

Erdősi Péter Máté:

Az elektronikus aláírás fogalmának megjelenése és változása

Hivatkozás/reference:

Erdősi Péter Máté, „Az elektronikus aláírás fogalmának megjelenése és változása”,

Információs Társadalom,

XIX. évf. (2019) 1. szám, 66–91. old.

<https://dx.doi.org/10.22503/inftars.XIX.2019.1.3>

Információs Társadalom

Z. Karvalics László
Utak a globális tudáskormányzáshoz -
Az elméleti megfontolásoktól egy hídfőállás koncepciójáig

Molnár Pál – Pintér Henriett
Szerzői láthatóság a hazai neveléstudományi
folyóiratok hálózatában

Erdősi Péter Máté
– Demetrovics Zsolt – Király Orsolya
Az elektronikus aláírás fogalmának megjelenése és változása

Tegyük a humanizmust a digitális transzformáció
központjává!

2019. XIX. évfolyam 1. szám

Az elektronikus aláírás (electronic signature) fogalmát a jog definiálta elsőként. A fogalom konzisztens elterjedését nem segíti, hogy értelmezése számos átalakuláson ment keresztül, használata során keverednek a digitális aláírás (digital signature), az azonosítás (identification), a hitelesítés (authentication) és a feljogosítás (authorization), valamint a bizalom (trust, reliance), hitelesség, szavahihetőség (trustworthiness) fogalmak. 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) a normál elektronikus aláírásokon túl. A fogalomrendszer bonyolultsága szintén nem kedvez a tömeges használatnak, azonban a fogalmak és követelmények ismerete nélkül nehezen eldönthető kérdés bizonyos esetekben, hogy használható-e az adott szolgáltatás teljes bizonyító erejű magánokirat vagy közokirat létrehozására vagy sem. A tanulmány az elektronikus aláíráshoz kapcsolódó fogalmak kialakulásának historikus vizsgálatát tűzte ki célul, amely révén átfogó kép alakítható ki a napjainkban használatos fogalmak jelentéséről és értelmezéséről. Ez a digitális világban alapvető fontosságúnak tűnik.

Kulcsszavak: elektronikus aláírás, digitális aláírás, teljes bizonyító erő, fogalomrendszer

The Emergence and Evolution of the Conceptual Framework of Electronic Signatures

The concept of the electronic signature was used for the first time by legislators. Consistent use of this concept is not helped by the fact that its interpretation has undergone many changes. Related words – digital signature, identification, authentication, authorization, trust, reliance and trustworthiness – are used interchangeably. Many aspects of the electronic signature have appeared in legislation (especially in creating and applying laws), for instance; advanced and qualified signatures may be used in addition to normal signatures. The complexity of this concept is not helped by the wide usage of electronic signatures; however, without knowing concepts and legal consequences, it is hard to decide whether a given service can be used for creating public or private documents with full probative force or not. It is argued that knowing concepts and legal effects of electronic signatures seems to be essential in the digital world.

Keywords: electronic signature, digital signature, full probative force, conceptual framework

A folyóiratban közzétett művek a *Creative Commons*
Neved meg! - Ne add el! - Így add tovább! 4.0
Nemzetközi Licenc feltételeinek megfelelően
használhatók.

Az elektronikus aláírás fogalmának megjelenése és változása

A probléma megfogalmazása

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. A hitelesség igénye a papíralapú aláírások digitalizálódásával sem változott, továbbra is alapvető fontosságúnak tartjuk, hogy egy üzenet tartalmáról meg tudjuk ítélni, ki volt a küldője (eredet), és időközben módosították-e (integritás). A papíralapú világ korabeli hamisításai a hitelesítő eszközök jogosulatlan használatán vagy hamis tanúsításon alapultak, az utólagos hamisítások előtt számos akadály tornyosult. Ilyen volt például a korabeli papír, a festékanyag, a bélyegző, a toll megszerzése, esetleg az írógép vagy a nyomdagép beszerzése és működtetése, amely mind-mind akadály lehet egy megtévesztő hamisítvány elkészítésének. A digitális világ eredet- és tartalomhamisításai ellen a digitális aláírás és az időbélyegzés nyújthatja a legnagyobb védelmet, habár ma már a korabeli adathordozók használata is meglehetősen problémásnak bizonyulhat (például CD, DVD, merevlemez, szalagok, lyukkártyák). A maradandó értékű iratok hamisításának megakadályozására vagy felismerésére tehát számos technológiai módszer létezik. A valódiság felismerése azonban a technológián túl a kapcsolódó egyéb adatok elemzését is szükségessé teheti (például adott iktatószámra megjelenő irat tartalma, kapcsolódó előkészítő iratok tartalma, fellelhető példányok konzisztenciája).

A hitelesség megértéséhez magát a fogalmat érdemes tovább boncolgatni. A hitelesség nem más, mint az állított azonosság megerősítése. Ebből következik, hogy hitelesség önmagában nem létezik, azt meg kell, hogy előzze egy állítás. Hitelességet három tényezőről tudunk állítani: személynél, adatról vagy tulajdonságról. A személynél által megtett állítások hitelességének megerősítésére jöttek létre azok a technológiák, amelyeket a digitális világban elektronikus aláírásnak nevezünk.

Az elektronikus aláírás (electronic signature) fogalmát széles körben használják a világban, és mára beszivárgott a hétköznapi gyakorlatba, mivel számos eljárásjogi aktusnak is alapvető elemévé vált. 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), a hitelesítés (authentication) és a 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)¹ vagy minősített elektronikus

¹ Fokozott biztonságú elektronikus aláírás olyan elektronikus aláírásokat kell érteni, amelyek alkalmasak az aláíró azonosítására, kizárólag az aláíróhoz köthetők, olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat, és olyan módon kapcsolódnak azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

aláírás (qualified electronic signature)² is az elektronikus folyamatokban, továbbá azt a kérdést sem egyszerű megválaszolni, hogy az elektronikus aláírások közül melyeknek van teljes bizonyító ereje, vagy melyek alkalmasak az írásbeliség alaki követelményének kielégítésére. Példa erre az Azonosításra Visszavezetett Dokumentum Hitelesítés (AVDH)³ szolgáltatás által biztosított elektronikus aláírás, amelyről önmagában, további információk begyűjtése nélkül nehezen eldönthető kérdésként vehető fel az, hogy használható-e teljes bizonyító erejű magánokirat létrehozására, vagy alkalmas-e közokirat elektronikus aláírására, ami alapvető fontosságú a felhasználhatóság tekintetében, és az újszerűség mellett szintén egyik oka lehet a használat és az elterjedtség alacsony fokának.

Végül felmerül az a kérdés is, hogy az elektronikus aláírások általános leírására alkalmas fogalmak használhatók-e magyar viszonylatban az elektronikus ügyintézés során bármilyen változtatás nélkül, azaz van-e értelme megkülönböztetni az elektronikus aláírások általános és magyar közigazgatásos belüli felhasználását? A megkülönböztethetetlenségnek az lenne a feltétele, hogy a magyar közigazgatás külön sajátos szabályok előírása nélkül legyen képes kibocsátani és befogadni elektronikus aláírásokat, illetőleg elektronikusan aláírt tartalmakat. A dolgok jelenlegi állása szerint azonban az eIDAS-rendelet⁴ (a továbbiakban: Rendelet) a tagállamok közigazgatási rendszerei számára csak részben tette kötelezővé az előírások alkalmazását, a Rendelet előírásainak nem kell például a közigazgatási belső eljárások lebonyolítására szolgáló és ehhez bizalmi szolgáltatásokat igénybe vevő rendszerekre vonatkozniuk. A harmadik felek számára is elérhető nyilvános bizalmi szolgáltatásokra nézve viszont kötelezően kell érvényesíteni az európai előírásokat.⁵ Mivel Magyarországon az ügyfelet megilleti az elektronikus ügyintézési jog az elektronikus ügyintézészt biztosító szerv előtti⁶, 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 módjáról⁷, a normativitást

² Minősített elektronikus aláírásoknak nevezzük azokat a fokozott biztonságú aláírásokat, amelyek nyilvános minősített bizalmi szolgáltató által kibocsátott minősített tanúsítványon alapulnak, és minősített aláírás-létrehozó eszköz által jöttek létre. A tanúsítványban a szolgáltató hitelesíti (lepecsételi) az aláírás-létrehozó titkos adathoz tartozó széles körben megismerhető aláírás-ellenőrző adatot.

³ A szolgáltatás elektronikus aláírási lehetőséget biztosít a természetes személy felhasználók számára anélkül, hogy saját tanúsítvánnyal vagy saját regisztrációval rendelkezniük. A megfelelő szintű azonosítás és hitelesítés után távolról – akár mobil eszközről – is igényelhető elektronikus aláírás a szolgáltató titkos kulcsának segítségével. (Bővebben lásd <http://www.nisz.hu/hu/avdh-azonos%C3%AADt%C3%A1sra-visszavezetett-dokumentumhiteles%C3%ADt%C3%A9s>)

⁴ eIDAS-rendelet alatt a továbbiakban az Európai Parlament és a Tanács 910/2014/EU rendeletét (2014. július 23.) értjük, amely 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.

⁵ 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.”

⁶ Eübszt. 3 § (1) Magyarországon az ügyfelet megilleti a jog, hogy az elektronikus ügyintézészt biztosító szerv előtti ügyét – az e törvényben meghatározott módon – elektronikusan intézze.

⁷ 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:

biztosítva az elektronikus ügyintézés szabályait a közigazgatás külön rendeletben tette közzé. A 137/2016. számú Kormányrendelet az elektronikus ügyintézés nyújtó szervezeteire, az ügyfélre, az alkalmazható bizalmi szolgáltatásokra és a felügyeleti szervre terjed ki. A Magyarország már korábban is élt a külön előírások definiálásának jogával a közigazgatási ügyek elektronikus intézése vonatkozásában, amit hazánk 2012-től folytatott. Ez indokoltá 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.

Az ügyintézés volumenére jellemző történeti adat, hogy az XR⁸ rendszer 2004-es használatának statisztikai adatai szerint a körülbelül 4 000 regisztrált felhasználó 370 ügyet indított (töltött ki űrlapokat) és 1 832 időpontfoglalás történt (űrlapkitöltések nélkül) akkoriban (Szittner 2011: 108). Az Ügyfélkapu statisztikai adatait szemügyre véve láthatjuk, hogy az elektronikus ügyintézésben jelentős növekedés történt, mivel 2019. márciusában a 3 859 760 regisztrált felhasználó 58 295 677 belépést követően összesen 20 311 153 dokumentumot küldött és kapott.⁹ Az Eübszt.¹⁰ hatályba lépésével körülbelül 1,2 millió szervezet lett kötelezve az elektronikus ügyintézésre, amelyhez ma már minden technikai feltétel (dokumentumok le- és feltölthetősége, illetékfizetés) elektronikusan is adott.

