságok ebben a csoportban az alábbi módon alakulnak:

$T(G_2)$	14	3	15
14	X	8554,26	14916,24
3	8554,26	X	19911,55
15	14916,24	19911,55	X

12. táblázat: A G_2 csoport elektronikus aláírásainak távolságai (forrás: saját táblázat)

Ebben a csoportban a távolságok maximális értékére 19 911,547, minimumára 8 554,260225 adódott. A G_1 csoport tehát összetartóbb, mint a G_2.

$T(G_3)$	2	13	16	19	20	12	10	11
2	X	3024,48	3024,48	3024,48	3024,48	3073,26	3427,88	3430,98
13	3024,475137	X	0,00	0,00	0,00	48,78	403,40	406,50
16	3024,475137	0,00	X	0,00	0,00	48,78	403,40	406,50
19	3024,475137	0,00	0,00	X	0,00	48,78	403,40	406,50
20	3024,475137	0,00	0,00	0,00	X	48,78	403,40	406,50
12	3073,26005	48,78	48,78	48,78	48,78	X	354,62	357,72
10	3427,877365	403,40	403,40	403,40	403,40	354,62	X	3,10
11	3430,976272	406,50	406,50	406,50	406,50	357,72	3,10	X

13. táblázat: A G_3 csoport elektronikus aláírásainak különbségei (forrás: saját táblázat)

A G_3 csoportban szintén vannak azonos tulajdonságokkal rendelkező aláírások, ezek közüzemi számlák voltak és a NAV aláírása egy meghiúsulási igazoláson, ami azt mutatja, hogy a szervezetek hasonlóan gondolkodnak olyan aláírások esetében, amelyeket nagy tömegben kell előállítani és személyes közreműködést (kiadmányozást) nem igényelnek. A minimális különbség tehát nulla, a maximális különbségre ebben a csoportban pedig 3 430,976272 adódott.

T(G_3)	2	13	16	19	20	12	10	11
2	X	6961,99	6961,99	6961,99	6961,99	6979,92	7297,63	7298,32
13	6961,99	X	0,00	0,00	0,00	500,00	2192,28	2190,00
16	6961,99	0,00	X	0,00	0,00	500,00	2192,28	2190,00
19	6961,99	0,00	0,00	X	0,00	500,00	2192,28	2190,00
20	6961,99	0,00	0,00	0,00	X	500,00	2192,28	2190,00
12	6979,92	500,00	500,00	500,00	500,00	X	2248,58	2246,35
10	7297,63	2192,28	2192,28	2192,28	2192,28	2248,58	X	100,00
11	7298,32	2190,00	2190,00	2190,00	2190,00	2246,35	100,00	X

14. táblázat: A G_3 csoport elektronikus aláírásainak távolságai (forrás: saját táblázat)

A távolságok értékei itt is nagyobbak, mint a különbségeknél mért értékek, a vektoriális ábrázolásból adódóan. A legkisebb érték az azonosság miatt itt is zéró lett, a legtávolabb egymástól ebben a csoportban pedig (7298,315148 értékkel) az ES(11) – biztosítói e-számla – és az ES(2) – nem minősített rövid távú személyes aláírás – volt.

Az utolsó csoport elemeinek különbségeit a következő táblázat mutatja be:

K(G_4)	21	1	8
21	X	0,36	1388,44
1	0,36	X	1388,08
8	1388,44	1388,08	X

15. táblázat: A G_4 csoport elektronikus aláírásainak különbségei (forrás: saját táblázat)

Minimális távolság adódott a biometrikus aláírás és a PGP aláírás között, és egy vállalati belső aláírás sincs túlságosan messze a PGP aláírásoktól – mindez a hozzá fűződő jogi vélelmekből adódik. Egy belső használatú aláírásnak nem kell teljesítenie a nyilvános szolgáltatásokkal szemben támasztott követelmények többségét.

T(G_4)	21	1	8
21	X	1929,01	2501,36
1	1929,01	X	1893,03
8	2501,36	1893,03	X

16. táblázat: A G_3 csoport elektronikus aláírásainak távolságai (forrás: saját táblázat)

Itt is lényeges különbség fedezhető fel a 0,36 hosszúságkülönbséggel rendelkező vektorok távolsága között (1 929,01).

6. AZ ELEKTRONIKUS ALÁÍRÁS TECHNOLÓGIAFÜGGETLENSÉGE

Az elektronikus közigazgatás kialakításában Juhász [125] nagy szerepet tulajdonít Magyary Zoltánnak, mivel „(…) Magyary Zoltán teoretikusként az elektronikus kormányzat előfutárának is tekinthető. Írásainak nagy része mit sem vesztett aktualitásából, így tehát a XXI. század viszonyaira is alkalmazható.” A digitalizáció tényleges megjelenése a közigazgatásban Magyary munkásságának idejétől későbbre tehető, az alapelvek azonban közösek az elektronikus és nem elektronikus közigazgatásban. Az információs társadalom fogalmát Yonei Masuda 1980-as műve már markánsan használta [131], innen számítható a globális érdeklődés és versenyfutás az az ipari kor után alkalmazható jövőbeli új technológiák és lehetőségek iránt. Az Európai Unió az 1980-as években nyolc keretprogramot (Framework Programme, FP1-8) indított négyéves ciklusokban, legalább kétéves felülvizsgálati igénnyel[211], az EU versenyképességének a megőrzését deklarálva[212]. A legutolsó program – az FB8, Horizon 2020 néven lett ismert[213]. Az első program (FP1) tudományos-technológiai célkitűzéseket tartalmazott[214], mivel korábban (1973-ban) is még csupán az elektronikai ipar volt a fejlesztés fókuszában[215], a mikrochip gyártás kezdeti időszakában vagyunk, a (mikro)számítógépek megjelenésére (Micral 1973 május, Altair 8800 1974) és elterjedésére várni kellett még, az 1980-as években jött létre az IBM PC (1981) és ekkor indult meg a mikroszámítógépek vállalati és otthoni elterjedése is. 1970-ben az Amerikai Egyesült Államokban kb. 100.000 számítógép működhetett [202], de mivel a mikroszámítógépek ekkor még nem voltak jelen, úgynevezett nagyszámítógépes (többfelhasználós) környezetek működtek ebben az időben, ezek irányították a szabályozási és folyamatalkotási elképzeléseket.

---

[211] Lásd Framework programme for research 1984-87, COM(83) 260 final, 17 May, 1983, Article 3: „The Council hereby approves the principle of framework programmes for periods of four years which will be reviewed at least every two years and revised if necessary.” (Bulletin of the European Communities, Supplement 5/83, pages 7-11)

[212] Lásd Growth, Competitiveness, Employment -the challenges and ways forward into the 21st century - White Paper. COM/93/700 Final

[213] Lásd https://ec.europa.eu/programmes/horizon2020/en (2019 február 21.)

[214] Lásd Council Resolution of 25 July 1983 on framework programmes for Community research, development and demonstration activities and a first framework programme 1984 to 1987, OJ C 208, 4.8.1983, p. 1–4, Annex I: Scientific and technical objectives (1984 to 1987)

[215] Lásd Scientific and Technological Policy Programme (submitted to the Council by the Commission on 1 August 1973), COM(73) 1250, Parts I & II, 25 July 1973.

A közigazgatás digitalizációja Európában a Bangemann-riport 1994-es korfui elfogadása után indult meg, ideértve az elektronikus közigazgatás központilag koordinált kialakítását és szabályozását[216], habár az elektronikus kommunikáció és adattovábbítás igénye már korábban is felmerült. Legelső magyar jogszabályként – a jelentős előkészítő munkát követően – a 2001. évi XXXV. törvényt (Eat.) említettük, amely az 1999/93/EK irányelv 13. cikke által előírt – de ekkor még nem kötelező érvényű – nemzeti jogalkotásként[217] került be a magyar jogrendbe, mivel teljes jogú tagságunk későbbre datálódik. Az irányelv fő célkitűzése, hogy keretet biztosítson az elektronikus aláírások európai alkalmazásához, továbbá katalizálja az elektronikus aláírások jogi elismerését minden tagállamban és a belső piac megfelelő működése érdekében hozza létre az elektronikus aláírásra és egyes hitelesítésszolgáltatásokra vonatkozó jogi keretet. Az irányelv nem foglalkozott a szerződések megkötésének és érvényességének szempontjaival, sem más olyan jogi kötelezettségekkel, amelyekre nemzeti vagy közösségi jogszabályokban előírt alaki követelmények vonatkoznak, továbbá nem sérthette a nemzeti vagy közösségi jogszabályokban előírt, a dokumentumok felhasználását szabályozó rendelkezéseket és korlátozásokat sem.

Az elektronikus aláírási törvény megalkotását széleskörű és sok résztvevő által figyelemmel kísért előkészítő munka előzte meg, ahol dönteni kellett a szabályozás egyes tulajdonságairól, így a technológiához való viszonyáról is. Fontos kérdés minden technológiát érintő normatív szabályozásban, hogy mekkora függést emelhet be a jogalkotó a szabályozásba, vagy mit tud elérni technológia-független szabályozók kialakításával. Az Európai Unió a kezdetektől törekedett arra, hogy a szabályozásban olyan fogalmakat használjon, amelyeket a műszaki szabványok még nem foglaltak el és ruháztak fel sajátos műszaki tartalommal. Habár számos helyen felfedezhető a hasonlóság a nyilvános kulcsú infrastruktúra elemei és az európai jogi szabályozás által használt fogalmak között, azonban a különbségek is lényegesek a technológiafüggetlenség biztosíthatóságában. Ugyanis egy aszimmetrikus kulcsú kriptográfia titkos kulcsát megfeleltethetjük az „aláírás-létrehozó adat” fogalomnak, illetve a nyilvános kulcsát az „aláírás-ellenőrző adat” fogalmának, azonban ebből nem következik az, hogy csak ez a két műszaki megvalósítás képes a jogi fogalomhasználat során bármilyen kontextusban

[216] A műszaki fejlődésnek abban a szakaszában vagyunk ekkor, amikor a 286, 386 és 486 PC-k után az Intel Pentium I. és ÍI. processzorára épülő számítógépek jelentek meg a világban.
[217] „A tagállamok hatályba léptetik azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek 2001. július 19-ig megfeleljenek.”

megjelenni. Amennyiben így lenne vagy ezt követné a bírói gyakorlat, akkor az a technológiafüggés megvalósítását jelentené a gyakorlatban. Technológiafüggetlen normatíva alapján technológiafüggő gyakorlat kialakulását nem tekinthetjük természetes és példaértékű folyamatnak a közigazgatásban, elismerve a jogbizonytalanság csökkentése iránti erős igényt[218]. A két szabályozási elv előnyeit és hátrányait Szilágyi [127] dolgozta fel 2000-ben az elektronikus aláírási törvény tervezete kapcsán, ahol megállapította, hogy a technológiafüggő szabályozás ugyan csökkenti a jogbizonytalanságot és kisebb teret ad a bírói gyakorlatban a jogértelmezésnek, de egy adott technológia preferálásával egyrészről folyamatos felülvizsgálati igényt generál, másrészről súlyosan beavatkozhat a piaci folyamatokba is[219]. A technológiafüggetlenség képes párhuzamosan több technológiának is tered adni, engedi új technológiák kifejlődését és használatba vételét, azonban csökkenti a jogbiztonságot a megfelelőség kereteinek tágításával, ami inkonzisztens bírósági ítéletekhez vezethet. Ezzel kapcsolatosan az írásbeliség magyar értelmezésénél mutatott rá Baranyi et. al. [129] arra, hogy egyrészről az általános definíciók a gyakorlatban nem használhatók, a résztvevőknek minden egyes esetben meg kell vizsgálniuk és el kell dönteniük, hogy az adott megoldás megfelel-e a definíciónak, ami gyakorlatilag arra a kérdésre vezeti vissza a megfelelőséget, hogy az erre vonatkozó állítást mivel tudja bizonyítani (hitelesíteni) az érdekelt fél. Másrészről az írásbeliség jogi vélelme az Eat. hatályának megszűnésével ugyan kikerült formailag a magyar jogrendből, de tartalmilag tovább él a bírósági gyakorlatokban, számos példa hozható fel arra nézve, hogy a bíróságok ahelyett, hogy az adott elektronikus aláírási forma megfelelőségét vizsgálnák meg az eIDAS 3. cikk 11. definíciójában, illetve a 26. cikkben foglaltak teljesülése tekintetében, arra való hivatkozással utasítják el az írásbeliség jogi vélelem fennállását, hogy az alkalmazott aláírás nem volt fokozott biztonságú elektronikus aláírás. A kialakult gyakorlatot segítették az irányelvhez kapcsolódó műszaki szabványok is, amelyek a bevezetőjükben kihangsúlyozták, hogy „a szabvány szerint készített elektronikus aláírások megfelelnek a jogszabály által a fokozott biztonságú elektronikus aláírásokkal szemben támasztott

[218] Az informatikai szabályozás problémáiról Szádeczky Tamás írt PhD értekezést 2011-ben [126]. Tudományos problémaként vizsgálta meg azt, „hogy a heterogén informatikai biztonsági szabályozás hazánkban olyan követelményeket támaszt a kötelezettek felé, amelyeket nehéz egyértelműen meghatározni. Ezzel a szabályozás hatékonysága romlik és a jogbizonytalanság is növekszik."

[219] A kormányzati szabályozás és a piaci igények közötti ellentmondásokról a finn eID példát érdemes megemlíteni, amelynek három szakaszát (bevezetés, kihasználatlanság, újratervezés) Rissanen [128] részletezi.

követelményeknek”[220], így a jogalkalmazóknak csak annyit kellett megnézniük, hogy az adott aláírás a hivatkozott szabványoknak megfelelően lett-e elkészítve vagy sem. Annak igazolása, hogy egy adott nem szabványos műszaki megoldás megfelel-e a fokozott biztonságú aláírásokkal szemben támasztott követelményeknek, sok esetben meghaladja egy bírósági eljárás lehetőségeit, ha eltérő mélységű indirekt, önkéntes-önszabályozott, a felületesen szabályozott és a részletesen szabályozott területek szabályozásai alapján kellene dönteni ahogyan azt Szádeczky megállapította ([126]: 85).

További probléma az írásbeliséggel, hogy az írásbeli formák eltérőek lehetnek az egyes országokban. A fentiekből adódóan Magyarországon írásbelinek számíthat egy fokozott biztonságú elektronikus aláírással ellátott dokumentum, amihez Németországban nem fűződik ugyanez, mivel a német Polgári Törvénykönyv (Bürgerliches Gesetzbuch) úgy rendelkezik[221], hogy amennyiben jogszabály elektronikus írásbeliséget rendel el, akkor a kibocsátónak a saját nevét és a minősített elektronikus aláírását el kell helyeznie az adott dokumentumon az írásbeliség elektronikus teljesítéséhez.

A kockázat egy fokozott biztonságú elektronikus aláírásnak mondott aláírás elfogadásában ott rejlik, hogy amennyiben az aláírás létrehozója (piaci termék esetében a gyártói nyilatkozat) alá is támasztja a követelményeknek való megfelelőség fennállását az adott műszaki megoldás esetében, egy bírósági eljárásban hogyan és mennyire lesznek ezek a bizonyítékok felhasználhatók, hogyan jelenik meg itt az „in dubio pro reo” elv például. Vélhetően az aláírás megtörténtének (eIDAS 3. cikk 10.) és a fokozott biztonságú aláírás követelményeinek való bizonyítást (eIDAS 26. cikk) kell majd kettéválasztani ilyen esetekben. A bírói mérlegelés szabadságáról és kötöttségeiről, a mérlegelési jog

[220] Lásd például ETSI ETSI TS 101 733 V2.2.1 (2013-04), p.7. „An electronic signature, as used in the present document, is a form of advanced electronic signature as defined in the Directive”, vagy ETSI TS 101 903 V1.4.2 (2010-12), p.6. „TS 101 733 [1] defines formats for advanced electronic signatures that remain valid over long periods, are compliant with the European Directive”, illetve ETSI TS 102 778-1 V1.1.1 (2009-07), p.4. „The formats defined in the present document, are able to support advanced electronic signatures as defined in the Directive”

[221] Lásd Bürgerliches Gesetzbuch, § 126a Elektronische Form: (1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen. ("Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 7 des Gesetzes vom 31. Januar 2019 (BGBl. I S. 54) geändert worden ist") (http://www.gesetze-im-internet.de/bgb/BJNR001950896.html, 2019. március 5.)

valódi funkciójáról Erdős és Kecskeméti adott rendszerszemléletű összefoglalást és illusztrálták ennek működését egy adójogi kitekintéssel [130].

Az elektronikus aláírás globális technológia révén számos más jogalkotási problémát is felvetett. Elegendő csak a Pp. 325. § (1) f) rendelkezésére visszautalni[222], ami teljes bizonyító erejűnek tekinti a minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást a keletkezés helyétől függetlenül. A „minősített tanúsítvány" kifejezés azt a kötöttséget tartalmazza, hogy a tanúsítványt egy az Európai Unióban székhellyel rendelkező minősített bizalmi – vagy ilyen szolgáltató által felülhitelesített – szolgáltatónak kell kiadnia az eIDAS-ban foglalt előírások betartása mellett, de nem köti meg az aláíró kilétét. Ez azt jelenti, hogy Magyarország teljes bizonyító erejűnek tekinti azt az elektronikus aláírást, amelyhez az aláírás-ellenőrző adatot minősített tanúsítványba foglalta egy EU-s minősített bizalmi szolgáltató, az aláírás-létrehozó adatot nem helyezték el minősített aláírás-létrehozó eszközön és amelyet a világban bárhol előállíthattak. Tekintettel arra, hogy az ilyen típusú aláírások uniós elfogadásra nézve előírásokat az eIDAS nem tartalmaz, csak az egyes nemzeti jogrendek adhatnak támpontot arra nézve, hogy az adott tagállamban milyen jogi vélelmek fűződnek a magyar részről teljes bizonyító erővel felruházott aláíráshoz.

6.1. AZ EIDAS

Az eIDAS rendelet 2014-ben került be az európai jogrendbe az 1999/93/EK irányelv felváltásaként és az addigi felülvizsgálatok által javasolt kiegészítések implementálásaként. Fontos különbség, hogy míg az irányelv, mint jogforrás, implementációs jogi aktusokat igényelt a tagállamok részéről, addig a rendelet azonnal és minden további tagállami jogi aktus nélkül hatályba lép minden tagállamban törvényi szinten.

A szabályozás alapvetően technológiafüggetlennek mondható annak ellenére, hogy az absztrakció során a már létező és Diffie-Hellman [20] óta erőteljes mértékben elterjedt aszimmetrikus kriptográfiára épülő nyilvános kulcsú infrastruktúra műszaki elemeit vették láthatóan alapul a jogszabály szövegezésében, illetve a referenciaként megadott műszaki szabványokban is. A technológiafüggetlenséget azonban mégis erősíti

[222] Pp. 325. § (1) Teljes bizonyító erejű a magánokirat, ha f) az elektronikus okiraton az aláíró a (...) minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírását vagy bélyegzőjét helyezte el, és – amennyiben jogszabály úgy rendelkezik – azon időbélyegzőt helyez el.

az, hogy a Rendelet nem használ műszaki fogalmakat, nem teszi kizárólagossá a PKI-t és nem mondja azt, hogy további szabványok beillesztése a követelmények közé nem lehetséges. Azonban ezeknek a nem tiltott aktusoknak a jövőbeli megvalósításához az európai jogalkotói szándék és akarat elsőrendű fontosságú.

A Rendelet szövegét és a műszaki szabványokat megvizsgálva, az egyes fogalmakat egymásnak meg lehet feleltetni, a jogi fogalmak megfeleltetése a műszaki fogalmaknak szürjektív leképezés lesz. A PKI és a Rendelet fogalmainak megfelelését – a teljesség igénye nélkül, példálózó felsorolást alkalmazva – az alábbi táblázatban ismertetjük – Rátai munkásságát [2] is felhasználva:

eIDAS referencia	**Jogi fogalom**	**Műszaki fogalom**
3. cikk 2.	elektronikus azonosító eszköz	eID[223] token
3. cikk 10.	elektronikus aláírás	digitális aláírás[224]
3. cikk 13.	elektronikus aláírás létrehozásához használt adat (aláírás-létrehozó adat)	titkos kulcs
3. cikk 14.	elektronikus aláírás tanúsítványa	X.509v3 tanúsítvány (letagadhatatlanság kulcshasználat jelzésével[225])
3. cikk 19.	bizalmi szolgáltató	tanúsítvány-kibocsátó (Certificate Authority, CA), időbélyeg-kibocsátó (Time Stamp Authority, TSA)
3. cikk 22.	elektronikus aláírást létrehozó eszköz	kriptográfiai modullal ellátott kártya, USB-token[226], szoftveres kulcskonténer
3. cikk 23.	minősített elektronikus aláírást létrehozó eszköz (MALE, QSCD[227])	tanúsított kriptográfiai modullal ellátott kártya, USB-token

[223] eID: electronic identification, elektronikus azonosítás
[224] A megfelelés nem teljeskörű, az elektronikus bélyegző és az elektronikus aláírás lehet digitális aláírás is, de nem minden digitális aláírás lesz elektronikus aláírás vagy elektronikus bélyegző.
[225] Bővebben lásd RFC 5280, 4.2.1.3. Key Usage fejezetét.
[226] USB: Universal Serial Bus, univerzális soros busz
[227] QSCD: Qualified Signature Creation Device, minősített aláírást létrehozó eszköz.

eIDAS referencia	Jogi fogalom	Műszaki fogalom
3. cikk 25.	elektronikus bélyegző	digitális aláírás
3. cikk 28.	elektronikus bélyegző létrehozásához használt adatok	titkos kulcs
3. cikk 29.	elektronikus bélyegző tanúsítványa	X.509v3 tanúsítvány (digitális aláírás, tanúsítvány aláírás vagy CRL[228] aláírás kulcshasználati jelzéssel[229])
3. cikk 30.	elektronikus bélyegzőt létrehozó eszköz	kriptográfiai modullal ellátott kártya vagy USB-token, szoftveres kulcskonténer
3. cikk 35.	elektronikus dokumentum	Word fáj (.docx), Excel fájl (.xlsx), aláírás fájl (.sig), szövegfájl (.txt), hangfájl (.mp3), video-fájl (.mp4) stb.
3. cikk 38.	weboldal-hitelesítő tanúsítvány	SSL/TLS[230] X.509v3 tanúsítvány
3. cikk 40.	érvényesítési adatok	X.509v3 tanúsítványok, tanúsítvány-visszavonási listák (CRL), online lekérdezett tanúsítvány állapotok (OCSP)

17. táblázat: ábra: Jogi és műszaki fogalmak a Rendeletben (forrás: saját táblázat)

Globálisan érvényes kölcsönösen egyértelmű (bijektív) megfeleltetést nem lehetséges megtenni a két fogalomrendszer között, mivel egyrészről különböző kultúrával rendelkező társadalmakban történt meg az evolúciójuk, ugyan erős kölcsönhatásokkal, de megőrizve a különbözőséget is, másrészről a fogalmak definíciója sem egységes a különböző társadalmakban, ami szintén korlátozza az egyértelmű megfeleltetések kialakítását. Példának okáért az Európai Unióban jogi személy nem hozhat létre elektronikus aláírást csak bélyegzőt, azonban ilyen korlátozást más társadalmak nem

[228] CRL: Certificate Revocation List, tanúsítvány-visszavonási lista
[229] Bővebben lásd RFC 5280, 4.2.1.3. Key Usage fejezetét.
[230] SSL: Secure Socket Layer, biztonságos internet csatlakozó réteg – az RFC 6101 specifikálja; TSL: Transport Layer Security: átviteli réteg biztonság – az RFC 5246 specifikálja. Biztonságos kommunikációt valósítanak meg a szállítási rétegben (pl. TCP, Transmission Control Protocol, átvitel vezérlő protokoll). A TLS az SSLv3 verzióján alapuló utódja.

vezettek be. Ez azt a furcsa helyzetet eredményezte, hogy EU jogi személy digitális aláírása nem lesz elektronikus aláírás. Elméletileg megoldást jelenthetne az atomizálás – olyan kis darabokra való felbontás, amelyek egyértelműek lennének minden fogalomrendszerben, de ez egyrészről újabb fogalmak felesleges bevezetését jelentené, másrészről az összegzésnél ismét előjönnének a mostani problémák, így ennek a módszernek a tárgyalásával itt nem foglalkozunk.

6.2. A BIOMETRIKUS ALÁÍRÁSOK

Az elektronikus ügyintézés elterjedését az elektronikus aláírásokra alapozva próbálták meg elterjeszteni 2009-ig, a Ket. akkori szellemiségének megfelelően, ami nem vált be és az elektronikus aláírásnak az X.509-es tanúsítványokon alapuló változata nem terjedt el széles körben állapította meg Balogh és Budai ([190]: 39). Ennek okaként az eszközigényt és a hozzáféréshez szükséges költséget nevezték meg az uniós felülvizsgálatok során. Az ezt követő korszakban a legnagyobb szerepet az elektronikus ügyintézésben az Ügyfélkapu kapta Magyarországon, ami nem az ügyfelek saját aláírására alapozta az ügyekben felmerülő dokumentumok hitelességét, hanem az ügyfelek hitelesítését követő központi digitális aláírásra. Ez indokolja annak a kérdésnek a felvetését, hogy vajon létezhet-e olyan modell, amelyik elterjedése széles körben valósulhat meg az ügyfelek saját – esetleg nem X.509 alapú, de központosítható – aláírására alapozva. Az elektronikus aláírás kollektív főnév. Beletartozik a papíralapú aláírás digitálisan szkennelt és fájlként tárolt változata, egy e-mail címén lévő gépelt név vagy az e-mai fejlécében lévő e-mail cím, de akár egy biztonságos, minősített elektronikus aláírással tárolt, kriptográfiai úton létrehozott elektronikus aláírás is. Fontos, hogy itt olyan elektronikus aláírásokról beszélünk, amelyek elektronikusan csatolva vannak egy másik dokumentumhoz. Az aláírás és a dokumentum közötti kapcsolat lehet fizikai és logikai, ez utóbbi esetben két különálló fájl is reprezentálhatja a dokumentumot és az aláírást. Meg kell említenünk, hogy az „elektronikus adatok” fogalma értelmezhető szigorúan (digitális értelemben) és szélesebb értelmezési körben, ami már a digitális, a digitalizált és az elektronizált adatokat is magában foglalja. Elektronizált aláírásra példa az autopen által generált aláírás [135], digitalizált aláírásra példa egy szkennelt dokumentumban szereplő kézi aláírás [136], digitális aláírásra példa a cégbíróságokra beadott beadványok aszimmetrikus kriptográfián alapuló aláírása[231]. A fókusznak az

[231] Lásd https://www.e-cegjegyzek.hu/e-cegeljaras/e_cegeljaras_utmutato.htm (2019. február 22.)

elektronizált információkra való kiterjesztése mellett érvel Haig, amikor rámutat arra, hogy ezek is képviselhetnek támadási célértéket, így a védelmük kívánatos lenne [138].

Számos vállalat valósított meg biometrikus aláírást az ügyfelek beleegyezésének vagy elfogadásának egyszerű eszközeként. Az aláírás-létrehozáshoz felhasználható adatok a nyilvános kulcsokon túlmenően más adatok is lehetnek, ha az eIDAS valóban technológiasemleges jogszabály. Ebben az esetben a biometrikus jellemzők vagy paraméterek is használhatók a PKI-világ „titkos kulcsának" megfeleltethető – de nem teljes mértékben azzal megegyező funkcionalitású – aláírás-készítő adatként elektronikus aláírás létrehozásához. Ebben az esetben az aláíró biometrikus paraméterét használják (és csatolják) a dokumentumhoz. Sok esetben a humán aláírás elektronikus képe az egyetlen alkalmazott biometrikus paraméter az aláíráshoz. Lehetséges az ujjlenyomat, a hang, a tenyérnyomtatás, az írisz vagy más ismert biometrikus attribútumok használata is, amelyeket a fizikailag jelen lévő természetes személy hitelesítésére már régóta használnak szabványos módon[232].

