ACTA HUMANA • 2022/3. 35–57. • DOI: 10.32566/ah.2022.3.2

Az elektronikus aláírások és bélyegzők dimenziói a közigazgatásban

ERDŐSI PÉTER MÁTÉ[1]

Az elektronikus aláírás fogalmát széles körben használják a közigazgatásban és a közigazgatási jogban is. Az elektronikus aláírás értelmezése számos átalakuláson ment keresztül az elmúlt négy évtizedben, továbbá használata során sokszor keverednek az azonosítás, hitelesítés és feljogosítás információbiztonsági és a bizalom, hitelesség, szavahihetőség köznyelvi fogalmak. Az elektronikus aláírás jogi definíciójából nem következik automatikusan annak mérhetősége, de számos aspektusa jelent meg az európai és magyar jogszabályokban. Ez a tanulmány arra a kérdésre keresi a választ, hogy létezik-e az elektronikus aláírásoknak mint az összes elektronikus aláírást tartalmazó halmaznak a magyar közigazgatásban alkalmazható legszűkebb rendszere, és ha igen, akkor ennek a legszűkebb rendszernek milyen leíró tulajdonságai vannak? Érvelésünk szerint egy ilyen modell teremtheti meg a mérhetőség és az összehasonlíthatóság alapjait.

Kulcsszavak: eIDAS, elektronikus aláírás, elektronikus bélyegző, metrikus modell, mérhetőség, összehasonlíthatóság

Dimensions of Electronic Signatures and Seals in the Hungarian Public Administration

The concept of electronic signature is widely used in public administration and in public administration law. The interpretation has undergone many transformations over the past four decades. There is often a confusion between the usage of terms of identification, authentication, and authorisation for information security with the more colloquial terms trust, authenticity and credibility. The legal definition of the concept does not automatically imply its measurability, but the closer scrutiny of the legislation reveals many aspects, which result in an implicit classification of signatures. This study seeks to answer the question of whether there is a basic set of properties as a set of all electronic signatures that can be used in Hungarian public administration, and if so, such a model can provide the basis for measurability and comparability.

Keywords: eIDAS, electronic signature, electronic seal, metric model, measurability, comparability

1 Külső kutató, Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Kar Választás és Képviselet kutatóműhely, e-mail: kutato@erdosipetermate.hu

Bevezetés

Az elektronikus aláírásnak *(electronic signature)* számos aspektusa jelent meg a jogalkotási és a jogalkalmazási területeken, például használható fokozott biztonságú elektronikus aláírás *(advanced electronic signature)* vagy minősített elektronikus aláírás *(qualified electronic signature)* is az elektronikus folyamatokban. Sok esetben nehezen eldönthető kérdésként vethető fel az, hogy az adott elektronikus aláírás – mint alaki jogi kellék – használható-e teljes bizonyító erejű magánokirat létrehozására, vagy alkalmas-e közokirat elektronikus aláírására? További kérdéseket is fel lehet még vetni a tárgyban, elegendő csak a konténerekre vagy az aszimmetrikus kriptográfián túlmutató vagy éppen ezzel ötvözhető megoldásokra (például biometrikus aláírásokra[2]) gondolni. Ezek a kérdések ugyanabba az irányba mutatnak, az elektronikus aláírások mérhetősége igényének irányába. Érvelésünk szerint az egyértelmű elhelyezhetőség teremti meg a mérhetőség és az összehasonlíthatóság alapjait az elektronikus aláírások tekintetében is.

Az elektronikus aláírás fogalmát 2014 óta az Európai Parlament és a Tanács 910/2014/EU rendelete[3] definiálja az Európai Unióban olyan elektronikus adatként, amelyet egy másik elektronikus adathoz csatolnak, és amelyet az aláíró *(signatory)* aláírásra használ.[4] Az aláíró kizárólag természetes személy *(natural person)* lehet, aki éppen aláír.[5] Az aláírásnak ebből adódóan három implicit jellemzője létezik:

- a természetes személy aláíró;
- az aláírás csatolása valamely más adathoz;
- az aláírt elektronikus adatok.

Az eIDAS hatálybalépését követően az Európai Unió megkülönbözteti a jogi személyek *(legal person)* aláírását a természetes személyek aláírásától,[6] és elektronikus bélyegzőnek *(electronic seal)* nevezi.[7] Az elektronikus aláírás és bélyegző tulajdonságai között azonban erőteljes hasonlóságot lehet felfedezni, mivel egyrészről az eIDAS megismétli szinte szóról szóra az elektronikus bélyegzők esetében az elektronikus aláírásra vonatkozó előírásokat, másrészről az elektronikus ügyintézésről szóló törvény (2015. évi CCXXII. törvény[8]) kodifikációs fikciót alkalmazva azt mondja ki, hogy – eltérő rendelkezés hiányában – az elektronikus bélyegzőt is elektronikus aláírásnak kell tekinteni.[9]

2 Egyik kutatási irány például a nem egzakt bemenetű privátkulcs-generálási módszerek kialakítása, ahol biometrikus bemenő adatok feldolgozását tűzték ki célul (lásd Takahashi et al. [2015]).
3 910/2014/EU európai parlamenti és tanácsi rendelet (eIDAS).
4 eIDAS 3. cikk 10.
5 eIDAS 3. cikk 9.
6 eIDAS 3. cikk 24.
7 eIDAS 3. cikk 25.
8 2015. évi CCXXII. törvény (Eüsztv.).
9 Eüsztv. 99. § (2).

Tekintettel arra, hogy a fentiek szerint az elektronikus aláírásokhoz számos további jellemző csatlakozik, felmerül a kérdés, hogy lehetséges-e az elektronikus aláírás jellemzőit dimenzionálni? Válaszunk szerint igen, meg lehet határozni azokat a dimenziókat, amelyekben az elektronikus aláírások elhelyezhetővé válnak, és lehetővé válik az így létrejött térben valamilyen metrika definiálása is. Ebben a metrikus térben – amelynek fogalmát Maurice Fréchet alapozta meg 1906-os doktori disszertációjával[10] – két elektronikus aláírás távolsága kizárólag nemnegatív lehet, továbbá akkor és csak akkor nulla, ha a leírásukban ugyanazok a tulajdonságok szerepelnek. A dimenziók – egy absztrakciós szintet megalkotva – az ugyanolyan tulajdonságokkal leírható elektronikus aláírásokat foglalják magukban, azaz jelen esetben nem a bináris reprezentánsok hordozzák az aláírás elhelyezhetőségéhez szükséges információkat, hanem az egyes bitsorozatok jelentései. Vagyis két különböző elektronikus aláírás akkor lesz ebben a leíró térben ugyanazon a helyen, ha absztrahált tartalmuk azonos. Egy ilyen metrika teszi lehetővé az elektronikus aláírás átfogó tárgyalását elméletben *(in thesi)* és gyakorlatban *(in praxi)* a közigazgatásban és a közigazgatási jogban egyaránt, amelyek mindegyike különbözik egymástól, Tamás András megállapítását alapul véve.[11]

Kérdésként felvethető továbbá az is, hogy az elektronikus aláírások általános leírására alkalmas dimenziókat meg kell-e különböztetni vagy ki kell-e egészíteni a közigazgatás számára. A megkülönböztethetetlenségnek az lenne feltétele, hogy a közigazgatás külön sajátos szabályok előírása nélkül legyen képes kibocsátani és befogadni elektronikus aláírásokat, illetőleg elektronikusan aláírt tartalmakat. Az eIDAS a tagállamok közigazgatási rendszerei számára csak részben tette kötelezővé az előírások alkalmazását, nem kell például a közigazgatási belső eljárások lebonyolítására szolgáló és ehhez bizalmi szolgáltatásokat igénybe vevő rendszerekre az eIDAS előírásainak vonatkozniuk. A harmadik felek számára is elérhető nyilvános bizalmi szolgáltatásokra nézve viszont kötelezően kell érvényesíteni az európai előírásokat.[12] Az eIDAS rendelkezésein túl az elektronikus ügyintézés szabályait a magyar jogalkotó külön törvényben és rendeletben tette közzé. Ez a rendelet az elektronikus ügyintézést nyújtó szervezetekre, az ügyfélre, az alkalmazható bizalmi szolgáltatásokra és a felügyeleti szervre terjed ki.[13] A magyar állam tehát élt a külön előírások definiálásának jogával a közigazgatási ügyek elektronikus intézése vonatkozásában, ami indokolttá teszi az általános célú vizsgálatok kiterjesztését a közigazgatásra vonatkozó speciális előírásokra is.