Az aláírások hitelessége a magyar történetiségben

Az írásbeliség szempontjából négy korszakot érdemes megkülönböztetni, az írásbeliség előtti, az általános írástudás előtti, a digitális írástudás előtti és a digitalizációs korszakokat. A két középső korszakot az írástudók számossága választja el egymástól. Lényeges különbség van társadalmi aspektusból aközött, hogy létezik írástudó vagy gyakorlatilag mindenki írástudó az adott társadalomban. Az írásbeliség kialakulására a polgárosodást követően volt szükség, amikor a városban a polgárok már nem tudtak az ismertségre támaszkodni, ha egymással szemben valamilyen kötelezettséget akartak felvállalni. Komjáthy Miklós így fogalmazza ezt meg, kiindulva a Magyar Királyság első két évszázadából (Komjáthy 1974):

„Annak azonban, hogy az emberi viszonylatok alakításában az írásbeliségnek alig volt szerepe, a magyar társadalmi és gazdasági élet akkori fejlettsége is magyarázatul szolgál. Az emberek tulajdonképpen része ügyes-bajos dolgát el tudta intézni, az élete fenntartásához szükséges dolgokat be tudta szerezni egy napi járóföldön belül. Az emberek ismerték egymást, a függőben levő ügyekre vonatkozó

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.

⁸ A kormányzati portálon 2003. október 28-tól elérhetővé vált az Internetes Közigazgatási Szolgáltató Rendszer (a továbbiakban: XR), amely megteremtette az elektronikus ügyintézés alapjait (Szittner 2011: 106).

⁹ Lásd Ügyfélkapu Statisztikai adatok (<https://ugyintezes.magyarorszag.hu/srv/letolt?id=43120643&lang=hu>)

¹⁰ 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.).

nézeteiket szóban cserélték ki. Szavuknak hitelt nem írás, nem pecsét, hanem az őket ismerő emberek tanubizonyossága 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 élőszo már nem bizonyult elégnek, az ügyek intézése, az emberi együttélésből származó ügyek maradandó rögzítése más segédeszközt kívánt, az írást. Az új technika, az ügyek intézésének új módja csak lassan, akadozva tört utat magának.”

Az írásbeliség kialakulása Magyarországon azonban korábbra tehető, mint a hozzákapcsolódó törvényi szabályozás kialakulása, mivel az intézményesülés nem megelőzte, hanem követte a királyok adományainak írásos rögzítésének igényét. A gyakorlatban a szokásjog, a valamelyest kialakult gyakorlat lett később a törvények által szabályozva. A hiteles iratok készítésére a hiteleshelyek, majd a közjegyzőség intézménye lett felhatalmazva hazánkban. 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 Sanguineti Vilmos apostoli és császári közjegyzők készítettek hiteles okiratot, amelyet a jelenlévő főpapok és főnemesek pecsétjeikkel megerősítettek (Érdújhelyi 1899: 105). A közhitelesség már a szóban kötött szerződéseknél is megjelent igényként, kezdetben a pristáldok (pristaldusok, azaz egyes értelmezésben „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.¹¹

A középkorban számos okirathamisítási eset látott napvilágot, amelyeknek két ismertetőjele volt: a) a legfontosabb motiváció a jogtalan haszonszerzés, b) az elkövetők többnyire papi személyek – az írásjegyek tudói. A hamisítás büntetési tételei a hűtlenség, a teljes vagyonelkobzás, tüzes vassal történő megbélyegzés, esetleg fejevesztés voltak, ennek ellenére számos dokumentált esetben megpróbálkoztak vele. Habár II. Endre 1298-ban elrendelte a periratok levéltári elhelyezését is¹², ennek ellenére viszonylag kevés ilyen tárgyú irat maradt fenn az utókor számára. A fennmaradó iratokból azonban kiderült, hogy a bizonyított esetekben a bírák nem voltak könyörületeseek, sok esetben halállal büntették a hamisítást. Érdekességgé megjegyezhető, hogy Hunyadi Jánosnak 1450-ben volt egy pere Hercegh Ráfael püspökkel, amelyben Gábor deák bevallotta az oklevélhamisítást (Érdújhelyi 1899: 235).

Bogdán István (Bogdán 1980: 72) a következő módon idézte III. Béla király 1181-ben kiállított birtokeladási oklevelének bevezető passzusát: *„Én, Béla, Magyarország nagyságos királya, megfontolván és királyi méltóságunkat a jövőre megőrizni akarván, nehogy bármely a mi jelenlétiünkben megtárgyalt és eldöntött dolog felforgattassék, szükségesnek láttam elrendelni, hogy a mi felséges kihallgatásunkon megtárgyalt minden ügy írott bizonyossággal megerősítessék.”*¹³

¹¹ Lásd 1874. évi XXXV. törvénycikk a királyi közjegyzőkről (<https://net.jogtar.hu/ezer-ev-torveny?docid=87400035.TV&searchUrl=/>)

¹² Lásd 1298. évi XLVII. törvénycikk: a bűnpereket a rendes bírácoknak az illetékes megye levéltárában kell elhelyezniök. A bűnügyekben a királyi kúriában a nádor úr, vagy az országbíró, vagy más rendes bíró által ítéendő 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=/>)

¹³ Lásd „8. Írott bizonyosság...” fejezet első bekezdése.

Falus (2014: 63) 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, ha a jogügylet tanúinak felsorolása az oklevélben, vagy ha a szöveget egy hártára – 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 hártát. Az irat akkor volt hitelesnek tekinthető, ha a darabok összeillettek.

„Nem volt azonban ritka eset, hogy a három példány egyikének őrzéséről maga a kiállító hiteleshely gondoskodott, sőt idővel más oklevéladók okleveleit is átvette megőrzésre, amivel megvetette a későbbi hiteleshelyi (vagy országos) levéltár alapjait. Az 1210-es évek után egyre gyakrabban meg is pecsételték a chirographált okleveleket a hiteleshelyi pecséttel, s így módon a tanúk felsorolásával együtt háromféle hitelesítési eszközt alkalmaztak a jogérvény biztosítására. Egyes hiteleshelyeknél, így a fehérvári johannita konvent esetében is így történt, királyi rendelkezés vezette be a pecséthasználatot a XIII. század dereka előtt nem sokkal. A chirographumot a pecsét lassanként kiszorította, s annak ellenére, hogy alkalmanként még a XV. században is előfordul, a XIII. század közepe után már egyre inkább pusztán díszítő szerep jutott számára az okleveleken.”

Nem nehéz felfedezni a hasonlóságot a hártya kalligrafikus jeleinek átvágása-összeillesztése és a számadórovás között, amelyről Réthy Lászlót idézi Tübay (2015: 185), 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.

Az elektronikus aláírás európai története és fogalmi keretei

Kriptográfia és társadalom

Az elektronikus aláírás fogalmának tárgyalásakor nem lehetséges elkerülni a kriptográfiai kitekintést, történeti okokból. Az első aláírási fogalom az elektronikus levelezés kapcsán jött létre, ami olyan előre megírt fix szöveget jelentett, amelyet a levelező rendszer minden egyes kimenő levélhez hozzáillesztett – és amelynek nem illett hosszú szöveget tartalmaznia.¹⁴ A digitális világban a kézi aláírást megszemélyesítő első objektum a digitális aláírás lett (Diffie és Hellman 1976: 649), amely már az aszimmetrikus kriptográfián alapult. Később történt meg a fogalom technológiafüggetlen szabályozási célú kiterjesztése „elektronikus aláírás” néven, aminek következtében az elektronikus aláírások és a digitális aláírások elkülönültek egymástól, habár az elektronikus aláírások egy része digitális aláírás, így bizonyosan alkalmaz valamilyen kriptográfiai megoldást – ahogyan a digitális aláírás definíciója is mutatja.¹⁵

¹⁴ Lásd RFC 1855, Netiquette Guidelines, <https://www.ietf.org/rfc/rfc1855.txt>

¹⁵ 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 (Definíció: digitális aláírás: egy adategységhez csatolt adat, vagy egy adategység kriptográfiai átalakítása, amely lehetővé teszi az adategység címzettjének az adategység integritásának bizonyítását és a (például címzett általi) hamisítás elleni védelmet.)

Auguste Kerckhoffs (1883: 12) hat követelményt fogalmazott meg a kriptográfiai rendszerek számára, amelyek hatása a későbbi korok kriptográfusaira elvitathatatlan volt. A második követelményét Kerckhoffs-elvnek is szokták nevezni, amely kimondja, hogy egy kriptográfiai rendszer nem követelheti meg a titokban tartását, és hogy a rendszer minden nehézség nélkül az ellenség kezébe kerülhet. Kerckhoffs harmadik követelménye szerint a kulcsnak könnyen megjegyezhetőnek kell lennie, de nem igényelhet feljegyzést, illetőleg a szereplők a kulcsokat tetszés szerint lecserélhetik vagy megváltoztathatják. Claude Elwood Shannon (1949) már 1946-ban kidolgozta a titkosítási rendszerek értékelési követelményeit, amelyet 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.

Nem lehetséges azonban a tisztán matematikai-műszaki megfontolásokra sem szorítkozni az elektronikus aláírások tárgyalásában, a technológia intézményesülésének számos kérdése megmutatta ennek relevanciáját is. Például a jogalkotás során olyan aláírásokhoz is fűződnek jogi vélelmek, amelyek nem felelnek meg a digitális aláírás műszaki definíciójának.¹⁶

A technológiának a jogrendszerbe illesztésekor továbbá olyan kérdések is felmerültek, amelyek túlmutatnak az elektronikus aláírás technológiáján, például az e-kereskedelem (Smedinghoff és Hill Bro 1999: 727), a jogi vélelem (Szilágyi 2000: 8), valamint az elektronikus írásbeliség (Rátai 2000: 15-16) kérdései már igen korán felmerültek. A koordinálatlan használat¹⁷ számos különböző implementációt eredményezett, ami szintén nem az általános elterjedés irányába ható tényezőnek bizonyult. Az Egyesült Államokban a digitális aláírás útja 1994-ben a szabványosításba (DSS¹⁸) és az elektronikus aláírási törvénybe (Electronic Signatures in Global and National Commerce Act 2000) torkollott. Az EU-ban pedig beavatkozások váltak szükségessé az elektronikus aláírás fogalmi rendszerébe, az

¹⁶ Erre hazai példa az a biometrikus aláírás, amellyel teljes bizonyító erejű magánokiratok készíthetők a fővárosi és megyei kormányhivatal ügyfélszolgálatain, a járási (fővárosi kerületi) hivatal kormányablakaiban, illetve a települési ügysegédnél. (Lásd 20/J. §, 2010. évi CXXVI. törvény a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról.)

¹⁷ A jogalkotó kezdetben nem határozott meg különösebb követelményeket a fokozott biztonságú elektronikus aláírások számára, a műszaki szabványok pedig számos választható opciót engedtek meg a programozóknak az implementálás folyamatában. A kialakult helyzetet leginkább a Magyar Elektronikus Aláírás Szövetség 2003-as ajánlásában megfogalmazott célkitűzésből lehet megérteni: „Egy olyan egységes formátum (...) elfogadása és értelmezése volt a cél, mely a letagadhatatlanság céljából készített fokozott biztonságú és minősített elektronikus aláírásokra nézve biztosítja a különböző fejlesztésű hazai alkalmazások együttműködő képességét, az alábbi értelemben: a jelen megállapodásnak megfelelő aláírás-létrehozó alkalmazások képesek az egymás által létrehozott aláírásokat ellenőrizni, s azokat (az egységes formátumon belül) azonos eredményre jutva egységesen értelmezni.” (<http://87.229.53.14/lang-hu/remository?func=startdown&id=56>)

¹⁸ „Barker, Elaine B., Federal Information Processing Standards Publication 186. Announcing the Standard for DIGITAL SIGNATURE STANDARD (DSS)., 19 May 1994. <https://www.nist.gov/publications/digital-signature-standard-dss-includes-change-notice-1-12301996>

időközben felmerült problémák kapcsán. Az elektronikus aláírás evolúciója ebből következően értelmezhető fogalom, erre bizonyíték, hogy már 2000-ben is globális koordinációs – és nem technológiai – problémaként tartották számon az együttműködés hiányát az elektronikus aláírások széles körű elfogadásában (Coglianese 2000: 3). Az Európai Unió az elektronikus aláírási irányelv végrehajtását folyamatosan értékelte, és ennek eredményeként az 1999 decemberében kiadott európai elektronikus aláírási irányelv tapasztalatait 2014-ben korrigálták.

