PKI-MEGOLDÁS AZ ALÁÍRÓPADOKON A GYAKORLATBAN

Erdősi Péter Máté
Doktorandusz, NKE Közigazgatás-Tudományi Doktori Iskola
2018. október 4.

Tartalom

- Az elektronikus aláírás, az elektronikus bélyegző és a digitális aláírás
- A biometrikus aláírás és a biometrikus hitelesítés
- Aláírások jogilag elismert biztonsági szintjei
- Fokozott biztonságú elektronikus aláírás aláírópadon
- Következtetések
- Irodalomjegyzék

Az elektronikus aláírás, az elektronikus bélyegző és a digitális aláírás

- **elektronikus aláírás**: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ (eIDAS Rendelet 3. cikk 10.)
- **elektronikus bélyegző**: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét (eIDAS Rendelet 3. cikk 25.)

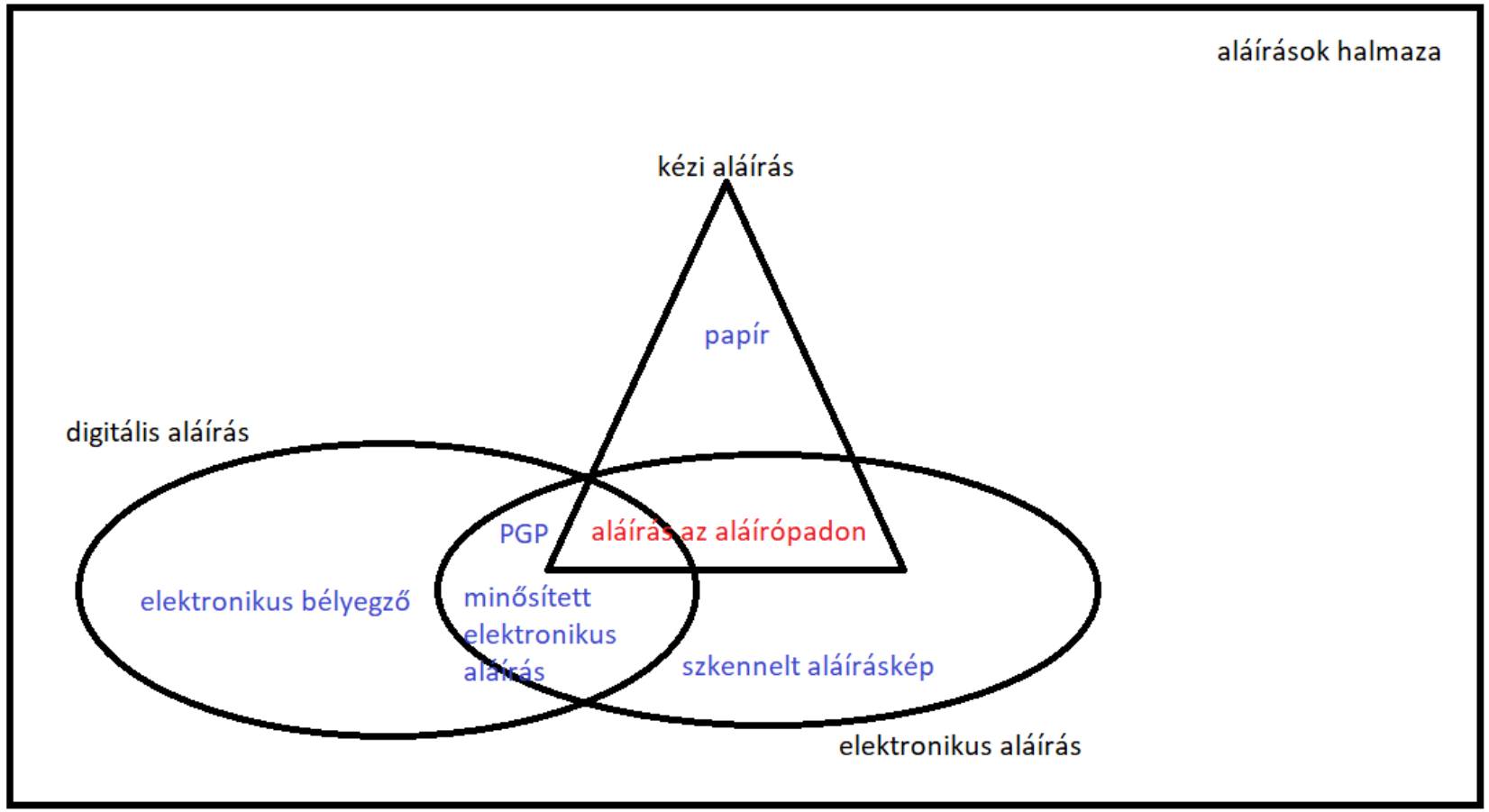
Az elektronikus aláírás, az elektronikus bélyegző és a digitális aláírás