10 Fréchet 1906
11 Tamás 2001, 16–18.
12 eIDAS Preambulum (21).
13 Lásd a 137/2016. (VI. 13.) Korm. rendelet hatályát.

Az elektronikus aláírás dimenziói

Az elektronikus aláírást a 93/1999 EU irányelv[14] definiálta először jogi szabályozási környezetben 1999-ben, az itt megfogalmazott definíciója szerint egy elektronikus aláírás a következőt jelenti: „olyan elektronikus adat, amely más elektronikus adathoz van csatolva, illetve logikailag hozzárendelve, és amely hitelesítés módszeréül (method of authentication) szolgál." A korábban hatályos elektronikus aláírási törvény úgy fogalmaz, hogy az elektronikus aláírás az „elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat".[15] A két definíció látszólagos ellentmondásban van, hiszen az azonosítás nem lehet egyenlő a hitelesítéssel. A kontraindikatív kapcsolatot a két definíció között a hitelesség meghatározása képes megszüntetni,[16] amely szerint általánosságban véve a hitelesség az állított azonosság megerősítése, így az elektronikus hitelesség az elektronikusan állított azonosság megerősítése. Azonosságot pedig – a korábban felismert dichotómiát alkalmazva – lehet állítani a forrásról *(signatory)* és a tartalomról *(content).* Egy aláírt adat esetében ennek az azonosságnak a megerősítése két vizsgálat – azaz az aláíró és a tartalom – hitelesítésének eredményét jelenti, összhangban az NIST FIPS 800-53 amerikai szabványban[17] a hitelesítésről megfogalmazottakkal:[18]

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

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

Az elektronikus aláírások dimenzionálásának az a legfontosabb célkitűzése, hogy rögzítve legyenek azok a dimenziók, amelyek az elektronikus aláírásokkal kapcsolatosan felmerülhetnek, valamint meg is legyenek határozva az egyes dimenziók értékkészletei. Tekintettel arra, hogy az egyes értékek között vannak nyilvánvaló és le-

14 1999/93/EK európai parlamenti és tanácsi irányelv.
15 2001. évi XXXV. törvény (Eat.).
16 Vasvári 2003, 68.
17 NIST 2013
18 NIST 2013, B-2: 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. (Hitelesség: az a tulajdonság, hogy valami eredeti, ellenőrizhető és meg lehet benne bízni; bizalom az átvitel, az üzenet vagy az üzenet küldőjének az érvényességében.)

hetnek 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 generátorrendszert is meg kell határozni.

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: „A jelen dokumentumnak megfelelően előállított elektronikus aláírás olyan bizonyítékot szolgáltat, amely feldolgozásával megbizonyosodhatunk arról, hogy valamely aláírási szabályzatban meghatározott kötelezettségvállalást az aláíró egy adott időpontban explicit módon felvállalt egy azonosító (egy név vagy egy álnév, és opcionálisan egy szerep) használatával."[19]

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.

Ezek után megkísérelhetjük összegyűjteni és felsorolni az elektronikus aláírásokkal és bélyegzőkkel kapcsolatosan fellelhető összes olyan tulajdonságot, amely elméleti vagy gyakorlati aspektusban felmerült a szakirodalomban. A dimenziók megnevezés elé ebben a megközelítésben jogos lenne a „potenciális" jelzőt kitenni, hiszen „valódi" dimenziók esetében elvárt a közöttük lévő függetlenség. Elméletileg (matematikai értelemben) végtelen sok generátorrendszere létezhet egy adott térnek, amelyben minden eleme reprezentálható, de a dimenziók függetlensége csak a bázisrendszerek esetében jelenik meg követelményként. Az elektronikus aláírások és bélyegzők tere különbözik a valós vagy komplex számokon értelmezett matematikai absztrakt tértől abban az értelemben, hogy a dimenziók értékkészletei nem feltétlenül skaláris tulajdonságúak, lehetnek kategoriális elemek is az egyes dimenziókban. Ortogonalitási vizsgálatot azonban csak a már ismert potenciális dimenziókon lehetséges elvégezni, ennek eredményeként állítható elő az a legszűkebb dimenzióhalmaz (bázisrendszer), amelyben egyrészről minden elektronikus aláírás vagy bélyegző egyértelműen felírható, másrészről további dimenziók felvételét csak úgy lehetséges megtenni, hogy valamely már létező dimenziótól való függés fennáll. A dimenziók elnevezése a szerző saját gondolatait tükrözi, megválasztásuk során az alkotói szabadság és a létező fogalomhasználat optimális konkatenációja volt az alapvető célkitűzés.

Az elektronikus aláírások dimenzióinak meghatározásakor először az elektronikus aláírás értelmezési keretét definiáljuk, vagyis az aláírás kontextusából, valamint annak jogi és technológiai környezetéből indulunk ki. A kontextus felveti az aláíró entitás, az aláírás-létrehozó adat és az aláírás-ellenőrző adat, illetve az aláírás osztályozását és az egyes osztályok kapcsolati hálóinak elemzését, ideértve a technológiai és jogi környezet elemeinek hozzákapcsolását az aláírások különböző osztályaihoz. Az értelmezési keretet ez a négyes és az ezekben megjelenő értékkészlet határozza tehát meg.

19 ETSI 2000, 8.

A megjelenítés

Az informatikai leíró nyelvek, dokumentumformátumok fejlődésével egyre több helyről jelent meg az igény az elektronikus aláírások beillesztésére. A szabványosítás követte ezeket az igényeket, és három különböző megjelenítésű elektronikus aláírástípus létrehozására és használatára alakultak ki szabványok. Közös jellemzőjük, hogy mindegyik aláírás kielégíti a fokozott biztonságú elektronikus aláírásokra a jogszabályban megfogalmazott követelményeket (illetőleg a PDF[20]-szabvány fogalmazása szerint „képes kielégíteni azokat"), ebből adódóan az eIDAS ilyen irányú követelményeit is. Ennek jelentősége abban áll, hogy ahol a jogszabály „fokozott biztonságú aláírás" létezését követeli meg, ott ezek szerint használható kriptográgiai üzenetszintaxis-alapú fokozott biztonságú elektronikus aláírás *(CAdES: CMS-based Advanced Electronic Signature),*[21] kiterjesztett jelölőnyelv-alapú fokozott biztonságú elektronikus aláírás *(XAdES: XML-based Advanced Electronic Signature)*[22] és PDF-alapú fokozott biztonságú elektronikus aláírás *(PAdES: PDF-based Advanced Electronic Signature)*[23] kódolású aláírás is.

A PAdES-szabvány a PDF-dokumentumok elektronikus aláírására vonatkozóan valójában nem ad meg új eljárásokat, hanem a már ismert CMS- és XML-alapú megoldásokat alkalmazza PDF-formátumra is.

A megjelenítés kérdéskörébe tartozhat a konténerek jellemzőinek ismertetése is,[24] azonban ezek a képződmények olyan bonyolultságúak, amelyekre önmagában is alkalmazható a modell, ezért ezeket nem tekintjük első körben a modell részének.

Az aláírás típusa

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

20 PDF: *portable document format,* hordozható dokumentumformátum, az ISO 32000 szabványcsalád írja le.
21 ETSI 2013a
22 ETSI 2010
23 ETSI 2009
24 ETSI 2013b

aláírás, amelyet az aláíró minősített elektronikus aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

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

Esetenként erre a tulajdonságra az aláírás biztonságaként is szoktak utalni, amely hétköznapi értelemben helytálló lehet, és a besorolások magyar fordítása is elősegítette ezt a vélekedést. A „fokozott biztonságú" angol megfelelője azonban itt az *„advanced"*, ami információbiztonsági értelemben már nem feltétlenül utal biztonságosabb aláírásra, mivel a fejlett elektronikus aláírás tulajdonságai egyrészről az aláíró fizikai személlyel való erősebb összekapcsolhatóságra, másrészt a dokumentum sértetlenségével való összefüggésére vonatkoznak – azaz az aláíró és a tartalom hitelességére. A hitelesség azonban csak az egyik biztonsági követelmény és a minősített aláírásnál is létezhet magasabb szintű biztonsággal létrehozható aláírás. Vagyis elképzelhető olyan aláírás, amelynek biztonsági szintje magasabb (biztonságosabb környezetben és módon hozták létre), de betű szerinti értelemben mégsem lehet például minősített ez az elektronikus aláírás, mert egy nem tanúsított eszközön vagy egy nem nyilvános szolgáltató által kibocsátott tanúsítványon alapul. Kérdésként vetődik fel továbbá a nyílt forráskóddal készített PGP-alapú elektronikus aláírások[25] besorolhatósága a fokozott biztonságú elektronikus aláírások körébe, ahol az aláírás készítésének a biztonsága és algoritmuskészlete teljes mértékben azonos lehet a nyilvános szolgáltatók által kibocsátott tanúsítványokon alapuló aláírásokéval, eltérés a tanúsítvány és az aláíró közötti kapcsolat hitelességében van csupán. Észrevehető a párhuzam a III. Béla király idejében – 13. században – megerősödő – és a 19. században megszűnő – hiteleshelyek[26] és a nyilvános bizalmi szolgáltatók funkcionalitása között.