A humán aláírás fogalmát a megfelelő elektronikus eszközökben létrehozott aláírásra is ki lehet terjeszteni. Ebben az esetben az elektronikus aláírás nem kizárólag a faxon látható grafikus megjelenést jelentheti, hanem a biometrikus aláírások alatt az emberi aláírással kapcsolatos további jellemzőket is tartalmazó adatállományokat is érteni kell, ha a fejlett elektronikus aláírás követelményeit teljesíteni szeretnék. Például egy elektronikus toll mozgatása során az elegendően magas mintavételezési aránnyal rögzített dinamika, sebesség és nyomás adatai lehetnek az adott aláírás vonatkozásában nagy megbízhatósággal egyediek a humán entitásra nézve. Ha matematikai értelemben nem is vehetjük ezt 100%-ra, annak ismeretében, hogy nagyon kis valószínűséggel fog az emberiség minden egyede ugyanott biometrikusan aláírni, az egyediség a kellő mértékben biztosítható lehet. Van egy másik oldala az egyediségnek, hiszen elméletileg senki sem hozhatja létre ugyanazt az aláírást kettő vagy több alkalommal, amit megfelelően finom mintavételezési eljárással ki is lehet használni az ellenőrzési gyakorlatban. Ez azonban a szimpla összehasonlítástól eltérő módszer alkalmazását igényli a megfelelő validálási folyamatokhoz, ugyanis a feladat az, hogy össze kell rendelni a különböző aláírásmintákat az aláíróval úgy, hogy lehetőleg nem utasítja el a rendszer az aláíró saját aláírásait (ezt mutatja a hamis elutasítási ráta, False Rejection

[232] Lásd NIST, Special Publication 800-63-2, Electronic Authentication Guideline, USA, 2013.

Rate, FRR) és meg kell akadályozni a hamis aláírások elfogadási küszöbön belülre kerülését (ezt mutatja a hamis elfogadási ráta, False Acceptance Rate, FAR). Az ellenőrzés során ki kell térni a már tárolt jellemzők statisztikai alapú módosításának (pl. Gauss-zajjal való kombinálásának) felismerésére és a másodlagos eljárásokkal generált aláírások elutasítására is. A kézi aláírások további aspektusaival csak olyan mértékben foglalkozom, amennyire azok képesek alátámasztani a fokozott biztonságú elektronikus aláírásokkal szemben támasztott követelményeket, további részletes technológiai vizsgálat nem volt célom.

Az alábbi kifejezéseket a következő technikai értelmezésben fogom használni a biometrikus aláírások tárgyalásában:

1. az elektronikus aláírás végrehajtása: speciális elektronikus adatok rögzítése és hozzákapcsolása egy dokumentumhoz, általában az elkötelezettség vállalása és az aláíró hitelesítése érdekében, egy kötelezettségvállalás elszámoltathatóságának biztosítására.

2. humán aláírás: egy adott személy által egy adott eszközzel (toll vagy ceruza) vagy esetleg az ujjával létrehozott aláírás.

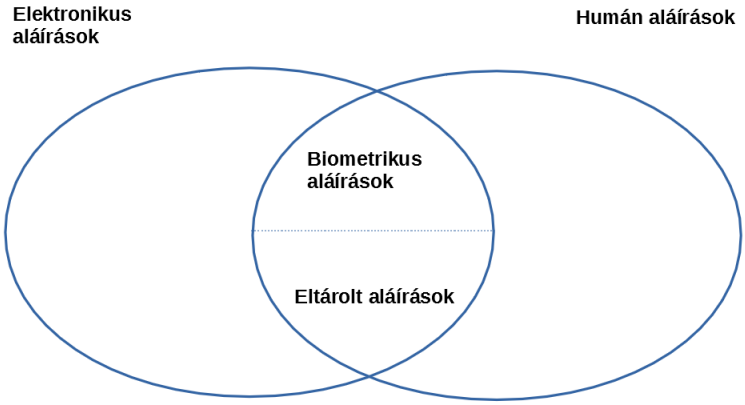
3. biometrikus elektronikus aláírás: a biometrikus adatok digitális formában történő rögzítésére és feldolgozására alkalmas elektronikus eszközön természetes személy aktív tevékenysége által létrehozott és rögzített adathalmaz.

4. elektronikusan mentett aláírás: olyan – tetszőleges időben és eszközzel készült – humán aláírásról rögzített adathalmaz, amelyet egy eszköz elektronikusan rögzített és egy (nem feltétlenül ugyanaz az) eszköz elektronikus formában tárol.

A biometrikus elektronikus aláírás és az elektronikusan mentett aláírás között a legfontosabb különbség az, hogy az aláírás készítésének és rögzítésének a folyamat elválasztott az elektronikusan mentett aláírásoknál, de nem választható el a biometrikus elektronikus aláírások esetében. Fontos visszautalni az aláírás eIDAS definíciójára, ezt az aláírást az aláíró valamely digitális tartalom aláírására használhatja, ilyen értelemben a kizárólag hitelesítési céllal történő aláírás nem számít elektronikus aláírásnak, ha nincs olyan elektronikus dokumentum, amelyhez hozzákapcsolódik[233]. Ekkor a mentett aláírás

[233] Az IBM 2018-ban készült tanulmánya szerint a kézi aláírás, mint hitelesítési módszer nem frekventáltan használt az online felmérést kitöltő 3.977 válaszadó szerint az USA-ban, az EU-ban, Indiában, Ausztráliában és Új-Zélandon [137] :7.

csak az emberi aláírás rögzített és újra felhasználható változatát jelenti, míg a biometrikus aláírás más, biometrikus adatokat is tartalmaz, amelyeket az emberi aláírás jellemez, amelyet feldolgozásra és validálásra lehet használni, de a definíció értelmében az ismételt felhasználás nem lehetséges. Ebben a tekintetben az autopen eszközben rögzített aláírásminta az elektronikusan mentett aláírások osztályába tartozik, mivel egy előre elkészített aláírás-programot ismétel nulla variábilitással. A definíciók közötti kapcsolatokat az alábbiakban mutatjuk be:



19. ábra: Kapcsolat a biometrikus elektronikus aláírások között (forrás: saját ábra)

Az ábrából az is leolvasható, hogy a humán aláírásoknak természetesen van elektronikus világon kívüli része is, illetve az elektronikus aláírások mindegyike nem lesz biometrikus aláírás, hiszen a kriptográfiával készült aláírások valóban csak a természetes személyekhez kapcsolhatók, de nem lesz biometrikus értelemben közük az aláíró aláírási aktivitásához.

Meg kell említeni ezen a ponton a biometrikus aláírások közigazgatási felhasználási lehetőségét. A 2010. évi CXXVI törvény[234] tette lehetővé a biometrikus aláírások használatát a fővárosi és megyei kormányhivatalok ügyfélszolgálatain, a járási (fővárosi kerületi) hivatalok kormányablakaiban, illetve a települési ügysegédeknél az elektronikus dokumentumok ügyfél általi hitelesítésére, megfelelő biometrikus adatok felhasználásával, biometrikus verifikáció céljából. Az aláírás megtörténte után a hivatal

[234] Lásd 2010. évi CXXVI. törvény a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról, 20/J. §, amelyet a 2016. évi CIV. törvény a központi hivatalok felülvizsgálatával és a járási (fővárosi kerületi) hivatalok megerősítésével összefüggő egyes törvények módosításáról, valamint egyes költségvetési szervek feladatainak átadásáról 88. § (11) iktatott be az Országgyűlés 2016. október 11-i ülésnapja alapján, 2016. október 20. kihirdetési dátummal és 2017. január 1-i hatállyal.

ellenőrzi a mintával való egyezést és a vizsgálat eredményéről tanúsított, zárt rendszer által kiállított, a dokumentumazonosítót is tartalmazó elektronikus igazolást csatol a dokumentumhoz[235]. Az így előállt elektronikus igazolással ellátott dokumentum teljes bizonyító erejű magánokirat[236].

6.3. A FOKOZOTT BIZTONSÁGÚ BIOMETRIKUS ALÁÍRÁS

Az Amerikai Egyesült Államok jogi rendszere hármas szabályozást követ az elektronikus aláírások kapcsán. A szövetségi jog hatálya alá tartozó, minden tagállamban üzleti tevékenységet folytató szervezetek az elektronikus aláírási törvény (ESIGN)[237] alapján, a magánszemélyek, üzleti vállalkozások és a kormányzat közötti szerződésekre az egységes elektronikus tranzakciós modelltörvényként megfogalmazott (UETA[238]) ajánlást állami szinten törvénybe iktató államok ennek alapján, illetve az UETA-t nem elfogadó államok (Washington[239], Illinois[240] és New York[241]) pedig saját, hasonló tartalmú törvényeik alapján értelmezik az elektronikus aláírást. Az elfogadható aláírásokkal szemben a jogszabályok a definíció teljesítésén túl további követelményeket rendeltek el, így jogosan merült fel az osztályozás igénye az elektronikus aláírások halmazán.

A biometrikus aláírásokkal kapcsolatosan több kérdés merülhet fel azok alkalmazhatóságával kapcsolatosan a jogi szabályozás által előírtak teljesítése kapcsán.

1. Kérdés: Melyek a fejlett elektronikus aláírás létrehozásának követelményei az eIDAS rendelettel kapcsolatban?

Az eIDAS-alapú fokozott biztonságú aláírás létrehozása csak nyilvános bizalmi szolgáltatások használatával volt lehetséges az eddigi gyakorlatban. A fokozott biztonságú elektronikus aláírások definíciójából és követelményeiből azonban nem

[235] 2010. évi CXXVI. törvény 20/J. § (5)
[236] 2010. évi CXXVI. törvény 20/J. § (6)
[237] Electronic Signatures in Global and National Commerce Act (ESIGN), PUBLIC LAW 106–229—JUNE 30, 2000
[238] Uniform Electronic Transactions Act (UETA), July 29, 1999.
[239] Lásd Session Laws Of The State Of Washington, 1996. március 29., Chapter 250, Electronic Authentication Act, 1996. március 29. (a hatályba lépés dátumát 1998. január 1-ével határozta meg a dokumentum, de a felkészülés megkezdéséről 1996. július 1-i hatállyal rendelkezett). A törvény a bevezetőjében már tartalmazta az „electronic signatures” kifejezést, habár a digitális aláírásokról rendelkezett leginkább.
[240] Lásd (5 ILCS 175/)Electronic Commerce Security Act, 1999. július 1.
[241] Lásd 9 CRR-NY 540. Electronic Signatures And Records Act, 2000. március 27.

következik, hogy bizalmi szolgáltatásnak kell léteznie az aláírásokkal kapcsolatosan az alkalmazhatóság feltételeként.

2. Kérdés: Lehetséges-e az eIDAS alapján fokozott biztonságú elektronikus aláírás létrehozása zárt rendszerekben és a közigazgatás háttérfolyamataiban?

Az eIDAS biztosan nem alkalmazható zárt rendszerekben, a közigazgatás belső zárt rendszereiben és háttér-eljárásaiban, illetve nem érintheti a szerződések megkötésére és érvényességére, sem más, alaki követelményekkel kapcsolatos jogi vagy eljárási kötelezettségekre vonatkozó nemzeti vagy uniós jogot.[242]. Azonban kérdés, hogy a definíciói tekinthetők-e érvényesnek ezekben a rendszerekben, vagyis az a kérdés, hogy a definíciók alkalmazása is tilos ezekben a rendszerekben vagy csupán a kötelező alkalmazásuk van megtiltva, de az önkéntes alkalmazás lehetősége fennállhat. Az Eübszt. definíciói és eIDAS-ra való hivatkozása az utóbbi értelmezést sugallják.

3. Kérdés: Lehetséges-e eIDAS-on alapuló fokozott biztonságú elektronikus aláírás készítése aláíró tanúsítvány létezése nélkül?

Habár az eddigi gyakorlatban ilyen megoldást idáig nem ismeretes, a definíciókból és a követelményekből nem következik az aláíró tanúsítvány létezésének szükségessége. Az aláíró tanúsítvány megkövetelése a nyilvános felügyeletet biztosítja az aláíráshoz szükséges szolgáltatásokhoz, ugyanis, ha létezik aláíró tanúsítvány, akkor azt csak nyilvánosan működő szolgáltató biztosíthatja. A nyilvános szolgáltatók ellenőrzöttsége pedig a nemzeti felügyeleti hatóságok által biztosított[243]. A kérdés tehát más megfogalmazásban annyit jelent, hogy lehetséges-e fokozott biztonságú elektronikus aláírást előállítani olyan módon, amely nincs a nemzeti felügyeleti hatóságok látókörében. Az eIDAS nem tartalmaz explicit előírást erre nézve.

4. Kérdés: különbözik-e az Eübszt. és az eIDAS hatóköre?

Igen, a két jogszabály hatóköre különbözik, mivel az eIDAS a bizalmi szolgáltatásokra és az elektronikus azonosításra vonatkozik, amelyeket az Eübszt. kiegészít a bizalmi szolgáltatásokkal szemben támasztott nemzeti előírásokkal és az elektronikus ügyintézésre vonatkozó szabályokkal.

[242] Lásd eIDAS Preambulum (21), 2. cikk (2) és (3)
[243] Lásd eIDAS 17. cikk (3)

5. Kérdés: használható-e az Eübszt által meghatározott fokozott biztonságú elektronikus aláírás fogalma zárt rendszerekben, megállapodásokban és a közigazgatás háttérfolyamataiban?

Az Eübszt. kiterjesztő hatása miatt a válasz igen, a fokozott biztonságú elektronikus aláírás fogalma használható zárt rendszerekben, megállapodásokban és a közigazgatás háttérfolyamataiban, de nem kötelező jelleggel. Műszaki értelemben mindenképpen létrehozhatók ezeken a területeken is olyan elektronikus aláírások, amelyek kielégítik a fokozott biztonságú elektronikus aláírással szemben támasztott követelményeket, a jogi megítélésüktől függetlenül.

6. Kérdés: ha jogszabály fokozott biztonságú elektronikus aláírást említ, az eIDAS vagy az Eübszt. definícióját kell alkalmazni Magyarországon?

Az a sajátos helyzet állt itt elő, hogy a jogszabályok érvényességi köre nem befolyásolta a fokozott biztonságú elektronikus aláírás fogalmát, ugyanis az eIDAS definícióját (eIDAS 3. cikk 11.) az Eübszt. meghivatkozza és nem definiál új definíciót erre nézve. Vagyis akár az Eübszt. akár az eIDAS felől jut el valaki a fokozott biztonságú elektronikus aláírás fogalmához, az erre vonatkozó követelmények (eIDAS 26. cikk) ugyanazok.

Mindezek alapján állítható, hogy fokozott biztonságú elektronikus aláírás készíthető az eIDAS és az Eübszt. alapján is, az erre vonatkozó feltételek megegyeznek, azaz ugyanazokat a követelményeket kell kielégítenie minden egyes aláírásnak, amelyik fokozott biztonságúnak tekinthető.

6.3.1. Követelmények

2016. július 1. után az elektronikus aláírások jogi definícióinak elemzéséhez az Európai Unió eIDAS-rendeletét kell alapul venni az Európai Unióban. Az eIDAS – akárcsak korábban az 1999/93/EK irányelv) az elektronikus aláírások három szintjét különbözteti meg, normál, fokozott biztonságú és minősített. A szabályozás a fokozott biztonságú aláírásokkal szemben a következő követelményeket határozta meg a 26. cikkben:

a) kizárólag az aláíróhoz köthető;

b) alkalmas az aláíró azonosítására;

c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;

d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Habár a biometrikus elektronikus aláírások vonatkozásában még hiányoznak a kapcsolódó szabványok és a szabványos aláírás-ellenőrzési folyamatok leírásai, számos szabvány áll rendelkezésre a különböző biometrikus adatok, például a kézírás, az ujjlenyomat és a hang rögzítésével, szállításával és tárolásával kapcsolatosan. A biometrikus adatok rögzítésével képzett digitális adatokat széles körben használják hitelesítésre [137] Európában, az Amerikai Egyesült Államokban és Ázsiában is. Egyes kutatási irányzatok azt a célt tűzték ki, hogy a biometrikus jellemzők (ujjlenyomatból származó minutia-pontok) segítségével digitális aláírásokat hozzanak létre [141] [142], de vannak kutatások, amelyek a fizikai személyhez tartozó biometrikus sablonból képeznének titkosító kulcsokat, amelyekkel digitális aláírás készíthető az aláírni kívánt dokumentumokon [144]. Más kutatók olyan kombinált módszert dolgoztak ki, amelyek az írisz leolvasásából nyert adatokat használják fel elliptikus görbén alapuló kriptográfiai kulcspár generálásához és a dokumentum aláírásához. Ezt a módszert azért tartják előnyösebbnek, mint a biometria nélküli nyilvános kulcsú kriptográfiát, mert a biometrikus adatokból generált kulcs esetében nem kell a titkos kulcs tárolásával foglalkozni [146]. A Magyar Elektronikus Aláírás Szövetsége kiadott egy szakmai véleményt [145] a biometrikus aláírások alkalmazásáról és használatáról, amelyben kijelenti, hogy a biometrikus aláírások többsége nem felel meg a fokozott biztonságú elektronikus aláírások követelményeinek, de a megfelelőség kialakítása további védelmi intézkedésekkel biztosítható. Ez azért számít mérföldkőnek ezen a területen, mert a szakemberekből és technológiai cégekből álló szakmai szervezet fő célkitűzése a nyilvános kulcsú infrastruktúrák és kapcsolódó technológiák elterjesztése, ennek ellenére kimondták, hogy létezhez nem kizárólag aszimmetrikus kriptográfián alapuló fokozott biztonságú aláírás is.

A biometrikus aláírások felhasználásában az automatizált aláírás ellenőrzés (Automated Signature Verification, ASV) megléte és minősége fontos tényező, a hibás elfogadások és a hibás elutasítások megfelelő szintjének eléréséhez. A területen elért eredményekről Diaz et.al. [139] adott részletes összefoglalást és megállapította, hogy az

eddig elért áttörések nagy és reprezentatív adatbázisokban tesztelt és validált, megbízható algoritmusok fejlesztéséből származnak, amelyekből a referenciaértékeket lehet kialakítani és összehasonlító elemzést lehet végezni, ami javasolható a globálisan elfogadható biometrikus aláírások esetében is. Az aláírások rögzítését két tényező befolyásolhatja, a külső körülmények (pl. zaj, ékszerek, hőmérséklet stb.) és a belső körülmények (pl. fáradtság, stressz, alkoholos befolyásoltság stb.). Az automatikus aláírás-ellenőrzés területén összehasonlító elemzések készültek az egyes algoritmusok megfelelőségének igazolására és egymáshoz viszonyított megbízhatóságuk kimutatására [140]. Az aláírás-paramétereket rögzítő eszközök gyártói által megadott referencia-értékek a gyakorlatban sosem tűntek reprodukálhatónak, így a kutatók figyelme a humán toleranciaszint vizsgálata felé fordult és azt találták, hogy bizonyos esetekben a felhasználók képesek elviselni a gyártói referenciaértékektől nagyságrendekkel nagyobb hibaarányt (kb. 3-5%) is a biometrikus hitelesítések esetében [143].

6.3.2. EGY LEHETSÉGES MEGVALÓSÍTÁS

A biometrikus aláírások megvalósítása során meg kell különböztetni – mint az eIDAS-ban – az aláírási célú adatokat és az azonosítási célú adatokat jogi és műszaki aspektusból is. Az aláírás olyan adat, amely más adatokhoz kapcsolódik, az azonosítás olyan folyamat, amely az adatokat felhasználja, de nem kapcsolódik más adatokhoz aláírási értelemben. A hitelesítés egy további folyamat, amely lehetővé teszi a természetes és jogi személyek (azonosítás során) állított személyazonosságának, vagy az adattartalom eredetének és integritásának megerősítését. A fokozott biztonságú aláírásra képes megoldások kifejlesztésénél az aláíró adatnak az aláírt adathoz való kapcsolódási módja tűnik a legfontosabbnak azon túlmenően, hogy az aláírásnak képesnek kell lennie az aláíró azonosítására. Ez a kapcsolódási rész hiányzik a hitelesítési folyamatokból, mivel azok csak a rögzített és prezentált elektronikus adatok közötti megfelelést (identikusan vagy transzformáltan egyező eredményt) erősítik meg vagy utasítják el. A megvalósítás során a fejlesztőnek olyan aláírási módszert kellett terveznie, fejlesztenie és megvalósítania, amely megfelel a fokozott biztonságú elektronikus aláírás követelményeinek.

Üzleti példám – mint egy lehetséges prototípus – bemutatásában a megrendelő az OTP Bank Nyrt.[244] volt. A bank Magyarország legnagyobb bankja a fiókok száma szerint

[244] A bankról további információk a https://www.otpbank.hu weboldalon találhatók (2019. február 25.)

(kb. 350-400). Az OTP Bank elődjét, a Nemzeti Takarékpénztár szervezetét 1949-ben alapították országos, állami tulajdonú szervezetként, amely lakossági betéteket és hiteleket nyújtott. Az OTP Bank privatizációja 1995-ben kezdődött, a nyilvános ajánlatok és a bank részvényeinek a Budapesti Értéktőzsdére történő bevezetése következtében az állam tulajdonában lévő banki részesedés egy szavazati preferencia (arany) részesedésre csökkent. 2019-ben a bank tulajdonjogi viszonyát a többnyire magán- és intézményi (pénzügyi) befektetők tulajdonában lévő részvények jellemzik. A privatizációs folyamat befejezését követően az OTP Bank megkezdte nemzetközi terjeszkedését a közép- és kelet-európai régió országaiban, a nagyobb gazdasági növekedési potenciál reményében, amelynek eredményeként 2019-ben az OTP Csoport közel 15,1 millió ügyfélnek majdnem 1 400 fiókkal, ügynöki hálózattal és korszerű elektronikus csatornákkal kínál pénzügyi megoldásokat.

A bank fő célja az volt, hogy a papíralapú dokumentumok helyett olyan elektronikus megoldást dolgozzon ki és vezessen be, amely a lehető legjobban hasonlít a papíralapú eljáráshoz, és amely megfelel a vonatkozó általános és specifikus banki jogi követelményeknek. A legfontosabb vonatkozó előírás szerint[245] a pénzügyi szolgáltatásra irányuló szerződéseket kizárólag írásban – ideértve a fokozott biztonságú elektronikus aláírást – lehet aláírni Magyarországon. A fejlesztés első fő fókusza emiatt a bank és az ügyfelek közötti szerződéskötési eljárás volt. Az eIDAS ugyan általános értelemben kizárta a szerződéskötések alaki követelményeit a kötelezően alkalmazni szükséges előírások hatóköréből, azonban a Hpt. és az Eübszt. azt – definíció szintjén – speciálisan meghivatkozta. A bank az ügyfelek digitális írástudásától függetlenül az elektronikus aláírás irányába szerette volna átirányítani az ügyfelek aláírási eljárását, hogy csökkentse a papíralapú dokumentumok számát. Mivel egy papíralapú dokumentum aláírása nem igényel sok tudást és sok eszközt az ügyfelektől, csak papírt és tollat kell biztosítani az ügyfelek fizikai jelenlétével együtt, a kifejleszteni kívánt megoldással szemben is hasonló volt az elvárás.

[245] Hpt. 279. § (1) A pénzügyi intézmény – az egyszeri fizetési megbízás kivételével, valamint az (1a) bekezdésben és a 285. §-ban meghatározott eltéréssel – pénzügyi és kiegészítő pénzügyi szolgáltatásra irányuló szerződést csak írásban – ideértve a legalább fokozott biztonságú elektronikus aláírással ellátott elektronikus okirati formát is – köthet. Az írásban kötött szerződés egy eredeti példányát a pénzügyi intézmény köteles az ügyfélnek átadni.
(1a) Az (1) bekezdéstől eltérően a hitelintézet pénzforgalmi szolgáltatási keretszerződést, valamint betét elfogadására vonatkozó szerződést azonosított elektronikus úton is köthet.

A nyílt beszerzési eljárás eredményeként a fejlesztő cég a Cursor Insight Kft. lett, aki 2015-ben megnyerte a német online aláírás-ellenőrzés versenyét [140]. A fejlesztés 2016. második negyedévében kezdődött és a kísérleti bevezetés 2017 első negyedévében történt meg. Az első két évben több mint egymillió dokumentumot (regisztrációs űrlapot, szerződést és megbízást) írtak alá az OTP ügyfelei ezzel a fokozott biztonságú elektronikus aláírással és az érintett dokumentumok száma folyamatosan növekszik. A fejlesztő a következő eljárásban gondolta megvalósítani a fokozott biztonságú biometrikus aláírást a regisztráció, aláírás és verifikáció szakaszok definiálásával és elválasztásával:

1. Regisztrációs folyamat
    a. az ügyfelek azonosítását és hitelesítését a vonatkozó törvényi előírás szerint közhiteles nyilvántartások és hivatalos dokumentumok felhasználásával el kell végezni,
    b. az ügyfélnek több kézírásos aláírást kell elhelyeznie egy regisztrációs űrlapra, amely tartalmazza a természetes azonosító adatait is.
2. Aláírási folyamat
    a. a banki tisztviselőnek azonosítania és hitelesítenie kell az ügyfeleket (a belső szabályzatokban előírtak szerint),
    b. a tisztviselő előkészíti az aláírandó dokumentumot aláírásra,
    c. a bank minősített elektronikus bélyegzőt és minősített időbélyegzőt helyez el az előkészített dokumentumon,
    d. az alkalmazás elküldi az aláírni kívánt dokumentumot az aláírópadra az aláíráshoz,
    e. az ügyfél aláírja a dokumentumot egy speciális toll mozgatásával az aláírópadon,
    f. az aláírópad összeköti a dokumentumot és az ügyfél biometrikus aláírását az aszimmetrikus magánkulcsával, amelyet egy nyilvános bizalmi szolgáltató tanúsít,

g. a bank minősített elektronikus bélyegzőt és minősített időbélyegzőt helyez el az egész dokumentumon,

h. az ügyfél az aláírt dokumentumot az internetes banki rendszeren keresztül megkapja.

3. Ellenőrzési folyamat

a. az ügyfél kéri az ellenőrzés lefolytatását egy adott dokumentumon,

b. a bank biztosítja az ellenőrzés elvégzéséhez szükséges eszközöket vagy adatokat, beleértve legalább a következő elemeket:

i. az aláírópadok érvényes listája a bankban

ii. az aláírópadok érvényes tanúsítványa,

iii. az ügyfél regisztrációs űrlapja, benne a kézírásos aláírásokkal.

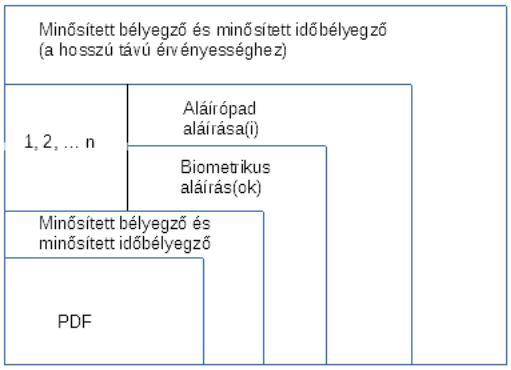
c. az ellenőrző ellenőrzi a minősített bélyegzők érvényességét,

d. az ellenőrző ellenőrzi a minősített időbélyegzők érvényességét,

e. az ellenőrző ellenőrzi az aláírópad nem minősített aláírásának/bélyegzőjének az érvényességét,

f. az ellenőrző összehasonlítja a dokumentum biometrikus aláírásait a regisztrációs űrlapon szereplő biometrikus aláírásokkal.

Az aláírás-készítési és -ellenőrzési folyamat lépéseit az alábbi ábrából lehet szemléletesen levezetni. Minden aláírást ellenőrizni és érvényesíteni kell a dokumentum elfogadása előtt. Az aláírások közötti kapcsolatok szekvenciálisak, minden egyes aláírás hatóköre kiterjed a korábbi aláírásokra is. A legkülső aláírásra jogi és archiválási okok miatt van szükség.