A digitális aláírás megjelenése

A kézírással egyenértékű digitális aláírás fogalmának legelső felbukkanásakor a kézi aláírást szerették volna kiváltani a szerződő felek között a számlázásban (Diffie és Hellman 1976: 649), egy számítógépes hitelesítési probléma megoldásának eredményeként. Szemléletes, és pontosan beleillik például Wiebe E. Bijker (1995: 13) SCOT¹⁹ elméletének a változási és stabilitási követelményének szükségességébe az, ahogyan a körvonalazódó és egyre inkább felmerülő igényt Diffie Whitfield és Martin Hellman 1976-ban megfogalmazta: „*A jelenlegi elektronikus hitelesítési rendszerek nem felelnek meg a tisztán digitális, nem hamisítható, üzenettel összekapcsolódó aláírásokkal szemben támasztott igényeknek.*”

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, Kengyel Miklós az okirati bizonyítás tárgykörében szintén megfogalmazza az okirat valóságának a szükségességét. Hamis okiratnak nevezi azt, amelyet nem a feltüntetett kiállítója írt alá, továbbá hamisított okiratnak nevezi azt, amelyet ugyan a kiállítója írt alá, de időközben megváltozott a tartalma (Kemény 2011: 209-211). Ez a dichotómia az információbiztonság témakörében is felbukkan.

A digitális aláírás elvének lefektetését követően hamarosan – 1978-ban – megjelent az első, gyakorlatban is használható nyilvános kulcsú kriptográfiai algoritmus leírása (Rivest, Shamir és Adleman 1978) a szerzők nevének kezdőbetűiből elnevezve, ez volt a RSA. A szerzők kiegészítették a digitális aláírás követelményeit az üzenet-függőség mellett az aláíró-függőséggel is, ellenkező esetben az aláírást fel lehetne használni bármilyen üzenethez, mivel egy digitális állomány másolatait megkülönböztetni egymástól és a legelső állománytól nem lehetséges a példányok tökéletes egyezősége miatt. A publikáció leírta az algoritmus matematikai működését, definiált egy számítási eljárást, és biztonsági megfontolásokat is megfogalmazott az új algoritmushoz. Az algoritmus igen elterjedtté vált az egész világon a felfedezését követő 35-40 évben. A kriptoanalízissel (cryptanalysis) foglalkozók népes tábora próbált az algoritmusban gyengeséget találni, tekintettel arra, hogy az algoritmus elméleti biztonságát nem sikerült bebizonyítani. A próbálkozások első 20 évét Dan Boneh (1999) foglalta össze. Már itt szétváltak az RSA matematikai hátterére és az implementációra vonatkozó támadási formák. Az implementálás során több előírást be kell tartani a biztonság érdekében (például megfelelően nagy és elég távoli prímszámokat kell létrehozni, továbbá az exponens értékének is elegendően nagynek kell lennie a kulcsok generálása során). A következő 10 évre – valójában összesen 33 évre – pedig Jingjing

¹⁹ SCOT: Social Construction of Technology, a technológia társadalmi konstrukciója

Wang (2011) megismételte a megtalált támadási módszereket, egyetlen egy új módszert hoz-
záteve az addig felfedezettekhez, amely azonban döntő fontosságúnak bizonyult 2017-ben
az észtt állampolgári tanúsítványok kompromittálódásában.²⁰

Elektronikus aláírás a szakirodalomban

Ha megvizsgáljuk az elektronikus aláírás tudományos szakirodalmát, azt találjuk, hogy szá-
mos publikáció foglalkozik az elektronikus aláírás valamely aspektusával, de olyan rend-
szerező összefoglalásra, amely a technológiai és a társadalmi kereteket integrálta volna,
nem találunk példát. A ScienceDirect keresőjében a kézirat lezárása előtt, 2018. december
17-én lefuttatott keresés az „electronic signature” kulcsszóra 1 959 darab cikket adott ered-
ményül az 1. ábrán látható éves bontásban:



1. ábra: Elektronikus aláírás témájú cikkek a ScienceDirect keresőben 2018. december 17-én

A Springer 2004 és 2013 között minden évben közzétette az EuroPKI²¹ konferencián
elhangzott előadások anyagát – összesen 186 cikkben, amely szintén széleskörű támpontot
nyújt a területet vizsgálni kívánók számára.²² A cikkek között számos esettanulmány és új
felvetés is található (például De Cock D. et. al. (2004) cikke a belga EID²³ kártyáról, Lopez
et. al. (2005) cikke a tanúsítványok osztályozásáról – amely négy dimenziót említ, Ølnes
és Buene (2006) cikke a Validációs Hatóságról, mint hatékony kockázatsökkentő eszköz-
ről, Zeng (2006) által kidolgozott álneves PKI rendszerről, Pala és Smith (2007) cikke az

²⁰ Az észtt kormány megszüntette 750 000 észtt állampolgári tanúsítvány érvényességét, mivel olyan
sérülékenység vált ismertté 2017 szeptemberében, amelynek 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)

²¹ PKI alatt ezen a területen a Public Key Infrastructure (Nyilvános Kulcsú Infrastruktúra) fogalmát
értik, ami az aszimmetrikus kriptográfiai algoritmusokra utal, ahol ugyanannak az üzenetnek a tit-
kosítására és az elolvasására használt kulcsok különböznek.

²² Lásd <https://link.springer.com/conference/eurocki>

²³ EID: electronic identification, elektronikus azonosítás

AutoPKI-ről, Montana és Reynolds (2008) írása az RPKI-ról,²⁴ Dent (2010) cikke a tanúsítvány nélküli aszimmetrikus titkosításról, Pala et. al. (2011) a PorPKI-ről (hordozható – portable – PKI), Van Damme et. al. (2012) leírása a PKI-alapú mobilbankolásról, Vigil et. al. (2013) a közjegyző-alapú hosszú távon hiteles PKI-ról, Kim et. al. (2013) felvetése a GeoPKI-ről²⁵ vagy akár Werlang et. al. (2014) cikke a felhasználó-központú digitális aláírási sémáról).

Az ábrát szemügyre véve a tudományos érdeklődésben két csúcspont tűnik szembe, az egyik 2000-ben, a másik pedig 2014-ben jelent meg, habár 2014 óta az érdeklődés – kis visszaesést követően gyakorlatilag folyamatosnak nevezhető az elektronikus aláírás iránt. A két csúcspont magyarázó tényezője az aláírások társadalmi integrációjának megváltozásában kereshető, ideértve az előkészítő és a bevezetést követő időintervallumokat is. Az új évezred kezdetén lett készen az USA, az EU és az ENSZ is az elektronikus aláírásra vonatkozó szabályozásaival, ami méltán felkelthette az egész világ érdeklődését, továbbá 2014-ben az EU kötelezővé tette a minősített elektronikus aláírás elfogadását minden tagállamában, ez szintén példaértékű lehetett a kutatók számára. A kvantumszámítógépek kapcsán is megjelentek már publikációk, de a 2018 utáni időszakra nézve korai lenne még bármilyen következtetést levonni. Mindenesetre érdekes lesz a publikációk számosságát összevetni az elkövetkező társadalmi és technológiai változások időpontjaival.

Európa és az elektronikus aláírás

Európában Martin Bangemann munkacsoportja²⁶ 1994-ben lefektette az Európai Információs Társadalom fejlesztésének alapelveit a Bangemann Report néven ismertté vált dokumentumban, amelynek „Electronic protection (encryption), legal protection and security”, azaz az elektronikus védelem (titkosítás), jogi védelem és biztonság fejezete foglalkozik az elektronikus biztonság kialakításával (European Commission 1994). A nyilvános kulcsú infrastruktúra ismert volt a csapat előtt, ez teljes bizonyossággal állítható, hiszen az akkori európai infokommunikációs cégek döntéshozói jelentős számban vettek részt ebben a munkában. Érdekesként 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 nevesítve mégsem került bele. Az IKT ipar képviselőinek döntő többségű bevonása valószínűleg jelentős hatást gyakorolt arra, hogy a változás motorját a jelentés az IKT iparban és az IKT 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 csapat által, akik kidolgozták az új európai szabá-

²⁴ RPKI: Resource PKI, erőforrás nyilvános kulcsú infrastruktúra, ami egy olyan speciális nyilvános kulcsú infrastruktúra, amelyik az internetes útválasztás biztonságának a megteremtésére szolgál (lásd RFC 6480 <https://tools.ietf.org/html/rfc6480>)

²⁵ GeoPKI: Geographic Public-Key Infrastructure, amely a térbeli elhelyezkedés hitelesítésére szolgál

²⁶ Lásd http://aci.pitt.edu/1199/1/info_society_bangeman_report.pdf

lyozás jogi háttérét 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 elektronikus²⁷ és technikai²⁸ 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), amelyet 1999. decemberében ki is hirdettek (EU irányelv). Ezt követően viszonylag gyorsan minden tagállam kidolgozta a saját elektronikus aláírással kapcsolatos nemzeti szabályozását, amely Magyarországon a 2001. évi XXXV törvény (Eat.) és végrehajtási rendeletei által lett szabályozva, egészen az Eübszt. 2015-ös hatályba lépéséig és az Eat. 2017. július 1-i teljes hatálytalanításáig. Az eIDAS-rendelet megerősítette a minősített aláírások egységes elfogadását minden tagállamban, és megtámogatta a tagállamok együttműködését az elektronikus azonosító eszközök vonatkozásában és a bizalmi szolgáltatások nyújtásának felügyeletében. Mindez alapvető fontosságú az elektronikus szolgáltatások határon átnyúló használatához az Európai Unió területén.

Elektronikus aláírás Magyarországon

A magyar jogalkotás és szolgáltatói piac néhány meghatározó lépcsőfokát érdemes feleleveníteni annak érdekében, hogy a magyar állampolgári elektronikus aláírás kialakulását megelőző erőfeszítésekről és az idáig megtett útról valamilyen képet lehessen alkotni (1. táblázat).

Dátum	Esemény
1997	megjelenik egy kormányhatározat tervezet az elektronikus aláírás kormányzati bevezetéséről, de a végrehajtás kormányváltás miatt akkor megakadt
1999.02.25.	a NetLock Kft. elindítja nem minősített hitelesítés-szolgáltatását, és elkezd értékesíteni az aláírási célú tanúsítványokat Rózsahegy Zsolt intuitív felismerését követően, amely szerint a bizalom webje (WoT) ²⁹ helyett a megbízható harmadik felek (TTP) ³⁰ modell fog támogatást kapni a jogszabályokban
1999.06.14.	megalakult a Közlekedési, Hírközlési és Vízügyi Minisztérium (KHVM) elektronikus aláírás munkacsoportja
1999.12.13.	megjelenik az Európai Parlament és a Tanács 1999/93/EK irányelve az elektronikus aláírásra vonatkozó közösségi keretfeltételekről
2001. május	megjelenik az elektronikus aláírásról szóló 2001. évi XXXV törvény (Eat)

²⁷ Az ETSI az elektronikus aláírással kapcsolatos szabványait a következő weboldalon hozza nyilvánosságra: http://www.etsi.org/deliver/etsi_cs/

²⁸ Az ETSI a technológiai szabványait (köztük az elektronikus aláírással kapcsolatosakat is) a következő weboldalon hozza nyilvánosságra: http://www.etsi.org/deliver/etsi_ts/

²⁹ WoT: Web of Trust, a „bizalom webje” néven ismert decentralizált modell, amelyben a szereplők kommunikációjának hitelességét az egymás közötti bizalom határozza meg, amelynek nagyságát egy gráf csomópontjaiba (szereplők) befutó élek (bizalom) számával lehet a legjobban szemléltetni.