Alaki bizonyító erő

Az elektronikus aláírások bizonyító erejét tekintve kizárólag az alaki bizonyító erővel lehetséges az aláírások tulajdonságainál foglalkozni, hiszen az anyagi bizonyító erőről az aláírás információt általánosságban nem tartalmazhat.[27] Az alaki bizonyító erőre általános szabályt az eIDAS fogalmaz meg, két esetben. Egyrészről az elfogadás meg nem tagadhatósága elv miatt minden egyes elektronikus aláírást megillet

25 OpenPGP szoftver honlapja (2022. május 9.): https://openpgp.org/
26 Eckhart 2012
27 Magyarország Kormánya 2015

a bizonyítékként való felhasználás vélelme,[28] másrészről a minősített elektronikus aláírás kézírással való egyenértékű elfogadása vált kötelezővé az Európai Unióban.[29]

Az írásbeliség tekintetében az Eat. megfogalmazta, hogy írásbelinek kell tekinteni egy elektronikus dokumentumot, ha azt legalább fokozott biztonságú aláírással látták el,[30] ez a vélelem azonban az Eat. hatályvesztésével *expressis verbis* kikerült a magyar jogrendből és máshol sem jelent meg. A Polgári Törvénykönyv (Ptk.)[31] írásbeliségre vonatkozó szabályait értelmezve (6:7. §) azt kapjuk, hogy írásbelinek azt kell tekinteni általánosságban, amit a felek aláírtak, azaz aláírásukkal láttak el. Ezt összevetve az eIDAS elektronikus aláírás definíciójával (aláírás az, amit a természetes személy aláíró aláírásra használ), azt kapjuk, hogy az elektronikus írásbeliség feltétele az elektronikus aláírás megléte minden érintett fél részéről, az aláírásra nézve minden további korlátozás nélkül. Ez túl tág teret biztosítana az írásbeli formáknak és a velük szembeni visszaéléseknek, mivel egy normál elektronikus aláírás nem biztosít elegendő védelmet a hamisíthatóság ellen. Egy normál elektronikus aláírás (például egy szkennelt aláírás képe vagy egy e-mail végére gépelt név) nagyon könnyen lemásolható vagy teljes egyezőséggel reprodukálható, és felhasználható az érintett tudta nélkül olyan dokumentumokon, amelyeket az érintett nem is látott, emiatt a Ptk. 6:7. (3) bekezdésére vonatkozó kommentár szerint az itt megfogalmazott elvárásoknak minden kétséget kizáróan csak a legalább fokozott biztonságú elektronikus aláírás képes megfelelni. Az írásbeliség vélelmét minden normál elektronikus aláíráshoz hozzáfűzni jogi szempontból logikailag rendben lévőnek tűnik, hiszen teljes bizonyító erő hiányában az aláírás létrejöttét állító félnek kell igazolnia vitás esetekben azt, hogy az aláírás minden érintett fél részéről valóban megtörtént, ellenkező esetben az aláíráshoz fűződő kötelmi vélelem megdönthetősége valószínűsíthető. Mivel a gyakorlatban az ilyen esetek száma idáig meglehetősen alacsony volt, nem lehet előrejelzést adni arra nézve, hogy a normál elektronikus aláírással ellátott dokumentumok írásbeliségének hamis vélelmezéséből adódó peres ügyek mekkora terhet jelentenek majd az ítélkezésben, ez nyilvánvaló módon függ majd a hamisítások mértékétől. Egyes jogszabályhelyek külön nevesítették a fokozott biztonságú elektronikus aláírás szükségességét mint alaki kelléket.[32]

Az okiratiság fontos szerepet tölt be a bírósági eljárásokban, két okból. Egyrészről az 1952. évi III. törvény a polgári perrendtartásról (Pp. 1952.),[33] illetve 2018. január 1-jétől a 2016. évi CXXX. törvény a polgári perrendtartásról (Pp. 2018.)[34] kimondja,

28 eIDAS 25. cikk (1) bekezdés.
29 eIDAS 25. cikk (2)–(3) bekezdés.
30 Eat. 4. § (1) bekezdés.
31 Ptk. A törvényt az Országgyűlés a 2013. február 11-i ülésnapján fogadta el. A kihirdetés napja: 2013. február 26. A hatálybalépésével összefüggő átmeneti és felhatalmazó rendelkezésekről lásd a 2013. évi CLXXVII. törvényt.
32 2013. évi CCXXXVII. törvény (Hpt.) 279. § (1), vagy a 11/2020. (II. 7.) Korm. rendelet 18. § (4), (5) és 26. § (4).
33 1952. évi III. törvény a polgári perrendtartásról. A törvényt a 2016. évi CXXX. törvény 633. §-a hatályon kívül helyezte 2018. január 1. napjával.
34 2016. évi CXXX. törvény.

hogy ha a tényállás okirattal bizonyítható, akkor a bíróság az egyéb bizonyítást mellőzheti,[35] másrészről a bizonyítási teher alól mentesül az a fél, aki – az ellenkező bebizonyításáig – teljes bizonyító erejű magán-[36] vagy közokirattal[37] tudja igazolni a tényállást. A teljes bizonyító erő vélelmezésében tehát az elektronikus aláírások fontos szerepet kaptak, magánokiratok vonatkozásában a Pp. 1952. 196. §, illetve a Pp. 2018. 325. §, a közokiratok terén pedig a Pp. 1952. 195. §, illetve a Pp. 2018. 323. § rendelkezik azokról az alaki követelményekről, amelyeket ezeknek az okiratoknak teljesíteniük kell.

A komplexitás

Az egyes aláírások komplexitásának belső szerkezetét a vonatkozó szabványok pontosan specifikálják. Az alapaláírások (AdES-BES,[38] AdES-EPES[39]) létrehozása nagyon könnyű, viszont a hosszú távú érvényességükkel probléma van, mivel hiteles időbélyeg hiányában az ellenőrzés mindig csak az aktuális pillanatra vonatkozóan végezhető el, nem pedig az aláírás pillanatára. Az időbélyegzett aláírások (AdES-T[40]) alkalmazása hiteles idő beépítésével és a hitelesség megváltozásának detektálhatóságával már lehetővé teszi az aláírás ellenőrzését bármelyik későbbi időpontban az aláírás létrehozásának idejére, de ha az érvényességi adatok időközben elérhetetlenné váltak (vagy felülíródtak), az ellenőrzés nem végezhető el, vagy igen körülményessé válhat. A komplex aláírások (AdES-C[41]) alkalmazása – akár az aláíró, akár az ellenőrző készíti azt el – megoldja a „hol vannak az akkori érvényességi adatok most" kérdését, azonban a letölthetőségtől függhet az ellenőrzés elvégezhetősége. Ezen a problémán segít a kiterjesztett aláírások (AdES-X, AdES-X-Long[42]) alkalmazása, amely az érvényességi adatokat hozzácsatolja az aláírásokhoz. Az archív aláírások (AdES-A[43]) létrejötte megteremtette az aláírások érvényességének hosszú ideig való fenntarthatóságát – bizonyos korlátokkal, de a többszörös archív aláírások kezelését még nem biztosította. A hosszú távon érvényes aláírások (AdES-LT, AdES-LTV[44]) létjogosult-

35 Pp. 1952. 192. §, Pp. 2018. 320. § (5) bekezdés.
36 Pp. 1952. 196. § (1), Pp. 2018. 325. § (3) bekezdés.
37 Pp. 1952. 195. § (7), Pp. 2018. 323. § (2) bekezdés.
38 AdES-BES: *advanced electronic signature: basic electronic signature* (Fokozott biztonságú elektronikus aláírás: alap elektronikus aláírás).
39 AdES-EPES: *advanced electronic signature: extended policy based electronic signature* (Fokozott biztonságú elektronikus aláírás: kifejezett hitelesítési rend alapú elektronikus aláírás).
40 AdES-T: *advanced electronic signature: timestamped electronic signature* (Fokozott biztonságú elektronikus aláírás: időbélyegzett elektronikus aláírás).
41 AdES-C: *advanced electronic signature: complex electronic signature* (Fokozott biztonságú elektronikus aláírás: komplex elektronikus aláírás)
42 AdES-X(-Long): *advanced electronic signature: extended (long) electronic signature* (Fokozott biztonságú elektronikus aláírás: kiterjesztett [hosszú] elektronikus aláírás).
43 AdES-A: *advanced electronic signature: archive electronic signature* (Fokozott biztonságú elektronikus aláírás: archív elektronikus aláírás).
44 AdES-LT(V): *advanced electronic signature: electronic signature with long term (validity)* (Fokozott biztonságú elektronikus aláírás: hosszú távú [-on érvényes] elektronikus aláírás).

ságát az adja, hogy bármilyen korábbi aláírást – az érvényességi adatok rendelkezésre állása esetén – képesek folyamatosan hitelessé tenni sok-sok éven keresztül is.