- **digitális aláírás:** olyan adat, mely vagy hozzákapcsolódik egy másik adathoz vagy annak kriptográfiai transzformációja és lehetővé teszi a fogadó fél számára a küldő és a sértetlenség megállapítását oly módon, mely véd a hamisítás ellen (pl. a fogadó sem képes azt hamisítani) – ETSI EN 319 411-1 (April 2018), Clause 3.1 (Lásd ISO/IEC 7498-2 / Recommendation ITU-T X.800.

PKI, szimmetrikus kriptográfia, hash

- **digitális aláírás:** az adat kriptográfiai transzformációjának eredménye, mely – ha megfelelően implementálják – eszközöket nyújt a küldő hitelességének, az adatok sértetlenségének ellenőrzéséhez és az aláíró aláírásának a letagadhatatlanságához. NIST FIPS 186-4 (July 2013), Chapter 2.1

Az elektronikus aláírás, az elektronikus bélyegző és a digitális aláírás



Forrás saját ábra

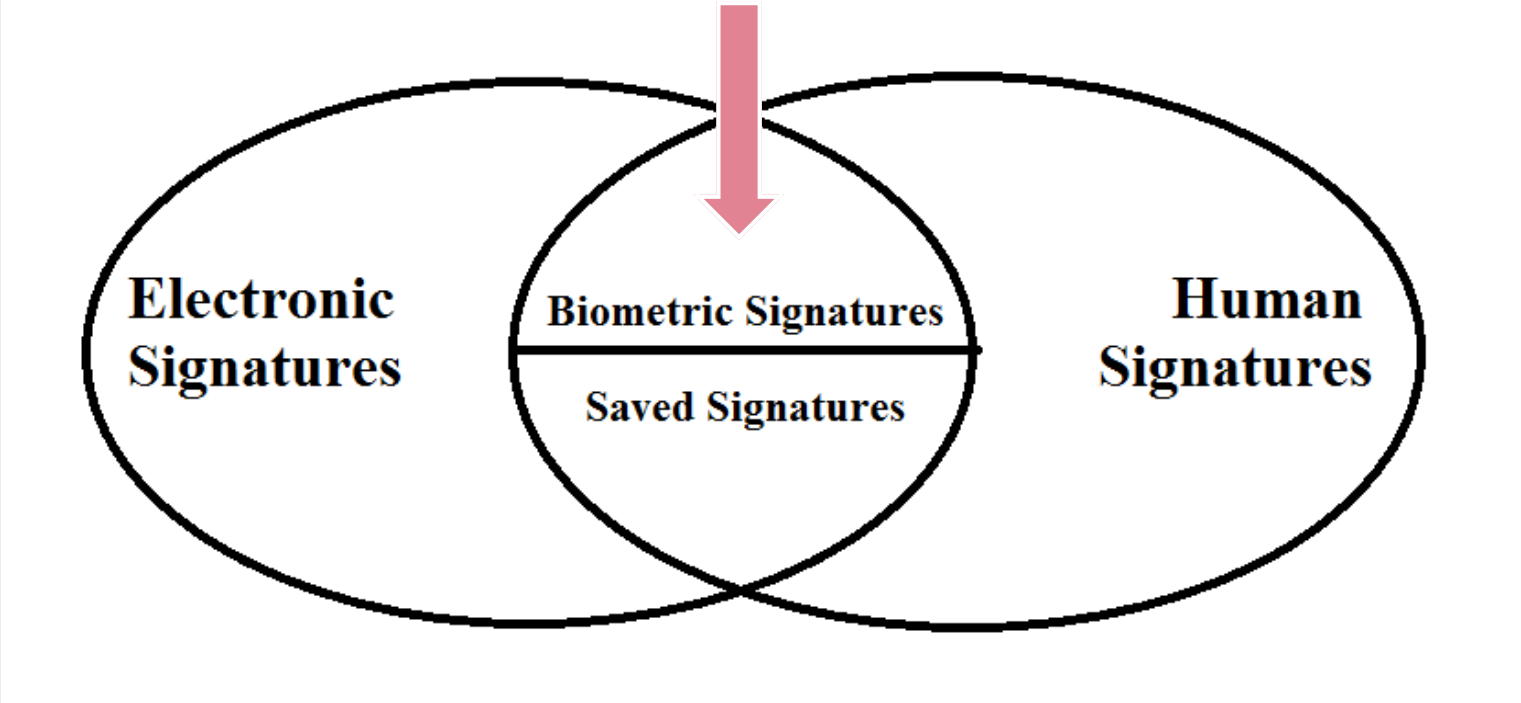
A biometrikus aláírás és a biometrikus hitelesítés