20. ábra: A biometrikus aláírással ellátott dokumentum belső struktúrája (forrás: saját ábra)

Nagyon fontos, hogy a biometrikus adatokat itt aláírásként használják, nem kizárólagosan hitelesítő adatként. A banki tisztviselő azonosítja az ügyfeleket a bemutatott azonosító dokumentumok (pl. személyi igazolvány, útlevél, vezetői engedély vagy PIN-kóddal rendelkező bankkártya) segítségével. A bankkártya kiadása előtt is szükséges volt legalább egy személyes megjelenés. Ez az azonosítási folyamat minden esetben megelőzi a biometrikus aláírás létrehozását. Ezért a banknak az azonosított személy által létrehozott biometrikus aláírás ellenőrzésére kell összpontosítania ahelyett, hogy ismeretlen biometrikus aláíráshoz keresne meg egy természetes személyt a regisztrációs adatbázisában. 2018 januárjában az IBM közzétette a biometrikus hitelesítéssel kapcsolatos kutatási anyagát [137], amely több kontinensre kiterjedő felmérésen alapul, és amely 3 977 választ tartalmaz, ebből 1 976 az USA-ból érkezett, 1 004 az EU-ból, és 997 válasz érkezett Ausztrália, India és Szingapúr térségéből. Megállapították, hogy a legbiztonságosabbnak tartott hitelesítési módszerek az ujjlenyomat-használat (44%) és a retinavizsgálat (30%). Más módszereket (arcfelismerés, kézlenyomat, hang- és szívritmus-felismerés) is használnak ezeken a területeken, de használati arányuk kumulatívan kevesebb (32%), mint az ujjlenyomat használati aránya. A kézírásos aláírás használata azonosítási módszerként a válaszadók kevesebb, mint 2%-ánál (egyéb módszerként) fordulhat elő. Azaz a kézi aláírás hitelesítési módszerként való elterjedtsége nem volt jellemző a vizsgált országokra.

Meg kell jegyezni, hogy a bankban csak olyan aláírópadok használhatók, amelyeket a bank saját maga vásárol, telepít és konfigurál, és amelyeknek érvényes X.509v3 aláírási tanúsítványa van egy az európai bizalmi listán szereplő nyilvános bizalmi szolgáltatótól, továbbá a kulcspárokat „on-board key generation” módszerrel az eszközön belül generálják, a titkos kulcs sosem hagyhatja el az ezközt, illetve amelyek

nem képesek az aláírási felületen túlmenően digitális adatok aláírásként történő elfogadására. Ezek a feltétel biztosítják azt, hogy az aláírások képesek legyenek teljesíteni a fokozott biztonságú aláírásokkal szemben támasztott követelményeket. Ha egy támadó megpróbálná meghamisítani az aláírásokat vagy a megismételt biometrikus adatokat – esetleg annak egy variánsát – csatolná egy másik dokumentumhoz, nyilvánvalóan valódinak látszó aláírások hozhatók létre. Ezeknek az aláírásoknak az ellenőrzése pozitív választ adhat egy olyan általánosan használt aláírás-ellenőrző eszközben, amelyik nincs felkészítve a fokozott ellenőrzésre. Ebben a banki rendszerben az ilyen típusú hamisítások észlelhetők, mert az aláírás érvényességének számos feltétele van. Egyrészről érvényes minősített bélyegzőt igényel a bank részéről, másrészről érvényes (banki) aláírást igényel az aláírópad részéről is és a biometrikus adatok összevetésének is pozitív eredményt kell adnia a regisztrációs dokumentumon tárolt aláírásokkal összehasonlítva. Kritikaként felvethető, hogy látszólag a bank minden olyan eszközzel rendelkezik, amelyik szükséges lehet egy hamis aláírás létrehozásához, mivel elvileg hozzáfér a tárolt biometrikus adatokhoz és az aláírópadok menedzselése is a bank kezében van. Erre válaszként megfogalmazható, hogy egyrészről az aláírópadokon a biometrikus adatok csak kézzel állíthatók elő, mivel minden más esetben az aláírópad aláírása nem lesz biztosítható. Tekintettel arra, hogy az érvényes aláírópadok listájának biztosítása szintén a bank feladata, így megtehető egy hamis eszköz listába való felvétele és arra tanúsítvány igénylése egy nyilvános szolgáltatótól, azonban ebben az esetben a nyilvános szolgáltató nem írhatja bele a tanúsítványba, hogy a titkos kulcs generálása az eszközben történt, ami szintén ellenőrzési pontot jelent az aláírások biztonságának megítélésében. A fenti folyamat garantálhatja, hogy nagy megbízhatósággal csak olyan aláírás hozható létre ebben a rendszerben, amelyiket az aláíró saját kézírásával tesz meg az erre a célra kijelölt és rendszerbe állított aláírópadokon. A megvalósított rendszerben az ügyfél aláírásának elemei és attribútumai a következők: voltak:

- aláírás-létrehozó adatok: az aláírás-létrehozó adatok alatt ebben az esetben egy speciális fizikai toll által létrehozott jeleket értünk, amelyet egy természetes személy aláíró mozgat egy adott speciális aláírópadon egy adott idő-intervallumban. Ezeket az analóg jeleket további feldolgozás (és az aláírás megtörténtének igazolása) céljából digitalizálják, de az aláírás jeleinek digitalizált változata nem használható további érvényes aláírások létrehozásához, mivel ez a továbbiakban csak ellenőrzési célokat szolgál,

- aláírás-ellenőrzési adatok: a kézírás ellenőrzéséhez a természetes személy aláíró kézírásos aláírásainak digitalizált és tárolt példányai szolgálnak, amelyeket a regisztráció folyamán rögzítettek és amelyek referenciaként szolgálnak az adott aláíró hitelesítéséhez, az aláírás és a dokumentum kapcsolódásának ellenőrzéséhez a dokumentumon szereplő digitális aláírások ellenőrzése szolgál támponttal,

- az így létrehozott aláírás egyedileg kapcsolódik az aláíróhoz, mivel csak az aláíró kézírása által jöhet létre,

- képes az aláíró azonosítására, mivel a digitalizált kézírásos aláírás fizikailag jellemző és egyedi minden aláíró esetében,

- olyan elektronikus aláírás-létrehozó adatok felhasználásával jön létre, amelyek nagy megbízhatósággal az aláíró ellenőrzése alatt állnak, mivel az aláírás-létrehozó adatok – a tollmozgások attribútumai – az aláíró nélkül nem digitalizálhatók és más aláíró által nem reprodukálhatók, illetve az aláírás során – mivel tárolt adatok nem injektálhatók be az aláírópadokba – az aláíró fizikai jelenlétére van szükség, továbbá

- olyan módon kapcsolódik az aláírt adatokhoz, hogy az aláírt adatok minden későbbi változása észlelhető legyen, ezt garantálja a minősített banki bélyegző a nem aláírt dokumentumon már az aláírni kívánt dokumentum vonatkozásában, az aláírópad digitális aláírása a biometrikus aláírás és a bélyegzővel ellátott dokumentum vonatkozásában, illetve a külső minősített bélyegző a minősített időbélyegzővel együtt pedig az aláírópad aláírása és minden további – az előbb felsorol – belső adat vonatkozásában.

A biometrikus aláírások lépéseit és az egyes lépések helyeit a következő táblázat foglalja össze:

Lépés	Eszköz
Aláírni kívánt dokumentum létrehozása	Front-office banki rendszer (PDF nyomtató)

Lépés	Eszköz
Dokumentum előkészítése aláírásra	Aláíró Eszköz Kontroller az ügyintéző számítógépén
A dokumentum banki bélyegzése és minősített időbélyegzése	Kripto-szerver a banki back-office oldalon (a kivonat a minősített időbélyeg-szolgáltatónál lesz időbélyegezve)
Ügyfél aláírása a dokumentumon és az aláírás digitalizálása	Aláíró pad (aláíró felület és toll)
A digitalizált aláírás és a dokumentum összekapcsolása	Aláíró pad (kripto-modul)
Az aláírt dokumentum minősített bélyegzővel és minősített időbélyegzővel való ellátása (az archiválás előtt)	Kripto-szerver a banki back-office oldalon (a kivonat a minősített időbélyeg-szolgáltatónál lesz időbélyegezve)

18. táblázat: A biometrikus aláírás lépései és helyei (forrás: saját táblázat)

Az aláíró pad és az ügyintézők számítógépe között az adatok titkosítással vannak védve. Az aláíró padon az aláírás felvétele során a folyamat ellenálló a lehallgatással vagy interferenciával szemben. A digitalizált adatok a dokumentummal való összekapcsolás során titkosítással is védve vannak. Az aláíró padnak tanúsítottnak kell lennie és a tanúsítás során igazolni kell a külső injektálással szembeni védettséget, illetve az aláíró pad titkos kulcsának a védettségét az aláíró padon belül, külső tanúsító szervezet által.

Tegyünk egy kitérőt az aláírások és joghatásuk irányába. Baranyi et.al. felveti, hogy a biometrikus aláírások alkalmazásának vannak kockázatai ([129]: 198), egyrészről az, hogy a kialakított megoldás hiába teljesíti a műszaki követelményeket, attól még nem feltétlenül fog joghatással is bírni, másrészről az eltérő értelmezések következtében eltérő jogalkalmazási gyakorlat is kialakulhat az egyes tagállamokban. Jogászi oldalról nézve az aláírás-létrehozó adat birtoklása látszik a kulcsnak egy aláírás fokozott biztonságának a megítélésében, azonban Berta [109] megállapítását alapul véve – egy nem biztonságos környezetben nincs olyan protokoll, amellyel biztonságos módon aláírásokat lehetne

készíteni, emiatt a kulcs fizikai birtoklásának véleményem szerint nincs akkora jelentősége, mivel az aláíró által birtokolt adat független az aláírás környezetétől és ha a környezet nem biztonságos, az aláíró által birtokolt adattal sem lehetséges joghatással bíró aláírást – ideértve a minősített elektronikus aláírásokat is – készíteni a biztonság hiányának bebizonyítása után, mivel az eredeti szándék nem bizonyítható a szándékos módosítások nyilvánvalóságát követően. Berta ennek a problémának a megoldására a biometria és a kriptográfia kombinálását javasolta és a korábban bemutatott kutatások is ebbe az irányba mentek el. Mahto és Yadav 2015-ben bemutatott egy kézvéna-elemzésen és elliptikus kriptográfián alapuló módszert [186] az üzleti tranzakciók egyszer használatos jelszavai biztonságának a növelésére, amely szintén a biometriát és a kriptográfiát kombinálta. A biztonságos környezet tehát alapvető fontosságú – és implicit módon feltételezett is – minden érvényes elektronikus aláírás esetében, akár tudatában vannak ennek a jogalkotók és jogértelmezők, akár nem.

A banki implementáció környezeti biztonságának megítéléséhez az egész folyamatot egy belső informatikai és biztonsági szakember, egy eIDAS auditor és egy igazságügyi informatikai szakértő auditálta, továbbá egy akkreditált hitelesítő szervezet is tanúsította, amelynek során kitértek arra, hogy az alkalmazott megoldás hogyan teljesíti az eIDAS 26. cikkében foglalt követelményeket. Ezek az evidenciák egy jogvita esetében képesek támpontként szolgálni az ebben a rendszerben generált biometrikus aláírások követelményeknek való megfelelőségéről az Európai Unióban. Amennyiben léteznének olyan szabványok, amelyek a biometrikus fokozott biztonságú aláírások készítésére írnának elő követelményeket, az ennek való tanúsítás tovább emelhetné a megfelelőség megítélhetőségének a szintjét – minősített tanúsítvány és eszköz tanúsítás megléte estében egészen a minősített elektronikus aláírás szintjéig, azonban ilyen tárgyú szabványok 2019-ben még nem voltak ismeretesek.

6.3.3. A FOKOZOTT BIZTONSÁGÚ BIOMETRIKUS ALÁÍRÁSHOZ TARTOZÓ TANÚSÍTVÁNY LEHETSÉGES FELÉPÍTÉSE

Ahhoz, hogy egy megfelelő tanúsítványszerkezetet ki lehessen alakítani a biometrikus aláírások számára, ismerni szükséges a már létező tanúsítványformátumokat. Nem minősített tanúsítványokat vagy hasonló objektumokat több szabvány alapján létre lehet hozni, ezek közül a legismertebb az ITU-T X.509 szabvány, az OpenPGP és ezek tengerentúli verziója, az RFC 5280. A mai Európában és a világban legelterjedtebb nyilvános szolgáltatások az X.509 tanúsítványokon alapulnak. Kérdésként itt az merül

fel, hogy az aláírás-létrehozó adatnak mit tekint az alkalmazó. Biometrikus aláírásoknál problémát okoz a tárolt adatok aláíráshoz való felhasználhatósága, tanúsítvány oldalról pedig az okoz problémát, ha nincs statikus aláírás-létrehozó adat az informatikai rendszerben. Mind a két esetben a fokozott biztonságú aláírás követelményeinek a teljesíthetősége a tét. Nagyon valószínűnek látszik, hogy változtatások nélkül nem lehetséges intézményesülnie a fokozott biztonságú biometrikus elektronikus aláírásnak és a tanúsítványának, azonban ezeknek a változtatásoknak a mértéke nem tűnik jelentősnek, csupán értelmezési – ideértve a műszaki szabványspecifikációt és jogszabály-kiterjesztési kérdéseknek tűnnek. Az értelmezés feladata az aláírás-létrehozó és aláírás-ellenőrző adatok definiálása, strukturálása és szabványosítása, a jogszabály-kiterjesztés feladata pedig egységes jogi vélelem kidolgozása modelltörvényi szinten azoknak a biometrikus aláírásoknak a részére, amelyek magasabb szintű elektronikus aláírásként történő jogi elfogadása releváns. Specifikusan a nyilvános bizalmi szolgáltató által kibocsátott tanúsítvány alapján létrehozott fejlett biometrikus elektronikus aláíráshoz egyetlen jogrendszer sem fűz ma még egyedi jogi vélelmet, általános vélelmek – bizonyíték, meg nem tagadhatóság – léteznek rájuk csupán. A következő fejezetekben a szabványosításhoz nélkülözhetetlen fogalomrendszert ismertetem.

6.3.3.1. Az ITU-T X.509-es szabványa

Az ITU (Nemzetközi Távközlési Unió) az X.509 szabvány 1-es verzióját 1988. július 3-án jelentette meg, amit az X.500 szabványnak megfelelően építettek fel. A tanúsítványok kiadása szigorú hierarchikus rendszerrel rendelkező tanúsító hatóságok (CA) láncolatát feltételezi. Ez a modell a „megbízható harmadik fél” modellje (TTP, Trusted Third Party) néven vált ismertté. Ez a megoldás, ellentétben a PGP-vel, ahol bárki aláírhatja, és ezáltal igazolhatja mások tanúsítványainak érvényességét, egy független kiemelt szereplőre, a megbízható harmadik félre delegálta a bizalom megteremtésének jogát. 2019-ben a szabványnak a 3-as verziója volt érvényben. Mivel az X.500 rendszer alkalmazásának penetrációja csökkent, az IETF Public Key Infrastructure (X.509) vagy PKIX munkacsoportja a szabványt az internet rugalmasabb szervezéséhez igazította. Valójában az X.509 tanúsítvány a legtöbb esetben az X.509 v3 tanúsítvány standard IETF PKIX tanúsítványát és CRL profilját jelenti, ahogyan az RFC 5280, a PKIX nyilvános kulcsú infrastruktúra (X.509) „de facto” szabványa leírja.

Az aláíró és más típusú tanúsítványok közötti különbség nem a struktúrában, hanem az egyes mezők közötti különbségben (pl. kulcs, kulcshasználati cél) rejlik. Az

ITU-T szabvány szerint egy hitelesítés-szolgáltató (CA) egy adott entitásnak (A) az alábbi formalizált módon adhat ki egy tanúsítványt, mellyel aláír egy olyan adathalmazt, amelyben a felhasználó megkülönböztető neve, nyilvános kulcsa és opcionális egyedi azonosítók lehetnek. Egy tanúsítvány a fentiek segítségével felírható a következő alakba, a szabvány jelöléseit használva:

CA<<A>> = CA{V, SN, AI, CA, UCA, A, UA, Ap, T^A}, ahol

V: a tanúsítvány verziója (kötelező),

SN: a tanúsítvány sorozatszáma (kötelező),

AI: a tanúsítvány aláírásához használt algoritmus azonosítója (kötelező),

CA: a kibocsátó hitelesítés-szolgáltató neve (kötelező),

UCA: a kibocsátó hitelesítés-szolgáltató egyedi azonosítója (opcionális),

A: a felhasználó megkülönböztető neve (kötelező),

UA: a felhasználó egyedi azonosítója (opcionális),

Ap: a felhasználó nyilvános kulcsa (kötelező), és

T^A: az érvényességi időintervallumot jelzi, és tartalmazza az érvényesség kezdő és végső időpontját másodpercre pontosan egy adott időzónát használva (pl. UTC +0000).

A tanúsítványnak a fentieken túl lehetnek kiterjesztései (extensions), amelyek alkalmazása három tevékenységet jelenthet a kibocsátó CA számára:

- a CA kizárja valamely kiterjesztés használatát,
- a CA a tanúsítványba beszúrja a kiterjesztést és annak állapotát kritikusra állítja,
- a CA a tanúsítványba beszúrja a kiterjesztést és annak állapotát nem kritikusra teszi.

Az érvényesítési eljárás számára lehetőség nyílik bizonyos kiterjesztések ignorálására és a tanúsítvány elfogadására (ha egyébként a tanúsítvány többi eleme érvényes), vagy a kiterjesztés feldolgozására és a feldolgozás eredményétől függően a tanúsítvány elfogadására vagy elutasítására. Ezeket az érvényesítési eljárás definiálásakor

kell meghatározni és javasolt az aláírási politika dokumentumban is részletezni. Ez teszi lehetővé egyébként azt, hogy nagyobb közösségek kisebb csoportjai használhatják ugyanazt a tanúsítványt némileg eltérő célokra és a másik csoport által használ attribútumokat figyelmen kívül hagyva, mivel nem kell minden kiterjesztést értelmezni az érvényesség megállapításához adott esetben.

6.3.3.2. Az OpenPGP szabvány

A szabványnak az alapját Phil Zimmermann hozta létre 1991-ben Pretty Good Privacy nevű programjával, ami képes volt szövegeket, e-maileket, fájlokat vagy akár egész partíciókat is aláírni vagy titkosítani. Az OpenPGP szabvány a „bizalom webje” (Web of Trust) modellre épít, amely szerint a kulcs generálója maga a felhasználó és annyira lehet egy kulcsban megbízni, amennyire mások is megbíznak benne. Ennek a megközelítési módnak ismert hátránya, hogy ha egy nagyobb csoport megbízik egy kulcsban szándékos vagy megtévesztésen alapuló csalárd műveleteket támogatva, akkor annak a bizalmát nem lehetséges felülírni csak akkor, ha vagy egy nagyobb számosságú csoport megvonja a bizalmat ettől a kulcstól, vagy a tulajdonosa a lejárati adatokat kezelve ezt a kulcsot megbízhatatlanná teszi.

Egy PGP tanúsítvány (nyilvános kulcs blokk) tartalmát a 14. ábra mutatta be az előzőekben. Ebben a becsomagolt adathalmazban a következő részletek lehetnek (a példában vannak is) elrejtve:

:public key packet:

version 4, algo 17, created 1454313743, expires 0

pkey[0]: [1024 bits]

pkey[1]: [160 bits]

pkey[2]: [1022 bits]

pkey[3]: [1023 bits]

keyid: 09AB96182938F849

:user ID packet: "x.y.z szervezet <valami@valahol.van>

:signature packet: algo 17, keyid 09AB96182938F849

version 4, created 1454313743, md5len 0, sigclass 0x13

digest algo 2, begin of digest e5 6d

hashed subpkt 2 len 4 (sig created 2016-02-01)

subpkt 16 len 8 (issuer key ID 09AB96182938F849)

data: [156 bits]

data: [158 bits]

:signature packet: algo 17, keyid D4E600D91D16DFE7

version 4, created 1455704996, md5len 0, sigclass 0x10

digest algo 8, begin of digest 17 6c

hashed subpkt 2 len 4 (sig created 2016-02-17)

subpkt 16 len 8 (issuer key ID D4E600D91D16DFE7)

data: [256 bits]

data: [252 bits]

:public sub key packet:

version 4, algo 16, created 1454313743, expires 0

pkey[0]: [1024 bits]

pkey[1]: [1023 bits]

pkey[2]: [1023 bits]

keyid: 991A4695C8139572

:signature packet: algo 17, keyid 09AB96182938F849

version 4, created 1454313744, md5len 0, sigclass 0x18

digest algo 2, begin of digest 1a 48

hashed subpkt 2 len 4 (sig created 2016-02-01)

subpkt 16 len 8 (issuer key ID 09AB96182938F849)

data: [157 bits]

data: [156 bits]

Tekintettel arra, hogy jelenleg nem egyértelmű az, hogy lehetséges-e OpenPGP szabványt alkalmazva fokozott biztonságú elektronikus aláírást létrehozni – általános esetben valószínűleg nem, mivel nehezen lehet igazolni az aláíró kulcs és a személy összetartozását a bizalmi körön kívüli személyek számára, emiatt ennek a szabványnak a további részletezésétől eltekintünk.

6.3.3.3. Az RFC 5280 alapú tanúsítvány alapvető mezői

Az RFC 5280 szerint egy tanúsítvány három kötelező szekvenciának az összességéből áll, mégpedig az aláírni kívánt tanúsítványból, az aláíró algoritmus azonosítójából és magából az aláírás értékéből.

1) Tanúsítvány mezők: magukban foglalják az aláírni kívánt tanúsítványt, az aláíró algoritmus azonosítóját és az aláírás értékét.

a) tbsCertificate: a „to be signed”, vagyis az aláírni kívánt tanúsítvány szekvenciája a fentebb ismertetett elemeket tartalmazza (az alany neve, a kibocsátó, az alany nyilvános kulcs, az érvényességi időtartam és más kapcsolódó információk, ideértve a kiterjesztéseket is).

b) signatureAlgorithm: annak az algoritmusnak az azonosítóját tartalmazza, amelyet a hitelesítés-szolgáltató a tanúsítvány aláírásához használ. Az azonosító szerkezete kötött, az algoritmus szabványos OID-jéből (Object IDentifier) és az algoritmus által esetleg még szükségesnek ítélt paraméterekből áll. Az OID-nek kötelezően meg kell egyeznie azzal az aláíró algoritmus azonosítóval, amelyik a tanúsítványon belül (tbsCertificate) jelöli annak aláíró algoritmusát.

c) signatureValue: az aláírás értéke az aláírni kívánt tanúsítvány ASN.1 DER kódolású verziójának digitális aláírásából, illetve annak is BIT STRING formájú ábrázolásából áll (jellemzően két hexadecimális számjegy ábrázol egy bájtot). Ezzel az aláírással a hitelesítés-szolgáltató gyakorlatilag igazolja a nyilvános kulcs és az alany összetartozását, ami – lévén egy nyilvános kulcshoz csak egy titkos kulcs tartozhat – egyben az alany titkos kulcshoz kötöttségét is jelenti.

2) tbsCertificate mezői: minden egyes tanúsítványnak kötelezően tartalmaznia kell az alannyal és a kibocsátóval kapcsolatosan minimális információkat, mint például az alany és a kibocsátó hitelesítés-szolgáltató neve, az alany nyilvános kulcsa, az érvényességi idő, a verziószám és a sorozatszám, továbbá egyéb opcionális egyedi azonosító mezők is lehetnek még a tanúsítványban az alábbiak szerint.

a) Version: megadja a tanúsítvány verziójának a számát. Amennyiben hiányzik, akkor a verziószám 1-es – ebben az esetben csak az alapvető mezők szerepelhetnek a tanúsítványban; ha a Unique identifiers mezők meghatározottak és kiterjesztések nincsenek, akkor a mező értéke 1-es, ami azt jelenti, hogy a verziószám 2-es; illetve ha vannak a tanúsítványban kiterjesztések, akkor a verziószám 3-as (az érték pedig 2-es).

b) Serial Number: a tanúsítvány sorozatszáma, ami nemnegatív egész szám lehet, ha a kibocsátó meg akar felelni a szabványnak. A hitelesítés-szolgáltatónak biztosítania kell, hogy minden egyes tanúsítvány sorozatszáma biztosan különböző legyen és ne lehessen két ugyanolyan sorozatszámú, de különböző tanúsítvány a hierarchiában. A sorozatszám maximális értéke 20 bájt lehet egy szabványos szolgáltató egy-egy tanúsítvány-kibocsátó egysége esetében (ami 2160 számú különböző sorozatszámú tanúsítványt enged meg, ez több mint 1,46 *1048 decimális számrendszerben CA egységenként).

c) Signature: annak az aláíró algoritmusnak az OID-jét tartalmazza, amellyel a kibocsátó aláírja a tanúsítványt. Ennek az értéknek kötelezően meg kell egyezni a Certificate szekcióban szereplő algoritmus OID értékével. A támogatott algoritmusokat különböző szabványok tartalmazzák (pl. RFC 3279, RFC 4055, RFC 4491), de lehetőség van más algoritmusokat is – amelyek rendelkeznek OID-vel – támogatni. Például a DSA algoritmus SHA224 hash függvénnyel kombinált aláíró algoritmus-készletének az OID-je 2.16.840.1.101.3.4.3.2, amelynek a következő a jelentése az OID fastruktúrán belül: {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) dsa-with-sha256(2)} .

d) Issuer: Ez a mező azonosítja azt az entitást, amelyik aláírja és kibocsátja a tanúsítványt és kötelezően egy nem üres megkülönböztető nevet (DN) kell tartalmaznia, ahogyan azt az X.501 név típusa leírja. A következő mezőket kötelezően értelmezni kell minden kibocsátó (és alany) esetében, további opcionális mezők lehetségesek:

i) ország (country),

ii) szervezet (organization),

iii) szervezeti egység (organizational unit),

iv) megkülönböztető név minősítő (distinguished name qualifier),

v) állam vagy tartomány neve (state or province name),

vi) common name (pl. „Erdősi Péter Máté”), és

vii) sorozatszám (serial number).

e) Validity: azt az időintervallumot határozza meg, amelyen belül a kibocsátó a tanúsítvány állapotára vonatkozó információkat karbantartja és menedzseli, amihez két időpontot határoz meg, amely előtt és ami után ezt már nem vállalja (notBefore és notAfter). Két formátum alkalmazható: UTCTime vagy GeneralizedTime.

i) UTCTime: az időpontok meghatározásának egyik szabványos formája a következő alakban másodperc pontossággal: YYMMDDHHMMSSZ, ahol ha az YY értéke kisebb mint 50, akkor a 20yy. évet kell érteni alatta, ellenkező esetben (yy >= 50) az 19yy. évet jelenti. A „Z” a „Zulu” rövidítése.

ii) GeneralizedTime: az időpontok meghatározásának másik szabványos formája a következő alakban másodperc pontossággal: YYYYMMDDHHMMSSZ, ahol a másodperceket akkor is ki kell írni, ha az értékük nulla, illetve töredék másodpercek nem engedélyezettek. Megjegyzésre kívánkozik, hogy ha az érvényességi idő lejárata későbbi, mint 2050, akkor csak ez a dátumformátum jöhet számításba.

f) Subject: ez a mező azonosítja azt az entitást, akinek a tanúsítványban szereplő nyilvános (és privát) kulcsot kibocsátották. Az alany neve itt vagy a SubjectAlternativeName (SAN) mezőben lehet, tanúsítvány-típustól függően. Szolgáltatói vagy CRL kibocsátói tanúsítvány esetében ez a mező nem lehet üres. Ha azonban csak a SAN mező tartalmazza az alany nevét, akkor ez a mező lehet üres, de ebben az esetben a SAN mezőnek kritikusnak kell lennie. Ha azonban a Subject mező nem üres, akkor egy X.500 Distinguished Name (DN) struktúrájú adathalmazt kell tartalmaznia, amelynek az adott tanúsítvány-kibocsátónál minden alany számára egyedinek kell lennie. Ez azt is jelenti, hogy ha azonos DN szerepel két különböző

tanúsítványban, amelyeket ugyanaz a tanúsítvány-kibocsátó bocsátott ki, akkor az alanynak is meg kell egyeznie, más alany számára nem bocsáthat ki egyező DN-nel tanúsítványt a szolgáltató. Az újabban kibocsátott tanúsítványokban a SAN mezőben kell az RFC 822-nek megfelelő módon az alany email címét feltüntetni, habár a Subject DN értékében az E (emailAddress) mező használható történeti okok miatt email cím feltüntetésére, ami már nem javasolt – lévén a „@” karakter nem számít bele a PrintableString karakterkészletbe, de ettől függetlenül elfogadható a használata.

g) Subject Public Key Info: Ez a mező hordozza a nyilvános kulcsot, továbbá a kulcshoz szükséges algoritmus (például RSA, DSA vagy Diffie-Hellman) azonosítására szolgál, a már ismertetett OID struktúra szerint (AlgorithmIdentifier).

h) Unique Identifiers: Ezek a mezők csak akkor alkalmazhatók, ha a tanúsítvány verziója 2 vagy 3, mivel 1-es verziójú tanúsítványban nem szerepelhetnek. Az alany és a kibocsátó egyedi azonosítói szerepelhetnek a tanúsítványban annak érdekében, hogy a nevek ismételt felhasználhatóságát menedzselni lehessen. Ajánlásként megfogalmazott, hogy a neveket ne lehessen újra felhasználni különböző entitások számára, és hogy az internetes tanúsítványok ne használjanak egyedi azonosítókat. A megfelelőséget biztosító szolgáltatók nem bocsátanak ki egyedi azonosítóval rendelkező tanúsítványokat, de a megfelelőséget biztosító alkalmazások képesek az egyedi azonosítókat tartalmazó tanúsítványok elemzésére, mindazonáltal az egyedi azonosítókhoz nincsenek feldolgozási követelmények.

i) Extensions: csak a 3-as verziójú tanúsítványokban jelenhetnek meg. Ha előfordulnak, akkor mindig egy vagy több kiterjesztés szekvenciájaként lehet ezeket alkalmazni, a következő pontban foglaltaknak megfelelően.