Az egyes aláírások részletes leírását – tekintettel arra, hogy ezek implementációja függ a megjelenítéstől – a vonatkozó szabványok (CAdES, XAdES, PAdES) részletezik.

Az érvényességi idő

Az aláírások érvényességi ideje alatt azt az időtartamot értjük, amely alatt az aláírásban megtett kötelezettség felvállalásáról az aláírás ellenőrzésével kell meggyőződni, más szóval eddig kell biztosítani az aláírás hitelesíthetőségét, hitelességét. Valójában itt a hiteles archiválás kérdéskörét kell figyelembe venni, ami kicsit több, mint egy egyszerű lemásolás és megőrzés. Ugyanis megőrzés közben a meg nem változás folyamatos detektálhatóságát is biztosítani kell egy hiteles archiválás során. Ezért felhasználva az archiválásról szóló 1/2018. ITM rendeletben foglaltakat,[45] az aláírásokat ebből a szempontból három csoportra oszthatjuk fel: azonnali, rövid távú és hosszú távú érvényességi időt megkövetelő aláírások. Az Itmr. nem terjed ki az állami vagy helyi önkormányzati feladatot vagy jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy által végzett elektronikus archiválásra,[46] az ilyen szerveknek az Eüsztv.-ben foglaltak alapján kell eljárniuk (például minősítettarchiválás-szolgáltatás vagy elektronikus dokumentumtárolás-szolgáltatás). Az egyes aláíráscsoportok főbb jellemzői az alábbiak:

- Az azonnali felhasználásra készített aláírások esetében az aláírást a létrehozásához képest közeli időpontban (percek, esetleg néhány óra múlva) használják fel, vagyis ellenőrzik a megfelelőségét az aláírt tartalom feldolgozása előtt, és a folyamatban többé nem lesz szükség az aláírás újbóli ellenőrzésére. Kétség vagy biztonsági kérdés esetén az ellenőrzéskor megőrzött auditnyomokat használhatják fel bizonyítékként. Ez a megoldás implicit módon biztosítja a hitelesség megőrzését.
- A rövid távú érvényességnek az a tulajdonsága, hogy az aláírást elkészítik, felhasználják, de a felhasználás alapjául szolgáló bizonylatot itt már meg kell őrizni egy bizonyos, előre meghatározott ideig (például pár napig, hétig, hónapig vagy évig). Ez a legtöbb számviteli bizonylatra elegendő időintervallum, egy, az utolsó évben megindított külső vizsgálat feltételezése esetében is. Különbség az előző esethez képest, hogy itt az aláírás hitelességét (sértetlenségét és az aláíró tanúsítvány adatait) a megőrzési idő végéig lehetséges ellenőrizni, mert az aláírás érvényességi időtartamán belüli ellenőrzéshez minden szükséges adat hitelesen a rendelkezésre áll az aláírás részeként. Ez a megoldás passzív módon biztosítja a hitelesség megőrizhetőségét.
- A hosszú távon érvényes aláírásokat több évtizedig meg kell tudni hitelesen őrizni, függetlenül a készítés eszközeitől és technológiájától. Ilyen lehet például

45 1/2018. (VI. 29.) ITM rendelet (Itmr.).
46 Itmr. 1. § (2) bekezdés.

egy elektronikus anyakönyvi kivonat vagy halotti bizonyítvány, egy közjegyzői közokirat, esetleg egy banki folyószámla- vagy hitelszerződés is. A megőrzési idő lehet előre definiált (például 20 év, 35 év, 50 év, 60 év stb.), de lehet előre meg nem határozott is. Különbség a rövid távú érvényességhez képest, hogy az őrzés során aktív tevékenységekkel biztosítják a hitelességet, ezért ez a módszer egy esetleges algoritmuskompromittálódás esetén is alkalmas a hitelesség fenntartására és folyamatos megőrzésére.

Lehetséges volt gazdálkodó szervezetek számára, hogy a rövid távú érvényességgel rendelkező aláírásaikat és kapcsolódó dokumentumaikat akár 11 évig egyszerűen megőrizzék. Ez az időtartam a digitális archiválásról szóló korábban hatályos 114/2007 GKM rendelet 4. § (3) és (4)-ből adódott,[47] mivel a jogszabály a 11 évnél rövidebb ideig megőrizni kívánt dokumentumok esetében egy minősített időbélyegzőt követel meg a legalább fokozott biztonságú elektronikus aláírás mellett. Technológiailag az van mögötte, hogy az időbélyegzett dokumentumokat jellemzően tovább lehet érvényesen megőrizni, mint a csak aláírással ellátottakat, mert az aláíró tanúsítványok két-három évig érvényesek, míg az időbélyeg-kibocsátók tanúsítványai 10-15 évig is használhatók lehetnek. A hosszabb ideig hitelesen megőrizni kívánt elektronikus aláírásokhoz be kell szerezni minden érvényességi adatot, és minősített időbélyegzőt kell elhelyezni azokon. A legutolsó érvényesítési és hitelesítési műveletet meg kell ismételni minden olyan eset előtt, amikor az archív időbélyegző algoritmusa kompromittálódik, vagy a kibocsátói tanúsítvány lejár. Ebből adódik, hogy az algoritmusok jelenbeli megfelelőségéből nem következik automatikusan azok jövőbeli megfelelősége, ennek biztosításához aktív tevékenységek lehetnek szükségesek.

A tanúsítvány szabványa

Elektronikus aláírás tanúsítványa alatt az eIDAS olyan elektronikus igazolást ért, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez (név vagy álnév) kapcsolja. Az aszimmetrikus kriptográfián alapuló digitális aláírás[48] területén két technológia terjedt el a világon, az egyik a PGP *(pretty good privacy),* a másik az X509, a korán felismert problémák ellenére.[49] Az ezekhez tartozó tanúsítványokat a vonatkozó szabványok részletezik:

- RFC 2440 *OpenPGP Message Format;*[50]
- ITU-T *X.509 Recommendation.*[51]

47 114/2007. (XII. 29.) GKM rendelet.
48 Az aláírást megalapozó cikket 1976-ban publikálta Diffie és Hellman (Diffie–Hellman 1976).
49 A problémák megfogalmazását lásd Ellison–Schneier 2000.
50 Callas et al. 1998
51 ITU 2016

Ezeken túlmenően nem szabványos megoldások is létrejöhetnek a technológiasemlegesség miatt, nem törvényszerű, hogy csak aszimmetrikus kriptográfián alapuló digitális aláírásokhoz létezik tanúsítvány. Lehetséges például biometrikus aláíráshoz is tanúsítványt generálni, vagy az is megengedett, hogy egy aláíráshoz ne is létezzen tanúsítvány.

A tanúsítvány típusa

A tanúsítványok típusait az eIDAS – a minősített tanúsítvány definiálásával – két kategóriába sorolja (minősített és nem minősített), ezenkívül elméletileg lehetőség van tanúsítvány nélkül is aláírást készíteni, hiszen az elektronikus aláírásnak a tanúsítvány megléte nem előfeltétele. A minősített tanúsítvány (eIDAS 3. cikk 15. pont szerint) olyan elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsátott ki, és amely megfelel az eIDAS I. mellékletében megállapított követelményeknek, ahol a melléklet a tanúsítványok tartalmára nézve fogalmaz meg további megkötéseket. A nem minősített tanúsítvány (eIDAS 3. cikk 14. pont szerint) olyan igazolás, amely az aláírás-ellenőrző adatot egy fizikai személyhez kapcsolja direkt (név) vagy indirekt (álnév) módon. Az álneves tanúsítvány mögötti személyt az azonosítási folyamat teszi láthatóvá az arra illetékes személyek előtt. Ha ilyen nincs, akkor az álnév mögött tetszőleges személy lehet.

Az aláírói tanúsítvány mellett a bélyegző tanúsítványt is meg kell említeni. A bélyegző tanúsítványa olyan elektronikus tanúsítvány, amely az érvényesítési adatokat egy jogi személyhez kapcsolja és egyen igazolja az érintett jogi személy nevét is (eIDAS 3. cikk 29. pont). Szintén létezik minősített kategória a bélyegzőtanúsítványok esetében is, amely alatt elektronikus bélyegző olyan tanúsítványát kell érteni, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS III. mellékletében megállapított követelményeknek (eIDAS 3. cikk 30. pont) – amelyek igen hasonlóak az I. mellékletben foglaltakhoz.