- **elektronikus azonosítás**: a természetes vagy jogi személyt, illetve jogi személyt képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata;
- **elektronikus azonosító eszköz**: olyan hardver- és/vagy szoftvereszköz, amely a személyazonosító adatokat tartalmazza, és amelyet online szolgáltatások céljából történő azonosításra használnak;
- **személyazonosító adat**: egy természetes vagy jogi személy vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő adat;
- **elektronikus azonosítási rendszer**: elektronikus azonosításra alkalmas rendszer, amelynek keretében természetes vagy jogi személy, illetve egy jogi személyt képviselő természetes személy számára elektronikus azonosító eszközöket bocsátanak ki;

A biometrikus aláírás és a biometrikus hitelesítés

- **hitelesítés**: olyan elektronikus folyamat, amely lehetővé teszi a természetes vagy jogi személy elektronikus azonosításának vagy az elektronikus adatok eredetének és sértetlenségének az igazolását; (eIDAS Rendelet 3. cikk 5.)
- **elektronikus aláírás**: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ (eIDAS Rendelet 3. cikk 10.)
- **érvényesítési adatok**: elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt adatok;
- **érvényesítés**: olyan folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus aláírás vagy bélyegző érvényes.

A biometrikus aláírás és a biometrikus hitelesítés



Forrás: Erdősi Péter Máté, Bartók Sándor P.: May the advanced biometric electronic signature be applicable in Public Administration?

Aláírások jogilag elismert biztonsági szintjei

eIDAS rendelet (910/2014 EU rendelet), Eübszt. (2015. évi CCXXII törvény)

- **elektronikus aláírás**: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ (eIDAS Rendelet 3. cikk 10.)
- **fokozott biztonságú elektronikus aláírás**: olyan elektronikus aláírás, amely megfelel az a 26. cikkben meghatározott követelményeknek;
- **minősített elektronikus aláírás**: olyan, *fokozott biztonságú elektronikus aláírás*, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás minősített tanúsítványán alapul;

Aláírások jogilag elismert biztonsági szintjei

26. cikk: A fokozott biztonságú elektronikus aláírásra vonatkozó követelmények

A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:

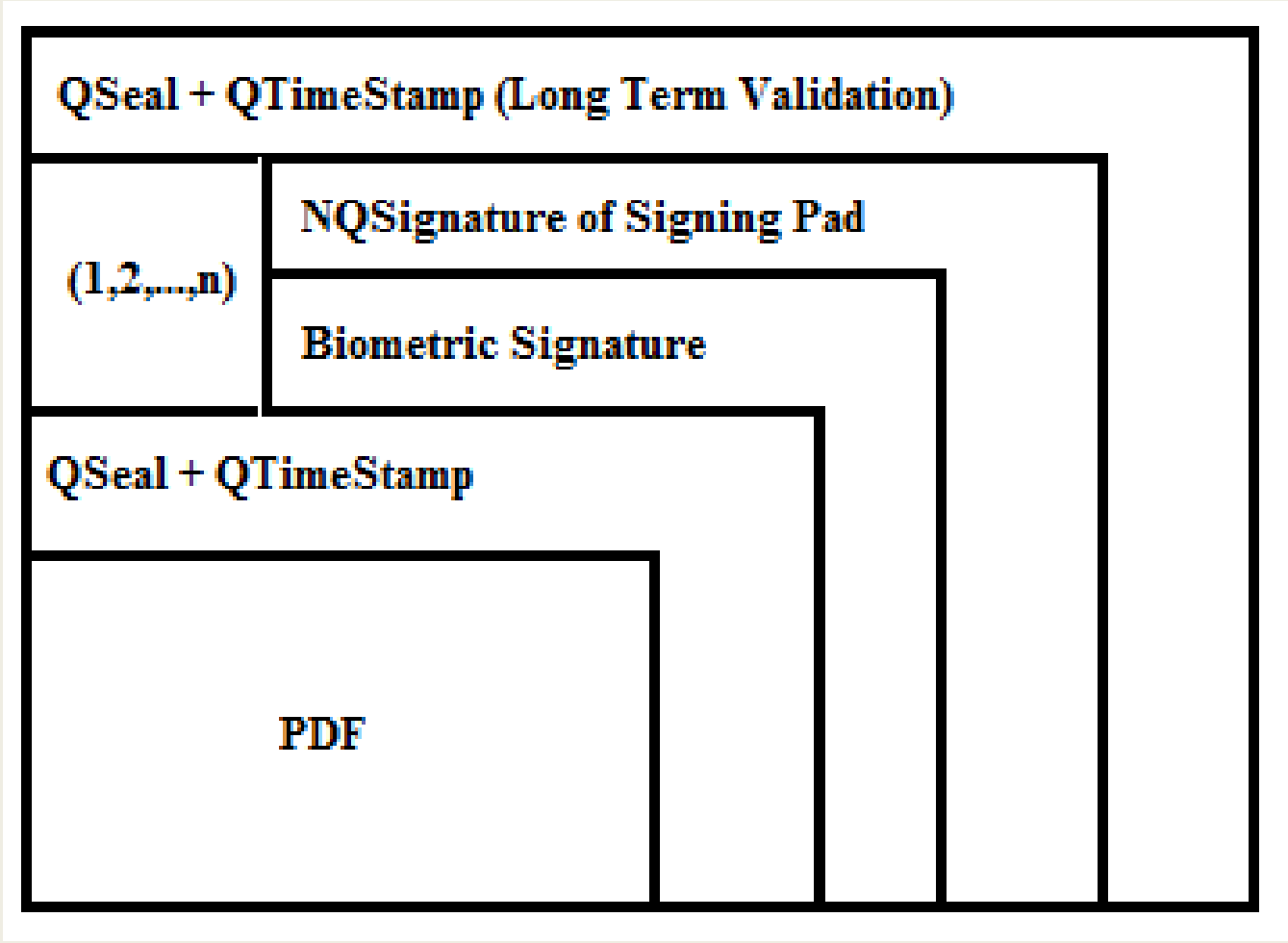
a) kizárólag az aláíróhoz köthető;

b) alkalmas az aláíró azonosítására;

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

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

Fokozott biztonságú elektronikus aláírás aláírópadon



Forrás: Erdősi Péter Máté: Advanced Biometric Electronic Signature in Practice: Lessons for the Public Administration from a Hungarian Case Study

Fokozott biztonságú elektronikus aláírás aláírópadon

Steps	Device
Creating document	Front-office banking system (PDF printer)
Preparing document for signing	Signature Device Controller on officer's desktop
Sealing and timestamping document	Crypto-server as back-office banking system
Signing document by client	Signing pad (sensor pad)
Signing document and client's biometric data by signing pad	Signing pad (crypto-module)
Sealing and timestamping document before archiving	Crypto-server as back-office banking system

Forrás: Erdősi Péter Máté: Advanced Biometric Electronic Signature in Practice: Lessons for the Public Administration from a Hungarian Case Study

Fokozott biztonságú elektronikus aláírás aláírópadon

- Miért nem minősített az aláírás?
  - *Mert szükséges lenne hozzá minősített tanúsítvány és tanúsított aláírás-létrehozó eszköz.*
- Felhasználható-e az aláírás készítéséhez bármilyen tárolt aláírás-biometria?
  - *Mivel az aláírópad az aláírás folyamatában nem teszi lehetővé az aláírás kívülről történő beinjektálását (erre lehet független tanúsítást szerezni), az aláírásnak ott kell elkészülnie az aláírópadon.*