3) Kiterjesztés (extensions) mezők: Az X.509v3 tanúsítványokhoz definiált kiterjesztések olyan módszereket biztosítanak, amelyek további attribútumok társítására ad lehetőséget a felhasználók, a nyilvános kulcsok vagy a kibocsátóval való kapcsolatok terén. Az X.509v3 tanúsítványformátum lehetővé teszi a közösségek számára, hogy magáncélú kiterjesztéseket határozzanak meg, amelyek csak ezekhez a közösségekhez tartozó egyedülálló információk is lehetnek. Minden egyes kiterjesztés lehet kritikus vagy nem kritikus. További privát kiterjesztések is definiálhatók, azonban a kritikus saját kiterjesztések megakadályozhatják a tanúsítvány általános felhasználását, mivel, ha egy kritikus kiterjesztést az érvényesítést végző nem tud értelmezni, akkor szabvány szerint

el kell utasítania a tanúsítvány elfogadását. A nem kritikus és nem értelmezhető kiterjesztések ignorálhatók. Vannak kötelezően értelmezni szükséges kiterjesztések (key identifiers, basic constrains, key usage és certificate policies, illetve adott esetben a SAN is ilyen), a többi kiterjesztés kezelése opcionális.

a) Standard kiterjesztések: az X.509 szabvány által definiált kiterjesztések, amelyekhez OID és ASN.1 struktúra is meghatározott. Minden standard kiterjesztés megtalálható a {joint-iso-itu-t(2) ds(5) certificateExtension(29)} OID-csomópont alatt (69 kiterjesztés van ezalatt definiálva), ezek közül az alábbiak kerültek bele az RFC 5280 szabványba.

i) Authority Key Identifier: a kibocsátó kulcsazonosítóját minden általa generált tanúsítványba bele kell tenni, a kibocsátó nevével és a kibocsátó tanúsítványának sorozatszámával együtt. Ez azt a célt szolgálja, hogy a kibocsátott tanúsítványt aláíró kulcsot egyértelműen meg lehessen különböztetni a szolgáltató többi aláíró kulcsától. Többféle képzési módszer is elképzelhető, de ha korábban még nem volt implementálva ilyen módszer, akkor a nyilvános kulcsból képzett 160 bites SHA-1 lenyomat, vagy a lenyomatnak a 0100 fél bájttal felvezetett legkevésbé szignifikáns (alsó) 60 bitje használata ajánlott.

ii) Subject Key Identifier: az alany nyilvános kulcsából képzett egyedi azonosító, amelynek képzési módja megegyezik a kibocsátói kulcsazonosító képzési módjával (lásd előző pont).

iii) Key Usage: a tanúsítványban szereplő nyilvános kulcs használatát jelölő kiterjesztés, amelynek kritikus státuszúnak kell lennie, ha megjelenik. A CRL-ek és más tanúsítványok aláírásainak ellenőrzésére szolgáló nyilvános kulcsok tanúsítványaiban ez a kiterjesztés kötelező. A kulcshasználatot jelző bit beállítása a következők lehetnek (bizonyos megkötésekkel, például végfelhasználói tanúsítványban nem lehet a kulcshasználat 5-ös):

- digitalSignature (0),
- nonRepudiation (1), (vagy contentCommitment)
- keyEncipherment (2),
- dataEncipherment (3),

- keyAgreement (4),
- keyCertSign (5),
- cRLSign (6),
- encipherOnly (7),
- decipherOnly (8).

iv) Certificate Policies: A tanúsítvány-irányelvek kiterjesztés egy vagy több olyan szekvenciát tartalmaz, amelyek mindegyike egy adott szabályzatra vonatkozó OID-ből és opcionális kiegészítő információkból áll. Egy policy OID-t csak egyszer szabad szerepeltetni ebben kiterjesztésben. Ebből következik, hogy minden nyilvános szabályzatnak egyedi OID-vel kell rendelkeznie. Két minősítő használható ebben a kiterjesztésben, az egyik a „CPS Pointer”, a másik pedig a „User Notice”. A CPS Pointer a szolgáltatási szabályzat (Certificate Practice Statement) elérhetőségét mutatja meg URI formájában, amely az adott hitelesítési rendhez (Certificate Policy) vagy rendekhez tartozik. Megjegyzésre kívánkozik, hogy a rendek és a szolgáltatási szabályzatok közötti kapcsolat nem „egy-az-egy”, hanem „n-az-m” típusú is lehet, vagyis több rendhez tartozhat egy vagy több szolgáltatási szabályzat és viszont. A felhasználóknak szánt megjegyzésben a kibocsátó szabad szöveges üzeneteket tud megjeleníteni a minősítő noticeRef és explicitText (200 karakteres) almezőiben (pl. felelősségvállalás mértéke, adatok őrzési ideje stb.).

v) Policy Mappings: Ezt a kiterjesztést szolgáltatói tanúsítványokban használják. Egy vagy több OID-párt sorol fel. Minden pár tartalmaz egy issuerDomainPolicy és egy subjectDomainPolicy OID értéket. A párosítás azt jelzi, hogy a tanúsítvány kibocsátó egység a saját issuerDomainPolicy szabályozását és a kibocsátott szolgáltatói tanúsítvány subjectDomainPolicy szabályozását egyenértékű módon veszi figyelembe a kibocsátás során.

vi) Subject Alternative Name: Az alany alternatív nevei olyan további azonosítókat jelölhetnek, amelyek ugyanazon nyilvános kulcshoz kötöttek a tanúsítvány által. Az alternatív nevek formátuma leggyakrabban email cím, domain név, IP cím vagy Uniform Resource Identifier (URI). Más formátumok (pl. egy zárt csoport által használt definíciók) is opcionálisan engedélyezettek lehetnek. Amennyiben több domain név szerepel itt, akkor ezekből az egyiknek kötelező a Subject mezőben szerepelnie.

Tekintettel arra, hogy az itt szereplő minden entitáshoz a nyilvános kulcs hozzá lesz kötve, a kibocsátónak minden itt szereplő adatot ellenőriznie kell a tanúsítvány aláírása előtt. Amennyiben az alany csupán egy email cím, akkor a Subject mezőt üresen kell hagyni és az RFC 822 email címet ebben a kiterjesztésben kell szerepeltetni, amelynek ebben az esetben kritikus státuszúnak kell lennie. Ha a Subject mező nem üres és ez a mező is tartalmaz értéket, akkor nem kritikus státuszt kell beállítani.

vii) Issuer Alternative Name: a kibocsátó internetes azonosítójának (egynek vagy többnek) a megjelölésére használhatják, a formátuma megegyezik az előző mező (SAN) formátumával. Az ellenőrzésben nincsen jelentősége, így ha szerepel is egy tanúsítványban, státusza nem kritikus.

viii) Subject Directory Attributes: Ez a kiterjesztés az alany azonosításához használható előre definiált tulajdonságokat (pl. nemzetiség) tartalmazza. A tulajdonságok egy vagy több szekvenciában jelenhetnek meg, maga a kiterjesztés nem kritikus.

ix) Basic Constraints: az alapvető megkötések két célt szolgálnak, egyrészről a szolgáltatói (CA) tanúsítványokra, másrészről az adott tanúsítványlánc mélységére adnak korlátozást a cA logikai változó (alapesetben hamis) és a pathLenConstraint numerikus változó értékének a beállításával. Ez utóbbinak csak akkor van jelentősége, ha a tanúsítvány egy kibocsátóhoz tartozik és azt a köztes kibocsátói tanúsítvány-számot jelöli, amennyi az érvényes tanúsítvány-láncban az önaláírt root és a végfelhasználói tanúsítvány (ami lehet egyébként CA tanúsítvány is) között maximum megjelenhet. Ha ez a szám zéró, akkor nem lehet köztes kibocsátó a root és a végfelhasználói tanúsítványok láncában, egyébként pozitív egész számnak kell lennie, ha szerepel. Ha nincs megadva, akkor nincs korlátozva az érvényes tanúsítvány-lánc mélysége.

x) Name Constraints: A nevek megkötése csak CA tanúsítványban használható és érvényessége kiterjed minden további kibocsátott tanúsítványra (a Subject és a SAN mezőkre). Kétfajta megkötés létezik, az egyik megengedő (permittedSubtrees), a másik tiltó (excludedSubtrees) hatású. Az itt specifikált nevek (jellemzően domain végződések) nem a szolgáltató működésének korlátozását célozzák, hanem megnehezítik a téves tanúsítvány-kibocsátások lehetőségét, ha akár szándékos, akár szándékolatlan módon történne ez meg.

xi) Policy Constraints: csak CA tanúsítványokban használható kritikus státuszú korlátozás, ami vagy megtiltja, vagy megköveteli a láncban a megjelölt hitelesítési rendeknek való megfelelést – jellemzően CA-k felülhitelesítése vagy kereszthitelesítése során lehet erre szükség. Ehhez két numerikus almezőt definiál, inhibitPolicyMapping és requireExplicitPolicy. Az inhibitPolicyMapping értéke megmondja, hogy a láncban hányadik tanúsítvány után lehet elhagyni a kibocsátói hitelesítési rendnek való megfelelést, míg a requireExplicitPolicy értéke azt mondja meg, hogy ha a megadott értéktől több tanúsítvány szerepel a láncban, akkor mindegyiknek meg kell felelnie az adott hitelesítési rendnek.

xii) Extended Key Usage: a kiterjesztett kulcshasználat (EKU) mezőt jellemzően végfelhasználói tanúsítványokban alkalmazzák, a kulcshasználat megjelölésének további finomítására. Lehet kritikus és nem kritikus státuszú is, a kibocsátótól függően. A kulcshasználatot kizárólag előre definiált OID-k jelezhetik, amelyeket az IANA vagy az ITU-T X.660 ajánlása tartalmaz. Például a {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3)} OID alatt 30 további OID található, kiterjesztett kulcshasználatként (pl. az emailek titkosítására használatos tanúsítványok kiterjesztett kulcshasználati mezője tartalmazhatja az 1.3.6.1.5.5.7.2.4 OID értéket {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) emailProtection(4)}).

xiii) CRL Distribution Points: Leggyakrabban a kibocsátóhoz tartozó CRL (Certificatge Revocation List, tanúsítvány visszavonási lista) helyét mutatja be, például egy URI típusú mezőben megadott webes hivatkozás (generalName) segítségével (pl. URI:http://sslca2014-crl1.e-szigno.hu/sslca2014.crl). A kibocsátóhoz tartozó összes CRL felsorolása szükséges, amelyek akár eltérő módokon is elérhetők lehetnek (pl. LDAP, URI). Habár a kiterjesztés státusza nem kritikus, javasolt minden alkalmazásnak ezt a kiterjesztést kezelnie.

xiv) Inhibit anyPolicy: Ha szerepel ez a numerikus kiterjesztés, akkor kritikusnak kell lennie, és az OID értéke pedig 2.5.29.32.0 {joint-iso-itu-t(2) ds(5) certificateExtension(29) certificatePolicies(32) anyPolicy(0)}. A numerikus érték – hasonlóan a Policy Constraint kiterjesztésnél mondottakhoz – megmondja, hogy a láncban hányadik tanúsítványtól nem kell alkalmazni az anyPolicy által közelebbről nem definiált hitelesítési rendet.

xv) Freshest CRL (vagy Delta CRL Distribution Point): amennyiben a kibocsátó Delta CRL-eket bocsát ki két teljes CRL között az addig felmerült változásokról, ezt a kiterjesztést kell – nem kritikus státusszal – használnia. A kiterjesztés struktúrája megegyezik a cRLDistributionPoints struktúrájával.

b) Privát internet kiterjesztések: előre definiált nem kritikus kiterjesztések leginkább alkalmazások számára, amelyek az interneten a kibocsátóról és az alanyról meghatározott további információkhoz való hozzáférés módját vagy helyét határozzák meg.

i) Authority Information Access: a felhasználók támogatására szánt információ, amelynek segítségével biztosabban fel tudja építeni az érvényes tanúsítvány-láncot a saját végfelhasználói tanúsítványához, aminek érdekében olyan protokollok és szolgáltatás-hozzáférési pontok vannak definiálva, amelyekkel a kibocsátó összes szükséges információjához hozzá lehet férni a sikeres érvényesítés elvégzéséhez.

ii) Subject Information Access: a felhasználói tanúsítványba (mely lehet CA is) berögzített olyan protokollok és szolgáltatás-hozzáférési pontok, amelyekkel az alany összes szükséges információjához hozzá lehet férni a sikeres érvényesítés elvégzéséhez.

Az egyes mezők tárgyalásakor nem vállalhattuk jelen dokumentum keretei között a teljeskörű ismertetést, számos korlátozás és további részletszabály létezik a fenti tanúsítványelemekhez, amelyeket a biometrikus tanúsítvány részleteinek specifikálásakor szükséges teljeskörűen feldolgozni és figyelembe venni. A célkitűzés egy átfogó ismertetés és koncepcióalkotáshoz való információgyűjtés megvalósítása volt.

6.3.3.4. Attribútum tanúsítványok

Az attribútum tanúsítványokat az az elgondolás hozta létre, hogy az aláírókhoz kapcsolódó, de az aláírástól eltérő életciklusú jellemzőket a PKI világban is kezelni lehessen. Ilyen például egy vezetői beosztáshoz tartozó döntési jog megjelenítése és elfogadhatóságának automatizálása, ahol a személyhez tartozó aláíró kulcs mellé oda lehet tenni a személy szerepeit és a kulcshoz tartozó privilégiumokat is egy külön struktúrában. Ennek előnye az, hogy a szerepkörök vagy privilégiumok változásakor nem kell aláírói kulcsokat cserélni, csupán a hozzárendelést kell megváltoztatni, az esetleges kapcsolódó tanúsítványok változatlanul hagyása mellett. Tekintettel arra, hogy a szerepköröket vagy privilégiumokat tartalmazó tanúsítvány célja nem az aláírás ellenőrzése, hanem az aláíróhoz tartozó jogosultság ellenőrizhetősége, emiatt az

attribútum tanúsítvány struktúrája eltér bizonyos mértékig az alany nyilvános kulcsú tanúsítványától. Egy alanynak több attribútum tanúsítványa is lehet, amelyek mindegyike ugyanahhoz a nyilvános kulcsú tanúsítványához kapcsolódhat – opcionálisan. Nincs szükség arra, hogy ugyanaz a kibocsátó hozza létre mind a nyilvános kulcsú tanúsítványt, mind az attribútum tanúsítványt a felhasználó számára, a gyakorlatban a feladatok szétválasztásának elve gyakran mást is követel meg. Ha különböző kibocsátók felelősek a nyilvános kulcsú és az attribútum tanúsítványok kiadásáért, a kibocsátó egység (Certificate Authority, CA) által kiadott nyilvános kulcsú tanúsítványok aláírásához és az attribútum tanúsítvány kibocsátó egység (Attribute Authority, AA) által kiadott attribútum tanúsítványok aláírásához használt aláíró kulcsok lehetnek különbözők. Olyan környezetekben, ahol egy kibocsátó adja ki mind a nyilvános kulcsú tanúsítványokat, mind pedig az attribútum tanúsítványokat, a szolgáltatói aláírói kulcsoknak erősen ajánlott különbözőknek lenniük, a vonatkozó szabványok előírásainak betartása végett.

Az attribútum-tanúsítvány nem más, mint az attribútum-tanúsítvány mezőinek összessége és ezek kibocsátó által történő digitális aláírása. A mezők az alábbi struktúrát vehetik fel (ASN.1 jelöléseket használva):

- version AttCertVersion, -- a verzió v2 (az 1-es szám jelöli)
- holder Holder,
- issuer AttCertIssuer,
- signature AlgorithmIdentifier,
- serialNumber CertificateSerialNumber,
- attrCertValidityPeriod AttCertValidityPeriod,
- attributes SEQUENCE OF Attribute,
- issuerUniqueID UniqueIdentifier OPTIONAL,
- extensions Extensions OPTIONAL

Jól látható, hogy nyilvános kulcs nem szerepel az attribútum-tanúsítványban, egyébként a felépítése hasonló mintázatot követ, mint a nyilvános kulcsú tanúsítványoké, természetesen a megfelelő eltérésekkel.

6.3.3.5. Biometrikus adatok a létező szabványokban

Jelenleg is van lehetőség szabványos alapon biometrikus adatokat kezelni és megjeleníteni bizonyos tanúsítványokban, példának okáért az RFC 3739 szabványban foglalt *biometricInfo* kiterjesztést ismertetjük. A szabvány elődje (RFC 3039) 2001 januárjában jelent meg és már akkor útmutatást adott a biometrikus információk – kiemelten a kézi aláírás – kezelésére. Az újrafelhasználhatóság elleni védekezés miatt már kezdetben sem javasolták részletes biometrikus adatok beágyazását a tanúsítványba, csupán az aláírás képe (picture) jelent meg előre definiált típusként itt. A 2004 márciusában újragondolt szabvány (RFC 3739) 3.2.5. fejezete (Biometric Information) definiálja a biometrikus információk tárolására szolgáló opcionális *biometricInfo* kiterjesztést, amely nem kritikus. A tanúsítványban azonban nem kell szerepeltetni magát a biometrikus információkat, csupán a biometrikus adatokat tartalmazó dokumentum kivonatát (hash) lehet itt megjeleníteni. Ennek a kiterjesztésnek az a célja, hogy eszközt biztosítson a biometrikus információk hitelesítésére. A hitelesítéshez szükséges a tanúsítványban szereplő hash értéket összehasonlítani egy másik biometrikus adatból képzett hash értékkel, ahol az adatokat tartalmazó fájlra mutató URI (sourceDataUri) szerepelhet a kiterjesztésben. Természetesen az érzékeny biometrikus adatokat védeni kell a jogosulatlan hozzáférés ellen, vagyis ebben az esetben biztosítani kell azt is, hogy külső fél által az URI és az érintett aláíró összerendelése ne történhessen meg, hasonlóan az adatok jogosulatlan kezekbe kerülése ellen is védelmi intézkedéseket kell életbe léptetni. Megjegyzésre kívánkozik, hogy egyrészről az URI által jelzett fájlon belüli struktúrára ez a szabvány nem ad útmutatót, továbbá, ha egy tanúsítványban szerepel egy ilyen URI, attól még a verifikációs adatok más módon is hozzáférhetők lehetnek, nem kizárólag ezen a módon. A biometrikus információk megadásakor meg kell határozni a biometrikus adat típusát, a hash algoritmus OID-jét és a megképzett hash értéket kötelező jelleggel, míg az adatokat tartalmazó fájlra mutató URI megadása itt opcionális lehetőség.

6.3.3.6. Biometrikus hitelesítés

A biometrikus adatokat a természetes személyekkel való nagy megbízhatóságú összekapcsolhatósága miatt régóta használják hitelesítésre, amelyben egy tárolt és egy dinamikusan rögzített adat összehasonlításából kell eldönteni azt a kérdést, hogy vajon a felvett adat valóban attól a személytől származik-e, mint a tárolt adatok. Az RFC 8176 szabvány 2017 júniusában az alábbi hitelesítési módozatokhoz (referencia név) tartotta szükségesnek a biometrikus információkat (2. fejezet):

- face: ez a biometrikus hitelesítés arcfelismerét alkalmaz.
- fpt: ez a biometrikus hitelesítés ujjlenyomat-felismerét használ.
- iris: ez a biometrikus hitelesítés az íriszt szkenneli.
- retina[246]: ez a biometrikus hitelesítés a retinát olvassa le.
- vbm: ez a biometrikus hitelesítés hanglenyomatot alkalmaz.

Feltűnő, hogy a hitelesítési metódusok statikus – és feltételezhetően önmaguktól lassan (de betegség, degeneratív változások esetében viszonylag hamar), külső behatástól pedig azonnal változó – adatokat sorolnak csupán fel, a természetes személyre jellemző dinamikus biometrikus adatok kimaradtak ebből a felsorolásból. A statikus biometrikus adatok alkalmazási köre leginkább a személyhitelesítésre terjed ki. Aláírásként csak és kizárólag abban az esetben lehet használni ezeket, ha kapcsolódnak egy másik adathoz, amit az aláíró szándéka szerint alá szeretett volna írni. Minden egyéb esetben a rögzített biometrikus adatok nem lehetnek elektronikus aláírásként felhasználhatók. Ez a legfontosabb különbség a biometrikus aláírás és a biometrikus hitelesítés között, amit sokan sokszor össze is kevernek.

6.3.3.7. A biometrikus aláíró tanúsítvány javasolt felépítése

Az eIDAS rendelet a preambulumában leszögezi, hogy tudatában van a technológiai változásokból adódó következményekkel és azzal, hogy a jövőben más technológiák is megjelenhetnek az elektronikus aláírások között, ezért a rendeletben előírtak mögötti technológiák változása nem elképzelhetetlen , azonban az új megoldások kidolgozásánál a már létező megoldások figyelembe vétele és az azokból való merítés erősen ajánlott az innovátorok számára is[247] (pl. a CAdES, XAdES, PAdES szabványokban foglaltak ismerete előnyös lehet).

A fentiek alapján a nem minősített biometrikus aláíró tanúsítvány tartalmára az alábbi koncepcionális javaslat lehet releváns és megvalósítható, ami egy aláírási célú

[246] A retina-szkennelés és az írisz-felismerés között van különbség, mivel a retina a szemgolyó belsejében, annak hátsó falán található és gazdagon átszőtt egyedileg jellemző vérerekkel, míg az írisz a szemgolyó külső részén van, a pupillát körülvevő gyűrű alakú részt nevezik így.

247 eIDAS Rendelet Preambulum (64) A fokozott biztonságú elektronikus aláírások és bélyegzők formátuma tekintetében a Bizottságnak a meglévő gyakorlatokból, szabványokból és jogszabályokból, különösen a 2011/130/EU bizottsági határozatból kell ihletet merítenie.

X.509v3 tanúsítvány és egy nyilvános kulcsot nem tartalmazó X.509v2 attribútum tanúsítvány „keresztezéséből” származtatható:

Biometrikus tanúsítvány mező	Leírás
Verziószám (AttCertVersion)	Attribútum-tanúsítványként kell tekinteni ezt a tanúsítványt a jelenlegi szabványok értelmében, mivel nincs nyilvános kulcs a tanúsítványban, így a javasolt érték: V2.
Sorozatszám (CertificateSerialNumber)	Legfeljebb 20 bájt valódi véletlen szám, az esetleges egyezőségek kizárásával.
Aláíró algoritmus azonosítója (AlgorithmIdentifier)	a választott tanúsítvány-aláíró algoritmustól függ (pl. RSA aláíró algoritmus SHA256 kivonatoló függvénnyel az {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} OID-t kapta (1.2.840.113549.1.1.11).
Kibocsátó neve (AttCertIssuer)	A kibocsátó neve.
Érvényességi időtartam (AttCertValidityPeriod)	A tanúsítvány érvényességi ideje (a biometria változásához vagy a szerződés érvényességéhez igazított lejárati dátummal):
Kezdete	érvényesség kezdete
Vége	érvényesség vége
Aláíró azonosítója (Holder)	A tanúsítvány birtokos neve (entityName), esetleg eID vagy eSZIG azonosító (baseCertificateID) is elképzelhető.
Atrribútumok (Sequence of Attribute)	Az attribútumok az attribútum-tanúsítványok attribútumaiként definiáltak, ahol csak a struktúra kötött, de a tartalom szabadon választott lehet.
Aláíró audit azonosító (*SignSpecimenID)	A regisztrációs dokumentum olyan azonosítója, hash-értéke, esetleg URI értéke, amely minden időpontban megképezhető és nem változik a dokumentum felülhitelesítését követően sem.
Aláírópad (aláírási rendszer) azonosító (*SigningSystemID)	A tanúsítvány kibocsátásának időpontjában az érvényes aláírópad-azonosítókra együttesen mutató hivatkozás (URI).
Validációs Hatóság (*ValidationAuthority)	A regisztrációs adatokat felvevő validációs hatóság adatai
elérhetőség (*AccessPointofValidationAuthority)	a validációs hatóság elérési pontja (a lekérdezések fogadásához)
azonosító (*EncPublicKeyofValidationAuthority or *EncPublicKeyIDofValidationAuthority)	a validációs hatóság azonosítója (lehet a nyilvános kulcsa vagy annak elérhetősége is), a titkosításhoz
Tanúsítvány aláírására használt algoritmus	Megegyezik a Signature Algorithm ID mezőben foglalt értékkel.
A tanúsítvány digitális aláírása	A tanúsítvány digitális aláírása.

19. táblázat: A biometrikus aláíró tanúsítvány lehetséges elemei (forrás: saját táblázat)

A tanúsítvány kibocsátója lehet nyilvános, nem minősített szolgáltató, aki a validációs hatóság igazolása alapján és az aláíró megfelelő azonosítását és hitelesítését követően kiállítja az X.509v2 attribútum-tanúsítványt a fenti tartalommal. Amennyiben a tanúsítványt össze lehet kapcsolni az aláíró elektronikus azonosítójával vagy elektronikus aláírásával, ez a módszer olyan helyeken is alkalmazható lehet, ahol az eID vagy eSIG[248] használatára minden aláíró esetében nincsenek felkészülve, de a későbbi ellenőrzés esetleg megoldható lehet. Amennyiben nem lehet, akkor meg kell oldani azt is, hogy aláíráskor az aláíró hivatkozni tudjon a speciális biometrikus aláíró tanúsítványára.

[248] Az eSZIG és aSIG különböző használata nem véletlen, az eSZIG utal a kártyán található elektronikus aláírást megvalósítni képes konténerre, az eSIG pedig magára az aláírási funkcióra, mint műveletre. Ebben az értelemben az eSZIG előfeltétele az eSIG-nek, az aláírás passzív feltételeként, az eSIG pedig az aláírás aktív elemeként értelmezett jelen kontextusban.

7. AZ ELEKTRONIKUS ALÁÍRÁSHOZ KAPCSOLÓDÓ TUDÁS INTENZITÁSA

Az elektronikus aláírás használatával kapcsolatosan fontos kérdés, hogy szükséges-e bármilyen tudás az aláírás használatához vagy elképzelhető-e az elektronikus aláírás használatának elterjedése zéró tudás feltételezésével. A digitális gazdaságban minden szolgáltatásként jelenik meg a felhasználók számára, ahol a szolgáltatások szükségszerűen további komponensekből állnak (a felhasználók által látható szolgáltatási funkciók megvalósításához szükséges technológiai elemek számossága általában több mint egy, ha a hardver és szoftver komponenseket is különbözőnek értékeljük, akkor pedig biztosan több mint egy). Az egyes komponensek négyszintű hierarchiába rendezhetők, a felhasználói, a szolgáltatási, a hálózati és az eszköz szinteket elkülönítve. Az elektronikus aláírás bonyolultságából adódóan a helyes felhasználáshoz szükséges felhasználói tudás szükséges mértéke ebből adódóan függ az aláírás létrehozásának szintjétől. Technológiai szinten – processz – készített aláírások esetében a felhasználónak nem szükséges semmilyen tudással sem rendelkeznie erről – például ha egy üzenettovábbító ügynök digitális aláírással biztosítja az üzenet sértetlenségének megállapíthatóságát, amit fogadó ügynök ellenőriz és az ellenőrzés eredményét felhasználva jeleníti meg az üzenetet – már az aláírás nélkül – a felhasználó számára, ebben a felhasználó és az aláírás között direkt kapcsolat nem jön létre, így az aláírás mibenlétéről sem szükséges az üzenetet küldő és fogadó humán entitásoknak további információkkal rendelkeznie. Attól függően, hogy az elektronikus aláírás melyik szinten jön létre, a felhasználóknak az alábbi táblázatban részletezett tudással szükséges rendelkezniük a sikeres felhasználás érekében.