Továbbá az előző fejezetben foglaltak szerint az is lehetséges, hogy nincs tanúsítvány, mert az aláírás-ellenőrző adatot nem foglalják semmilyen tanúsítványba (ettől függetlenül továbbítható formában létrejöhet).

Az aláíró típusa

Az aláíróknál különbséget kell tenni a végfelhasználói és a szolgáltatói aláírók között, mivel más-más követelmények vonatkoznak az aláírás-létrehozó adatok védelmére, tulajdonságaira. A végfelhasználók típusai magukban foglalják a személyek aláíró tanúsítványait, mint például természetes személy, jogi személy természetes személy képviselője, kódaláíró vagy gépi aláíró, aki az aláírást elrendelő személy. A szolgáltatói aláírók kapcsán lehetséges beszélni gyökér-hitelesítésszolgáltatóról, közteshitelesítés-szolgáltatóról, időbélyeg-szolgáltatóról, archiválásszolgáltatóról és online tanúsítványállapot-

szolgáltatóról egyaránt, mind különböző kulcsokat használhatnak az aláírásaik elkészítéséhez.

A végfelhasználói aláírásokat meg kell különböztetni aszerint, hogy magánszemély vagy jogi személy az aláíró, az eIDAS szellemének megfelelően. A bélyegzők és aláírások közötti különbséget ebben a dimenzióban fogjuk megjeleníteni.

Az aláíró algoritmus

Az aláíró algoritmusok tekintetében mértékadó szabványként az aláíróalgoritmus-készletekre vonatkozó ETSI TS 119 312 szabványt[52] kell tekinteni. Algoritmusoknak lehetséges választani szimmetrikus kriptográfiát (például Advanced Encryption Standard, AES; Triple-DES Encryption Algorithm, TDEA, Escrowed Encryption Standard, EES, Secure Hash Standard, SHS, illetve Hashed Message Authentication Code, HMAC), vagy aszimmetrikus kriptográfiát használó elemeket (például az RSA,[53] DSS[54] és ECDSA különböző változatait).[55] Az aláíróalgoritmus-készletek minden olyan algoritmust tartalmaznak, amely az aláírás létrehozásához a gyakorlatban szükséges. Az aláíráskészleteket meg kell különböztetni az aláírási sémáktól, amelyek kizárólag az aláírásoldali algoritmusokkal foglalkoznak, és nem érintik az aláírandó dokumentumokat. A specifikált algoritmusok a kor adott műszaki fejlettségének megfelelően változhatnak, a digitális aláírásoknak létezhet kvantumkriptográfiai verziója is.[56] A kvantumkriptográfia megjelenését követően elindultak olyan kutatások is,[57] amelyek a megfelelő algoritmusok megtalálását és specifikálását tűzték ki célul a kvantumszámítógépek megjelenését követő időszakban is. A munkát az európai szabványosító testület is élénk figyelemmel kíséri.[58]

Az aláírás-létrehozó adat hossza

Az aláírás-létrehozó adatok hossza és a biztonság között esetenként jelentős összefüggés található – de ez nem automatikus, ami az algoritmusok matematikai hátteréből adódik. Jellemzően a faktorizáció nehézségén (vagyis egy megfelelően nagy szám szorzótényezőkre bontásának műveletigényén) múlik egy algoritmus gyakorlati biztonsága. Ha azokat megfelelően – például prímként – választják meg és további követelményeknek is megfelelnek (például megfelelő távolság), akkor az algoritmus biztonsága gyakorlatilag megfelelővé válik. Ezek a megfelelőségek a számítási

52 ETSI 2022
53 Az első ilyen algoritmust publikálta Rivest–Shamir–Adleman 1978.
54 NIST 1994
55 Az algoritmusok közötti különbségeket jól meghatározza Schneier könyvének 10. fejezetében: Schneier 1995, 213–229.
56 Lásd Daniel Gottesman és Isaac Chuang kutatási jelentését, amelyben megadnak egy digitális aláírási protokollt kvantum-kriptográfiai alapon (Gottesman–Chuang 2001).
57 Bernstein–Buchmann–Dahmen szerk. 2009
58 ETSI 2015

kapacitások fejlődésével[59] természetszerűleg folyamatosan avulnak, mivel mindig más számít „nehéz" problémának a gyakorlatban, attól függően, hogy mekkora a hozzáférhető elvi és gyakorlati számítási kapacitás. Az implementáció problémáját itt most nem érintjük, ebben a dimenzióban az aláírás-létrehozó adatok hossza az algoritmusok matematikai jóságától függ. A kulcsok hosszait minden esetben bitekben határozzák meg (például 128 bit, 256 bit, …, 1024 bit, 2048 bit, 4096 bit stb.).

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

Az aláírás-létrehozó adat tárolója

Az aláírás-létrehozó adat biztonsága szempontjából létfontosságú annak tárolása. Nyílt adatként sehol sem szabad megjelennie, ezért különböző kriptográfiai védelemmel ellátott szoftveres tárolókban (például Microsoft: certmgr.msc, Mozilla: keyx.db, PGP: private key block) vagy hardveres kulcstároló eszközökben, úgynevezett hardver security modulokban (HSM) vagy minősített aláírás-létrehozó eszközökben ([MALE] – *qualified signature creation device,* QSCD) jönnek létre és vannak eltárolva. Különbséget jelent az is a tárolók között, hogy a tárolási mód megengedi-e az aláírókulcs exportálását, tárolóból való kimásolását, vagy sem – a MALE jellemzően ezt meg tudja tiltani, míg a nem ennyire biztonságos aláírás-létrehozó eszközök (ALE) lehetővé tehetik ezt. Az eszközök lehetnek hardveres intelligens kártyák, USB-tokenek, SIM-kártyák vagy szoftveres konténerfájlok (például pfx, p7b, p12) is. A szoftveres konténerfájlok bármelyik infokommunikációs eszközön megjelenhetnek.

Az aláírások elhelyezkedése

Az aláírások elhelyezkedésekor meg kell különböztetni az egyszeres és a többszörös aláírást tartalmazó dokumentumokat, illetve a rajtuk elhelyezett aláírások egymáshoz viszonyított helyzetét, dokumentum – aláírás és aláírás – aláírás viszonylatban. Egyetlen egy aláírásnál csak az a kérdés, hogyan viszonyul az elhelyezkedése az aláírt tartalomhoz, míg többes aláírás esetén ezen túlmenően az aláírások egymáshoz képesti elhelyezkedése is vizsgálható elem. Az egyszerű *(single)* és a párhuzamos *(parallel)* digitális aláírások mellett létrehozhatók szekvenciális *(sequential)* aláírások is, amikor az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni. A párhuzamos aláírások elkészítésénél akár egyszerre több ember is aláírhatja a dokumentumot, de ezzel az aláírások nem épülnek egymásba, az aláírások egymás mellett léteznek és kezelhetők, ellenőr-

59 Schaller 1997

zésük tetszőleges sorrendben elvégezhető, hiszen csak az adott tartalomra vonatkoznak, az aláírt tartalmak hatókörébe a másik aláírás nem tartozik bele. Vegyes aláírásra példa lehet például a különböző szerződések ellenjegyzése *(countersigned),* amely a szerződő felek két párhuzamos aláírásából jön létre – ezek hatóköre külön-külön csak a dokumentum és ezeknek egy következő szinten való szekvenciális aláírásából áll, amely lehet az ügyvédi vagy közjegyzői ellenjegyzés. Az ellenjegyzés hatóköre kiterjed a dokumentumra és mind a két aláírásra egyaránt. Az aláírások a dokumentumhoz viszonyítottan felvehetnek beágyazott *(embedded),* beágyazódó *(embedding)* vagy elkülönült *(detached)* pozíciót is. Kérdésként merül fel, hogy az elhelyezkedési dimenziónak két aldimenzióját célszerű-e felvenni (aláírt tartalomhoz és más aláírásokhoz való viszony), vagy érdemes külön dimenzióként tárgyalni ezt a két esetet.