Fokozott biztonságú elektronikus aláírás aláírópadon

- Tudok-e érvényes aláírást készíteni otthon, ha megveszek egy hasonló eszközt?
  - *Megtévesztésre alkalmas (pl. phishing) aláírást igen, de érvényeset addig nem, amíg nem sikerül szerezni minősített bizalmi szolgáltatótól a kibocsátó nevére szóló gépi aláíró tanúsítványt, amivel az eszköz hitelesíti az ott elkészült biometrikus aláírás és az aláírt dokumentum kapcsolódását. Ha a kibocsátónál történne meg a visszaélés, ehhez számos belső ellenőrzési eljárás és védelmi intézkedés létezik*

Fokozott biztonságú elektronikus aláírás aláírópadon

- Hogyan tudom ellenőrizni a biometrikus aláírást?
  - *Először is a saját aláírásunkat nem szoktuk ellenőrizni normál esetben, hiszen általában tudjuk mikor mit írunk alá. Ha azonban kétség merülne fel azzal kapcsolatban, hogy az aláírás valódi-e, többszintű ellenőrzési lehetőség van beépítve a folyamatba a vitás esetek eldönthetősége érdekében. Lehetőség van ellenőrizni a minősített bizalmi szolgáltató által hitelesített kibocsátó fél minősített aláírását vagy bélyegzőjét, az adott időpillanatban érvényes eszközök listáját, az adott időpillanat hitelességét és az aláíró fél aláírásának mondott aláírás biometriai jellemzőit is.*

Fokozott biztonságú elektronikus aláírás aláírópadon

- Fűződik-e teljes bizonyító erő ehhez az aláíráshoz?
  - *Mivel a biometrikus aláírás a fokozott biztonságú aláírás követelményeit teljesíti, és a minősített aláíráséit pedig nem, ezért magához a biometrikus aláíráshoz önmagában nem fűződik teljes bizonyító erő. A dokumentumokon lévő minősített aláírások, bélyegzők és időbélyegzők viszont már teljes bizonyító erővel rendelkeznek.*
  - *Megjegyzés: eltérő kormányzati megoldást definiál a 2010. évi CXXVI. Törvény 20/J. §-ban (a 2016: CIV. törvény 88. § (11) bekezdése iktatta be. A törvényt az Országgyűlés a 2016. október 11-i ülésnapján fogadta el. A kihirdetés napja: 2016. október 20.)*

Fokozott biztonságú elektronikus aláírás aláírópadon

(1) A fővárosi és megyei kormányhivatal ügyfélszolgálatain, a járási (fővárosi kerületi) hivatal kormányablakaiban, illetve a települési ügysegédnél az elektronikus dokumentumok ügyfél általi hitelesítésére az aláírás képi, dinamikai és íráserősségi adatainak elektronikus felvételezésére képes hitelesítő eszköz rendszeresíthető.

(2) Az (1) bekezdés szerinti eszközök rendszeresítése esetén a Kormány által rendeletben kijelölt fővárosi és megyei kormányhivatal az aláírás képi, dinamikai és íráserősségi adatait tartalmazó kormányhivatali aláírás-minta nyilvántartást vezet.

(3) A kormányhivatali aláírás-minta nyilvántartás a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény szerinti összerendelési nyilvántartással, annak szabályai szerint kapcsolati kóddal rendelhető a természetes személyhez, az aláírás-minta kiértékeléshez szükséges adatokon túl egyéb személyazonosító vagy biometrikus adatot nem tartalmazhat.

2010. évi CXXVI. törvény a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról 20/J. §

Fokozott biztonságú elektronikus aláírás aláírópadon

(4) A nyilvántartásba csak az ügyfél önkéntes beleegyezésével lehet mintát rögzíteni, az ügyfél az (1) bekezdés szerinti hitelesítési mód alkalmazására nem kötelezhető.