Aláírás készítője	Szituáció	Szabadsági fok	Felhasználói tudásszint	Szint
Ember	tetszőleges	maximális	teljes	felhasználó
Folyamat	meghatározott	korlátozott	részleges	szolgáltatás
Gép	felsorolt	véges	fókuszált	hálózati
Processz	egyedi	egydimenziós	zéró	eszköz

20. táblázat: Felhasználói tudásszintek (forrás: saját táblázat)

Az aláírás létrehozásával járó felelősség felvállalása abban az esetben képzelhető el tudatos módon, ha a felelősséget vállaló legalább az aláíráshoz fűződő jogi vélelmeknek a tudatában van, illetve képes az alkalmazhatósági feltételek teljesülésének megítélésére. Ez egyre növekvő mértékű tudást tételez fel a technológiai szinttől haladva

a társadalmi szint felé. Legfontosabb különbség az, hogy amíg az eszköz aláírási képességét a programozó állítja elő és az eszköz nem képes olyan aláírások létrehozására, amelyeket nem programoztak a forráskódjába, addig az aláírás társadalmi használatában a polgár állapítja meg és készíti elő az adott elektronikus aláírást és szabadon dönthet az egyenértékű alternatívák között a folyamatba épített korlátok figyelembevételével.

7.1. AZ OKTATÁSI PROBLÉMAKÖR ELEMZÉSE

A közigazgatásban mindig alapvető fontosságú volt a kiadmányok, az ügyfelek és a kommunikáció hitelességének biztosítása, így kell ennek lennie az e-közigazgatásban is. A hitelesség biztosításának egyik lehetséges eszköze az elektronikus aláírás, amely a magyar közigazgatásban részletesen szabályozott technológia. Az elektronikus aláíráshoz kapcsolódó tudás nem integrálódott be a graduális oktatásba és meghaladja önképzéssel hatékonyan elsajátítható szintet. Felmerül az a kérdés, hogy a köztisztviselők részére ennek a tudásnak az átadására milyen internet-alapú tudásmenedzsment-folyamatelem lehet alkalmas, ha a használat kérdése komolyabban felmerül. Ehhez kapcsolódóan a 2013. évi L. törvénnyel – és így az információbiztonsággal – összefüggő kérdésként kell azt is feltenni, hogy hogyan alakul a biztonság az internet-alapú tudásmenedzsment eszközök alkalmazásában. Tekintettel arra, hogy a közigazgatásban az érintett szereplők számossága jóval meghaladja a tantermek átlagos befogadó képességeit (százezres nagyságrendű résztvevői körről is beszélhetünk), korlátoztam a tudásmegosztási módszerek vizsgálatát és két olyan módszert elemeztem, amelyek mindegyike internet-alapú és alkalmas az érintett szereplők közelítőleg valós idejű képzésének lebonyolítására.

Az Európai Unió kibocsátotta az 1999/93/EK irányelvet az elektronikus aláírás közösségi alkalmazásáról 1999 év végén, amely azonban nem hozta meg a várt áttörést az alkalmazás terén. A piaci szereplők a szabályozó hatóságokon kérték számon a kritikus tömeget megteremtő alkalmazás („killer application”) megszületésének hiányát, a hatóságok pedig a piacon kérték számon az egész Európában működőképes aláírási formák létrejöttét. Mivel az irányelv nem fogalmazott minden téren egyértelműen, illetve tág teret engedett a nehezen szinkronizálható nemzeti eltéréseknek is – és az egységes európai elektronikus aláírás megszületése még mindig nem látszott a láthatáron, az Unió az irányelv felülvizsgálatát tűzte ki célul, továbbra is támogatva az elektronikus aláírási technológiákat. Ennek eredményeként 2014 második felében létrejött a 910/2014. EU

Parlamenti és Tanácsi Rendelet (eIDAS), ami az eddig nélkülözött egységességet biztosíthatja az egész Európai Unióban. A rendelet egyes elemei 2014. szeptember 17-én léptek hatályba, más elemei 2016. július 1-jétől váltak hatályossá, a fokozatos bevezetés elvét követve.

A hazai közigazgatási ügyintézés elektronikus formájának preferálását először a vonatkozó törvény (Ket., 2004) a következőképpen aposztrofálta: *„28/A. § (3) Több igénybe vehető kapcsolattartási forma közül a hatóság a költségtakarékosság és a hatékonyság szempontjai alapján választ, előnyben részesítve az elektronikus utat."* A paragrafus (2) pontja szerint ezt a szabályt megfelelően alkalmazni kellett az ügyfél és a hatóság, valamint a hatóságok egymással történő kapcsolattartására is.

Az elektronikus ügyintézésre való áttérést számos jogszabály jelzi 2013 óta. A legfontosabbak ezek közül a Szabályozott Elektronikus Ügyintézési Szolgáltatók, a SZEÜSZ-ök, amelyekről a 83/2012. (IV. 21.) Korm. rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról, azaz a SZEÜSZ-rendelet tartalmazott elsőként részletes leírást. Definíciója szerint a szabályozott elektronikus ügyintézési szolgáltatások a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény 172. § j) pontja szerinti szolgáltatások, amelyek újra lettek szabályozva a 2015. évi CCXXII. törvénnyel és a 451/2016 Korm. rendelettel, míg a Ket. helyett az Ákr. (2016. évi CL. törvény az általános közigazgatási rendtartásról) szabályozza a közigazgatási rendtartást 2018. január 1-től. A SZEÜSZ-ök és a Központi Elektronikus Ügyintézési Szolgáltatások (KEÜSZ) továbbra is azt a célt szolgálják, hogy a törvény hatálya alá tartozó szervezetek építőkockaként használhassák őket a saját elektronikus ügyintézési szolgáltatásaik kialakításában. Az elektronikus hitelesség szempontjából az egyik kiemelt SZEÜSZ a Kormányzati Hitelesítés-szolgáltató, a GovCA.

A kormányzati hitelesítés-szolgáltatás feladata, hogy az állami szervek, valamint intézmények részéről az elektronikus aláírással kapcsolatos igényeket a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló SZEÜSZ-rendelethez kapcsolódóan kiszolgálja. 2013 őszétől a NISZ Zrt. elviekben kész volt fogadni az állami szervek és intézmények részéről az elektronikus aláírással és 2017. július 1-től az elektronikus bélyegzéssel kapcsolatban felmerülő igényeket is, a szolgáltatás kiterjedt a fokozott biztonságú és minősített

elektronikus aláírás vagy bélyegzés, minősített időbélyegzés-szolgáltatás, vagy egyéb, például titkosító vagy azonosítás célú tanúsítványok kiadására és a kapcsolódó feladatok elvégzésére.

Az elektronikus ügyintézés kialakítása Európában is kiemelt prioritást kapott az elmúlt időszakban, számos pilot projekt indult több közszolgáltatási területen. Az új eIDAS rendelet szabályozása is ilyen projektek tapasztalataira alapozott, ezek a Pan-European Public Procurement On-line (PEPPOL) és a Secure idenTity acrOss boRders linKed (STORK).

Mivel az elektronikus információs rendszerek biztonsága alapvető fontosságú, meg kell említenünk az állami és önkormányzati szervek elektronikus információbiztonságáról szóló a 2013. évi L. törvény és az ennek kapcsán elindult információbiztonsági oktatási formákat is (hagyományos kontaktórák és e-learning továbbképzések), amelyek képzési terveiben azonban az elektronikus aláírás hangsúlyosan nem jelenik meg (lásd Nemzeti Közszolgálati Egyetem Elektronikus Információbiztonsági Vezető Szakirányú Továbbképzési Szak Képzési Program). Kérdésként merül fel, hogy ez a rendszer mennyire alkalmas a többszázezer közszférában dolgozó tisztviselő, ügyintéző vagy ennek első vezetői szintje készségszintű tudásának (közel) egyidejű bővítésére.

Az elektronikus aláírás oktatási vetületét tekintve megállapítható, hogy habár a hiteles információ fogalma szerepel a Nemzeti Alaptantervben, a heti egy informatika órában ennek ismertetése a közoktatási graduális képzésben reménytelen vállalkozás. Egyetemi kurzusok ugyan léteznek a kriptográfiával vagy az informatikával foglalkozó tanszékeken specializált tudás átadására, de készségszinten eredményes tömeges képzésről itt sem beszélhetünk. Létrejött az elektronikus aláírási készségeknek az elsajátítására ECDL modul is, amely most már szabadon választható mind a START, mind a SELECT programban is. Habár a vizsgaközpontok negyede (kb. 50 központ) akkreditáltatta magát első körben ennek a modulnak a vizsgáztatására is, ennek ellenére jelentős vizsgázási számosságról itt sem lehet még beszámolni a modul indulását követő első 8 évben. Ennek oka lehet, hogy a modul ismerete gyakorlatilag sehol sem követelmény, és vagy minden érintett saját képzést akar létrehozni ennek a tudásnak az elsajátítására, vagy elvárja a munkavállalótól ennek ismeretét, illetve önképzéssel történő megtanulását, következménye pedig az, hogy 2018-ban már csak 40 vizsgaközpont

tartotta fontosnak megtartani ezt a képzési modult a palettáján. Ellentmondásos helyzetet eredményezett az is, hogy miközben a fentebb ismertetett projektek – és szélesebb értelemben az európai digitális szolgáltatások – elvárják az elektronikus hitelességi technikák egyszerűbb és bonyolultabb formáinak a készségszintű ismeretét, az oktatási rendszerek ilyen irányú felkészültsége a tananyag kidolgozásánál megállt, és úgy látszik, hogy további jelentős erőfeszítéseket kell tenni ahhoz, hogy ez a tudás a hétköznapi kultúra szerves részévé válhasson szélesebb körben, amilyen például a köztisztviselők köre. Az első lépés mindenesetre megtörtént, az elektronikus ügyintézési törvény által elektronikus ügyintézésre kötelezett mintegy egymillió-kétszázezer szervezet ma már nem tudja kivonni magát ez alól. Mentséget kínál számukra az ügyfélkapu és a központi aláírási szolgáltatás együttes használata, ez nem igényli az aláírással kapcsolatos tudás elsajátítását, ebben az esetben az elektronikus aláírás a felhasználói szint alatt működve fejti ki hatását az infrastruktúra részeként. Ez azonban meg is fosztja az aláírások szabad alkalmazásától a szereplőket. Ha a központosított modell terjedne el, akkor minden érintett szereplő vagy kialakítaná a maga infrastrukturális szintjén a szükséges aláírások kezelését, vagy pedig a központi létező megoldást fogja elfogadni. Ha azonban a szabad felhasználás terjedne tovább, akkor a felhasználói szintű tudás létrejötte alapvető fontosságúvá válik. A kérdés ebben az esetben az, hogy miért törődne bárki is egy olyan tudáselem megszerzésével, aminek a jövőbeli használhatósága kérdéses és a központi szolgáltatások sem igénylik, illetve logikailag nem teszik lehetővé a használatát akkor sem, ha a fizikai eszköz jelenléte megkövetelt (pl. eID a KAÜ-ben). További kérdésként merül fel, hogy egy esetleges hiba következtében tömegesen hibásan aláírt dokumentumok későbbi elfogadása hogyan valósulhat meg a közigazgatás részéről, hiszen az ügyfél önhibáján kívül juthat így olyan hiteles forrásból származó dokumentumokhoz, amelyek hitelességében csupán megbízhat, mivel az ellenőrzéséhez szükséges tudással nem rendelkezik, és amelyeket később teljes joggal kíván felhasználni az ügyeinek elintézéseiben. A jelszavas azonosítás használatának megtiltásával is csupán az eID része válhat frekventáltabbá a személyazonosító igazolványnak, ami fizikai értelemben ugyan az igazolványon található, de logikai értelemben kívül esik az elektronikus aláírás funkcionalitásán. Nem érintené az elektronikus azonosítás és aláírás funkciókat az Ügyfélkapu hitelesítésének kétfaktorossá szigorítása sem, azonban új lehetőségeket nyitna – feltételezve az okostelefon meglétét minden Ügyfélkapu azonosítóval rendelkező állampolgár esetében – a mobilalkalmazások számára. Az

elektronikus aláírást akkor lehetne ezekbe az alkalmazásokba integrálni, ha a telefonok NFC olvasói tudnának kommunikálni az állampolgári kártya eSIG funkciójával is.

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. 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 válasz a tudásmenedzsment eszközeiben véljük megtalálni.

7.2. A TUDÁSMENEDZSMENT ESZKÖZEI - A TUDÁS, AMIT MENEDZSELÜNK

Mit nevezünk egyáltalán tudásnak? Bergeron szerint hiába töltött el az akadémiai szféra évtizedeket a tudáshoz kapcsolódó fogalmak tisztázásával, ez a terület igencsak zavarosnak mondható a gyakorlatban [39]. Bergeron a következő definíciókat javasolja alkalmazni ([39]:11):

- adat: számokból álló numerikus mennyiség vagy tulajdonság, amely megfigyelés, tapasztalat vagy számítás eredménye;
- információ: az adat az összefüggéseivel együtt, vagyis olyan halmaza az adatoknak és a kapcsolódó magyarázatoknak, értelmezéseknek és más szövegeknek, amely az egyes tárgyakra, eseményekre vagy folyamatokra vonatkozik;
- metaadat: az információra magára vonatkozó adat. magában foglalja az adatok összefoglaló leírását és az adatok, illetve információk magas szintű kategorizálását is, azaz információ az információ felhasználási kontextusáról;
- tudás: a felfogóképesség, tudatosság vagy érthetőség növelésére szolgáló strukturált, szintetizált vagy összegzett információk összessége. ennek

értelmében a tudás a metaadat és a metaadat sikeres alkalmazhatósági összefüggéseiről való ismeret kombinációja;

- instrumentális megértés: valamely dolog természetéről, jelentőségéről vagy magyarázatáról alkotott tiszta és teljes elképzelés. ez egy személyes, belső képesség a tapasztalatok érthető formában történő visszaadására, a vonatkozó alapvető fogalomrendszer speciális ismerete által.

A tudást a fent említettek szerint tehát lehetséges és értelmes dolog kategorizálni. A tudásmenedzsment kategóriák azonban nem mindig lesznek matematikai értelemben diszjunktak. Karl Erik Sveiby amellett érvel, hogy egy gazdálkodó szervezet könyv szerinti értéke és a piaci értéke közötti különbség az immateriális javak értéke, ideértve a dolgozók kompetenciáját, a szervezet belső szerkezetét és a szervezet külső kapcsolatrendszerét is ([45]: 74), ezért azt fogalmazta meg a vezetők számára, hogy a szervezeteikre tudásszerkezetként és nem tőkeként kellene tekinteniük. Sveiby a kompetencia tárgyalásánál felhasználja a hallgatólagos tudás és fokális tudás kategóriákat is, amelyek nem diszjunkt elemekként vannak jelen, hanem ugyanannak az objektumnak a különböző nézeteiként értendők. A kompetencia – vagyis a cselekvőképesség – alapja ugyanis a tudás, mégpedig a fokális és a hallgatólagos tudás. Minden tevékenységet ezek segítségével hajtunk végre, de az explicit tudás mögött létező implicit tudás alapvetőbb, mivel az vagy hallgatólagos, vagy a hallgatólagos tudásban gyökerezik ([45]: 87). Ha a valódi felfedezéseket nem lehetséges száz százalékosan szavakba önteni, vagy formalizálni, akkor lennie kell egy olyan tudásnak, amely a „mélyben” van. Vagyis minden ismeretünknek van rejtett dimenziója – adódik a következtetés. A fokális tudás feleltethető meg a fenti definíciók szerint az információnak, míg a hallgatólagos tudás metaadatként van jelen. Ebből következik, hogy információ nem létezhet metaadat nélkül és fordítva, valamint ez igaz a tudásra is – mivel definíciónk szerint a tudás az információ és metaadat kombinációja.

A tudást transzformáló folyamatoknak létezik általánosan elfogadott interpretációja. Az egyes tudástranszformációs folyamatokat az alábbiakban szemléltethetjük Gupta et. al. alapján [41]:

- szocializáció (tacit → tacit),
- externalizáció (tacit → explixit),

- kombináció (explicit → explicit),
- internalizáció (explicit → tacit).

A szocializáció → externalizáció → kombináció → internalizáció → szocializáció folyamat, mint később kiderült, felülről nézve egy kört is alkothat. Ez a kör azonban oldalról nézve spirális alakot mutathat, ahogyan Gottschalk [40] felvetette, amely szerint a tudás létrehozását emelkedő körkörös folyamatnak javasolja tekinteni a tacit és explicit tudás kölcsönhatását tekintve. Ezt a spirált a fent leírt transzformációs módszerekből álló körök alkotják. Az emelkedő spirál képe felveti a magasabb szintű tudások lehetőségét – amennyiben az ilyen módon transzformálódott tudás nem toroid természetű, azonban a tudás különbözőségeinek és a tudásszintek hierarchiájának vizsgálata nem szerepelt a célkitűzések között.

A fentebb említett problémát át lehet fogalmazni tudásmenedzsment fogalmakkal kifejezve: hogyan lehetséges egy tudáskombinációt a kicsit több mint 820 000 költségvetési intézményben foglalkoztatott alkalmazottal, vagy a majdnem 360 000 szellemi foglalkozású közalkalmazottal, esetleg a több mint 76 000 köztisztviselővel és kormánytisztviselővel[249] véges időtartamon belül internalizáltatni, attól függően, hogy ki találkozhat elektronikus dokumentumokkal az ügyfelekkel vagy az intézményben folytatott munkájával kapcsolatosan. Más szóval felvetődik az externalizált tudáskombináció elsajátíthatóságának, esetünkben eléggé széles körben (legteljesebb esetben a magyar népesség 8,39%-ának körében) történő disszeminációjának a kérdésköre. Ennek megoldása egyébként a vezetőcentrikus elmélet megfogalmazásában a tudásalapú hálózati működésnek is a lényeges eleme lehet, ahogyan azt Koronváry [44] megfogalmazta. Az internalizáción kívül más módszer nem lehet eredményes, ha a tacit tudás az, amelynek segítségével egy-egy feladat megoldásához a közigazgatásban dolgozók hozzálátnak és ami a fokális tudás mögött aktívan működik. Ha a köztisztviselői kar nem rendelkezik az elektronikus aláírásra vonatkozó tacit tudással és az oktatási rendszerben sincs ilyen irányú képzés jelenleg, akkor ez jó indok a szocializáció és a kombináció elvetésére, hiszen nincsenek meg az előfeltételei a tudás ilyen módszerekkel történő átadásának. Várható, hogy az internalizációt meg kell előznie egy externalizációnak, amely azonban szintén nem jöhet a köztisztviselői karon belülről, ha

[249] A KSH adatai szerint 2018 szeptemberében 820,5e alkalmazott volt a költségvetési intézményekben, közülük 357,9e szellemi foglalkozású közalkalmazottat, 34,9e köztisztviselőt és 41,2e kormánytisztviselőt tartott nyilván az adatbázis (http://www.ksh.hu/docs/hun/xstadat/xstadat_evkozi/e_qli006.html).

nincs meg az ehhez szükséges tacit tudás. A következőkben megvizsgálom, hogyan lehetséges a tudást – ideértve az elektronikus aláírással kapcsolatos tudást is – menedzselni.

7.3. A TUDÁS MENEDZSELÉSE

Tserng és Lin (2008) [46] a tudás menedzselésének öt fázisát különböztette meg a tudásmenedzsment teljes életciklusát tekintve:

1. a tudás megszerzése (bármilyen formában),
2. a tudás extrakciója (tárolható formába hozási értelemben),
3. a tudás tárolása (az adott eszközökön),
4. a tudás megosztása (az adott eszközökhöz történő hozzáférés által),
5. a tudás frissítése (új tudás létrejötte, visszacsatolható a tudás megszerzése fázishoz).

Az adat és a belőle létrejött információ ebben a megközelítésben a tudás megszerzéséhez (első fázis) kötődő elemek, a tudásmenedzsment további lépéseiben már csak a meglévő tudással kapcsolatos műveletek játszanak szerepet.

A köztisztviselői kar elektronikus aláírással kapcsolatos tudásproblémájának megoldásához a tudás szétosztására kell fókuszálnunk, így felmerül a kérdés, hogy milyen eszközök lehetnek megfelelők erre, látván a hagyományos oktatási rendszerek lassúságát (egy emberöltő) és tehetetlenségi nyomatékát. Keresnünk kell tehát egy rugalmas, azonnal felépíthető, széles körben gyorsan megismertethető eszközt, ami rendelkezésre is áll vagy könnyen ilyenné tehető. Murray E. Jennex 2008-ban összefoglalta az internet minden olyan tulajdonságát, amelyek hatékonyan támogatják egy tudásmenedzsment-rendszer működését ([43]: 566), az internet képes lehet tehát tudásmenedzsment rendszerek infrastruktúrájaként működni. Azóta a gyakorlatban egyre több internetes tudásmegosztó megoldás terjedt el (például online kurzusok, hírportálok). Ezekből adódóan két tudástranszfer megoldást vizsgálunk meg a következőkben:

- nyílt internet alapú megoldás: a tudásmenedzsment internetes technikákkal történik, nyilvános, bárki által látható és hozzáférhető módon (integritás biztosításával),

- zárt internet alapú megoldás: a tudásmenedzsment internetes technikákkal történik, de csak egy zárt közösség által látható és hozzáférhető módon.

7.4. A POTENCIÁLIS TUDÁSMEGOSZTÁSI MEGOLDÁSOK ÖSSZEHASONLÍTÁSA

A két megoldás összehasonlítását biztonsági aspektusból végeztük el. A biztonsági aspektusok alatt – összhangban a 2013. évi L. törvénnyel és az informatikai biztonság Muha [4] által kidolgozott egy lehetséges rendszertanával – a következőket kell érteni:

- bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;
- sértetlenség: az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;
- rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Modell / biztonsági követelmény	Bizalmasság	Sértetlenség	Rendelkezésre állás
Nyílt internet alapú megoldás	a korlátlan láthatóság miatt bizalmasság csak erős titkosítással, korlátozott ideig (az	nyilvános kulcsú infrastruktúrával, a kezdeti algoritmus	a rendelkezésre állásra csak szerződéssel van garancia, egyébként „szokásjog” a

Modell / biztonsági követelmény	Bizalmasság	Sértetlenség	Rendelkezésre állás
	algoritmus valószínűsíthető kompromittáló-dásáig)	valószínűsíthető kompromittálódásáig	működés megbízhatósága
Zárt internet alapú megoldás	a korlátozott láthatóság miatt hozzáférés-védelemmel vagy titkosítással is megvalósítható, korlátlan ideig (ki nem kerülést feltételezve)	nyilvános kulcsú infrastruktúra folyamatos alkalmazásával lehetséges	katasztrófatűrő rendszer is kiépíthető, a belső üzemeltetés megbízhatóságától függ

21. táblázat: Internetes tudásmegosztó megoldások biztonságának összehasonlítása. (forrás: saját táblázat)

Fő különbség a megoldások biztonságának megítélésénél, hogy egy nyilvános internetes csomópontot az egész internetes közösség (minden szintű hálózatból) láthat és hozzáférhet a kitett információkhoz, még azt követően is, hogy a kiadmányozó ezt már nem szeretné, hiszen a nyílt interneten nincs ismert hatékony módszer a nyilvánosan hozzáférhetővé tett információk törlésére, visszahívására. A nagy internetes csomópontoknál (pl. Facebook, Instagram) lehetséges kérni az adott információ megosztásának megszüntetését, ami hatékony eszköz a hozzáférhetőség korlátozására, de ez nem szünteti meg a privát weboldalakon való elérhetőséget, továbbá a nagy internetes csomópontok felhasználhatók privát webes linkek terjesztésére is (ami persze szintén korlátozható). A belső csomópont esetében az információkhoz történő hozzáférés csupán a jogosultakon keresztül történhet, és nem valósítható ez meg mindegyik internetes hálózatból és alhálózatból. A jogosultak száma jóval kisebb szám, mint a teljes internethasználók elvi hozzáférési számossága, ami közel három és félmilliárd internet

felhasználót jelentett 2016-ban és több mint négymilliárdot 2019 február elején[250], ez jelentős változásnak tekinthető az 1993-as 14 millió, illetve az 1995-ös 44 milliós felhasználói számhoz képest és az internet emergens használatát támasztja alá.

Ugyancsak emiatt kérdéses lehet a sértetlenség hosszú távú védelme internetes csomópontra kitett információk esetében kriptográfiai védelem alkalmazása mellett is, hiszen egy internetes olvasó tetszőleges ideig megőrizheti a titkosított vagy digitálisan aláírt információt, akár az algoritmus kompromittálódása után is, amikor az már észrevétlenül módosíthatóvá válik. A rendelkezésre állás biztosítása szerződéses kötelem nélkül csak jóindulat alapján képzelhető el, ami nem tekinthető komoly garanciavállalásnak közigazgatási környezetben. Így a belső üzemeltetés ugyan többletterhet jelent, de a rendelkezésre állás magasabb szinten biztosítható, mint egy szerződés nélkül használt internetes csomópont esetében; arról nem is beszélve, hogy a teljesen nyilvános közösségi oldalak „fizetsége" általában a feltöltött információk, amiket a csomópontok tulajdonosai alapesetben szabadon felhasználhatnak, minden lényegi korlátozás nélkül. Ha létezik olyan szerződés, amely a katasztrófatűrő környezetet képes biztosítani, akkor a két modell között rendelkezésre állás szempontjából nincs különbség; a modellek megvalósítási és üzemeltetési (TCO) költségeit pedig nem volt célunk összehasonlítani. Az elektronikus aláírással és bélyegzéssel kapcsolatos tudás közigazgatásban történő szétosztási felületének biztonsági szempontból legkedvezőbb eszköze ezekből következően egy belső tudásmegosztó felület (pl. probono.uni-nke.hu) lehetne.

[250] Lásd Internet Live Stats (www.internetlivestats.com/internet-users/#trend) historikus adatait

8. AZ EREDMÉNYEK HASZNOSÍTÁSA

8.1. TOVÁBBI LEHETŐSÉGEK

8.1.1. AZ ELEKTRONIKUS ALÁÍRÁS MÉRHETŐSÉGÉNEK ALKALMAZÁSI LEHETŐSÉGEI

Az elektronikus aláírás mérhetősége hozzájárul a hatékonyság növeléséhez a közhatalom gyakorlásában, az elektronikus vélemény-nyilvánítási 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 maximális szintjének 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 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 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 Dimenzió Modell 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 és törvényi kötelezettség is Magyarországon és az Európai Unióban egyaránt, amelyben 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 preventív, detektív és korrektív kontrollok is szükségesek, ezek közül a modell szervesen kapcsolható a digitális állam fenyegetései és a kiberkatasztrófák elleni védekezés detektív kontrolljaihoz is.

További fejlesztési lehetőséget kínál a modell 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.

8.1.2. 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 mégis korlátozott lehet, mert az ilyen aláírások határokon átnyúló elfogadása esetében szükséges a nemzeti jogszabályok kiterjesztése. Míg 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. Szintén anomália forrása lehet, hogy egyrészről a minősített elektronikus aláírás egyenértékű a kézi aláírással, másrészről teljes bizonyító erővel bír a magyar jogrendszerben, holott egy kézírásos dokumentum kézi aláírással nem lesz teljes bizonyító erejű magánokirat mindaddig, míg két tanú azt alá nem írja. Ilyen értelemben a minősített bizalmi szolgáltatók regisztrációs folyamata lehet egyenértékű a két tanú aláírásával a magánokiratokon, amennyiben a regisztráció során rögzített adatokat az aláírásokat ellenőrző érintett felek – vagy az erre feljogosított szervek – számára hozzáférhetővé teszik, ellenkező esetben a minősített aláírás tanúsítottsági szintje alacsonyabb lesz, mint a papíralapú teljes bizonyító erejű magánokiratoké

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 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 validációs hatóságok („validation authority") kialakítása[251], akik 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 a természetes aláíró mindegy, hogy 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

[251] Lásd Jon Ølnes és Leif Buene felvetését [82]

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[252].