A tanúsítványok kibocsátója

A tanúsítványokat az Európai Unióban kibocsáthatja hatóságilag felügyelt nyilvános hitelesítésszolgáltató, aki szerepel az európai bizalmi szolgáltatók magyarországi listájában[60] (*trusted list,* bizalmi lista). Lehetséges zártkörű szolgáltatót igénybe venni, amelynek működése nem tartozik az eIDAS hatálya alá, így nem is kell teljesítenie a nyilvános szolgáltatásokra vonatkozó – esetenként igen szigorú – követelményeket. Ennek az a következménye, hogy a zárt körben létrejött szolgáltatásokhoz korlátozott jogi vélelem fűződik, de a felek egymás közötti megállapodásait az eIDAS nem kívánta korlátozni, azokat ettől függetlenül érvényesnek kell tekinteni. Ki lehet bocsátani tanúsítványokat otthoni felhasználásra is, például egy nyílt forráskódú szoftver segítségével, nyilvánvaló módon ehhez teljes bizonyító erőt fűzni nem célszerű, de bizonyítékként való megtagadása is ugyanilyen célszerűtlen lehet. A zárt körben működő bizalmi szolgáltatók megítélésénél a zárt kör meghatározása nagyon fontos.[61] Egy holland meghatározás szerint egy csoport zártnak minősül akkor, ha az alábbi négy követelmény teljesül:

- a kibocsátott tanúsítvány kizárólag a csoporton belül használható fel. A tanúsítványban ezt jelezni is szükséges;
- a tanúsítvány csoporton kívüli felhasználásáért a felelősség erősen korlátozott.
- a tanúsítvány használatát szerződésben korlátozzák;
- a tanúsítványt kibocsátó szolgáltatónak aktívan közre kell működnie a csoporton kívüli használat megakadályozásában (például technikai intézkedések vagy szerződésben foglalt szankciók bevezetésével).

Habár ez a meghatározás a csoport méretére vonatkozóan nem ad támpontot, helyes alkalmazásához a megfelelő különbséget az adott populáció és a csoport között egyértelműen meg kell határozni. Felmerülhet az a kérdés is, hogy lehet-e nemzeti

60 A lista közhiteles verziója itt található: www.nmhh.hu/tl/pub/HU_TL.pdf
61 FESA 2003

szinten zártkörű egy szolgáltatás, más szóval lehet-e csoport egy nagy létszámú biológiai populáció?

Az aláírások szerkeszthetősége

Egy szerkesztőségi rendszerben a hatékonyság növelése érdekben vetette fel Qian és Xu a szerkeszthető elektronikus aláírás fogalmát.[62] Gyakorlatilag arról van szó, hogy a szerző több opciót előzetesen hitelesít, amelyek közül a szerkesztő a későbbi történések függvényében kiválasztja az alkalmas opciót és azzal dolgozik a továbbiakban. A szerkeszthetőség dimenzióként való kezelését negligálja az a tény, hogy a szerkeszthető aláírásokon önmagában lehetséges alkalmazni ezt a modellt, fel lehet vetni és el is lehet vetni, mindkettő mellett szólnak érvek és ellenérvek. Jelen modellben ezt a tulajdonságot nem szerepeltetjük dimenzióként.

Az aláírások implementációs környezete

Az aláírás biztonságára az algoritmusok matematikai tulajdonságai mellett azok gyakorlati tulajdonságai is hatással vannak, ahogyan ezt az elmúlt időszak negatív példái megmutatták. Az elméleti jó tulajdonságok mit sem érnek, ha a gyakorlati implementáció gyengíti le az algoritmusokat. Két példa kívánkozik ide, az egyik a Heartbleed-probléma,[63] a másik az észt kártyaprobléma.[64]

A Heartbleed-problémát 2014. április elején tette közzé az amerikai számítógépes vészhelyzeti központ, amely szerint az érintett programverziók rosszul megírt memóriakezelési eljárásai miatt egy támadónak lehetősége van a felhasználó azonosítási adatait – ideértve a titkos kulcsait is – megismerni. A probléma nagyságát az okozta, hogy habár a hiba egy szűk és speciális területet, illetve programverziókat érintett (OpenSSL 1.0.1 – 1.0.1f, OpenSSL 1.0.2-beta), azonban ezeket a programverziókat számos alkalmazás és szervezet használta fel világszerte saját szolgáltatásainak megvalósításában. Az érintettségi adatok alapján a hiba szinte minden nagy Unix-alapú biztonsági termék gyártóját és felhasználóját érintette,[65] például az Amazon, az Aruba Networks, a CA Technologies, a Cisco Systems, a Debian GNU/Linux, az Extreme Networks, a Fedora Project, a Fortinet, a FreeBSD Project és a Gentoo Linux is érintett volt.

62 Qian–Xu 2011

63 Az általánosan használt OpenSSL programcsomag olyan hibája vált ismertté 2014 áprilisában, amelynek kihasználásával a támadó hozzáférhetett a memóriában tárolt titkos kulcsokhoz (Cybersecurity & Infrastructure Security Agency 2014).

64 Bruce Schneier arról írt a blogjában, hogy az észt kormány megszüntette 750 ezer észt állampolgári tanúsítvány érvényességét, mivel olyan sérülékenység vált ismertté 2017 szeptemberében, amelynek kihasználásával a támadó a nyilvános kulcs ismeretében ki tudta számítani a titkos kulcsot (Schneier 2017).

65 Lásd a VU#720951 alatt megjelent sérülékenységet, és az itt megnevezett gyártókat (Software Engineering Institute, CERT Coordination Center 2014).

2017. augusztus 30-án egy nemzetközi kutatócsoport olyan sérülékenységre bukkant az észt állampolgári kártya hardverében és szoftverében, amely lehetővé tette a támadó számára, hogy csupán a nyilvános kulcs ismeretében kiszámítsa a titkos kulcsot. A kutatócsoport nem megbízható elemek felhasználását kutatja megbízható infrastruktúrák kiépítésében.[66] A kérdés a technológiafüggés fennállásáig folyamatosan releváns, hasonlóan ahhoz, hogy milyen társadalmi intézményeket érinthet egy-egy kiterjedt technológiai probléma. A probléma felmerülését követően az észt kormány az összes tanúsítványt felfüggesztette (körülbelül 750 ezer tanúsítványról van szó), és felszólította az észt polgárokat, hogy a mobil-ID-megoldást használják a probléma megoldásáig.

A fentiek rávilágítottak arra, hogy ha egy termék egyik komponense súlyosan kompromittálódik, minden érintett és erre a komponensre épülő megoldás kompromittálódása várható, így annak ismerete, hogy a megoldások milyen komponensekre épülnek, alapvető fontosságú a biztonsági események kezelhetősége szempontjából.[67] Annak a kérdésnek a vizsgálata a metrika kialakításában megkerülhetetlennek látszik, hogy a programkönyvtár használata dimenzionális probléma vagy információbiztonsági kérdés. Az információbiztonsági vetületet erősíti Muha Lajos,[68] amikor a kritikus infrastruktúrák tárgyalásában felveti egyrészről a közigazgatási informatikát és kommunikációt megvalósító rendszereket (például ilyen a Kormányzati Hitelesítés Szolgáltató[69]) és a kritikus infrastruktúrák létfontosságú infokommunikációs rendszereit, illetve javasolja a védelmet kiterjeszteni azokra a szervezetekre is, amelyek az infokommunikációs rendszereket működtetik, vagy ezzel összefüggő szolgáltatásokat nyújtanak (ilyenek például a bizalmi szolgáltatók és a szabályozott elektronikus ügyintézési szolgáltatók is). Az észt probléma azonban arra is rávilágított, hogy egy információbiztonsági eseménynek az egész társadalomra kiterjedő hatását nem lehet az esemény információbiztonsági menedzselésével megszüntetni, más olyan elemekre is szükség lehet, amelyek technológiailag megalapozottan teszik lehetővé alternatív társadalmi intézmények kiépülését és működtetését.

Közigazgatási kiegészítések

Az elektronikus aláírások általános leírására alkalmas dimenziók nem használhatók kiegészítések nélkül a magyar közigazgatásban, így van értelme megkülönböztetni az elektronikus aláírások általános és közigazgatási célú felhasználását Magyarországon. Az eIDAS szerint nem kell a közigazgatási belső eljárások lebonyolítására szolgáló és ehhez bizalmi szolgáltatásokat igénybe vevő rendszerekre az eIDAS előírásainak vonatkozniuk, de a harmadik felek számára is elérhető nyilvános bizalmi

66 Mavroudis et al. 2017

67 Az RSA-kriptorendszer ellen kidolgozott támadásokat összefoglalóan ismerteti Dan Boneh (Boneh 1999) és Jinging Wang (Wang 2011).