³⁰ TTP: Trusted Third Party, „megbízható harmadik felek” modell, amelyben erre a feladatra kijelölt szereplők által lehetséges csak bekerülni a bizalmi körbe, és csak így lehet megbízhatóvá válni, illetve hiteles tranzakciókat létrehozni. Az Európai Unióban az eIDAS-rendelet által definiált bizalmi szolgáltatásokat csak ilyen szolgáltatók nyújthatják.

Dátum	Esemény
2001	az APEH (mai nevén NAV) KAIG megkezdi a tízezer kiemelt adózó számára az aláíró eszközök és tanúsítványok kibocsátását, csak adóbevallási célzattal – 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
2001.10.27.	a Nemzeti Hírközlési Hatóság (NHH) nyilvántartásba veszi a NetLock nem minősített szolgáltatásait (NHH regisztrációs szám: FA 6133-5/2001)
2001.12.21.	a Matáv (mai nevén Magyar Telekom) szintén elindítja nem minősített szolgáltatásait, a Deutsche Telekomra építve
2001.12.23.	a GIRO Elszámolásforgalmi Zrt. megindította nem minősített hitelesítés-szolgáltatásait tanúsítvány és eszköz kibocsátására – első és harmadik szolgáltatások voltak ezek az Eat. szerint (NHH regisztrációs szám: FA 7717-1/2001)
2002.04.26.	megjelenik a 2/2002 MeHVM irányelv a minősített szolgáltatókra és a biztonsági követelményekre vonatkozó követelményekről, ami egyedülálló eszközként vonult be a magyar jogrendszerbe
2002.05.30.	A Microsec Kft. bekerült a Hatóság nyilvántartásába nem minősített szolgáltatóként (NHH regisztrációs szám: MH 6834 1/2002)
2002.11.06.	a MÁV INFORMATIKA is csatlakozott a nem minősített szolgáltatókhoz
2002. december	kormányhatározat születik arról, hogy az államigazgatásban meg kell születnie egy nem minősített hitelesítés-szolgáltatónak, majd egy minősített hitelesítés-szolgáltatónak is, 2003. december 31-ig
2003.03.19.	Az NHH nyilvántartásba vette a NetLock Kft.-t minősített szolgáltatóként (NHH regisztrációs szám: MH-1372-12/2003), de az archiválás-szolgáltatás nem lett még elindítva
2003.04.03.	a MÁV INFORMATIKA Zrt. elindította minősített hitelesítés-szolgáltatásait – a négyből az első hármat (NHH regisztrációs szám: MH-2460-8/2003)
2003.09.04.	megjelent a 2205/2003. (IX. 4.) Korm. határozat a közigazgatási szervek egységes iratkezelési szabályozásának koncepciójáról, ami már tartalmazta a papírmentes ügyintézés biztosításának elvét
2004.07.27.	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
2004.10.01.	a Matáv is elindította a minősített hitelesítés-szolgáltatásait, a négy Eat-szolgáltatásból az első hármat
2005.03.11.	megjelenik a 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól
2005.03.18.	megjelenik a 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
2005.05.15.	minősített szolgáltatóként működik a Microsec Kft. (a hatósági nyilvántartásban 2005. május 30 szerepel kezdeti dátumként), mind a négy Eat-ben felsorol szolgáltatással
2005.10.27.	megjelenik a 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól

Dátum	Esemény
2006.03.01.	hatályba lép a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) hitelesítési rendje és megkezdí a szolgáltatói tanúsítványok felülhitelesítését
2006.03.15.	az EU Bizottság jelentést készít a 93/1999 irányelv működéséről, annak végrehajtásáról
2006.10.30.	megjelent az 1103/2006. (X. 30.) Korm. határozat az Új Magyarország Fejlesztési Terv elfogadásáról, amely különösen nagy problémaként írta le az elektronikus közigazgatási szolgáltatások és közszolgáltatások körében a kétoldali interakciós és tranzakciós szintű szolgáltatások szerény kínálatát
2007.01.01.	választható a cégeljárásban az elektronikus aláírt dokumentumok használata minden cégforma esetében
2007.02.01.	minősített elektronikus archiválás szolgáltatást is nyújt a Microsec Kft. (NHH regisztrációs szám: HL-3549-2/2007) a világon elsőként
2007.08.06.	az Educatio Társadalmi Szolgáltató Nonprofit Kft. kibocsátotta első hitelesítési rendjét
2007.12.29.	megjelenik a 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól
2008.07.01.	kötelező a cégeljárásban az elektronikus aláírt dokumentumok használata
2008.10.29.	a GIRO Zrt. befejezte a nyilvános hitelesítés-szolgáltatásait
2008.12.20.	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
2009.02.05.	a SIEMENS Zrt. úgy döntött, hogy február 5-én elindítja minősített archiválás-szolgáltatását (virtuálisan) a közjegyzői digitális levéltári érintettsége miatt, de ezt a MOKK nem kezdte el használni, emiatt ennek a hatósági nyilvántartásból való törlését is kérte 2011. június 7-én
2009.07.01.	az Educatio Társadalmi Szolgáltató Nonprofit Kft. nyilvános szolgáltatóvá vált
2010.03.15.	kibocsátották a 78/2010. (III. 25.) Korm. rendeletet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól
2010.05.14.	a Magyar Telekom befejezte – a minősített időbélyeg-szolgáltatását kivéve – az Eat. szerinti szolgáltatásainak nyújtását
2010.09.15.	a hatóság bejegyezte a NetLock Kft. minősített archiválás-szolgáltatását, a hatósági nyilvántartás december 15-i dátumot rögzített (NMHH regisztrációs szám: HL/18188-4/2010)
2011.08.05.	a Digitoll Kft. elindította nem minősített tanúsítvány-, eszköz- és időbélyeg-szolgáltatásait
2012.04.21.	megjelennek a SZEÜSZ-rendeletek (83/2012, 84/2012 és 85/2012 Korm. rendeletek)
2012.12.21.	az Educatio Társadalmi Szolgáltató Nonprofit Kft. befejezte a szolgáltatását
2013.11.23.	bejegyzésre kerül a Kormányzati Hitelesítés Szolgáltató mind a minősített, mind a nem minősített szolgáltatásaival, négyből hárommal
2013.12.30.	elindulnak a kormányablakok az 515/2013. (XII. 30.) Korm. rendelet alapján

Dátum	Esemény
2014.07.23.	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
2015.12.16.	megjelent a 2015. évi CCXII. törvény az egyes törvényeknek a gazdasági növekedéssel összefüggésben történő módosításáról, amely kötelezővé tette az elektronikus kapcsolattartást a bírósági eljárásokban
2015.12.23.	kihirdetik a 2015. évi CCXXII. törvényt az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, amely hatályon kívül helyezi az Eat-t
2016.06.13.	megjelenik a 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről
2016.06.30.	az utolsó pillanatban megjelenik a 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről, amely lecseréli a 3/2005. IHM rendeletet
2016.12.19.	kibocsátásra kerül a 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
2017.05.25.	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
2018.01.01.	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
2018.07.01.	hatályba lépett a 114/2007. GMK rendeletet leváltó 1/2018. (VI. 29.) ITM rendelet a digitális archiválásról
2019.01.23.	a NISZ Kormányzati Hitelesítés Szolgáltató négy új időbélyegző szervert állított üzembe, így megduplázta az eddigi kapacitását

1. táblázat: Az elektronikus aláírás időrendi lépései Magyarországon

A magyar e-közigazgatás fejlődését három szakaszra lehet felbontani (Budai 2014), egyre növekvő léptékeket alkalmazva. Az első szakasznak a reményteli kezdeti évek tekinthetők, amikor megjelentek az elektronikus ügyintézéssel kapcsolatos igények, és megfogalmazták az első cselekvési terveket az Európai Információs Társadalom kiépítése érdekében (1993–1999). Magyarországon már ekkor explicit formában megjelent a kormányzati hitelesítés-szolgáltatás létrehozása iránti igény. Ezt a szakaszt lázas tervezés követte, amelynek során létrejöttek a szabályozási keretek. Ekkor az ügyfél még nem kötelező jelleggel, hanem önkéntesen, a saját választását követve tudott volna elektronikusan ügyet intézni az elektronikus ügyintézés nagyszerűségét felismerő és elismerő, de erősen centralizált elveket valló közigazgatással (1994–2004). Ezt követően a kijózanodás és a realitások korszaka következett, amely mind a mai napig tartó folyamat (2005-től), és amely további szakaszokra bontható fel különböző aspektusok mentén. Például a centralizáció alapkövét jelentő központi rendszer és a technológiai jellegű szabályozás 2011-től átalakult decentralizált alapon működő szolgáltatások halmazává és eljárás-alapú szabályozássá, továbbá az addig csak lehetőségként működő

elektronikus szolgáltatások a bevezetési időszakot követően kötelezővé váltak. A kötelező jelleget az eIDAS-rendelet is megátmodatta 2014-ben.

A táblázatból kitűnik, hogy a kezdeti ötletelés után – kell-e nekünk hazai elektronikus aláírás – a piac igen korán elindította a szolgáltatásait. Az általános igény azonban jóval később fogalmazódott meg a vállalati szegmensben, a magánszemélyeknél pedig elenyésző mértékű volt az érdeklődés kezdetben. A jogi szabályozás megpróbált minden területre adekvát válaszokat megfogalmazni, amelyek hasznosak és használhatók is voltak a mindennapi gyakorlatban, esetenként kicsit bürokratikus felütéssel (példaként a közigazgatási tanúsítványoknál kötelező viszontazonosítást említhetnénk). Igazán nagy áttörést 2016-ig a cégeljárás elektronikus útra terelése és a közjegyzői digitális levéltár (KDL) elindítása jelentett, azonban ezekről az áttörésekről sokat elárul az, hogy a Kormányzati Hitelesítés-szolgáltató állampolgárok felé történő 2016-os nyitását követően több tanúsítványt bocsátottak ki (68 490 darab), mint amennyit a cégügyvédek, a közjegyzők és a vállalatok addig összesen használtak (22 501 darab), az arányuk 3,04 volt, ellenben az aláírt és időbélyegzett dokumentumok számosságának az aránya ugyanebben az időszakban a magánszemélyeknél (537 408 darab) és a többi szereplőnél (299 688 858 darab, amiből kormányzati 30 463 912 darab) volt, az arányuk pedig 0,00179, ami a használat frekvenciáját az egyes szereplőknel egészen pontosan jelzi. Az elektronikus ügyintézési törvény hatályba lépésével számos szereplő számára vált kötelezővé az elektronikus ügyintézés, amihez a szabályozott elektronikus ügyintézési szolgáltatások komoly támogatást is nyújtanak. Habár ezek hatása néhány év múlva lesz értékelhető, az már ma is látszik, hogy az elektronikus ügyintézés számos esetben megkerülhetetlenné és elkerülhetetlenné vált.