A bemutatott megoldás 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 [153], és független a digitális szegénységtől [154], valamint az e-részvétel (e-participation) minden területén [155] nemzeti szinten is alkalmazható. A hatékonyság növelhető az e-aláíró eszközök (kártyaolvasók) és biometrikus aláíró eszközök (aláírópadok) integrálásával a közigazgatásban, amíg a távoli aláírási alkalmazások kifejlesztésre nem kerülnek. 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).

8.1.3. AZ ELEKTRONIKUS ALÁÍRÁS HASZNÁLATÁHOZ KAPCSOLÓDÓ OKTATÁS FEJLESZTÉSE

Oktatási szempontból megállapítottuk, hogy az elektronikus aláírási technológiák elterjedése tudásfüggő, a hozzákapcsolódó 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, lévén 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[253],

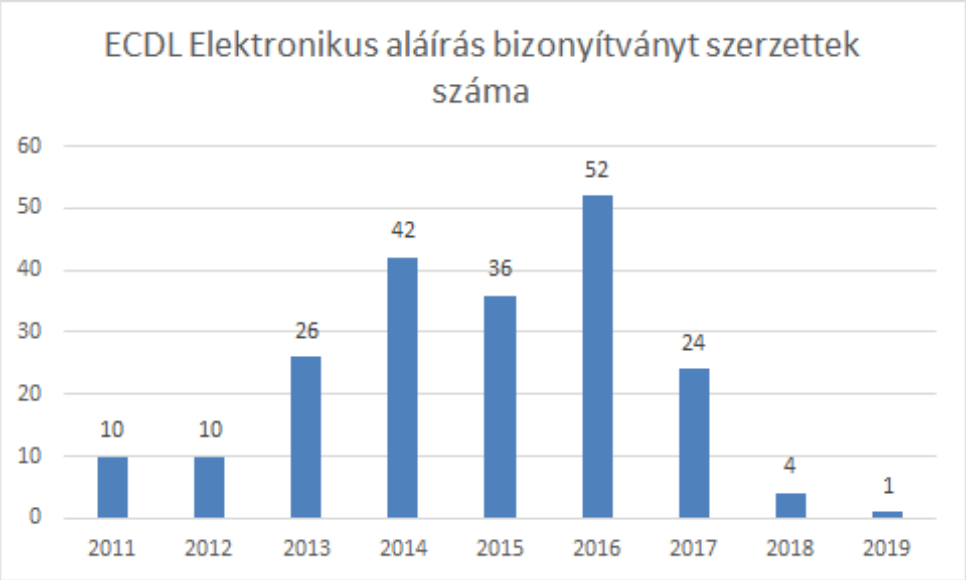
[252] Jambrik a holland minta megismerése után javasolta ezt a megközelítésmódot az internetes szerződéskötésről szóló korai tanulmányában, amit a hágai T.M.C. Asser Institute támogatott. [198]
[253] Tradicionális megoldási példaként említhető az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programja keretében megvalósult elektronikus eljárási jogról szóló jegyzet [187].

2. nem graduális, de széles társadalmi támogatottságot élvező oktatási rendszerből származó tanúsítvány preferálása (létező példák az IKER[254] vagy ECDL[255]) vagy

3. minimálisan invazív oktatás lehetővé tétele[256], a 3. hipotézis gyakorlati igazolásával ([73]: 370)

A 3. változat létjogosultságát erősíti, hogy a graduális oktatásban a Nemzeti Alaptanterv hitelességre vonatkozó elemeken kívül nem került 2019 januárjáig be a terület. Az további vizsgálatot igényelhet, hogy létezik-e az átadható tudás komplexitásának felső korlátja minimálisan invazív módszerek esetében, valamint kidolgozható-e felnőttek számára is ilyen konstrukció.

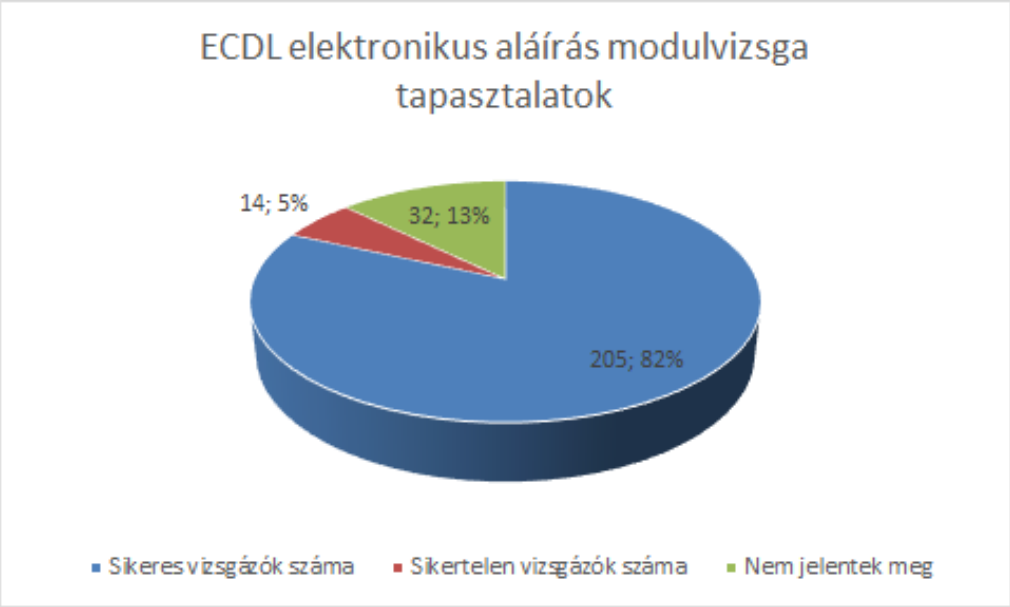
Az ECDL modul 2010 óta elérhető, de lényeges számosságot nyolc év alatt sem sikerült elérni (az NJSZT ECDL Iroda adatai szerint 205 fő szerzett bizonyítványt 2011.01-2019.01 között), így lehetséges, hogy új módszerek felé kell nézni a terjedés elősegítéséhez, mivel az oktatás kulcsszerepe Vrabie által is megerősítést nyert [71].



21. ábra: ECDL elektronikus aláírás modul sikeres vizsgázóinak a száma 2011-2019.01. között[257] (forrás: saját ábra)

[254] Lásd https://www.nive.hu/index.php?option=com_content&view=article&id=665 (2019.02.04)
[255] Lásd http://njszt.hu/ecdl/hir/20180612/digitalis-kompetenciak-europai-keretrendszere
[256] A „minimálisan invazív oktatás" kifejezést Sugata Mitra „lyuk a falon" névvel elhíresült kísérlete teremtette meg 1999-ben Indiában [72], amelyet azóta széles körben használnak az oktatási rendszerek megreformálásának egyik lehetőségeként. A kifejezést a sebészettől kölcsönözte.
[257] Készült az NJSZT ECDL Iroda által 2019. február 6-án átadott adatok alapján.

Az elektronikus aláírással kapcsolatos tudás komplexitásának egyik jelzőszáma lehet az ECDL modulvizsgát sikertelenül teljesítők számossága és ennek aránya a sikeres vizsgázókhoz képest. A vizsgált időszakban csupán a vizsgán megjelentek 6,39%-a tett sikertelen vizsgát, így ez egyrészről azt bizonyítja, hogy a sikeres vizsgához valamennyi tudás megszerzése szükséges, másrészről azt, hogy ennek a tudásnak a megszerzése széles társadalmi rétegekben sem jelent problémát, mivel az ECDL nem korfüggő és nem követel meg semmilyen előzetes képzettséget a vizsgára való jelentkezéshez.



22. ábra. ábra: ECDL elektronikus aláírás modul sikertelen vizsgázóinak a száma 2011.01-2019.01 között[258] (forrás: saját ábra)

Az ekvivalencia a graduális képzésben résztvevőknél áll fenn, a posztgraduális generáció esetében csak a 2. vagy 3. megoldás jöhet számításba graduális képzés hiányában. Kontraindikatív megállapítás, hogy habár a digitális kompetenciákra sok esetben a „digitális írástudás" kifejezéssel hivatkoznak, az európai digitális kompetenciák körébe az elektronikus aláírás mégsem férhetett be 2019 januárjáig[259]. Az e-közigazgatásban a digitális tartalmak létrehozásához vagy a hiteles kommunikáció kialakításához és ellenőrzéséhez ez a tudás márpedig nélkülözhetetlennek látszik.

[258] Készült az NJSZT ECDL Iroda által 2019. február 6-án átadott adatai alapján.
[259] Lásd http://njszt.hu/sites/default/files/ecdl_digcomp_competences_nagyobb.jpg (2019.04.02.)

Sorszám	Megyék (és Budapest)	Elektronikus aláírás modulra akkreditált vizsgaközpontok száma
1	Bács-Kiskun	0
2	Baranya	1
3	Békés	3
4	Borsod-Abaúj-Zemplén	2
5	Budapest	14
6	Csongrád	1
7	Fejér	1
8	Győr-Moson-Sopron	0
9	Hajdú-Bihar	0
10	Heves	1
11	Jász-Nagykun-Szolnok	3
12	Komárom-Esztergom	1
13	Nógrád	0
14	Pest	6
15	Somogy	0
16	Szabolcs-Szatmár-Bereg	4
17	Tolna	2
18	Vas	0
19	Veszprém	0
20	Zala	1
	Összesen	40

22. táblázat: ECDL vizsgaközpontok elektronikus aláírás akkreditációval 2019.02.04.[260]

(forrás: saját táblázat)

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*

[260] Készült az ECDL nyilvánosan elérhető nyilvántartása alapján (http://njszt.hu/ecdl/vizsgakozpontok)

az „intelligens polgárok” létezése *is* szükséges feltétele a minőségi e-közigazgatás létezésének, különben a polgárok tudás vagy bizalom hiányában a papíralapú módszereknél maradnak vagy visszatérnek hozzájuk [71], aminek következtében a fejlesztések kihasználatlanul üzemelnek az esetleges megszüntetésükig. Az Elektronikus Aláírás Dimenzió Modell 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 az oktatási anyag egyszerűen képezhető.

9. ÖSSZEFOGLALÁS

Az elektronikus aláírás triviális mérhetőségén (azaz bináris számként való megjelenítésén) túl definiálható egy olyan metrikus tér – az Elektronikus Aláírás Dimenzió Modell, 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 egy olyan generalizált eszközt biztosít ez a modell, ami 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 felvetése [9] 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 hálózatának[261] 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 [69] 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 ([70]: 25) következtetései az információs szegénységről, amely szerint egyrészről a technológiákhoz való hozzáférés vagy annak hiánya jelentős hatást gyakorol a társadalom szereplőire, másrészről 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

[261] Az IoT az „Internet of Things” dolgok internete, az IoD pedig az „Internet of Devices” eszközök internete kifejezések rövidítéseként vált ismertté. Kusper az „Internet ott Tárgyak” magyarítást javasolja [194], Rutledge et. al. [195] technológiai riportjukban amellett érvelnek, hogy az IoT jobban konceptualizálható IoD értelemben, mivel nem az okoseszközök funkcióit (pl. hűtés, mosás stb.) kötjük az internetre, hanem egy olyan technológiai eszközt, amelyik képes adatokat fogadni és továbbítani az interneten attól függetlenül, hogy mi a funkciója és meg is adja az eszközök egy lehetséges osztályozását. Konszenzusként az „IoT (connected) devices” (dolgok internetében összekapcsolódó eszközök) kifejezés is kezd ma már elterjedni [197] annak bizonyítékaként, hogy a két fogalom nem választható el élesen. A jelenség nagyságát szemlélteti, hogy az összekapcsolt eszközök számát a 2019-es 26,66 milliárdos értékről 2025-re 75,44 milliárdra teszik (https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/)

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[262], 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. A kontextusra egy példa az elektronikus ügyintézés, amelyben a digitális szakadék elektronikus aláírásra vonatkozó nagysága mérhetővé válik a köztisztviselők elektronikus aláírási ismeretanyaga és az e-közigazgatás által megkövetelt elektronikus ügyintézésben szükséges elektronikus aláírási kompetenciák közötti különbség számszerűsítése következtében. Ugyanez a metódus alkalmas az ügyfelek pozícionálására 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.

9.1. KÖSZÖNETNYILVÁNÍTÁS

Hálás köszönettel tartozom mindenkinek, aki a mű elkészítésében bármilyen módon és mértékben közreműködött, ideértve családomat is, akik elfogadták azt, hogy egy ilyen vállalkozás olyan időt és energiát is megkövetel, amit tőlük kellett elvonnom. Remélem sikerült ennek ellenére elegendő mértékben jelen lennem az ő életükben is, mialatt az értekezésen dolgoztam. A teljesség igénye nélkül legyen szabad néhány nevet külön kiemelnem és megemlítenem. Ezt a művet Székely Zoltán László (Larsen) és Vasvári György emlékének ajánlom, akik nélkül nem kezdtem volna bele és akik sajnos már nem érhették meg a mű befejezését. Köszönetemet szeretném kifejezni témavezetőm Muha Lajos iránymutatásáért és kitartó ösztönzéséért, és a MELASZ, Microsec, Magyar Telekom, illetve TÜViT szakértőinek a sok-sok szakmai tanácsért, tapasztalatért és segítségnyújtásért.

Az értekezésben felhasznált empirikus adatokat nem tudtam volna prezentálni azok nélkül, akik kérésemre ezeket a rendelkezésemre bocsátották az általam definiált

[262] A megkövetelt tudásba itt beleérthető az „írni tudás” is, mivel az elektronikus világban a kézírás kevésbé használt és kevésbé fejlett készséggé válhat. Ennek ellenére az alkalmazhatóság továbbra is fennállhat, mivel a hatályos jogszabályok nem azt követelik meg, hogy az aláíró a saját nevét írja le aláírásként, hanem az állandóságot (szokásos aláírás) feltételezik, amit az aláíró leír, azt írja le ezt követően is aláírásként. A gyakorlatban ez általában az aláíró neve, de nem minden esetben.

módon és mértékben. Különös köszönettel tartozom tehát Alföldi Istvánnak, Miltényi Gábornak (NJSZT), Hajagos Szilárdnak (NJSZT ECDL Iroda), dr. Tamási Attilának (MOKK), Szilvia Buzoganynak (Románia), Kisfalvi Bencének, Pálfi Gergőnek és Oláh Istvánnak (OTP Bank), Ferencz Attilának, Kővári Ferencnek és Joláthy Dánielnek (NISZ Kormányzati Hitelesítés Szolgáltató), Golda Bencének és Bogár Attilának (Cursor Insight) egyaránt. Nélkülük ez az értekezés nem tartalmazhatott volna ennyi empirikus adatot és nem tudtam volna a gyakorlatot ilyen mértékben bemutatni, megvizsgálni és következtetéseket levonni. Ezúton is köszönöm mindenkinek a szíves közreműködést!

10. IRODALOMJEGYZÉK

[1] Komjáthy Miklós. 1974. A magyarországi írásbeliség kialakulása. (Irástudó réteg, kancellária oklevelek, - Az ügyek intézése során keletkezett iratok.) In. Pintér Márta (összeállító). Régi könyvek és kéziratok. Tanulmánygyűjtemény. Országos Széchényi Könyvtár, Könyvtártudományi és Módszertani Központ, Népművelési Propaganda Iroda. Budapest. 151-154. old.

[2] dr. Rátai Balázs. 2000. Az elektronikus aláírás szabályozásának kulcskérdései az 1999/93/EC irányelv alapján. Jogi Fórum. Letöltve: 2018. április 3. http://www.jogiforum.hu/files/publikaciok/ratai-1993_93_ec(jf).doc

[3] Muha Lajos. 2009. Infokommunikációs biztonsági stratégia. Hadmérnök IV. évfolyam 1. szám: 2009. március. 214-224. old.

[4] Muha Lajos. 2008. Az informatikai biztonság egy lehetséges rendszertana. Bolyai Szemle. 17. évfolyam 4. szám. 137-156. old.

[5] Carl Ellison – Bruce Schneier. 2000. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. Computer Security Journal, Volume XVI, Number 1, 2000. ISSN: 0277-0865. pp.1-7.

[6] Fleiner Rita – Munk Sándor. 2012. Közigazgatási adatbázisok összekapcsolásának biztonsági kérdései. Hadmérnök, VII. Évfolyam 4. szám - 2012. december. ISSN 1788-1919. pp.119-127.

[7] WILLIAM H. DeLONE AND EPHRAIM R. McLEAN. 2003. The DeLone and McLean model of information systems success: a ten-year update. Journal of Management Information Systems, 19(4), pp. 9-30.

[8] István, Tózsa. 2013. Virtual Reality and Public Administration. Transylvanian Review of Administrative Sciences, No. 38 E/2013, pp. 202-212

[9] Nemeslaki András. 2011. Tűz és víz határán a gazdaságinformatikában. Információs társadalom. Infokommunikáció és E-Business különszám, XI. évfolyam 1-4. szám, pp. 11-30.

[10] Az Informatikai és Hírközlési Minisztérium (IHM) ajánlása a közigazgatásban a hitelesítés-szolgáltatók által végzett viszontazonosítás protokolljának műszaki specifikációjára, 2005. december 6.

[11] Felber Zsófia: Úton az interoperabilitás felé. Pro Publico Bono, 2014/1. ISSN 2063-9058. pp.154-167.

[12] EUROPEAN COMMISSION Bruxelles, le 16.12.2010 COM(2010) 744 final Annex 2. Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services'.

[13] van Dalen, Dirk, Mystic, Geometer, and Intuitionist: The Life of L. E. J. Brouwer 1881–1966. Volume 2: Hope and Disillusion, Clarendon Press, Oxford, 2005.

[14] Szittner Károly (2011): E-ügyintézés Magyarországon. E-Government Tanulmányok XXXI. Budapest, E-Government Alapítvány a Közigazgatás Modernizációjáért.

[15] Szerkesztő-lektor Prof. Emeritus Dr. Kilényi Géza (2009): A közigazgatási eljárási törvény kommentárja. Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest

[16] Bijker, Wiebe E., Of Bicycles, Bakelites, and Bulbs. Toward a Theory of Sociotechnical Change, MIT Press, Cambridge, Massachusetts, London, England, 1995.

[17] Coglianese, Cary, "Globalization and the Design of International Institutions". 2000. In Governance in a Globalizing World (Joseph S. Nye, Jr. & John D. Donohue eds., Brookings 2000). http://scholarship.law.upenn.edu/faculty_scholarship/1549

[18] Smedinghoff, Thomas J. and Hill Bro, Ruth, „MOVING WITH CHANGE: ELECTRONIC SIGNATURE LEGISLATION AS A VEHICLE FOR ADVANCING E-COMMERCE”, The John Marshall Journal of Information Technology & Privacy Law, Vol. 17, (1999), Issue. 3, pp. 723-768.

[19] Szilágyi Károly Bálint, „Az elektronikus aláírásról szóló törvénytervezet egyes alapvető kérdéseinek elméleti vizsgálata”, Jogi Fórum Portál, 2000, http://www.jogiforum.hu/files/publikaciok/szk_meh_ea_tv.pdf

[20] Diffie, Whitfield and Hellman, Martin E., „New Directions in Cryptography”, IEEE Transactions On Information Theory, Vol. IT-22, (1976), No. 6, pp. 644-654.

[21] Kemény Miklós, „Magyar Polgári Eljárásjog”, Digitális Tankönyvtár, https://www.tankonyvtar.hu/en/tartalom/tamop425/2011_0001_520_magyar_polgari_eljarasjog/2011_0001_520_magyar_polgari_eljarasjog.pdf

[22] Kerckhoffs, Auguste, „La Cryptographie Militaire”, Journal des sciences militaires, Vol. IX, (1883), pp. 5–38, Janvier, pp. 161–191, Février.

[23] Shannon, Claude Elwood, „Communication Theory of Secrecy Systems”, Bell System Technical Journal, (1949), Vol. 28-4, pp. 656-715.

[24] Rivest, Ron, Shamir, Adi, Adleman, Leonard, „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, Vol 21, (1978), Issue 2, pp. 120–126. https://doi.org/10.1145/359340.359342

[25] Boneh, Dan, „Twenty Years of Attacks on the RSA Cryptosystem”, Notices of the American Mathematical Society (AMS), Vol. 46, (1999), Issue 2, pp. 203–213.

[26] „Jingjing, Wang, Thirty Years of Attacks on the RSA Cryptosystem. Report in Cryptographic algorithms and protocols, Computer Science, SJTU”, 2011, https://cryptjwang.files.wordpress.com/2012/05/rsa_attacks.pdf

[27] „IBM developerWorks Lotus: The History of Notes and Domino”, November 14, 2007 (First published December 20, 2005), https://www.ibm.com/developerworks/lotus/library/ls-NDHistory/ls-NDHistory-pdf.pdf

[28] Swartzbeck, Michael: The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies (U) Responding to a Complex Problem, 1999(?), https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf

[29] Rózsa György, „Információs társadalom – UNESCO – információs szupersztráda”, Tudományos és Műszaki Tájékoztatás, 44. évf., (1997), 9. szám, 337-339 old.

[30] European Commission, Report on Europe and the Global Information Society: Recommendations of the High-level Group on the Information Society to the Corfu

European Council, Bulletin of the European Union, Supplement No. 2/94, 1994. http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf

[31] Commission of The European Communities, Proposal for a EUROPEAN PARLIAMENT AND COUNCIL, DIRECTIVE on a common framework for electronic signatures, Brussels, 13.05.1998, COM(1998) 297 final, 98/0191 (COD).

[32] D. Harrison McKnight, Norman L. Chervany. 2001. Trust and Distrust Definitions: One Bite at a Time. In R. Falcone, M. Singh, and Y.-H. Tan (Eds.): Trust in Cyber-societies, LNAI 2246, pp. 27–54, 2001.

[33] Vasvári György: A társadalmi és szervezeti (vállalati) biztonsági kultúra. Budapest, Ad Librum Kft., 2009. ISBN 978-963-9934-66-5. p11

[34] Carl E. Landwehr: Formal Models For Computer Security. Association for Computing Machinery (ACM), USA. 1981. ISSN:0360-0300. Computing Surveys; Vol 13. No. 3. pp247-278

[35] Jøsang A., Presti S.L. (2004) Analysing the Relationship between Risk and Trust. In: Jensen C., Poslad S., Dimitrakos T. (eds) Trust Management. iTrust 2004. Lecture Notes in Computer Science, vol 2995. Springer, Berlin, Heidelberg. pp.135-145.

[36] Daniel W. Manchala. 2000. E-commerce trust metrics and models. IEEE Internet Computing, USA, California. 2000/3 Volume 4. Issue 2. pp.36-44.

[37] Budai Balázs Benjámin. 2014. Az e-közigazgatás elmélete (Második, átdolgozott kiadás), Budapest, Akadémiai Kiadó Zrt.

[38] Capgemini, IDC, Sogeti, and Politecnico di Milano. 2017. eGovernment Benchmark 2017. Taking stock of user-centric design and delivery of digital public services in Europe.

[39] BERGERON, Bryan (2003): Essentials of Knowledge Management. Hoboken, New Jersey, John Wiley & Sons, Inc.

[40] GOTTSCHALK, P. (2007): Knowledge Management. 130–143. In. JENNEX, M. E. (Ed.): Knowledge Management. Concepts, Methodologies, Tools, and Applications, Volume I. Herhey: Information Science Reference

[41] GUPTA, J. N. D., SHARMA, S. K., HSU, J. (2008): An Overview of Knowledge Management. 1–22. In. JENNEX, M. E. (Ed.): Knowledge Management. Concepts, Methodologies, Tools, and Application. Volume I. Herhey: Information Science Reference

[42] Internet Live Stats (2018): Internet users in the world. www.internetlivestats.com/internet-users/#trend (A letöltés dátuma: 2018. 03. 08.)

[43] JENNEX, Murray E. (2008): Chapter 2.9. Internet Support for Knowledge Management Systems. 564–570. In. JENNEX, M. E. (Ed.): Knowledge Management. Concepts, Methodologies, Tools, and Application. Volume II. Herhey: Information Science Reference

[44] KORONVÁRY P. (2008): Gondolatok a vezetéstudomány feladatáról. Hadmérnök, III 2, 161–168.

[45] SVEIBY, K. E. (2001): Szervezetek új gazdagsága: a menedzselt tudás. Budapest: KJK-KERSZÖV Jogi és Üzleti Kiadó Kft.

[46] TSERNG, H. P., LIN Y-C. (2008): A Knowledge Management Portal System for Construction Projects Using Knowledge Map. 692–710. In. JENNEX, M. E. (Ed.): Knowledge Management. Concepts, Methodologies, Tools, and Applications, Volume I. Herhey: Information Science Reference

[47] BERGERON, Bryan (2003): Essentials of Knowledge Management. Hoboken, New Jersey, John Wiley & Sons, Inc.

[48] GOTTSCHALK, P. (2007): Knowledge Management. 130–143. In. JENNEX, M. E. (Ed.): Knowledge Management. Concepts, Methodologies, Tools, and Applications, Volume I. Herhey: Information Science Reference

[49] Kenta TAKAHASHI et. al. (2015): A Signature Scheme with a Fuzzy Private Key. 2015. pp.105-126.

[50] Maurice FRÉCHET: Sur Quelques Points Du Calcul Fonctionnel. PhD thesis. Memorie E Comunicazioni. Palermo, 1906. http://libarch.nmu.org.ua/bitstream/handle/GenofondUA/26139/e9aaa2b682f199cb27a56ad8d42a5abb.pdf (2019.01.24.)

[51] TAMÁS András: A közigazgatási jog elmélete. 2001. Budapest, Szent István Társulat. ISBN 963 361 303 5, ISSN 1417-7285. pp.16-18.

[52] VASVÁRI György: Bankbiztonság. Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság és Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék, Budapest, Magyarország. 2003. p.68.

[53] Hamming, R. W. (1950). Error Detecting and Error Correcting Codes. Bell System Technical Journal, 29(2), 147–160. doi:10.1002/j.1538-7305.1950.tb00463.x p.155.

[54] Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec, Vashek Matyas: The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. 24th ACM Conference on Computer and Communications Security (CCS'2017), 2017, ISBN: 978-1-4503-4946-8/17/10. ACM. pp. 1631-1648.

[55] Eckhart Ferenc: Hiteleshelyek a középkori Magyarországon. MOKK, Budapest, Magyarország. 2012. ISBN: 978-963-88147-9-1

[56] ETSI White Paper. Quantum Safe Cryptography V1.0.0 (2014-10), Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges. ISBN 979-10-92620-03-0. 2014.

[57] William Stallings: Cryptography and Network Security Principles and Practice (Sixth Edition). 2014. ISBN 13: 978-0-13-335469-0 (Table 19.1)

[58] National Institute of Standards and Technology: Federal Information Processing Standards Publication 186-4. Digital Signature Standard (DSS). 2013 July.

[59] Bruce Schneier: Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth). John Wiley & Sons, Inc., Hoboken, USA, 1996.

[60] Daniel GOTTESMAN, Isaac CHUANG: Quantum Digital Signatures. arXiv Quantum Physics, Cornell University, Ithaka, USA. 2001.

[61] Ed. Daniel J. BERNSTEIN, Johannes BUCHMANN, Erik DAHMEN: Post-Quantum Cryptography. Springer-Verlag Berlin Heidelberg, Germany. 2009.

[62] ETSI White Paper No. 8: Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges. June 2015.

[63] Walter Fumy, Frank Morgner, Andreas Hülsing: D5.2 Standardization: Final report, Revision: 1.6, 2018. PQCRYPTO Post-Quantum Cryptography for Long-Term Security, Project number: Horizon 2020 ICT-645622, https://pqcrypto.eu.org/deliverables/d5.2-final.pdf (2019. január 28.)

[64] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone: NISTIR 8105 Report on Post-Quantum Cryptography. 2016. http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (2019. január 28.)

[65] Robert R. Schaller: Moore's law: past, present and future. IEEE Spectrum, New York, USA. 1997. Vol. 34. Issue 6. pp.53-59. DOI: 10.1109/6.591665

[66] William Buchanan, Alan Woodward (2017) Will quantum computers be the end of public key encryption?, Journal of Cyber Security Technology, 1:1, 1-22, DOI: 10.1080/23742917.2016.1226650. p13.

[67] Haifeng Qian, Shouhuai Xu: Non-Interactive Editable Signatures for Assured Data. 2011. ProvenanceCODASPY'11, February 21–23, 2011, San Antonio, Texas, USA.