68 Muha 2009

69 Lásd a Kormányzati Hitelesítés Szolgáltató honlapját (www.hiteles.gov.hu).

szolgáltatásokra nézve viszont ezeket kötelezően érvényesíteni kell. Az érvényesítés során azonban a közigazgatási szervek által nyújtott online szolgáltatások határokon átnyúló igénybevétele tekintetében a tagállamok nem követelhetnek meg a minősített elektronikus aláírásnál vagy bélyegzőnél magasabb biztonsági szintű elektronikus aláírást.[70] Ez azt jelenti, hogy a közigazgatás számára a minősített elektronikus aláírás és bélyegző lehet a legmagasabb szint, amelyet előírhat és befogadhat. A fokozott biztonságú elektronikus aláírások és bélyegzők elismerésénél szintén van kötelem. Ha egy tagállam egy közigazgatási szerv által nyújtott online szolgáltatás használatához fokozott biztonságú elektronikus aláírás alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie minden olyan fokozott biztonságú elektronikus aláírást, amely a végrehajtási aktusokban meghatározott, ideértve a nem minősített tanúsítványon vagy minősített tanúsítványon alapuló fokozott biztonságú aláírásokat, és a minősített elektronikus aláírásokat is.[71] Amennyiben csak a minősített tanúsítványon alapuló elektronikus aláírásokat vagy bélyegzőket kívánja egy tagállam elfogadni, akkor mentességet kap az ettől alacsonyabb szintű, nem minősített tanúsítványon alapuló fokozott biztonságú aláírások elfogadása alól, de a magasabb szintű minősített aláírásokat ebben az esetben is el kell fogadnia.[72]

Magyarországon a közigazgatás saját nyilvános kulcsú infrastruktúrát működtet annak érdekében, hogy elkülönítse az általános célra használható és csak a közigazgatás által felhasználható elektronikus aláírásokat. A közigazgatás számára a közigazgatási gyökér-hitelesítésszolgáltató elektronikus bélyegzőjével hitelesíti az elektronikus ügyintézést biztosító állami szervek által használt bizalmi szolgáltatáshoz tartozó tanúsítvánnyal szemben meghatározott követelményeknek megfelelő tanúsítványt kibocsátó bizalmi szolgáltató nyilvános kulcsát.[73] A szolgáltató működtetését a Nemzeti Média- és Hírközlési Hatóság (NMHH) látja el, köztisztviselők által. Egyszerűbben szólva, az NMHH által működtetett Közigazgatási Gyökér Hitelesítés-Szolgáltató (KGyHSz) hitelesíti felül minden olyan tanúsítványkibocsátó szolgáltatói tanúsítványát, amelyekkel a közigazgatásban használható tanúsítványokat szeretnének kibocsátani, akár piaci, akár kormányzati szolgáltatóról van szó.[74] Az Eüszr. az alábbi részterületeken fogalmaz meg előírásokat:

- az elektronikus ügyintézési célra, illetve közigazgatási célra használható elektronikus aláírással, elektronikus bélyegzővel és tanúsítványokkal szembeni követelmények;

70 eIDAS 27. cikk (3) és 37. cikk (3).
71 eIDAS 27. cikk (1) és 37. cikk (1).
72 eIDAS 27. cikk (2) és 37. cikk (2).
73 Eüszr. 3. § (1).
74 „A Közigazgatási Gyökér Hitelesítés-Szolgáltató (KGyHSz) a tanúsítvány kiadásával igazolja a hitelesítés-szolgáltató és a tanúsítvány adatainak egyezését, valamint hogy a megfelelő Hitelesítési rend, Szolgáltatási Szabályzat és Általános Szerződési Feltételek előírásainak megfelelőségét ellenőrizte, működését biztonságosnak tekinti és folyamatosan felügyelet alatt tartja. A felültanúsított hitelesítés-szolgáltató a tanúsítvány elfogadásával magára nézve kötelezőnek ismeri el a KGyHSz által kiadott szabályzatokat és a KGyHSz felügyeleti, ellenőrzési jogát." NMHH (é. n.)

- a kiadmányozásra nem jogosult személy (ügyintéző) által használt aláíráshoz tartozó tanúsítvánnyal szembeni követelmények;
- a kiadmányozásra feljogosított személy (ügyintéző) által használt aláíráshoz tartozó tanúsítvánnyal szembeni követelmények;
- az ügyintézési célú elektronikus bélyegző létrehozásához használt tanúsítvánnyal szembeni követelmények.

A közigazgatásban használható elektronikus aláírások terén meg kell említeni a kormányablakokban lehetővé tett biometrikus aláírások használatát is, amelyet a fővárosi és megyei kormányhivatal ügyfélszolgálatain, a járási (fővárosi kerületi) hivatal kormányablakaiban, illetve a települési ügysegédnél az elektronikus dokumentumok ügyfél általi hitelesítésére lehet az aláírás képi, dinamikai és íráserősségi adatainak elektronikus felvételezésére képes hitelesítő eszköz rendszeresítésével alkalmazni.[75] A rendszeresített eszközön történő aláírásnál az aláíró és a tárolt minták közötti egyezés vizsgálatának eredményéről tanúsított, zárt rendszer által kiállított, a dokumentumazonosítót tartalmazó, de az aláíró biometrikus jellemzőit már nem tartalmazó elektronikus igazolást a dokumentumhoz kell csatolni. Az ilyen elektronikus igazolással ellátott dokumentum teljes bizonyító erejű magánokiratnak minősül. Ez a fajta aláírás ebben a formában kizárólag a magyar közigazgatásban használható, így elfogadottsága is csak a magyar közigazgatásra korlátozódik. Ilyen korlátozott aláírási rendszert azonban bármelyik csoport számára létre lehet hozni annak ismeretében, hogy az általános célú biometrikus aláírás nem biztonságos[76], tehát célszerű erősíteni az aláírás környezetének biztonságát. A fokozott biztonságú biometrikus aláírás létrehozását nehezíti, hogy egyrészről zárt rendszerben nem lehetséges eIDAS szerinti fokozott biztonságú aláírást létrehozni – még akkor sem, ha a követelményeket mindenben teljesíti az adott aláírás, mivel egyrészről az eIDAS kizárta a hatálya alól a zárt rendszereket[77] és a szerződések alaki követelményeivel sem foglalkozik[78], másrészről nyilvános szolgáltatás biometrikus tanúsítványokra Európában 2017 év végéig nem indult el, ami ahhoz szükséges, hogy az eIDAS hatálya alá tartozó bizalmi szolgáltatás alapján jöjjön létre az aláírás. Az Eüsztv. szerinti fokozott biztonságú elektronikus aláírás létrehozásának nincs akadálya zárt körben sem, mivel az Eüsztv. kiterjesztő hatállyal bír a nemzeti jogban, így Eüsztv.-nek megfelelő fokozott biztonságú elektronikus aláírás már szélesebb körben készíthető, mint az eIDAS-szerinti fokozott biztonságú elektronikus aláírás. Tekintettel arra, hogy az Eüsztv. a fokozott biztonságú elektronikus aláírás definiálásakor kihivatkozik az eIDAS definíciójára, ebből

75 2010. évi CXXVI. törvény. 20/J. § (1).

76 MELASZ 2016

77 Lásd eIDAS 2. cikk (2): „E rendelet nem alkalmazandó a nemzeti jogszabályokon vagy meghatározott résztvevők közötti megállapodásokon alapuló, kizárólag zárt rendszerekben alkalmazott bizalmi szolgáltatások nyújtására."

78 Lásd eIDAS 2. cikk (3): „E rendelet nem érinti a szerződések megkötésére és érvényességére, sem más, alaki követelményekkel kapcsolatos jogi vagy eljárási kötelezettségekre vonatkozó nemzeti vagy uniós jogot."

adódóan, ha egy zárt körben létrejött elektronikus aláírás teljesíti az eIDAS-ban a fokozott biztonságú elektronikus aláírással szemben megfogalmazott követelményeket, akkor azt a magyar nemzeti jog alapján fokozott biztonságú elektronikus aláírásnak kell tekinteni. Ennek következménye, hogy zárt körben létrejött fokozott biztonságú elektronikus aláírás határon átnyúlóan akkor őrzi meg a fokozott biztonságú státuszát, ha az adott tagállam nemzeti joga szintén kiterjeszti ennek a definíciónak a hatályát az eIDAS rendelkezésein túlmenően. Az implementációk biztonságára azonban kiemelt figyelmet kell fordítani zárt és nyílt körben egyaránt.

Következtetések

Az elektronikus aláírás mérhetőségére és az egyes aláírási megoldások összehasonlíthatóságára vonatkozó igény a technológia elterjedésének természetes következménye. A technológia társadalmi integrációja jelenti azt a lépcsőt, amely során egy beágyazott, rejtett, jelentősebb tudás nélkül is felhasználható informatikai eszközből kifejlődhet az az intézményesült metódus, amely emergensen áthatja a digitális kormányzás, elektronikus közszolgáltatások minden egyes szintjét, és a teljes digitalizáció irányába hat. Az integrációhoz szükséges a technológiai vetület és a jogszabályi háttér harmonizációja nemzeti, regionális és globális szinten egyaránt, hiszen a globális elfogadhatóságnak egyaránt alapfeltétele a technológiai interoperabilitás és a nemzetközi jogi háttér megteremtése. Az tény, hogy a „traktorülésszabványok" harmonizációja nem elegendő az integrációhoz,[79] ennek szükségességét azonban nehezen lehetne megkérdőjelezni. Az eIDAS elsődleges célkitűzése az európai közszolgáltatások határokon átívelő támogatása (Európai Közigazgatási Tér), amelyhez egyrészről képesnek kell lenni egy másik tagállamban megfelelő módon létrehozott elektronikus aláírás elfogadására, másrészről képesnek kell lenni elektronikus aláírások létrehozására olyan módon, amely egy másik tagállamban is elfogadható. Az elfogadás alapjául az elfogadhatósági követelmények megfogalmazása és az adott gyakorlati megvalósítás tulajdonságainak a követelményekkel való összevethetősége szolgál, ennek egy lehetséges módszere a fentebb ismertetett modell, nevezhetjük az elektronikus aláírás és bélyegző dimenziómodelljének. A modell alkalmas numerikus számítások elvégzésének támogatására is, amivel az egyes elektronikus aláírási implementációk – és ezzel együtt az implementáció tulajdonságai – strukturáltan összehasonlíthatókká válnak, függetlenül az alkalmazott technológiától. A közigazgatási kitekintéssel pedig alkalmas eszközt adhat a magyar közigazgatás és közigazgatási alaki jog elméletének és gyakorlatának fejlesztéséhez is.