Az elektronikus aláíráshoz kapcsolódó fogalmak vizsgálata

Az elektronikus aláírás és az aláírás létrehozójának fogalma a kezdetek óta számos változáson ment keresztül, továbbá nem is egységesen értelmezett a különböző országok jogrendszereiben. Természetesen nagyfokú hasonlóság mutatható ki az egyes definíciók között, azonban az eltérések konkrét esetekben komoly nemzetközi jogi következményekkel is bírhatnak. A történetiség magyar és európai vetületének áttekintését követően foglalkoznunk kell az elektronikus aláírás fogalmának időbeni változásával is magyar és európai viszonylatban, illetve egy kis tengerentúli kitekintéssel.

Az elektronikus aláírást a 93/1999 EU Irányelv definiálta először jogi szabályozási környezetben 1999-ben, az itt megfogalmazott definíció szerint egy elektronikus aláírás a következőt jelentette: „olyan elektronikus adat, amely más elektronikus adathoz van csatolva, illetve logikailag hozzárendelve, és amely hitelesítés módszerül (method of authentication) szolgál;”

Az Eat. úgy fogalmazott, hogy az elektronikus aláírás az „elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.” A két definíció látszólagos ellentmondásban volt, hiszen az azonosítás nem lehet egyenlő a hitelesítéssel. A kontraindikatív kapcsolatot a két definíció között a hitelesség meghatározása képes megszüntetni (Vasvári 2003: 68), amely szerint általánosságban véve a hitelesség az állított azonosság megerősítése, így az elektronikus hitelesség az elektronikusan állított azonosság megerősítése. Azonosságot pedig az aláírások esetében – a korábban felismert dichotómiát alkalmazva – lehet állítani

a forrásról (signatory) és a tartalomról (content). Egy aláírt adat esetében ennek az azonosításnak a megerősítése két vizsgálat – azaz az aláíró és a tartalom hitelesítésének eredményét jelenti – összhangban a NIST FIPS 800-53³¹ amerikai szabványban a hitelesítésről megfogalmazottakkal³²:

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

Ez azonban technológiafüggetlen megfogalmazás, ezért az eIDAS-rendelet még jobban egyszerűsítette az elektronikus aláírás definícióját 2014-ben. Elektronikus aláírás az, amit az aláíró aláírásra használ – ez általánosította az aláírás eddigi gyakorlati szemléletmódját, amely egy kötelezettség felvállalására fókuszált, annak minden paraméterével együtt. Számos olyan implementáció jött létre az általánosított definíciónak megfelelően, amelyek teljesen különböző paraméterekkel rendelkeztek. Az elektronikus aláírási rendszerek tervezésekor ezek közül választja ki a bevezetést végző a paramétereket az előre megfogalmazott kritériumok alapján (explicit választás), vagy a megvalósítás során alakulnak ki a további paraméterek értékei (implicit választás).

Az Amerikai Egyesült Államokban az elektronikus aláírási törvény a következőképpen definiálta az elektronikus aláírást 2000. június 30-án: „*Elektronikus aláírás – Az „elektronikus aláírás” kifejezés olyan elektronikus hangot, szimbólumot vagy folyamatot jelent, amelyet egy szerződéshez vagy egyéb feljegyzéshez fizikailag csatoltak vagy logikailag társítottak, és amelyet egy személy a rögzített adat elfogadásának vagy aláírásának a szándékával hajtott végre.*”³³

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 2000 januárjában ezt így fogalmazta meg (ETSI³⁴ ES 201 733): „*A jelen dokumentum szerint készített elektronikus aláírás bizonyítékot szolgáltat annak bizonyosságául, hogy bizonyos kötelezettségeket valamely aláírási politika figyelembevételével egy adott időben az aláíró – valamely azonosítóval azonosítottan (pl. név, álnév vagy szerepkör) felvállalt.*”

Az aláírás szerepe tehát itt az arról való bizonyosság megszerzése, hogy egy név, álnév vagy opcionálisan egy szerepkör által azonosított aláíró valamely kötelezettséget egy adott szabály szerint egy adott időben felvállalt. Ez a szerep jelentős mértékben túlmutat az aláírás és az aláíró közötti fizikai kapcsolat bizonyítási igényén (azonosítás), hiszen arra nézve is tartalmaz információt, hogy az aláírás milyen kontextusban jött létre és használható fel.

Az elektronikus aláírás fogalmát 2014 óta az eIDAS-rendelet írja le az Európai Unióban, amely szerint az elektronikus aláírás olyan elektronikus adat, amelyet egy másik elektronikus adathoz csatolnak, és amelyet az aláíró (signatory) aláírásra használ³⁵. Mivel

³¹ „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.”, 22 January 2015. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

³² 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. (B-2) [Hitelesség: az eredetiség, az igazolhatóság és megbízhatóság tulajdonsága; bizalom az átvitel, az üzenet vagy a küldő érvényességében.]

³³ Lásd US Electronic Signatures in Global and National Commerce Act 2000, SEC. 106 (5).

³⁴ ETSI: European Telecommunications Standards Institute, Európai Távközlési Szabványok Intézete

további megköttést a Rendelet nem ad meg, ezért azt kell mondanunk, hogy a gyakorlatban bármilyen elektronikus adat lehet aláírás, mindaddig, amíg hozzákapcsolható egy dokumentumhoz és egy aláírás szándékhoz. Például lehet aláírás egy név az e-mail végén vagy a „Feladó:” mezőben, de lehet egy kattintás eredményeként létrejövő beikszelt szövegdoboz is, ha arra a kérdésre jelent választ, hogy „hozzájárul az adatai kezeléséhez?”. Továbbá nem szükséges aszimmetrikus kriptográfia sem egy elektronikus aláírás létrehozásához, szimmetrikus kriptográfia vagy egy kivonatoló (hash) függvény alkalmazásával is elő lehet állítani elektronikus aláírásokat technológiai értelemben. Társadalmi vonatkozásban az aláírási szándék nélkülözhetetlen eleme az aláírásnak. Az aláíró fogalma tehát a folyamat és az alany összekapcsolásán alapul, mivel olyan természetes személyt (natural person) kell aláíró alatt érteni, aki éppen aláír.³⁶ 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 az Európai Unió megkülönbözteti a jogi személyek aláírását a természetes személyek aláírásától, és külön szóval is illeti azt. Ez a fogalom az elektronikus bélyegző³⁷ (electronic seal), létrehozója pedig kizárólag jogi személy lehet.³⁸ Az elektronikus aláírás és bélyegző fogalmi közötti erőteljes hasonlóságot mutatja az, hogy egyrészt az eIDAS-rendelet megismétli szinte szóról szóra az elektronikus bélyegzők esetében az elektronikus aláírásra vonatkozó előírásokat, másrészt az elektronikus ügyintézésről szóló törvény (Eübszt.) kodifikációs fikcióval élve előírja, hogy – eltérő rendelkezés hiányában – az elektronikus bélyegzőt is elektronikus aláírásnak kell tekinteni.³⁹ Ebből adódóan a fentiekhez hasonló három kérdés fogalmazható meg az elektronikus bélyegző értelmezésének tárgyában is.

Egy elektronikus aláírás létrehozáskor számos olyan műszaki jellegű kérdésre választ kell adni, amelyek az aláírás létrehozásához elengedhetetlenül szükségesek. Ezek az ismeretek az aláírásokat létrehozó szoftverekbe vannak választható lehetőségekként bekódolva, és amelyeknek az ismerete általában nem jellemző az aláíró szoftvereket használók többségére. Ennek oka egyrészt az elektronikus aláírások komplexitásában, másrészt az

³⁵ eIDAS-rendelet 3. cikk 10: „elektronikus aláírás”: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ;

³⁶ eIDAS-rendelet 3. cikk 9: „aláíró”: elektronikus aláírást létrehozó természetes személy;

³⁷ 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;

³⁸ eIDAS-rendelet 3. cikk 24: „bélyegző létrehozója”: elektronikus bélyegzőt létrehozó jogi személy

³⁹ 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.;

elektronikus aláírásokkal kapcsolatos ismeretek átadásának hiányosságaiban kereshetők. Az adott kontextusban érvényesen felhasználható aláírás kiválasztásához és elkészítéséhez szükséges ismeretek elvárhatók lennének az aláíróktól, amennyiben az aláírásokat széles körben és variábilis módon használnánk. Nyilvánvaló módon az aláíró szoftverek készítéséhez szükséges programozói ismeretek ettől jóval bővebbek is lehetnek. Az aláírások összehasonlíthatósága vagy a jogszabályban előírtaknak való megfelelésértelmezése azonban megkövetelheti az elektronikus aláírások olyan mértékű megismerését, amelyik szükséges az alkalmazhatóság eldöntéséhez vagy az elutasításhoz. Tekintettel arra, hogy az elektronikus aláírásoknak számos jellemzője van, felmerül a kérdés, hogy lehetséges-e az elektronikus aláírás jellemzőit csoportosítani, és ha igen, milyen alapelvek mentén? Hogyan lehetséges megítélni az egyes aláírások alkalmazhatóságát és elfogadhatóságát, ha azok különböző tulajdonságokat vehetnek fel? Hogyan lehetséges megítélni az egyes aláírások határon átnyúló elfogadhatóságát? Ha szabadon meg lehet választani az aláírás készítésekor az aláírási jellemzőket, akkor számos különböző aláírás jöhet létre a gyakorlatban. Ha azonban az alkalmazás szintjére besülylesztjük az aláírási funkciót, akkor csak az aláírási szándék kinyilvánítása a feladat, mivel az aláírási funkció mindig ugyanolyan aláírást fog létrehozni a programjának megfelelően. Az aláírások összehasonlításához vagy a megfelelésértelmezés megítéléséhez rendelkezni kellene egy olyan mértékkel, amelyikben egyértelműen elhelyezhető minden elektronikus aláírás. 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. Ilyen modell létezéséről egyelőre a szakirodalom nem tesz említést, emiatt kutatási kérdésként felvethetőnek tűnt egy ilyen modell kidolgozhatóságának tudományos igényű vizsgálata.⁴⁰

Az elektronikus aláírásokhoz kapcsolódó fogalmak értelmezése

Az elektronikus aláírások összehasonlíthatóságához vagy az előírt követelményeknek való megfelelésük megítéléséhez hasznos segédeszköz lehet egy olyan értékelési rendszer, amely minden olyan dimenziót magában foglal, amelyek alapján az egyes aláírások megkülönböztethetők. A 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, amennyire pontosan azt lehetséges meghatározni. 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 bázisrendszert is meg kell határozni, a generátor-rendszerek lehetséges egyszerűsítésével.

Ez a fejezet megkísérli összegyűjteni és felsorolni az elektronikus aláírásokkal és bélyegzőkkel kapcsolatosan fellelhető összes olyan tulajdonságot, amelyek elméleti vagy gyakorlati aspektusban felmerültek korábban a szakirodalomban. A fogalomkö-

⁴⁰ Lásd https://akk.uni-nke.hu/document/akk-uni-nke-hu/EPM_PhD_tervezet_Az_elektronikus_alairas_merese_v20_leadva_KDI_20190409_signed.pdf

rökon ortogonalitási vizsgálatot nem végeztünk, emiatt lehetnek közöttük függések. Nem volt cél ebben a felsorolásban előállítani azt a legszűkebb dimenzió-halmazt (bázis-rendszer), amelyben egyrésről minden elektronikus aláírás vagy bélyegző egyértelműen felírható, másrésről további dimenziók felvételét csak úgy lehetséges megtenni, hogy valamely már létező dimenziótól való függés fennállna. A fogalomkörök elnevezése a szerző saját gondolatait tükrözik, megválasztásuk során az alkotói szabadság és a létező fogalomhasználat optimális konkatenációja volt az alapvető célkitűzés.