[68] Vasilios MAVROUDIS, Andrea CERULLI, Petr SVENDA, Dan CVRCEK, Dusan KLINEC, George DANEZIS: A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, (CCS 2017), Dallas, TX, USA, October 30 - November 03, 2017. 1583—1600.

[69] Molnár Szilárd, „A megrekedt magyar modernizáció kiútkeresése a sokrétű digitális megosztottság útvesztőjéből", Információs Társadalom, XVII. évf. (2017), 2. szám, 30–47. old. http://dx.doi.org/10.22503/inftars.XVII.2017.2.2

[70] Csótó Mihály, „Aki (információ)szegény, az a legszegényebb? Az információs szegénység megjelenési formái", Információs Társadalom, XVII. évf. (2017) 2. szám, 8-29. old. http://dx.doi.org/10.22503/inftars.XVII.2017.2.1

[71] Catalin Vrabie: Education – A Key Concept for E-Administration. Procedia - Social and Behavioral Sciences, 2015, Volume 186, pp.371-375. doi: 10.1016/j.sbspro.2015.04.121

[72] Sugata Mitra: Minimally Invasive Education for mass computer literacy. 2000. CRIDALA ('Conference on Research in Distance and Adult Learning in Asia ') 2000 conference, Hong Kong, 21-25 June, 2000.

[73] Sugata Mitra: Minimally invasive education: a progress report on the “hole-in-the-wall” experiments. 2003. *British Journal of Educational Technology*, 34(3), 367–371. doi:10.1111/1467-8535.00333

[74] Resperger István: II. *A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések*. 2018. In: (Szerk:) Resperger István: A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest. 10. táblázat, p.89.

[75] Kovács László – Krasznay Csaba: Digitális Mohács, Egy kibertámadási forgatókönyv Magyarország ellen. 2010. Nemzeti Közszolgálati Egyetem, Budapest. Nemzet és biztonság, 2010. február. pp.44-56.

[76] Bogdán István: *Régi magyar históriák*. Budapest, Magvető, 1980.

[77] Falus Orsolya: *Ispotályos keresztes lovagrendek az Árpád-kori Magyarországon*. Doktori disszertáció, Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kara Doktori Iskolája, 2014. https://ajk.pte.hu/files/file/doktori-iskola/falus-orsolya-fruzsina/falus-orsolya-fruzsina-vedes-ertekezes.pdf (2019. február 11.). 63. old.

[78] Tubay Tiziano: *Titokzatos örökség – A székely írás kutatásának nehézségei*. In: kultúrjav. Írásbeliség és szóbeliség irodalma – újrahasznosítva: Fiatalok Konferenciája 2014, szerk. Bartók Zsófia Ágnes, Fajt Anita, Görög Dániel, Maróthy Szilvia, Budapest, reciti, 2015 (Arianna könyvek, 9), 2014, http://real.mtak.hu/90056/1/TubayTiziano2015TitokzatosoroksegKulturjav.FIKON_183-196.pdf

[79] Réthy László: Az úgynevezett hún-székely írás. Írásmintákkal. *In: Szerk. Hampel József, Archaeologiai Értesítő*. Magyar Tudományos Akadémia, Budapest. Új folyam, VIII. kötet. pp.54-60. (http://real-j.mtak.hu/315/, 2019. február 11.)

[80] Danny De Cock, Karel Wouters, Bart Preneel: Introduction to the Belgian EID Card. *Lecture Notes in Computer Science*, (2004), vol. 3093. pp.1-13.

[81] Javier Lopez, Rolf Oppliger, Günther Pernul: Classifying Public Key Certificates. *Lecture Notes in Computer Science*, (2005), vol. 3545. pp.135–143. doi:10.1007/11533733_9

[82] Jon Ølnes, Leif Buene: Use of a Validation Authority to Provide Risk Management for the PKI Relying Party. *Lecture Notes in Computer Science*, (2006), Vol. 4043. pp.1–15.

[83] Ke Zeng: Pseudonymous PKI for Ubiquitous Computing. Lecture Notes in Computer Science, (2006), vol. 4043. pp.207–222. doi:10.1007/11774716_17

[84] Massimiliano Pala, Sean W. Smith: AutoPKI: A PKI Resources Discovery System. Lecture Notes in Computer Science, (2007), vol. 4582. pp.154–169. doi:10.1007/978-3-540-73408-6_11

[85] David Montana, Mark Reynolds: Validation Algorithms for a Secure Internet Routing PKI. Lecture Notes in Computer Science, (2008), Vol 5057. pp.17–30. doi:10.1007/978-3-540-69485-4_2

[86] Alexander. W. Dent: A Brief Introduction to Certificateless Encryption Schemes and Their Infrastructures. Lecture Notes in Computer Science, (2010), Vol. 6391. pp.1–16. doi:10.1007/978-3-642-16441-5_1

[87] Massimiliano Pala, Sara Sinclair, Sean W. Smith: PorKI: Portable PKI Credentials via Proxy Certificates. Lecture Notes in Computer Science, (2011), Vol. 6711. pp.1–16. doi:10.1007/978-3-642-22633-5_1

[88] Gauthier Van Damme, Nicolas Luyckx, Karel Wouters: A PKI-Based Mobile Banking Demonstrator. Lecture Notes in Computer Science, (2012), Vol. 7163. pp. 147–158. doi:10.1007/978-3-642-29804-2_10

[89] Martín A.G. Vigil, Cristian T. Moecke, Ricardo F. Custódio, Melanie Volkamer: The Notary Based PKI. Lecture Notes in Computer Science, (2013), Vol. 7868. pp.85–97. doi:10.1007/978-3-642-40012-4_6

[90] Tiffany Hyun-Jin Kim, Virgil Gligor, Adrian Perrig: GeoPKI: Converting Spatial Trust into Certificate Trust. Lecture Notes in Computer Science, (2013), Vol. 7868. pp.128–144. doi:10.1007/978-3-642-40012-4_9

[91] Felipe Carlos Werlang, Ricardo Felipe Custódio, Martín A.G. Vigil: A User-Centric Digital Signature Scheme. Lecture Notes in Computer Science, (2014), Vol. 8341. pp.152-169. doi:10.1007/978-3-642-53997-8_10

[92] Jos Dumortier, Stefan Kelm, Hans Nilsson, Georgia Skouma, Patrick Van Eecke: The legal and market aspects of electronic signatures. Study for the European Commission – DG Information Society, Service Contract Nr, C 28.400. 2003. Belgium, EU. Interdisciplinary Centre for Law and ICT (ICRI – IBBT) of the Faculty of Law of the Catholic University of Leuven, Belgium, https://www.secorvo.de/publikationen/electronic-sig-report.pdf

[93] Nicole van der Meulen: DigiNotar: Dissecting the First Dutch Digital Disaster. *Journal of Strategic Security*, (2013), Vol 6, No. 2. pp.46-58.

[94] Tózsa István: e-Közigazgatás Európában – Jelen és jövő. 2011. *Vezetéstudomány* XLII. ÉVF. 2011. 3. szám. pp.10-18.

[95] Martin Gardner: Mathematical Games – A new kind of cipher that would take millions of year to break. Scientific American, 1977. August, Volume 237 Number 2, pp.120-124.

[96] Simon Singh: Kódkönyv. A rejtjelzés és rejtjelfejtés története. Park Könyvkiadó, Budapest. 2001.

[97] Ronald L. Rivest, Adi Shamir, Len Adleman: On Digital Signatures and Public-Key Cryptosystems. 1997. USA, Massachusetts, Cambridge. https://apps.dtic.mil/dtic/tr/fulltext/u2/a039036.pdf (2019. február 17.)

[98] Stafford E. Tavares, A. F. Webster: On the design of S-Boxes. Lecture Notes in Computer Science, (1986), Vol. 218. pp.523–534. doi: 10.1007/3-540-39799-X_41

[99] Neumann János: Túlélhetjük-e a technikát? (Can we survive technology? Fortune, June 1955). In: Neumann János Válogatott írásai. Válogatta és az előszót írta: Ropolyi László. 2005. TYPOTEX Kft. Elektronikus Kiadó, Budapest

[100] Bárdos Zoltán: A villamosenergia-ellátás biztonságáról. 2009. Nemzeti Közszolgálati Egyetem, Budapest. Bolyai Szemle, XVIII. évf. 1. szám, 77-84. old.

[101] Gyebrovszki Tamás: Folyamatos fenyegetések a kibertérben. 2014. Nemzeti Közszolgálati Egyetem (NKE) Hadtudományi és Honvédtisztképző Kar (HHK), Budapest. Hadmérnök, IX. Évfolyam, 3. szám, 137-153. old.

[102] Som Zoltán: A közigazgatási informatikai felelősök oktatásának kérdései. 2013. Nemzeti Közszolgálati Egyetem (NKE) Hadtudományi és Honvédtisztképző Kar (HHK), Budapest. Hadmérnök, VIII. évf. 4. szám. 223-237. old.

[103] Leonard M. Adleman: An Abstract Theory of Computer Viruses. Lecture Notes in Computer Science, (1990), Volume 403. pp.354-374.

[104] Gene Bransfield: The Welchia Worm. 2004. SANS Institute, USA. https://www.giac.org/paper/gcih/517/welchia-worm/105720 (2019. február 18.)

[105] Póserné Oláh Valéria: Közigazgatási informatikai rendszerek informatikai biztonsági kérdései. PhD Értekezés. 2011. Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Hadmérnöki Kar, Hadmérnöki Doktori Iskola, Budapest.

[106] Bukovics István: A természeti és civilizációs katasztrófák paradigmatikus elmélete. 2007. MTA doktori disszertáció. *2. fejezet: Logikai kockázatelmélet.* p.20.

[107] S. Benedikt, I. Kun, G. Szász: Individual and Collective Risk Perception in Decision Criteria. In: Ed: Robert Trappl: CYBERNETICS AND SYSTEMS 2004. VOLUME I. Proceedings of the Seventeenth European Meeting on Cybernetics and Systems Research, organized by the Austrian Society for Cybernetic Studies, held at the University of Vienna, Austria, 13-16 April 2004. pp321-325.

[108] Kun István - Fáy Gyula - Bukovics István: Logikai Hadviselés - Kritikus Pontok Harca. Hadmérnök, VI. Évfolyam 4. szám - 2011. december. pp.189-203.

[109] Berta, István Zsolt: Mitigating the attacks of malicious terminals. PhD dissertaion. 2005. Budapest University of Technology and Economics.

[110] Szabó Katalin, Hámori Balázs: Információgazdagság. Digitális kapitalizmus vagy új gazdasági rendszer. 7. fejezet: Bizalom, reputáció és identitás az elektronikus piacokon. Budapest, Akadémiai Kiadó. 2006. pp188-205

[111] Z. Karvalics László: Az univerzális kvantor rémuralma, avagy a veszélydiskurzusok logikai szerkezetéről. 2010. In: Az Internet. A kockázatok és mellékhatások tekintetében (Szerk: Talyigás Judit), Scolar Kiadó, Budapest.

[112] Valentina Casola, Antonino Mazzeo, Nicola Mazzocca, Valeria Vittorini: A policy-based methodology for security evaluation: A Security Metric for Public Key Infrastructures. Journal of Computer Security, (2007), vol. 15, no. 2, pp.197–229. DOI: 10.3233/JCS-2007-15201.

[113] Hossein Bidgoli: Handbook of Information Security. Key Concepts, Infrastructure, Standards and Protocols, Volume 1. John Wiley & Sons Inc, 2006. p.871

[114] Ken Polsson: Chronology of Personal Computers. Last updated: 2017 April 29. http://pctimeline.info/comp1986.htm (2019. február 19.)

[115] Whitfield Diffie, Susan Landau: Privacy on the Line. The Politics of Wiretapping and Encryption. 2007, Updated and Expanded Edition. The MIT Press, USA, England. p.229.

[116] Stephan Grill: An Approach to Formally Compare and Query Certification Practice Statements. 2004. In: (Ed.) John R. Vacca: Public Key Infrastructure: Building Trusted Applications and Web Services. pp.115-126.

[117] Ronald J. Brachman, Deborah L. McGuinness, Peter F. Patel-Schneider, Lori Alperin Resnick, Alexander Borgida: LIVING WITH CLASSIC: When and How to Use a KL-ONE-Like Language. 1991. In: (Ed.) John F. Sowa: Principles of Semantic Networks. Explorations in the Representation of Knowledge, USA, California.

[118] Bruce Schneier: Attack Trees – Modeling Security Threats. Dr. Dobb's Journal, 1999/12., p.21-29.

[119] Bruce Schneier: Secrets & Lies. 2000. John Wiley & Sons, USA. Part 3, Chapter 21. pp.318-333.

[120] Charles H. Bennett, Gilles Brassard: An Update On Quantum Cryptography. In: G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS (1985), Volume 196, pp.475-480.

[121] John D. Howard: An Analysis Of Security Incidents On The Internet 1989-1995. A dissertation submitted to the graduate school in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Engineering and Public Policy. Carnegie Mellon University, Pittsburgh, Pennsylvania 15213 USA. April 7, 1997.

[122] John D. Howard and Thomas A. Longstaff: A Common Language for Computer Security Incidents. 1998. Sandia National Laboratories [Technical Sandia Report: SAND98-8667].

[123] Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban. Hadmérnök, VII. Évfolyam 4. szám - 2012. december. ISSN 1788-1919. pp.142-151.

[124] Munk Sándor: A biztonság kérdéseinek dekompozíciója. Hadmérnök, V. Évfolyam 2. szám - 2010. június. pp.404-417.

[125] Juhász Lilla: Magyary Zoltán, az elektronikus közigazgatás előfutára. 7. Világosság, 2006:(1), 21-28. old.

[126] Szádeczky Tamás: Szabályozott biztonság Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan. 2011. PhD értekezés, Pécs. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola.

[127] Szilágyi Károly Bálint: Az elektronikus aláírásról szóló törvénytervezet egyes alapvető kérdéseinek elméleti vizsgálata. Szilágyi Ügyvédi Iroda készítette a Miniszterelnöki Hivatal Informatikai Kormánybiztosságának Szabályozási Főcsoportfőnöksége részére. Pécs, 2000. november 18. http://www.jogiforum.hu/files/publikaciok/szk_meh_ea_tv.pdf (2019. február 21.)

[128] Teemu Rissanen: Identity in the Information Society (2010) 3: 175. https://doi.org/10.1007/s12394-010-0049-8

[129] Baranyi Bertold, Homoki Péter, Kovács A. Tamás: Magyarázat az elektronikus ügyintézésről. 2018. Budapest, Wolters Kluwer Hungary Kft.

[130] Erdős Éva, Kecskeméti Ágnes: A mérlegelési jog sajátosságai a jogalkalmazói gyakorlat tükrében. Publicationes Universitatis Miskolcinensis. Sectio Juridica et Politica (2014): Tomus XXXII. pp.147-162

[131] Yoneji Masuda: The Information Society as Post-industrial Society. 1980. Institute for the Information Society, Tokyo, Japan

[132] Szerk: Tóth András: Technológia jog – Új globális technológiák jogi kihívásai. 2016. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar

[133] Adi Shamir: Identity-Based Cryptosystems and Signature Schemes. Lecture Notes in Computer Science, (1985): Volume 196. Berlin Heidelberg, Springer-Verlag Berlin Heidelberg, pp.47-53.

[134] Phil Zimmermann: PGP: Source Code and Internals. 1995. USA, Massachusetts, The MIT Press.

[135] McCarthy, J., Winchester, J., The Autopen, in: Journal of Forensic Sciences, 18/4 (1973), pp. 441-447

[136] İlkhan Cüceloğlu, Hasan Oğul: Detecting handwritten signatures in scanned documents. CVWW 2014: Zuzana Kúkelová and Jan Heller (eds.), Proceedings of the 19th Computer Vision Winter Workshop, February 3-5, 2014, Křtiny, Czech Republic, pp.89-94.

[137] Limor Kessem: Future of Identity Study – Consumer perspectives on authentication: Moving beyond the password. 2018. USA, Cambridge, IBM Security.

[138] Haig Zsolt: Információ – társadalom – biztonság. 2015. Budapest, Nemzeti Közszolgálati Egyetem Szolgáltató Kft.

[139] Diaz, Moises, Ferrer, Miguel, Impedovo, Donato, Imran Malik, Muhammad, Pirlo, Giuseppe, Plamondon, Réjean: A Perspective Analysis of Handwritten Signature Technology. 2019. ACM Computing Surveys, Vol. 51, No. 6, Article 117.

[140] Muhammad Imran Malik, Sheraz Ahmed, Angelo Marcelli, Umapada Pal, Michael Blumenstein, Linda Alewijns, Marcus Liwicki: ICDAR2015 competition on signature verification and writer identification for on-and off-line skilled forgeries (SigWIcomp2015). In: 13th IAPR International Conference on Document Analysis&Recognition (ICDAR), August 23-26, 2015, Prouvé Congress Center, Nancy, France Conference Proceedings, IEEE Computer Society, pp. 1186-1190.

[141] Orvos Péter, Hornák Zoltán, Selényi Endre: Biometrikus azonosítás felhasználása hiteles digitális aláírások előállítására. Networshop Konferencia, 2001, Sopron. https://nws.niif.hu/ncd2001/docs/eloadas/80/index.htm (2019. február 23.)

[142] Orvos Péter, Hornák Zoltán, Selényi Endre: Biometriával ötvözött digitális aláírások irányába. Networkshop Konferencia, 2002, Eger. http://nws.niif.hu/ncd2002/docs/ahu/17.html (2019. február 23.)

[143] Otti, Csaba, Kolnhofer-Derecskei, Anita: Az emberek elfogadási küszöbe a biometrikus rendszerek megbízhatóságával szemben, Szakmai Szemle, XVI (3), pp.133–147, 2018.

[144] Deep Mann, Shashank Gupta, Ankit Sharma, Shakil Akhtar: Digital Signature Using Biometrics. In: Proceedings of the World Congress on Engineering and Computer Science 2015 Vol I WCECS 2015, October 21-23, 2015, San Francisco, USA. pp. 119-122.

[145] MELASZ Állásfoglalás a biometrikus aláírások alkalmazása tekintetében. 2016. április 8. https://www.melasz.hu/lang-hu/a-melasz-hirei/1290-melasz-allasfoglalas-a-biometrikus-alairasok-alkalmazasa-tekinteteben (2019. február 23.)

[146] Shahriar Mohammadi, Sanaz Abedi: ECC-Based Biometric Signature: A New Approach in Electronic Banking Security. 2008. In: International Symposium on Electronic Commerce and Security, 2008 (ISECS 2008), August 4-5 Guangzhou, 2008, China. pp.763-766.

[147] Szerk: Kaiser, Tamás: Jó Állam Jelentés 2018, Dialóg Campus, 2018.

[148] Szerk: Kaiser Tamás: Jó Állam Jelentés 2017, Dialóg Campus, 2017.

[149] Szerk: Kaiser Tamás: Jó Állam Jelentés 2016, Dialóg Campus, 2016.

[150] Szerk: Kaiser Tamás: Jó Állam Jelentés 2015, Dialóg Campus, 2015.

[151] Szerk: Csuhai Sándor: Jelentés a Jó Állam Véleményfelmérésről. 2016. Budapest, Nordex Nonprofit Kft. – Dialóg Campus Kiadó.

[152] Szerk.: Demeter Endre, Petényi Sára: Jelentés a Jó Állam Véleményfelmérésről. 2017. Budapest, Nordex Nonprofit Kft. – Dialóg Campus Kiadó.

[153] Dan S. Sorin: Digital Divide in the EU countries from the Danube Region, In Hendrik Hansen, Robert Müller-Török, András Nemeslaki, Johannes Pichler, Alexander Prosser, Dona Scloa (eds.), CEE e|Dem and e|Gov Days 2017, Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment? Proceedings of the Central and Eastern Eurpoean e|Dem and e|Gov Days 2017 May 4-5 Budapest. (pp. 79-86), Austrian Computer Society, Vienna, Austria, 2017.

[154] Csótó Mihály: Aki (információ)szegény, az a legszegényebb? Az információs szegénység megjelenési formái, Információs Társadalom, XVII. évf. (2017) 2. szám, 8-29. old. http://dx.doi.org/10.22503/inftars.XVII.2017.2.1, 2017.

[155] Uros Pinterič: Limitations of the e-Participation, In Hendrik Hansen, Robert Müller-Török, András Nemeslaki, Johannes Pichler, Alexander Prosser, Dona Scloa (eds.), CEE e|Dem and e|Gov Days 2017, Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment? Proceedings of the Central and Eastern Eurpoean e|Dem and e|Gov Days 2017 May 4-5 Budapest (pp. 89-96), Austrian Computer Society, Vienna, Austria, 2017.

[156] Merkle, Ralph C. (1988) A Digital Signature Based on a Conventional Encryption Function. In: Pomerance C. (eds) Advances in Cryptology — CRYPTO ’87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg

[157] Rando Kulla: Migrating PDF Signing To New KSI Format. Master thesis. 2016. TALLINN UNIVERSITY OF TECHNOLOGY, Faculty of Information Technology Department of Computer Science, TUT Centre for Digital Forensics and Cyber Security.

[158] Dongyoung Koo, Youngjoo Shin, Joobeom Yun, Junbeom Hur: Improving Security and Reliability in Merkle Tree-Based Online Data Authentication with Leakage Resilience. Applied Sciences, (2018), Volume 8, Issue 12, Article 2532.

[159] Francis Fukuyama: A történelem vége és az utolsó ember. 2014. Budapest, Európa Könyvkiadó.

[160] Samuel P. Huntington: A civilizációk összecsapása és a világrend átalakulása. 2018. Budapest, Európa Könyvkiadó.

[161] ISACF: Digital and Electronic Signatures: A Global Status Report. 2002. USA, Rolling Meadows, IL, Information Systems Audit and Control Foundation.

[162] Dongoh Park: Social Life of PKI: Sociotechnical Development of Korean Public-Key Infrastructure. 2015. IEEE Annals of the History of Computing. Apr-June. 2015, Volume: 37, Issue: 2. pp.59-71.

[163] Jassim Khalid AL-Hamar: Towards Internet Voting in the State of Qatar UK, Loughborough. Doctoral Thesis, 2011.

[164] Maher O. Al-Fakhri, Robert A. Cropf, Patrick Kelly, Gary Higgs: E-Government in Saudi Arabia: Between Promise and Reality. 2008. International Journal of Electronic Government Research (IJEGR), April-June 2008, Vol 4, Issue 2, pp.5-82.

[165] Malathi Subramanian, Anupama Saxena: E-Governance in India: From Policy to Reality, a Case Study of Chhattisgarh Online Information System for Citizen Empowerment (Choice) Project of Chhattisgarh State of India. 2008. International Journal of Electronic Government Research (IJEGR), April-June 2008, Vol.4, Issue 2, pp.12-26.

[166] Asaad Alzayed, Ray Dawson, Abdulaziz Alkandari: Towards a Trusted e-Election In Kuwait: Requirements and Principles. 2014. International Journal of Managing Information Technology (IJMIT), August 2014, Vol.6, No.3. pp.31-50.

[167] Erdélyi Ferenc, Tóth Tibor: Az összetett műszaki rendszerek tervezésének és irányításának szakterülete a mérnökképzésben. 2008. In: Szerk: Pethő Attila Herdon Miklós: Informatika a felsőoktatásban 2008 Konferencia kiadvány Debrecen, 2008. augusztus 27-29.

[168] Uganda Law Reform Commission: 2004 A Study Report On Electronic Transactions Law (Law Com Pub. No. 10 of 2004)

[169] Robert M. Solow: Technical Change and the Aggregate Production Function. 1957. The Review of Economics and Statistics, Vol. 39, No. 3, pp. 312-320

[170] Robert M. Solow: A Contribution to the Theory of Economic Growth. USA, The Quarterly Journal of Economics. Feb., 1956, Vol. 70, No. 1. pp. 65-94.

[171] Robert M. Solow: Information Technology and the Recent Productivity Boom in the US. 2001. Cambridge-MIT National Competitiveness Summit, November, 2001, Cambridge. http://mit.edu/cmi-videos/solow/text.html (2019. március 4.)

[172] Susan Christopherson, Michael Kitson, Jonathan Michie: Innovation, networks and knowledge exchange. 2008. Cambridge Journal of Regions, Economy and Society, July 1, 2008, Volume 1, Issue 29. pp.165–173.

[173] Karol Śledzik: Schumpeter's View on Innovation and Entrepreneurship. In: Management Trends in Theory and Practice, (ed.) Stefan Hittmar, Faculty of Management Science and Informatics, University of Zilina & Institute of Management by University of Zilina. 2013. DOI: 10.2139/ssrn.2257783

[174] Everett M. Rogers: Diffusion of innovations. 1962. USA, New York: Free Press of Glencoe (1st edition)

[175] Hámori Balázs, Szabó Katalin: A gyenge hazai innovációs teljesítmény intézményi magyarázatához. Közgazdasági Szemle, LVII. évf., 2010. október, 876–897. old.

[176] Douglass C North, John Joseph Wallis, and Barry R. Weingast: A Conceptual Framework for Interpreting Recorded Human History. NBER Working Paper, No. 12795, December 2006.

[177] Carlisle Adams, Mike Burmester, Yvo Desmedt, Mike Reiter, and Philip Zimmermann. 2000. Which PKI (public key infrastructure) is the right one? (panel session). In Proceedings of the 7th ACM conference on Computer and communications security (CCS '00), Pierangela Samarati (Ed.). ACM, New York, NY, USA, pp.98-101. DOI=http://dx.doi.org/10.1145/352600.352615

[178] Jens Bender, Marc Fischlin, Dennis Kugler: Security Analysis of the PACE Key-Agreement Protocol. Lecture Notes in Computer Science, 2009-12-18, Vol. 5735. pp.33-48.

[179] Christian Geuer-Pollmann: Confidentiality of XML documents by Pool Encryption. Forschungsberichte, UNIVERSITÄT SIEGEN, Institut für Digitale Kommunikationssysteme, Siegen, Germany. Approved dissertation. 2004.

[180] Arjen Lenstra, Thorsten Kleinjung, Emmanuel Thomé. Universal Security; From bits and mips topools, lakes - and beyond. Lecture Notes in Computer Science, 2013. Vol. 8260. pp.121-124. DOI: 10.1007/978-3-642-42001-6_9. HAL-00925622.

[181] Erdem Alkim, Paulo S. L. M. Barreto, Nina Bindel, Patrick Longa, Jefferson E. Ricardini: The Lattice-Based Digital Signature Scheme qTESLA. 2019. Cryptology ePrint Archive, 2019, Report 2019/085. (https://eprint.iacr.org/2019/085, 2019. március 8.)

[182] Jeff Hoffstein, Nick Howgrave-Graham, Jill Pipher, William Whyte: Chapter 1: Practical lattice-based cryptography: NTRUEncrypt and NTRUSign. In: Phong Q. Nguyen, Brigitte Vallée (eds.): The LLL Algorithm. Survey and Applications. Springer-Verlag Berlin Heidelberg, Germany. 2010.

[183] Stefania Cavallar, BruceDodson, Arjen Lenstra, Paul Leyland, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman te Riele, Paul Zimmermann: Factorization of RSA-140 Using the Number Field Sieve. Lecture Notes in Computer Science, 1999.,Volume 1716. pp.195-207.

[184] Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman te Riele, Karen Aardal, Jeff Gilchrist, Gerard Guillerm, Paul Leyland, Joël Marchand, Francois Morain, Alec Muffett, Chris Putnam, Craig Putnam, Paul Zimmermann: Factorization of a 512-bit RSA Modulus. Lecture Notes in Computer Science, 2000., Vol. 1807. pp.1-19.

[185] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery,Dag Arne Osvik, Herman te Riele, Andrey Timofeev, Paul Zimmermann: Factorization of a 768-Bit RSA Modulus. Lecture Notes in Computer Science, 2010., Vol. 6223. pp.333-350.

[186] Dindayal Mahto, Dilip Kumar Yadav: Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Biometrics for E-Commerce Applications. 2015. In: Proceedings of the 2015 3rd International Conference on Computer, Communication, Control and Information Technology (C3IT 2015), Hooghly, India 7-8 February 2015. pp.375-381.

[187] G. Karácsony Gergely (szerk.): Az elektronikus eljárások joga. 2018. Gondolat Kiadó, Magyarország, Budapest. (http://real.mtak.hu/80535/1/e-eljárás-jog_Tankönyv_LO.pdf, 2019. március 10.)