(5) Az (1) bekezdés szerint rendszeresített eszközön történő aláírásnál csak a mintával való egyezés ellenőrizhető, a vizsgálat eredményéről tanúsított, zárt rendszer által kiállított, a dokumentumazonosítót is tartalmazó elektronikus igazolást a dokumentumhoz kell csatolni. Az igazolás az aláírás dinamikai és íráserősségi adatait nem tartalmazhatja.

(6) Az (5) bekezdés szerinti elektronikus igazolással ellátott dokumentum teljes bizonyító erejű magánokirat.

(7) A kormányhivatali aláírás-minta nyilvántartás kizárólag az aláírások egyezőségének ellenőrzése céljából, az (5) bekezdésben meghatározottak szerint használható fel, a kormányhivatali aláírás-minta nyilvántartásból adattovábbítást – törvény eltérő rendelkezése hiányában – nem lehet teljesíteni.

2010. évi CXXVI. törvény a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról 20/J. §

Következtetések

- „Nem mind arany, ami fénylik.”
  - *Nem minden digitális aláírás lesz elektronikus aláírás (pl. bélyegző)*
  - *Nem minden elektronikus aláírás lesz kriptográfiai (pl. aláírópad)*
  - *Nem minden ETSI alapú digitális aláírás lesz a NIST szerint is az*
  - *Nem minden digitális aláírás lesz PKI alapú (pl. HMAC)*
  - *Nem minden elektronikus aláírás lesz minősített (pl. PGP)*
  - *Nem minden digitális aláírás lesz RSA alapú (pl. GOST R 34.10-2012)*
  - *Nem minden hitelesítés lesz aláírás (pl. vénaszkennelés)*
  - *Nem minden kézi aláírás lesz fokozott biztonságú (pl. szkennelt aláírásképp)*
  - *Nem minden teljes bizonyító erejű elektronikus aláírás lesz fokozott biztonságú elektronikus aláírás (pl. kormányhivatalok)*

Irodalomjegyzék

- Erdősi Péter Máté, Bartók Sándor P.: May the advanced biometric electronic signature be applicable in Public Administration? Central and Eastern European eIDem and eIGov Days 2017: Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?
  Budapest, Magyarország, 2017.05.04-2017.05.05.
- Erdősi Péter Máté: Advanced Biometric Electronic Signature in Practice: Lessons for the Public Administration from a Hungarian Case Study. Central and Eastern European e|Dem and e|Gov Days 2018: Conference proceedings.
  Budapest, Magyarország, 2018.05.03-2018.05.04.
- ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- KESSEM, L., Future of Identity Study – Consumer perspectives on authentication: Moving beyond the password. IBM Security, Cambridge, USA. 2018.

Irodalomjegyzék

- V. Dolmatov, A. Degtyarev : Request for Comments: 7091 – GOST R 34.10-2012: Digital Signature Algorithm, December 2013. https://tools.ietf.org/rfc/rfc7091.txt
- ORVOS, P., SELENYI, E., HORNYAK, Z., Towards Biometric Digital Signatures, in: Networkshop 2002 Conference, Eger, 2002.
- NIST, Special Publication 800-63-2, Electronic Authentication Guideline, USA, 2013.
- MOHHAMADI, S., ABEDI, S., ECC-BASED BIOMETRIC SIGNATURE: A NEW APPROACH IN ELECTRONIC BANKING SECURITY, In: International Symposium on Electronic Commerce and Security, 2008.
- MANN, D., GUPTA, S., SHARMA, A., AKHTAR, S., Digital Signature Using Biometrics, in: Proceedings of the World Congress on Engineering and Computer Science 2015 Vol I, San Francisco, USA, 2015.

Irodalomjegyzék

- MALIK, M. I., AHMED, S., MARCELLI, A., PAL, U., BLUMENSTEIN, M., ALEWIJNS, L., LIWICKI, M., ICDAR2015 competition on signature verification and writer identification for on-and off-line skilled forgeries (SigWIcomp2015), In Document Analysis and Recognition (ICDAR), 2015 13th International Conference on (pp. 1186-1190), IEEE, Nancy, France, 2015.
- Ed. KAISER, T., Jó Állam Jelentés 2017 (Good State Report 2017), Dialóg Campus, 2017.
- Magyar Elektronikus Aláírás Szövetség Egyesület: Állásfoglalás a biometrikus aláírásokról, Budapest, 2016.