1. *a megjelenítés:* ehhez használható a CADES (CMS based Advanced Electronic Signature), a XAdES (XML-based based Advanced Electronic Signature) és a PAdES (PDF-based based Advanced Electronic Signature) néven ismert szabványoknak megfelelő kódolással aláírás vagy bélyegző. A CMS aláírás a gyakorlatban egy bináris adathalmazként jelenik meg, az XML aláírás egy XML-struktúrába ágyazott base64-kódolt bináris adatként, illetve a PDF aláírásban ezek hexadecimális kódjai jelennek meg.

2. *az aláírás típusa:* a normál, fokozott biztonságú (advanced) és minősített (qualified) aláírások vagy bélyegzők egymás valódi részhalmazai, más szóval a legszűkebb halmaz lesz a minősített halmaz, ez valódi részhalmaza a fokozott biztonságú halmaznak, amit teljes egészében tartalmaz – és még sok mást is⁴¹ – a normál elektronikus aláírások és bélyegzők halmaza.

3. *a bizonyító erő:* az eIDAS-rendelet azt fogalmazza meg, hogy egyrésről az elfogadás meg nem tagadhatósága elv miatt minden egyes elektronikus aláírást (Rendelet 25. cikk (1) bek.) és bélyegzőt (Rendelet 35. cikk (1) bek.) megillet a bizonyítékként való felhasználás vélelme, másrésről a minősített elektronikus aláírás kézírással való egyenértékű elfogadása (Rendelet 25. cikk (2) bek.), illetve a minősített bélyegzőkben foglalt adatok elfogadása (Rendelet 35. cikk (2) bek.) vált kötelezővé a nemzeti szint mellett az egész Európai Unióban (Rendelet 25. cikk (3) bek. és 35. cikk (3) bek.).

4. *a komplexitás:* az aláírások és bélyegzők komplexitása az egyszerű digitális aláírástól a hosszú távon érvényes komplex aláírásig terjed, amely magában foglalja az időbélyegzést, az érvényesítési adatokra való hivatkozást, valamint azok beillesztését is, továbbá az érvényesítési adatok hosszú távú hitelességének biztosítását.

5. *az érvényességi idő:* az aláírások és bélyegzők érvényességi idején azt az időtartamot kell érteni, ameddig azok hiteles felhasználhatóságáról gondoskodni szükséges. Ez az időintervallum lehet rövid, pontszerű és lehet tetszőlegesen hosszú is. Tekintettel arra, hogy az elektronikus adatok hitelességének időbeli dinamikája van, azaz önmagában nem lehet állandó, ez a dimenzió kiemelten fontos a hosszú távon megőrizni kívánt információk esetében. Az időintervallumok definiálásához fel lehet használni a megőrzésükhöz szükséges időintervallumokat funkcionális megközelítésben (például pénzügyi bizonylatok, magánokiratok, közokiratok, maradandó értékű okiratok).

6. *a tanúsítvány szabványa:* az elektronikus aláírás, illetve bélyegző tanúsítványa alatt olyan igazolást kell érteni, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja (név vagy álnév igazolható), illetőleg amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja (jogi személy neve

⁴¹ Például egy gépelt név, egy szkennelt aláírás, egy biometrikus aláírás vagy egy kipipált válaszdoboz ugyanúgy elektronikus aláírásnak tekinthető a definíció alapján, de már fokozott biztonságú aláírás csak olyan aláírás lehet, amelyik egyértelműen az aláíróhoz köthető – ez egy szkennelt aláírásról mindaddig nem mondható el, amíg az azt birtokló bármilyen dokumentumhoz hozzá tudja azt csatolni aláírásként.

igazolható). Az igazolás kapcsán több problémát is megfogalmaztak (Ellison és Schneier 2000), amelyekre a gyakorlatban létrejött szabványok megpróbálták megoldásokat nyújtani (X.509⁴², PGP⁴³).

7. *a tanúsítványok típusa*: a tanúsítványok típusait az eIDAS-rendelet két kategóriában adja meg (minősített és nem minősített), ezen kívül lehetőség van tanúsítvány nélkül is aláírást készíteni, hiszen az elektronikus aláírásnak a tanúsítvány megléte nem szigorúan vett előfeltétele.

8. *az aláíró típusa*: az aláíróknál különbséget kell tenni a végfelhasználói és a szolgáltatói aláírók vagy bélyegzők között, mivel más-más követelmények vonatkoznak az aláírás-létrehozó, illetve bélyegző-létrehozó adatok védelmére, tulajdonságaira. A végfelhasználók típusai magában foglalják a személyek aláíró vagy bélyegző tanúsítványait, mint például természetes személy, jogi személy, jogi személy természetes személy képviselője, kód-aláíró vagy gépi aláíró – aki az aláírást elrendelő személyként értelmezett.

9. *az algoritmus*: az aláírás vagy bélyegző létrehozásához használható algoritmusok tekintetében mértékadó szabványként az aláíró algoritmus-készletekre vonatkozó ETSI TS 119 312 szabványt kell alkalmazni. Az alapproblémát az okozza, hogy nem lehetséges elméletileg biztonságos algoritmusokat használni a gyakorlatban, így az algoritmusok megfelelősége függ a rendelkezésre álló számítási kapacitásoktól, amelyek viszont folyamatosan változnak (Schaller 1997). A jelenleg használt algoritmusokat nagy valószínűséggel le kell cserélni a kvantum-számítástechnika fejlődésével így már az ETSI is foglalkozik kvantum-kriptográfiával és számos kutató dolgozik az újfajta algoritmusok kifejlesztésén. Az algoritmusok alkalmazhatósága sok esetben összefügg a kulcsok hosszúságával. A leginkább elterjedt aláíró algoritmusok az RSA, az ECC és a DSA.⁴⁴

10. *az aláírás-létrehozó vagy bélyegző-létrehozó adatok hossza*: a titkos kulcsok hosszait minden esetben bitekben határozzák meg (például 128 bit, 256 bit, 512 bit, 1024 bit, 2048 bit, 4096 bit stb.). Kezdetben az RSA algoritmus is – mint a legnépszerűbb algoritmus – 256 bites kulcsokkal operált, azonban az RSA kulcsok törésére vonatkozó kihívások sikeres teljesítéseit követően a javasolt kulcsméret növekedett. Az 1024 bites RSA-kulcs avulását követően a 2048 bites RSA kulcs használata a leggyakoribb, az ECC⁴⁵ kulcsok térnyerésében pedig a 256 bites kulcshossz alkalmazása játszik jelentős szerepet, Magyarországon az állampolgári tanúsítványokban alkalmazzák ezt. Mindkét algoritmusnak van kedvező tulajdonsága, ami a népszerűségüket alátámasztja (Endrődi, Hornák és Selényi 2002).⁴⁶

11. *a létrehozó adat tárolója*: az aláírás-létrehozó vagy bélyegző-létrehozó adatok tárolásához használható eszközök lehetnek hardveres intelligens kártyák, USB⁴⁷ tokenek,

⁴² 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.”

⁴³ PGP: Pretty Good Privacy (Elég Jó Privátszféra), Philip Zimmermann készítette 1991-ben (lásd RFC 1991: Derek Atkins – William Stallings and Philip Zimmermann, “PGP Message Exchange Formats”, August 1996. <https://tools.ietf.org/pdf/rfc1991.pdf>)

⁴⁴ DSA: Digital Signature Algorithm, digitális aláíró algoritmus rövidítése

⁴⁵ ECC: Elliptic Curve Cryptosystem, elliptikus görbén alapuló kriptográfiai rendszer rövidítése

⁴⁶ Endrődi Csilla, Hornák Zoltán és Selényi Endre „ECC vagy RSA?”. Networkshop, 2002. <https://nws.niif.hu/ncd2002/docs/ehu/65/index.html>

⁴⁷ USB: Universal Serial Bus (Univerzális Soros Busz – egy számítógépes csatlakozási módszer) rövidítése

SIM⁴⁸ kártyák vagy szoftveres konténerfájlok (például pfx, p7b, p12) is. A szoftveres konténerfájlok bármelyik IKT eszközön megjelenhetnek, védelmüket kriptográfiai titkosítás biztosítja.

12. *az aláírások elhelyezkedése*: az aláírások elhelyezkedésének vizsgálatához meg kell különböztetni az egyszeresen és a többszörösen aláírt információkat, illetve a rajtuk elhelyezett aláírások egymáshoz viszonyított helyzetét, dokumentum – aláírás és aláírás – aláírás viszonylatban is. 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 (szekvenciális, párhuzamos vagy ellenjegyző).

13. *a tanúsítványok kibocsátója*: A tanúsítványokat az Európai Unióban kibocsáthatja hatóságilag felügyelt nyilvános bizalmi szolgáltató, aki szerepel az európai bizalmi szolgáltatók magyarországi listájában (Hungarian Trusted List), avagy egy olyan zártkörű szolgáltatót is igénybe lehet venni, amelynek működése nem tartozik az eIDAS-rendelet hatálya alá.

14. *az aláírások vagy bélyegzők szerkeszthetősége*: egy szerkeszthetőségi rendszerben a hatékonyság növelése érdekében vetette fel Quian és Xu (2011) a szerkeszthető elektronikus aláírás fogalmát. Gyakorlatilag arról van szó, hogy a szerző több opciót előzetesen hitelesít, amely közül a szerkesztő a későbbi történések függvényében kiválasztja az alkalmas opciót és azzal dolgozik a továbbiakban.

15. *az implementációs környezet (programozási könyvtár)*: Az aláírás és bélyegző biztonságára az algoritmusok matematikai tulajdonságai mellett azok gyakorlati tulajdonságai is hatással vannak, ahogyan ezt az elmúlt időszak negatív példái megmutatták. Az elméleti jó tulajdonságok nem érvényesülnek, ha a gyakorlati implementáció gyengíti le az algoritmusokat. Két példa kívánczik ide, az egyik a Heartbleed probléma⁴⁹, a másik az észti kártyaprobléma. Mindkettő implementációs problémaként okozott jelentős biztonsági incidenseket az adott implementációt használó szoftverrendszerekben.

Annak a kérdésnek a vizsgálata is megkerülhetetlennek látszik, hogy egy programkönyvtár használata csupán információbiztonsági kérdés, vagy kihathat az adott aláírások teljes halmazára. Az információbiztonsági vetületet erősíti Muha (2009), mikor a kritikus infrastruktúrák tárgyalásában felveti egyrésről a közigazgatási informatikát és kommunikációt megvalósító rendszereket (például ilyen a Kormányzati Hitelesítés Szolgáltató) 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 észti probléma azonban arra is rávilágított, hogy egy információbiztonsági eseménynek az egész társadalomra kiterjedő hatását nem lehet az esemény információbiztonsági menedzselésével megszüntetni, más olyan elemekre is szükség lehet, amelyek technológiailag megalapozottan teszik lehetővé alternatív társadalmi intézmények kiépülését és működtetését. Észtországban a polgárok az incidens követően használhatták a mobil ID megoldást az e-ügyintézésben, nem kellett leállítani az e-közigazgatási szolgáltatásokat.