[188] Gellén Márton: A közigazgatási reformok az államszerep változásainak tükrében. Doktori értekezés. 2012. Széchenyi István Egyetem Állam-és Jogtudományi Doktori Iskola.

[189] Fred Piper, Simon Blake-Wilson, John Mitchell: Digital Signatures. Security & Controls. 1999. Information Systems Audit and Control Foundation. USA, Rolling Meadows.

[190] Balogh Zsolt György, Budai Balázs Benjámin: E-önkormányzat. Az elektronikus-önkormányzati modernizáció fejlesztéspolitikai alapjai című tantárgy egyetemi tankönyve. 2018. Dialóg Campus Kiadó: Budapest. ISBN 978-615-5889-16-5 (elektronikus)

[191] Balogh Zsolt György: Az információs társadalom jogi keretei. Doktori Értekezés. 2000. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola.

[192] Balogh, Zsolt György: Az elektronikus aláírás technikai alapjai és szabályozási keretei pp. 137-159. , 22 p. In: Balogh, Zsolt György; Józsa, Zoltán; Siket, Judit - Közigazgatási eljárásjogi ismeretek Szeged, Magyarország : Szegedi Tudományegyetem Állam- és Jogtudományi Kar, (2014)

[193] Z. Karvalics László: Információs társadalom - mi az? Egy kifejezés jelentése, története és fogalomkörnyezete. 2007. In: Szerk: Pintér Róbert: Az információs társadalom. Az elmélettől a politikai gyakorlatig. Budapest: Gondolat - Új Mandátum. ISBN 978 963 693 061 5

[194] Kusper Gábor: Az Internet ott Tárgyak témakörének áttekintése. In: Körtesi, Péter (szerk.) MAFIOK 2013 közlemények - online : Matematikát, Fizikát és Informatikát Oktatók Konferenciájának kiadványa – online. 2013. Miskolc, Magyarország: Miskolci Egyetem. pp. 137-146. ISBN 978-963-358-037-0

[195] Richard L. Rutledge, Aaron K. Massey, Annie I. Antón, Peter Swire: Defining the Internet of Devices: Privacy and Security Implications Georgia Institute of Technology. 2014. Technical Report: GIT-GVU-14-01

(https://smartech.gatech.edu/bitstream/handle/1853/52020/plsc2014-IoD.pdf, 2019. március 31.)

[196] Budai Balázs, Gerencsér Balázs Szabolcs, Veszprémi Bernadett: A digitális kor hazai közigazgatási specifikumai. 2018. Budapest: Nordex Nonprofit Kft. – Dialóg Campus Kiadó. ISBN 978-615-5889-62-2 (elektronikus – PDF)

[197] Williams, R., McMahon, E., Samtani, S., Patton, M., & Chen, H. (2017). Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. In: (Eds): Xiaolong Zheng, Hui Zhang, Chunxiao Xing, G. Alan Wang, Lina Zhou, and Bo Luo: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI): Security and Big Data. doi:10.1109/isi.2017.8004904. ISBN: 978-1-5090-6727-5

[198] Gergely Jambrik: Contract formation via the Internet. 2000. Budapest: Európai Tanulmányok Alapítvány és EU 2002 Bt. ISSN: 1585-9096. Európa 2002, 2. évf., 2. szám. Annex c). pp. 18-29.

[199] Sallai Gyula (szerk.): Az okos város (Smart City). 2018. Dialóg Campus Kiadó, Budapest. ISBN 978-615-5920-23-3 (elektronikus)

[200] Orbók Ákos: 10. Az okos város kiberbiztonsága. In: Sallai Gyula (szerk.): Az okos város (Smart City). 2018. Dialóg Campus Kiadó, Budapest. ISBN 978-615-5920-23-3. 187-201. old.

[201] Érdújhelyi Menyhért: A közjegyzőség és hiteles helyek története Magyarországon. 1899. Budapest: M. Kir. Közjegyzők Országos Egyesülete. (2004, MOKK, reprint kiadás)

[202] Schiff Ervin: A tájékoztatási munka computer-igényének kielégítési módjai. 1970. Tudományos és Műszaki Tájékoztatás, ISSN: 0041-3917. 17. évf. 2. szám, 93-102. old.

10.1. ÁBRÁK JEGYZÉKE

10.2. TÁBLÁZATOK JEGYZÉKE

11. A SZERZŐ TÉMÁBAN MEGJELENT PUBLIKÁCIÓI

Erdősi, Péter Máté: Elektronikus aláírás e-közigazgatási használatához kapcsolódó tudás szétosztási megoldásainak összehasonlító elemzése biztonsági aspektusból. TÁRSADALOM ÉS HONVÉDELEM 2016/2 pp. 31-40. , 10 p. (2018)

Attila, Horváth; Péter, Máté Erdősi; Ferenc, Kiss: The Common Vulnerability Scoring System (CVSS) generations – usefulness and deficiencies pp. 137-154. , 18 p. In: Kiss, Ferenc; Horváth, Attila (szerk.) IT ÉS HÁLÓZATI SÉRÜLÉKENYSÉGEK TÁRSADALMI-GAZDASÁGI HATÁSAI, Budapest, Magyarország : Információs Társadalomért Alapítvány, (2016) 243 p.

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, Magyarország : Információs Társadalomért Alapítvány, (2016) pp. 31-48. , 18 p.

Dr. Horváth, Attila ; Erdősi, Péter Máté: Sérülékenységek hatásának vizsgálata a biztonsági követelmények aspektusából pp. 49-58. , 10 p. In: Kiss, Ferenc; Horváth, Attila (szerk.) IT ÉS HÁLÓZATI SÉRÜLÉKENYSÉGEK TÁRSADALMI-GAZDASÁGI HATÁSAI, Budapest, Magyarország : Információs Társadalomért Alapítvány, (2016) p. 243

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: Közigazgatás-tudomány, matematika- és informatikai tudomány, műszaki tudomány, művészeti és művészettudomány, nyelvtudomány, orvos- és egészségtudomány, Budapest, Magyarország : Doktoranduszok Országos Szövetsége, (2016) pp. 34-40. , 7 p.

Erdősi, Péter Máté: A személyiségjegyek és a szervezetek típusai közötti kapcsolat vizsgálatának tervezése információbiztonsági aspektusból. MAGYAR RENDÉSZET XVI. : 2016/6 pp. 13-23. , 11 p. (2016)

Erdősi, Péter Máté ; Horváth, Attila ; Kiss, Ferenc: Az információbiztonsági törvény által előírt biztonsági besorolások és kapcsolódó intézkedések lehetséges

hatásainak vizsgálata a szoftveres sérülékenységek szempontjából pp. 13-30. , 18 p. In: Kiss, Ferenc; Horváth, Attila (szerk.) IT ÉS HÁLÓZATI SÉRÜLÉKENYSÉGEK TÁRSADALMI-GAZDASÁGI HATÁSAI, Budapest, Magyarország : Információs Társadalomért Alapítvány, (2016) p. 243

Erdősi, Péter Máté ; Horváth, Attila ; Kiss, Ferenc: Információrendszerek biztonsági kockázatainak vizsgálata a szoftverek nyíltsága szerint pp. 3-12. , 10 p. In: Kiss, Ferenc; Horváth, Attila (szerk.) IT ÉS HÁLÓZATI SÉRÜLÉKENYSÉGEK TÁRSADALMI-GAZDASÁGI HATÁSAI, Budapest, Magyarország : Információs Társadalomért Alapítvány, (2016) p. 243

Horváth, Attila ; Erdősi, Péter Máté ; Kiss, Ferenc: Az informatikai sérülékenységek gazdasági összefüggései – A kiberbiztonság megjelenése a makro- és mikroelemzésekben pp. 109-136. , 28 p. In: Kiss, Ferenc; Horváth, Attila (szerk.) IT ÉS HÁLÓZATI SÉRÜLÉKENYSÉGEK TÁRSADALMI-GAZDASÁGI HATÁSAI, Budapest, Magyarország : Információs Társadalomért Alapítvány, (2016) 243 p.

Horváth, Attila ; Erdősi, Péter Máté ; Kiss, Ferenc ; Benkő, Zsanett ; Szanyi, István ; Török, Marianna: A szoftver sérülékenységek kihasználási módozatai – Informatikai támadások, támadók és biztonság 2013-2016. pp. 59-108. , 50 p. In: Kiss, Ferenc; Horváth, Attila (szerk.) IT ÉS HÁLÓZATI SÉRÜLÉKENYSÉGEK TÁRSADALMI-GAZDASÁGI HATÁSAI, Budapest, Magyarország : Információs Társadalomért Alapítvány, (2016) 243 p.

Erdősi, Péter Máté: Electronic Written Forms As A Constraint Of E-administration: Formal Requirements Of The Legal And Probative Force In The Digital World pp. 40-42. , 3 p. In: Bende, Zsófia (szerk.) A NEMZETI KÖZSZOLGÁLATI EGYETEM KÖZIGAZGATÁS-TUDOMÁNYI KAR KÖZIGAZGATÁS-TUDOMÁNYI DOKTORI ISKOLÁJA 2013/2014-ES TANÉVÉNEK KUTATÓI FÓRUMA : tanulmánykötet, Budapest, Magyarország : Nemzeti Közszolgálati Egyetem, Közigazgatástudományi Kar, (2014) p. 132

Erdősi, Péter Máté: Elektronikus aláírások ortogonális dimenzionálása pp. 57-64. , 8 p. In: Kiss, Natália; Nagy, Bálint; Németh, István Péter (szerk.) Tudományos terek, Dunaújváros, Magyarország : DUF Press, (2014) 286 p.

Erdősi, Péter Máté: Magyar bizalmi szolgáltatások felügyeletének összehasonlító elemzése. MŰSZAKI KATONAI KÖZLÖNY 2014/1 pp. 200-212. , 13 p. (2014)

Erdősi, Péter Máté: Elektronikus írásbeliség a magyar jogban. TÁRSADALOM ÉS HONVÉDELEM 3-4 : 17 pp. 589-595. , 7 p. (2013)

Erdősi, Péter Máté: ECDL/ICDL IT Biztonság. Budapest, Magyarország : Neumann János Számítógép-tudományi Társaság (NJSZT) (2013) , 98 p.

Erdősi, Péter Máté: 3. ELŐADÁS: AZ INFORMÁCIÓ HITELESSÉGE. In: Kalotay, Balázs; Kovács, Zoltán; Erdősi, Péter Máté; Kovács, Árpád; Ozsvár, Ferenc; Kancsár, Attila - Kalotay, Balázs (szerk.) E-Government Tanulmányok V. : Elektronikus rendszerek a közigazgatásban, Budapest, Magyarország : E-government Alapítvány, (2011) pp. 37-47. , 11 p.

Erdősi, Péter Máté: Információ és információs társadalom pp. 17-45. , 28 p. In: ALMÁSI, János; BALÁZS, László; ERDŐSI, Péter Máté; KOVÁCS, Árpád; RÁTAI, Balázs; SCHVÉGER, Judit - Erdősi, Péter Máté (szerk.) Elektronikus hitelesség, elektronikus aláírás : ECDL Modultankönyv. Budapest, Magyarország : OTY StarTel Kft., (2010)

Erdősi, Péter Máté ; Domokos, Zoltán ; Springel, János: Elektronikus hitelesség, PKI rendszerek alkalmazási feladatai tömegméretekben pp. 1-31. (2009). INFORMÁCIÓS TÁRSADALOMÉRT ALAPÍTVÁNY Biztonságmenedzsment Kutatócsoport.

Erdősi, Péter Máté: AZ ELEKTRONIKUS ALÁÍRÁS KÖTELEZETTSÉGVÁLLALÁSI SZINTJEI ÉS KÖVETKEZMÉNYEI pp. 1-29. (2008). INFORMÁCIÓS TÁRSADALOMÉRT ALAPÍTVÁNY Biztonságmenedzsment Kutatócsoport.

Péter, Máté Erdősi: Electronic signature and climate change .In: Dr. Kiss, Ferenc; Török, Marianna (szerk.) Studies On Information And Knowledge Process 13. Budapest, Magyarország : Információs Társadalomért Alapítvány, (2008) pp. 81-88. , 8 p.

Nyíry, Géza ; Erdősi, Péter ; Vasvári, György: Biztonsági változások a CobiT 4-ben pp. 1-9. (2006). Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság- és

Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék Biztonságmenedzsment Kutatócsoport

Erdősi, Péter: Digitális archívumok megvalósításának alapkérdései .In: Kiss, Ferenc (szerk.) Alma Mater sorozat az információ- és tudásfolyamatokról 9. Budapest, Magyarország : Budapesti Műszaki és Gazdaságtudományi Egyetem, (2005) pp. 251-268. , 18 p.

Krisztián, Egerszegi ; Péter, Erdősi: PROBLEMS IN THE IMPLEMENTATION OF THE ELECTRONIC SIGNATURE. PERIODICA POLYTECHNICA-SOCIAL AND MANAGEMENT SCIENCES 11 : 1 pp. 67-82. , 16 p. (2003)

Egerszegi, Krisztián ; Erdősi, Péter: Az elektronikus aláírás és a tanúsítvány - Megvalósítási lehetőségek. In: Egerszegi, Krisztián; Kiss, Ferenc (szerk.) Sokszínű e-világ. Budapest, Magyarország : BME GTK Információ- és Tudásmenedzsment Tanszék, (2002) pp. 127-144. , 18 p.

Erdősi, Péter: Az elektronikus aláírás alkalmazásának háttere. HIRADÁSTECHNIKA: HÍRKÖZLÉS-INFORMATIKA LVII : 2002/9 pp. 41-44. , 4 p. (2002)

Erdősi, Péter: Az elektronikus aláírás megvalósítási problémái. In: Kiss, F; Egerszegi, K; Rácz, Cs (szerk.) Vállalat, információ, tudomány. Budapest, Magyarország : BME GTK Információ- és Tudásmenedzsment Tanszék, (2002) pp. 111-118. , 8 p.

Erdősi, Péter: A hazai informatikai biztonsági helyzet és az elektronikus aláírás. In: Egerszegi, K; Kiss, F; Gelléri, Péter; Rácz, Csaba (szerk.) Intelligens rendszerek, hatékony alkalmazások. Budapest, Magyarország : Budapesti Műszaki és Gazdaságtudományi Egyetem, (2001) pp. 119-131. , 12 p.

11.1. KONFERENCIA KIADVÁNYOK

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 (szerk.) Central and Eastern European e|Dem¸and e|Gov Days 2018 : Conference proceedings, Wien, Ausztria : Facultas Verlags- und Buchhandels AG, (2018) pp. 407-418. , 12 p.

Erdősi, Péter Máté: Legislation Challenges of Electronic Signature in Hungarian Public Administration. In: Juraj, Nemec - 25th NISPAcee Annual Conference : Innovation Governance in the Public Sector, Bratislava, Szlovákia : NISPAcee, (2017) pp. 1-8. , 8 p.

Erdősi, Péter Máté; Bartók, Sándor P.: May the advanced biometric electronic signature be applicable in Public Administration? In: Hendrik, Hansen; Robert, Müller-Török; Nemeslaki, András; Johannes, Pichler; Alexander, Prosser; Dona, Scola (szerk.) Central and Eastern European eIDem and eIGov Days 2017 : Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment? Wien, Ausztria : Austrian Computer Society, (2017) pp. 455-461. , 7 p.

Erdősi, Péter Máté: Electronic Signature Technology In Hungarian Governmental IT Projects In 2010-2015 Paper: Electronic , 6 p. In: 24th NISPAcee Annual Conference : Spreading Standards, Building Capabilities: European Administrative Space in Progress, Zágráb, Horvátország : NISPAcee Press, Forumi Shqiptar Social Ekonomik (ASET), (2016)

Erdősi, Péter Máté: Digitális tanúsítvány kiosztási modelljének elemzése különböző regisztrációs feltételek mentén pp. 141-150. , 10 p. In: Csiszár, Imre; Kőmíves, Péter Miklós (szerk.) Tavaszi Szél 2014 / Spring Wind 2014: I. kötet Közgazdaságtudomány, Debrecen, Magyarország : Doktoranduszok Országos Szövetsége, (2014) p. 614

Som, Zoltán ; Erdősi, Péter Máté ; Papp, Gergely Zoltán: Elektronikus aláírás, jelszó és e-befogadás, avagy tudás és bizalom kérdése pp. 230-230. , 1 p. In: Takácsné, György Katalin (szerk.) XV. Nemzetközi tudományos napok: Innovációs kihívások és lehetőségek 2014 - 2020 között, Gyöngyös, Magyarország : Károly Róbert Főiskola, (2016) p. 290

Som, Zoltán ; Erdősi, Péter Máté ; Papp, Gergely Zoltán ; Pólya, Balázs: Információbiztonsági pillanatkép és helyzetértékelés a magyar közigazgatásban. Különös tekintettel az e-szolgáltatások és e-befogadás, a jelszóhasználati nemzetközi kitekintéssel és az Ibtv. tervezett változásaira, mindezek gazdasági hatására. In: Rajnai, Zoltán; Fregan, Beatrix; Marosné, Kuna Zsuzsanna; Ozsváth, Judit (szerk.) Tanulmánykötet a 6. Báthory-

Brassai nemzetközi konferencia előadásaiból, Budapest, Magyarország : Óbudai Egyetem Biztonságtudományi Doktori Iskola, (2015) pp. 395-408. , 14 p.

Erdősi, Péter Máté: Az elektronikus hitelesség vizsgáztatási tapasztalatai. In: Networkshop 2011 : Kaposvár, [2011]. április 27-29. Budapest, Magyarország : Nemzeti Információs Infrastruktúra Fejlesztési Intézet (NIIFI), (2011)

Erdősi, Péter Máté: Elektronikus hitelesség e-társadalomban - mit, miért, és hogyan? In: Networkshop, 2010 : Debrecen, 2010. április 7-9. Budapest, Magyarország : Nemzeti Információs Infrastruktúra Fejlesztési Intézet (NIIFI), (2010)

Erdősi, Péter Máté: Az elektronikus aláírás oktatásában megtett lépések. In: Networkshop 2009 : 18. Országos Konferencia : Budapest, Magyarország : Nemzeti Információs Infrastruktúra Fejlesztési Intézet (NIIFI), (2009)

Erdősi, Péter Máté: The Integration of Electronic Signature into the Information Society in Hungary. Kaunas, Litvánia : Kaunas University of Technology (2008). In: Aleksandras, Targamadzé; Rimantas, Butleris; Rita, Butkiené (szerk.) 14th International Conference on Information and Software Technologies. Kaunas, Litvánia : Kaunas University of Technology, (2008) pp. 241-248. , 8 p.

Erdősi, Péter Máté: Az elektronikus aláírás oktatásának fő kérdései a köz-, felső- és posztgraduális oktatásban. In: Networkshop 2008 17. Országos Konferencia : Előadás kivonatok. Dunaújváros, Magyarország : Nemzeti Információs Infrastrukúra Fejlesztési Program Iroda, (2008)

Erdősi, Péter Máté: Digitális archívumok megvalósításának biztonsági alapkérdései. In: Koltay, T - Networkshop 2006 : Miskolci Egyetem, Miskolc, 2006. április 19 - április 21. Budapest, Magyarország : Nemzeti Információs Infrastruktúra Fejlesztési Iroda, (2006)

Erdősi, Péter Máté: Mégis, kinek a felelőssége?: Gondolatok az elektronikus aláírás és a felelősség vállalása körül. In: Networkshop 2003 : A NIIF közösség 12. éves konferenciája (2003)

Erdősi, Péter Máté: Az elektronikus aláírás és a tanúsítványok helyzete Magyarországon. In: Fulajtár, P (szerk.) Networkshop 2002 Konferencia. Budapest, Magyarország : NIIF Koordinációs Iroda, (2002)

12. FÜGGELÉKEK

12.1. EU28+ ORSZÁGOK

A Capgemini 2016-os felmérése az EU28+ országokra terjedt ki, amelyeket a tanulmány az alábbiakban határozott meg a 78. oldalán:

Ország	Rövidítés
Ausztria	AT
Belgium	BE
Bulgária	BG
Svájc	CH
Ciprus	CY
Csehország	CZ
Németország	DE
Dánia	DK
Észtország	EE
Görögország	EL
Spanyolország	ES
Finnország	FI
Franciaország	FR
Horvátország	HR
Magyarország	HU
Írország	IE
Grönland	IS

Ország	Rövidítés
Olaszország	IT
Litvánia	LT
Luxemburg	LU
Lettország	LV
Málta	MT
Montenegró	ME
Hollandia	NL
Norvégia	NO
Lengyelország	PL
Portugália	PT
Románia	RO
Szerbia	RS
Svédország	SE
Szlovénia	SI
Szlovákia	SK
Törökország	TR
Egyesült Királyság	UK (*)

23. táblázat: Az EU28+ országai (forrás: Capgemini 2017 [38])

(*) Az Egyesült Királyság kilépése az Európai Unióból folyamatban volt 2019-ben.

12.2. EIDAS ÉS VÉGREHAJTÁSI RENDELETEI (2019. MÁRCIUS 5.)

Az eIDAS rendelet és végrehajtási aktusainak adatait az alábbi táblázatban foglaltam össze 2019. március 5-i állapot szerint:

Rövid név	Dátum	Cím	Megjelenés
910/2014/EU rendelet	2014. július 23.	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	OJ L 257, 28.8.2014, p. 73–114
2015/296 végrehajtási határozat	2015. február 24.	A Bizottság (EU) 2015/296 végrehajtási határozata (2015. február 24.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 12. cikkének (7) bekezdése értelmében vett, a tagállamok által az elektronikus azonosítás területén folytatandó együttműködésre vonatkozó eljárási szabályok megállapításáról EGT-vonatkozású szöveg	OJ L 53, 25.2.2015, p. 14–20
2016/650 végrehajtási határozat	2016. április 25.	A Bizottság (EU) 2016/650 végrehajtási határozata (2016. április 25.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt	OJ L 109, 26.4.2016, p. 40–42

Rövid név	Dátum	Cím	Megjelenés
		létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról (EGT-vonatkozású szöveg) C/2016/2303	
2015/806 végrehajtási rendelet	2015. május 22.	A Bizottság (EU) 2015/806 végrehajtási rendelete (2015. május 22.) a minősített bizalmi szolgáltatások uniós bizalmi jegyének formájára vonatkozó előírások megállapításáról (EGT-vonatkozású szöveg) C/2015/3364	OJ L 128, 23.5.2015, p. 13–15
2015/1501 végrehajtási rendelet	2015. szeptember 8.	A Bizottság (EU) 2015/1501 végrehajtási rendelete (2015. szeptember 8.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 12. cikkének (8) bekezdése szerinti átjárhatósági keretről (EGT-vonatkozású szöveg)	OJ L 235, 9.9.2015, p. 1–6
2015/1502 végrehajtási rendelet	2015. szeptember 8.	A Bizottság (EU) 2015/1502 végrehajtási rendelete (2015. szeptember 8.) az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó minimális technikai specifikációknak és eljárásoknak a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 8. cikkének (3) bekezdése szerint történő megállapításáról (EGT-vonatkozású szöveg)	OJ L 235, 9.9.2015, p. 7–20

Rövid név	Dátum	Cím	Megjelenés
2015/1505 végrehajtási határozat	2015. szeptember 8.	A Bizottság (EU) 2015/1505 végrehajtási határozata (2015. szeptember 8.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 22. cikkének (5) bekezdése szerinti bizalmi listákhoz kapcsolódó technikai specifikációk és formátumok meghatározásáról (EGT-vonatkozású szöveg)	OJ L 235, 9.9.2015, p. 26–36.
2015/1506 végrehajtási határozat	2015. szeptember 8.	A Bizottság (EU) 2015/1506 végrehajtási határozata (2015. szeptember 8.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 27. cikkének (5) bekezdése és 37. cikkének (5) bekezdése szerint a közigazgatási szervek által elismert fokozott biztonságú elektronikus aláírások és fokozott biztonságú bélyegzők formátumaira vonatkozó specifikációk meghatározásáról (EGT-vonatkozású szöveg)	OJ L 235, 9.9.2015, p. 37–41
2015/1984 végrehajtási határozat	2015. november 3.	A Bizottság (EU) 2015/1984 végrehajtási határozata (2015. november 3.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 9. cikkének (5) bekezdése	OJ L 289, 5.11.2015, p. 18–25

Rövid név	Dátum	Cím	Megjelenés
		szerinti bejelentés feltételeinek, formátumainak és eljárásainak megállapításáról (az értesítés a C(2015) 7369. számú dokumentummal történt) (EGT-vonatkozású szöveg)	
2010/425/EU	2010. július 28.	A Bizottság határozata (2010. július 28.) a 2009/767/EK határozatnak a tagállamok által felügyelt/akkreditált megbízható hitelesítésszolgáltatók listájának létrehozása, vezetése és közzététele tekintetében történő módosításáról (az értesítés a C(2010) 5063. számú dokumentummal történt) EGT-vonatkozású szöveg	OJ L 199, 31.7.2010, p. 30–35
A tagállamoktól származó tájékoztatás	2019.02.28.	A belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 9. cikkének (1) bekezdése szerint bejelentett elektronikus azonosítási rendszerek	OJ C 75, 28.2.2019, p. 3–5

24. táblázat: Az eIDAS és végrehajtási rendeletei (készült az EUR-lex[263] alapján)

12.3. A VIZSGÁLT ELEKTRONIKUS ALÁÍRÁSOK RÉSZLETES ÉRTÉKELÉSE

Sorszám	Megjelenítés	Aláírás típus	Alaki bizonyító erő	Komplexitás	Érvényességi idő (nap)	Tanúsítvány szabvány	Aláíró kiléte	Aláíró algoritmus	Aláírás-létrehozó adat	Aláírás-létrehozó adat tárolója	Aláírás [illegible]	Aláírás elhelyezkedése	Tanúsítvány kiállító	Speciális
1	100	100	100	50	365	50	100	1000	1024	100	0	200	0	0
2	200	1000	1000	500	365	1000	100	1000	4096	100	0	200	500	0

[263] Lásd https://eur-lex.europa.eu/homepage.html?locale=hu (2019. március 4.)

Sorszám	Megjelenítés	Aláírás típus	Alaki bizonyító erő	Komplexitás	Érvényességi idő (nap)	Tanúsítvány szabvány	Aláíró kiléte	Aláíró algoritmus	Aláírás-létrehozó adat	Aláírás-létrehozó adat tárolója	Aláírás	Aláírás elhelyezkedése	Tanúsítvány kiállító	Speciális
3	200	1000	10000	4500	1825	1000	150	7600	256	100	0	100	1000	2
4a	200	1000	10000	4500	3650	1000	100	7600	256	20000	0	100	1000	1
4b	300	1000	10000	5000	3650	1000	100	7600	256	20000	0	100	1000	1
5	200	1000	10000	4500	365	1000	100	1000	2048	20000	0	150	1000	0
6	300	1000	10000	5000	365	1000	100	1000	2048	20000	0	150	1000	0
7	100	1000	10000	500	365	1000	100	1000	2048	20000	0	150	1000	0
8	100	1000	1000	50	365	1000	100	1000	2048	100	0	150	100	0
9	300	1000	10000	1000	3650	1000	100	1000	2048	20000	0	150	1000	0
10	200	1000	1000	5000	2555	1000	150	1000	2048	5000	0	150	500	0
11	300	1000	1000	5000	2555	1000	150	1000	2048	5000	0	150	500	0
12	300	1000	1000	5000	365	1000	150	1000	2048	5000	0	150	1000	0
13	300	1000	1000	5000	365	1000	150	1000	2048	5000	0	150	500	0
14	300	1000	10000	5000	365	1000	150	1000	2048	5000	0	150	1000	0
15	100	1000	100	500	365	1000	150	1000	4096	15000	0	150	1000	0
16	300	1000	1000	5000	365	1000	150	1000	2048	5000	0	150	500	0
17	300	1000	10000	5000	2555	1000	100	1000	2048	20000	0	150	1000	2
18	300	1000	10000	5000	365	1000	100	1000	2048	20000	0	150	1000	0
19	300	1000	1000	5000	365	1000	150	1000	2048	5000	0	150	500	0
20	300	1000	1000	5000	365	1000	150	1000	2048	5000	0	150	500	0
21	300	1000	1000	50	365	0	100	0	0	0	0	200	0	0

25. táblázat: A vizsgálatba bevont elektronikus aláírások értékei (forrás: saját táblázat)