79 A kifejezés magyarázatát lásd Fazekas 2016.

Irodalomjegyzék

Bernstein, Daniel J. – Johannes Buchmann – Erik Dahmen szerk. (2009): *Post-Quantum Cryptography.* Berlin–Heidelberg, Springer. Online: https://doi.org/10.1007/978-3-540-88702-7

Boneh, Dan (1999): Twenty Years of Attacks on the RSA Cryptosystem. *Notices of the American Mathematical Society (AMS),* 46(2), 203–213. Online: www.ams.org/notices/199902/boneh.pdf

Callas, Jon et al. (1998): *Request for Comments: OpenPGP Message Format.* RFC 2440. Online: www.rfc-editor.org/rfc/rfc2440.txt

Cybersecurity & Infrastructure Security Agency: *Alert (TA14-098A), OpenSSL 'Heartbleed' Vulnerability (CVE-2014-0160)* Online: www.us-cert.gov/ncas/alerts/TA14-098A

Diffie, Whitfield – Martin E. Hellman (1976): New Directions in Cryptography. *IEEE Transactions On Information Theory,* 22(6), 644–654. Online: https://doi.org/10.1109/TIT.1976.1055638

Eckhart Ferenc: *Hiteleshelyek a középkori Magyarországon.* Budapest, MOKK, [1914] 2012.

Ellison, Carl – Bruce Schneier (2000): Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. *Computer Security Journal,* 16(1) 1–7. Online: www.schneier.com/academic/archives/2000/01/ten_risks_of_pki_wha.html

ETSI (2000): ES 201 733 V1.1.2 draft (2000-01). *Electronic Signature Formats.* Online: www.etsi.org/deliver/etsi_es/201700_201799/201733/01.01.02_50/es_201733v010102m.pdf

ETSI (2009): 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.* Online: www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf

ETSI (2010): TS 101 903 V1.4.2 (2010-12). *Technical Specification. Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).* Online: www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf

ETSI (2013a): TS 101 733 V2.2.1 (2013-04). *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).* Online: www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf

ETSI (2013b):TS 102 918 V1.3.1 (2013-06) *Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC).* Online: www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.03.01_60/ts_102918v010301p.pdf

ETSI (2015): *White Paper No. 8: Quantum Safe Cryptography and Security – An Introduction, Benefits, Enablers and Challenges.* Online: www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

ETSI (2022): TS 119 312 V1.4.2 (2022-02) *Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.* Online: www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.02_60/ts_119312v010402p.pdf

Fazekas Marianna (2016): Láthatatlan közigazgatási reformok – avagy hogyan befolyásolják életünket a traktorülésszabványok? *Pro Publico Bono – Magyar Közigazgatás,* 3. 70–79. Online: https://epa.oszk.hu/04200/04294/00015/pdf/EPA04294_pro_publico_bono_2016_3_070-079.pdf

Forum of European Supervisory Authorities for Electronic Signatures (FESA) (2003): *Working Paper On „To the Public" (Art. 3.3) and On Closed Systems (REC. 16), April 7, 2003.* Online: www.fesa.eu/public-documents/WorkingPaper-ToThePublic-20030407.pdf

Fréchet, Maurice M. (1906): Sur quelques points du calcul fonctionnel. *Rendiconti del Circolo Matematico di Palermo,* 22(1) 1–72. Online: https://doi.org/10.1007/BF03018603

Gottesman, Daniel – Isaac Chuang (2001): *Quantum Digital Signatures.* arXiv Quantum Physics. Online: https://doi.org/10.48550/arXiv.quant-ph/0105032

International Telecommunication Union, Telecommunication Standardization Sector of ITU (2016): *ITU-T Recommendation X.509. 10/2016.* Online: https://handle.itu.int/11.1002/1000/14033

Magyar Elektronikus Aláírás Szövetség Egyesület (MELASZ) (2016): *Állásfoglalás a biometrikus aláírások alkalmazása tekintetében.*

Magyarország (Hungary) (2022): *Trusted List.* Online: www.nmhh.hu/tl/pub/HU_TL.pdf

Magyarország Kormánya (2015): *Az új polgári perrendtartás koncepciója.* Online: https://2015-2019.kormany.hu/download/6/42/40000/20150224%20PP%20koncepci%C3%B3.pdf

Mavroudis, Vasilios et al. (2017): A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, (CCS 2017), Dallas, TX, USA, October 30 – November 03, 2017*. 1583–1600. Online: https://doi.org/10.1145/3133956.3133961

Muha Lajos (2009): Infokommunikációs biztonsági stratégia. *Hadmérnök,* 4(1), 214–224. Online: www.hadmernok.hu/2009_1_muha.pdf

National Institute of Standards and Technology (1994): *Federal Information Processing Standards Publication 186. 1994 May 19. Announcing the Standard for Digital Signature Standard (DSS).* Online: https://nvlpubs.nist.gov/nistpubs/Legacy/FIPS/fipspub186.pdf

National Institute of Standards and Technology (2013): *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. Online: https://doi.org/10.6028/NIST.SP.800-53r4

Nemzeti Média- és Hírközlési Hatóság (é. n.): *Közigazgatási Gyökérhitelesítés-szolgáltató fogalma és szerepe a Magyar Közigazgatás Nyilvános Kulcsú Infrastruktúrában.* Online: https://nmhh.hu/dokumentum/206170/kgyhsz_ismerteto.pdf

Qian, Haifeng – Shouhuai Xu (2011): Non-Interactive Editable Signatures for Assured Data. In *CODASPY '11: Proceedings of the first ACM conference on Data and application security and privacy, February 21–23, 2011*. New York, Association for Computing Machinery, 145–156. Online: https://doi.org/10.1145/1943513.1943533

Rivest, Ron – Adi Shamir – Leonard Adleman (1978): A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM,* 21(2), 120–126. Online: https://doi.org/10.21236/ADA606588

Schaller, Robert R. (1997): Moore's Law: Past, Present and Future. *IEEE Spectrum,* 37(6), 53–59. Online: https://doi.org/10.1109/6.591665

Schneier, Bruce (1995): *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C.* Hoboken, John Wiley & Sons, Inc. Online: https://doi.org/10.1002/9781119183471

Schneier, Bruce (2017): Security Flaw in Estonian National ID Card. *Schneier on Security blog,* 2017. szeptember 5. Online: www.schneier.com/blog/archives/2017/09/security_flaw_i.html

Software Engineering Institute CERT Coordination Center (2014): *OpenSSL TLS Heartbeat Extension Read Overflow Discloses Sensitive Information – Vulnerability Note VU#720951.* Carneige Mellon University. Online: www.kb.cert.org/vuls/id/720951

Takahashi, Kenta – Takahiro Matsuda – Takao Murakami – Goichiro Hanaoka – Masakatsu Nishigaki (2015): A Signature Scheme with a Fuzzy Private Key. In *Lecture Notes in Computer Science* 9092. 105–126. Online: https://doi.org/10.1007/978-3-319-28166-7_6

Tamás András (2001): *A közigazgatási jog elmélete.* Budapest, Szent István Társulat.

Vasvári György (2003): *Bankbiztonság.* Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság és Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék.
Wang, Jinging (2011): *Thirty Years of Attacks on the RSA Cryptosystem.* Online: https://cryptjwang.files.wordpress.com/2012/05/rsa_attacks.pdf

Jogforrások

1952. évi III. törvény a polgári perrendtartásról (Pp.)
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.)
2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (Hpt.)
2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (Eüsztv.).
2016. évi CXXX. törvény a polgári perrendtartásról (Pp.)
137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről
11/2020. (II. 7.) Korm. rendelet a felnőttképzésről szóló törvény végrehajtásáról
114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól
1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól (Itmr.)
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 (eIDAS)