⁴⁸ SIM: Subscriber Identity Module (Előfizető Azonosító Modul) rövidítése

⁴⁹ Az általánosan használt OpenSSL programcsomag olyan hibája vált ismertté 2014 áprilisában, amelynek kihasználásával a támadó hozzáférhetett a memóriában tárolt titkos kulcsokhoz (<https://www.us-cert.gov/ncas/alerts/TA14-098A>)

Következetések

Az elektronikus aláírás fogalmainak tárgyalásakor illik különbséget tenni a digitális aláírások, az elektronikus aláírások, az elektronikus bélyegzők és az időbélyegzők között, továbbá nem árt felismerni az egyes aláírások biztonsági szintjét is (normál, fokozott biztonságú vagy minősített) az egyes jogi vélelmek fennállásának megítéléséhez, illetve az aláírások határon átnyúló megfelelő használatához. Fontos tudni azt is, hogy Magyarországon ugyan minden minősített elektronikus aláírásnak és a minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírásnak is teljes bizonyító ereje van, azonban más európai tagállamok ettől eltérő módon is rendelkezhetnek, mivel az eIDAS-rendelet csak a kézírással való egyenértékűséget követeli meg, és csak a minősített aláírások esetében, a bizonyító erő tekintetében nem fogalmaz meg egységes európai álláspontot. Feltétlenül az elektronikus aláírások előnyére válik az, hogy számos esetben már jól kialakult jogi vélelmek fűzhetők hozzájuk, ez az új technológiáknál nem minden esetben mondható el, gondoljunk csak a kriptovalutákra (crypto-currency) vagy a blokkláncokra (block-chain). Globálisan egységes elfogadásról azonban az elektronikus aláírások esetében sem beszélhetünk, hiszen a minősített aláírás fogalma az EU-n kívüli jogrendszerekben nem feltétlenül ismert, továbbá egy széles körben elfogadott PGP aláírásnak az Európai Unióban nincsenek a normál aláíráson túlmutató tulajdonságai, hiába készítették esetleg műszaki értelemben teljesen egyenértékű módon egy fokozott biztonságú elektronikus aláírással. Valószínűleg nem várható egy már létező technológia (például minősített elektronikus aláírás, PGP) globális elfogadottságának megvalósulása, sokkal valószínűbb egy új technológia megjelenése, és ennek hasonló szinten történő beintegrálódása minden érintett társadalomba, azaz, ha az elektronikus kommunikáció egységesítése megköveteli, inkább az új dolgok hasonló szintű befogadása várható, mintsem a régi dolgok azonos szinten való elfogadása, és a fennálló eltérések megszüntetése. A minősített elektronikus aláírások kézírással való egyenértékűsége az Európai Unióban vélhetően megmarad, és emellé más technológiák felzárkózása – a jogszabályban rögzített magas technológiai szint miatt – rövid távon nem várható. A hitelesség biztosítása az internetre kötött eszközök esetében is kardinális kérdés, erre utal a Biztonságos Dolgok Internetre fogalmának és támogató szervezeteinek megjelenése is⁵⁰, ahol az integritást blokklánc segítségével képzelik el biztosítani. A blokklánc azonban alapesetben személytelen, a lánc egy-egy eleme nem feltétlenül köthető természetesen vagy jogi személyekhez, továbbá a lánc véglegesítését követően már a kibocsátóra nincs szükség az ellenőrzéshez, így az aláírásban általános céllal történő felhasználása nem várható, hiszen az aláíróhoz való kötöttségi feltétel nem teljesül. A harmadik felek felé kötelezően elvárt bizalom (TTP) modellje mellett mindig létezik olyan lehetőség is, amelyik kizárólag az egymásban megbízó egyénekre építi a bizalmat (WoT). Ilyen például az „okosszerződés” (smart contract) elve⁵¹, aminek Al-Bassam (2017) szerint a nyilvános kulcsú infrastruktúrában is meg kell jelennie. Érdekes lehetőséget rejtenek a biometrikus aláírások, amennyiben globális szabványok jönnének létre az azonos tulajdonsággal rendelkező aláírások létrehozására és ellenőrzésére, azonban ennek számos feltétele még nem adott⁵² – az ígéretes helyi kezdeményezések⁵³ ellenére.

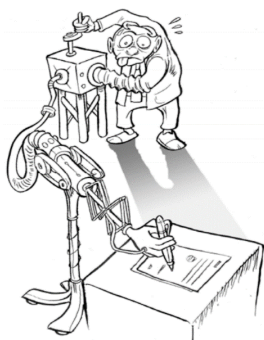
⁵⁰ Lásd <https://www.trusted-iot.org/>

⁵¹ A fogalmat Nick Szabo vezette be 1997-ben (Szabo 1997).

⁵² Erről lásd a MELASZ állásfoglalását a biometrikus aláírásokról: <http://www.melasz.hu/lang-hu/repository?func=fileinfo&id=186>

Ha rendszerszemléletben kívánjuk megfogalmazni az elektronikus aláírások jelentőségét, akkor az elektronikus aláírások hatásait minden kapcsolódó társadalmi rendszerben valamilyen explicit módon kellene kifejezni. Egy olyan generalizált eszközt ajánlott ehhez felhasználni, amely mérhetővé teszi az elektronikus aláírások, mint objektumok absztrakt tulajdonságai által létrejött objektumtér kapcsolódási pontjait, mélységét és természetét minden további érintett rendszer esetében. Az elektronikus aláírási rendszerek önmagukban is rendszereknek vagy alrendszereknek tekinthetők, amelyek saját magukra nézve is felvethetnek kérdéseket, de társadalmi aspektusból fontosabbnak látszik annak vizsgálata, hogy az elektronikus aláírás technológiai rendszere egyrészt milyen más rendszerekkel van kapcsolatban és gyakorol rá hatást, illetve fordított irányban, milyen társadalmi rendszerek hatnak rá, és hogyan. Az elsőre példa lehet az e-közigazgatás – illetve ennek minden releváns alrendszere, míg a másodiknak a normatíva, a közigazgatási jog lehet egy jól körülhatárolt alkalmazási területe. Nemeslaki András (2011) felvetése reálisnak látszik az elektronikus aláírás mint kollaboratív, mindenhová beépülő IKT-rendszer esetében is, hiszen jól látható módon a technológiát és a társadalmi rendszereket nem lehetett a múltban izoláltan elválasztani egymástól, és vizsgálatukban a technológiai eszközökön túl a társadalomkutatói módszerekre is szükség van.

Tudomásul kell vennünk azt is, hogy ha elektronikusan alá tudunk írni elektronikus dokumentumokat, még nem lesz „killer application”⁵⁴ – mondta Ricardo Genghini, aki a következő ábrával szemléltette, hogy hol is tart jelenleg az elektronikus aláírás technológiája:



2. ábra: Elektronikus aláírás⁵⁵

A társadalmi aspektus egyik kiemelt vetülete a digitális megosztottság, amelynek hatása az elektronikus aláírás területén is jelentkezik. A digitális megosztottság mindhárom – Molnár Szilárd (2017: 33) által összefoglalt – szintjén (hozzáférés, használat, használati

⁵³ Két megoldásról is lehet tudni, amelyik teljesíti a fokozott biztonság elektronikus aláírással szemben támasztott követelményeket. Az egyik az OTP Bank aláírópados megoldása (<https://www.otpbank.hu/portal/hu/Hirek/Alairopad>), a másik pedig a K&H Bank aláíró kódos fejlesztése (<http://webpub-ext.nmhh.hu/esign2016/showPdfAction.do?tipus=fb&mod=csat&id=8931>).

⁵⁴ „Killer application” a marketing területen azt az alkalmazást jelöli, amelyik jelentős mértékben segít növelni az eladásokat.

⁵⁵ Forrás: Ricardo Genghini „eIDAS und ETSI-Normierung”, 08.06.2017. https://netlab.hs-harz.de/TREATSWS/slides/010_2017-06-08_14_35_15_00_TREATS_Genghini.pdf

minőség) beavatkozás szükséges ahhoz, hogy a fejlettebb elektronikus aláírási technikák jelen lehessenek a hétköznapi életben, különös tekintettel az elektronikus ügyintézésre. Nem hagyhatók figyelmen kívül Csótó Mihály (2017: 25) következtetései az információs szegénységről, amely szerint egyrészt a technológiákhoz való hozzáférés vagy annak hiánya jelentős hatást gyakorol a társadalom szereplőire, másrészt az eddigi tapasztalatok alapján a technológia inkább fokozza az egyenlőtlenségeket, nem pedig megszünteti, harmadrészt általában vett információs szegénység nem definiálható, ezt a fogalmat csak egy adott kontextusban van értelme mérni egy adott normarendszer alapján. Ebből adódik, hogy várhatóan az elektronikus aláírás használata tovább mélyítheti a digitális szakadékot, továbbá az információs szegénység az elektronikus aláírás kontextusában is értelmezhető fogalom, a fentebb vázolt fogalmak pedig segíthetnek a kontextusok pontosabb feltérképezésében. A kontextusra egy példa az elektronikus ügyintézés, amelyben a digitális szakadék elektronikus aláírásra vonatkozó nagysága mérhetővé válik a résztvevők elektronikus aláírási ismeretanyaga és az e-közigazgatás által megkövetelt elektronikus ügyintézésben szükséges elektronikus aláírási kompetenciák közötti különbség számszerűsítése következtében. Ugyanez a metódus alkalmas az elektronikus ügyintézésben résztvevő partnerek pozicionálására és az esetlegesen elvárt elmozdulás folyamatos mérésére is. A fenti érveléssel belátható, hogy az elektronikus aláírások és bélyegzők fogalmi rendszere és egy erre épülő metrika generikusan alkalmazható szabályozási, tervezési, implementálási, oktatási és monitorozási célokra egyaránt.

Irodalom

- 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól
 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól
 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről (Eübszt.R)
 1952. évi III. törvény a polgári perrendtartásról
 2001. évi XXXV. törvény az elektronikus aláírásról (Eat.)
 2010. évi CXXVI. törvény a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról
 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (Eübszt.)
 2016. évi CXXX. törvény a polgári perrendtartásról (Pp.)
 2016. évi CL. törvény az általános közigazgatási rendtartásról (Ákr.)
 Al-Bassam, Mustafa, "SCPki: A Smart Contract-based PKI and Identity System", *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17*, Abu Dhabi, United Arab Emirates — April 02 - 02, 2017, pp. 35–40. <https://doi.org/10.1145/3055518.3055530>
 Az Európai Parlament és a Tanács 1999/93/EK irányelve (1999. december 13.) az elektronikus aláírásra vonatkozó közösségi keretfeltételekről
 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, 73–114. old.
 Bijker, Wiebe E., *Of Bicycles, Bakelites, and Bulbs. Toward a Theory of Sociotechnical Change*, MIT Press, Cambridge, London, 1995.
 Bogdán István, *Régi magyar históriák*, Magvető, Budapest, 1980.

- 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.
- Budai Balázs Benjámin, *Az e-közigazgatás elmélete*, Akadémiai Kiadó, Budapest, 2014.
- Coglianesi, Cary, "Globalization and the Design of International Institutions", *Faculty Scholarship at Penn Law*, 1549, 2000. http://scholarship.law.upenn.edu/faculty_scholarship/1549
- 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).
- 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/infars.XVII.2017.2.1>
- De Cock Danny, Karel Wouters and Bart Preneel, "Introduction to the Belgian EID Card", in Sokratis K. Katsikas, Stefanos Gritzalis and Javier López (eds.), *Public Key Infrastructure. First European PKI Workshop: Research and Applications, EuroPKI 2004, Samos Island, Greece, June 25-26, 2004. Proceedings*, Springer, Berlin, Heidelberg, 2004, pp. 1–13. http://dx.doi.org/10.1007/978-3-540-25980-0_1
- Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen (eds.), *Post-Quantum Cryptography*, Springer-Verlag Berlin Heidelberg, 2009.
- Dent, Alexander W., "A Brief Introduction to Certificateless Encryption Schemes and Their Infrastructures", in Fabio Martinelli and Bart Preneel (eds.), *Public Key Infrastructures, Services and Applications. EuroPKI 2009. Lecture Notes in Computer Science, vol 6391.*, Springer, Berlin, Heidelberg, 2010, pp. 1–16. https://doi.org/10.1007/978-3-642-16441-5_1
- Diffie, Whitfield and Martin E. Hellman, "New Directions in Cryptography", *IEEE Transactions On Information Theory*, Vol. 22. (1976), No. 6., pp. 644–654. <https://doi.org/10.1109/TIT.1976.1055638>
- Electronic Signatures in Global and National Commerce Act, Public Law 106–229, USA, June 30, 2000.
- Ellison, Carl and Bruce Schneier, "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", *Computer Security Journal*, Vol.16, (2000), No. 1., pp. 1–7. <https://www.schneier.com/academic/paperfiles/paper-pki.pdf>
- „ETSI TS 101 733 V2.2.1 (2013-04). Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CADES).”, April 2013, http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf
- „ETSI TS 101 903 V1.4.2 (2010-12), Technical Specification. Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).”, December 2012, http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf
- „ETSI TS 102 778-1 V1.1.1 (2009-07), Technical Specification. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES.”, July 2009, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf
- „ETSI TS 119 312 V1.2.1 (2017-05). Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.”, May 2017, http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.02.01_60/ts_119312v010201p.pdf
- „ETSI White Paper No. 8: Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges”, June 2015, <http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>
- 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
- Érdújhelyi Menyhért, *A közjegyzőség és hiteles helyek története Magyarországon*, M. Kir. Közjegyzők Országos Egyesülete, Budapest , 1899. (2004, MOKK, reprint kiadás)

- Falus Orsolya, *Ispotályos kereszties lovagrendek az Árpád-kori Magyarországon*, Doktori disszertáció, Pécsi Tudományegyetem Állam- és Jogtudományi Kara Doktori Iskolája, Pécs, 2014.
<https://ajk.ptt.hu/files/file/doktori-iskola/falus-orsolya-fruzsina/falus-orsolya-fruzsina-vedes-ertekezes.pdf>
- Kemény Miklós, „Magyar Polgári Eljárásjog”, *Digitális Tankönyvtár*,
https://www.tankonyvtar.hu/en/tartalom/tamop425/2011_0001_520_magyar_polgari_eljaras-jog/2011_0001_520_magyar_polgari_eljarasjog.pdf
- Kerckhoffs, Auguste, „La Cryptographie Militaire”, *Journal des sciences militaires*, Vol. IX, (1883), pp. 5–38.
- Komjáthy Miklós, „A magyarországi írásbeliség kialakulása. (Írástudó réteg, kancellária oklevelek, - Az ügyek intézése során keletkezett iratok.)”, in Pintér Márta (összeállító), *Régi könyvek és kéz- iratok. Tanulmánygyűjtemény*, Országos Széchényi Könyvtár, Könyvtártudományi és Módszertani Központ, Népművelési Propaganda Iroda, Budapest, 1974, 151–154. old.
- Lopez, Javier, Rolf Oppliger and Günther Pernul, „Classifying Public Key Certificates”, in David Chadwick and Gansen Zhao (eds), *Public Key Infrastructure. EuroPKI 2005. Lecture Notes in Computer Science*, vol. 3545., Springer, Berlin Heidelberg, 2005, pp. 135–143.
https://doi.org/10.1007/11533733_9
- Molnár Szilárd, „A megrekedt magyar modernizáció kiütkeresése a sokrétű digitális megosztottság útvesztőjéből”, *Információs Társadalom*, XVII. évf. (2017), 2. szám, 30–47. old.
<http://dx.doi.org/10.22503/infarts.XVII.2017.2.2>
- Montana, David and Mark Reynolds, „Validation Algorithms for a Secure Internet Routing PKI”, in Stig F. Mjølsnes, Sjouke Mauw and Sokratis K. Katsikas (eds.), *Public Key Infrastructure. EuroPKI 2008. Lecture Notes in Computer Science*, vol. 5057., Springer, Berlin Heidelberg, 2008, pp. 17–30. https://doi.org/10.1007/978-3-540-69485-4_2
- Muha Lajos, „Infokommunikációs Biztonsági Stratégia”, *Hadmérnök*, IV. évf., (2009), 1. szám, 214–224. old.
- Nemeslaki András, „Tűz és víz határán a gazdaságinformatikában: a technológiai konstruálás és a társadalmi konstruktivizmus összekapcsolásának lehetősége.”, *Információs Társadalom*, XI. évf. (2011) 1-4. szám, 11-30. old.
- Ølnes, Jon and Leif Buene, “Use of a Validation Authority to Provide Risk Management for the PKI Relying Party”, in Andrea S. Atzeni and Antonio Liroy (eds.), *Public Key Infrastructure. EuroPKI 2006. Lecture Notes in Computer Science*, vol 4043., Springer, Berlin, Heidelberg, 2006, pp. 1–15.
https://doi.org/10.1007/11774716_1
- Pala, Massimiliano, Sara Sinclair and Sean W. Smith, “PorKI: Portable PKI Credentials via Proxy Certificates”, in Jan Camenisch and Costas Lambrinoudakis (eds.), *Public Key Infrastructures, Services and Applications. EuroPKI 2010. Lecture Notes in Computer Science*, vol 6711., Springer Berlin Heidelberg, 2011, pp. 1–16. https://doi.org/10.1007/978-3-642-22633-5_1
- Pala, Massimiliano and Sean W. Smith, “AutoPKI: A PKI Resources Discovery System”, in Javier Lopez, Pierangela Samarati and Josep L. Ferrer (eds.), *Public Key Infrastructure. EuroPKI 2007. Lecture Notes in Computer Science*, vol 4582., Springer Berlin Heidelberg, 2007, pp. 154–169.
https://doi.org/10.1007/978-3-540-73408-6_11
- Qian, Haifeng and Shouhuai Xu, „Non-Interactive Editable Signatures for Assured Data”, in *Proceeding CODASPY '11 Proceedings of the first ACM conference on Data and application security and privacy*, San Antonio, TX, USA — February 21-23, 2011, pp. 145–156.
<https://doi.org/10.1145/1943513.1943533>
- Rátai Balázs, „Az elektronikus aláírás szabályozásának kulcskérdései az 1999/93/EC irányelv alapján”, *Jogi Fórum Portál*, 2000. [http://www.jogiforum.hu/letoltes/!/files/publikaciok/ratai-1993_93_ec\(jf\).doc!1505835549!/publikaciok/16](http://www.jogiforum.hu/letoltes/!/files/publikaciok/ratai-1993_93_ec(jf).doc!1505835549!/publikaciok/16)
- Rivest, Ron, Adi Shamir and Leonard Adleman, “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>
- Schaller, R. R., „Moore’s law: past, present and future”, *IEEE Spectrum*, Vol. 34., (1997), Issue 6., pp. 53–59. <https://doi.org/10.1109/6.591665>

- Shannon, Claude Elwood, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, Vol. 28. (1949), Issue 4., pp. 656–715.
- Smedinghoff, Thomas J. and Ruth Hill Bro, "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.
- Szabo, Nick, "Smart Contracts: Formalizing and Securing Relationships on Public Networks", *First Monday*, Vol. 2. (1997) Number 9. <https://doi.org/10.5210/fm.v2i9.548>
- 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
- Szittner Károly, *E-ügyintézés Magyarországon. E-Government Tanulmányok XXXI.*, E-Government Alapítvány a Közigazgatás Modernizációjáért, Budapest, 2011.
- Tubay Tiziano, „Titokzatos örökség – A székhely írás kutatásának nehézségei”, in Bartók Zsófia Ágnes, Fajt Anita, Görög Dániel, Maróthy Szilvia (szerk.), *kultúrjav. Írásbeliség és szóbeliség irodalma – újrashoznosítva*, Fiatalok Konferenciája 2014, reciti, Budapest, 2015, 183-196. old.
- Van Damme, Gauthier, Nicolas Luyckx and Karel Wouters, "A PKI-Based Mobile Banking Demonstrator", in Svetla Petkova-Nikova, Andreas Pashalidis and Günther Pernul (eds), *Public Key Infrastructures, Services and Applications. EuroPKI 2011. Lecture Notes in Computer Science, vol 7163.*, Springer Berlin Heidelberg, 2012, pp. 147–158. https://doi.org/10.1007/978-3-642-29804-2_10
- Zeng, Ke, "Pseudonymous PKI for Ubiquitous Computing", in Andrea S. Atzeni and Antonio Lioy (eds.), *Public Key Infrastructure. EuroPKI 2006. Lecture Notes in Computer Science, vol 4043.*, Springer Berlin Heidelberg, 2006, pp. 207–222. https://doi.org/10.1007/11774716_17
- Vasvári György, *Bankbiztonság*, Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság és Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék, Budapest, 2003.
- Vigil, Martín A. G., Cristian T. Moecke, Ricardo Felipe Custódio and Melanie Volkamer, "The Notary Based PKI", in Sabrina De Capitani di Vimercati and Chris Mitchell (eds), *Public Key Infrastructures, Services and Applications. EuroPKI 2012. Lecture Notes in Computer Science, vol 7868.*, Springer Berlin Heidelberg, 2013, pp. 85–97. https://doi.org/10.1007/978-3-642-40012-4_6
- Wang, Jingjing, *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
- Werlang, Felipe Carlos, Ricardo Felipe Custódio and Martin A. G. Vigil, "A User-Centric Digital Signature Scheme", in Sokratis Katsikas and Isaac Agudo (eds), *Public Key Infrastructures, Services and Applications. EuroPKI 2013. Lecture Notes in Computer Science, vol 8341.*, Springer, Berlin Heidelberg, 2014, pp. 152–169. https://doi.org/10.1007/978-3-642-53997-8_10

Erdősi Péter Máté, PhD jelölt, 1969-ben Salgótarjánban született. 1994-ben a KLTE Természettudományi Karán szerzett diplomát, matematika-informatika okleveles tanárként. 2000 és 2005 között a BME GTK Információ- és Tudásmenedzsment Tanszék Biztonságmenedzsment Kutatócsoportjában külső tag, kutatóként dolgozott továbbá 2005 januárjától 2006 októberéig az Információs Társadalomért Alapítványban is. 2016-ban abszolutóriumot szerzett az NKE Közigazgatás-tudományi Doktori Iskolájában, mely az ország első ilyen képzése. Több magyarországi egyetemen tanított, számos publikációja jelent meg az elektronikus aláírás témakörében. Jelenleg elektronikus aláírási szakértő és az NKE külső oktatója, továbbá a Digitális Kormányzás és Digitális Állam Kiemelt Kutatóműhely PhD jelölt tagja. A Magyar Elektronikus Aláírás Szövetség (MELASZ) alapító és oktatásért felelős elnökségi tagja, valamint az Informatika-Számítástechnika Tanárok Egyesületének vezető oktatója. Kutatási területei: elektronikus aláírás, hitelesség, közigazgatási információs rendszerek biztonságának növelése.