MAY THE ADVANCED BIOMETRIC ELECTRONIC SIGNATURE BE APPLICABLE IN PUBLIC ADMINISTRATION?

Sándor P. Bartók[1] and Péter Máté Erdősi[2]

Abstract[3]
Electronic signature is a technology-neutral collective noun. Therefore, several different implementations compose the known types of electronic signatures. Many classifications may be defined, for instance from technological and legal aspects. In reference to acceptability, legal status of a given signature seems to be the most important attribute for transaction partners in the e-Administration. Full probative force is usually required by Public Administration and it is also a need for building trust between untrusted partners. It can be achieved by the well-known qualified electronic signature. The qualified signature creation method requires a secure qualified electronic signature creation device and qualified certificate, although in many cases a simpler but still secure signature is also able to fulfil legal requirements ensuring the validity of transactions. On the citizen side, device dependency and relating costs were considered the major obstacles against overall usage of electronic signature technology between 2005 and 2015. Our paper intends to argue that creating advanced electronic signature is not impossible by using the signatory's biometric data and it may also be an optionally client-friendly, but not a device-free part of the e-Administration, beside the citizen card.

1. Can the human signature be used for signature or not?

Electronic signature is a widely used and misused collective noun. Unfortunately, it has a lot of definitions, which have implied a lot of different implementations. It covers the normal (paper based) signature, which is scanned into a file, a typed name in the tail of an e-mail as well as the electronic signature which is created by cryptographically computed signature creation data stored on a secure qualified electronic signature creation device. Here we discuss electronic signatures, which are attached electronically to a document. The connection between signature and document may be both physical and logical. We have to mention that the meaning of electronic data has a tight interpretation - which is used -, and a wider interpretation - which is not used - nowadays. The tighter meaning contains only digital electronic data, and the wider meaning contains non-digital but electronical data also (e.g. autopen [4]).

There are two mainstream implementations of electronic signatures today. One is based on Public Key Infrastructure (PKI). The main idea is that the signer has two different keys combined mathematically, that is a key-pair. The first key is the private key, which is used to sign a document and it is secret for anyone else. The other key of this key-pair is the public key, as is in the name of this technology. It can be used by anyone to check whether the secret key's owner was the person,

[1] BSP&Partners Ltd., 1026 Budapest, Szilágyi Erzsébet fasor 89., bsp@bspp.hu
[2] National University of Public Service, Institute of e-Government, 1118 Budapest, Ménesi út 5., erdosi.peter.kdi@office.uni-nke.hu
[3] This paper has been written with the support and within the framework of KÖFOP-2.1.2-VEKOP-15-2016-00001 Public Service Development for Establishing Good Governance: Digital Governance and Digital Government Research Program.

who has signed the received document or not. Two trust models apply to the PKI technology, the "Web of Trust" and the "Trusted Third Party" model. In the second model, there must be a third party who confirms that the personal key and the physical person belong together. It supposes the correct identification of the natural person.

What about the second implementation? A number of companies implemented biometric signatures as a simple tool of gathering clients' consent or acceptance. The signature creation data may be other than a public key if eIDAS regulation[4] is really technology-neutral legislation. We argue in this paper that biometric characteristic or parameters can also be used as signature creation data corresponding to the "secret key" in the PKI world. In this case the signer's biometric parameter is used (and attached to) the document. In the most widely used solutions electronic picture of the human signature is usually the only applied biometric parameter for the signature. Another is the usage of the fingerprint, voice, palm print, iris or several other known biometric attributes that authenticate a natural person who is physically present [6]. We have used biometry long time ago. The present paper extends the concept of human signature to the signature created in any appropriate electronic devices. We state there are no legal and technical obstacles to advanced biometric signatures as a valid subset of biometric signatures. In this case, electronic signature does not mean only the graphical appearance as visible on a facsimile. We argue that proper biometric signatures shall contain additional features also in connection with a human signature to fulfil the requirements of advanced electronic signature. For instance, the data of dynamism, speed and pressure recorded with a very high sampling rate are unique for everyone. There is another side of the uniqueness. Theoretically nobody can create the same signature twice or more. However, it requires applying different method for the appropriate validation processes.

2. Definitions of electronic signature

We can group the definitions of electronic signature into two classes, legal and technological. We argue that both definitions can be applied to human biometric signatures. These two system of concepts are really different, legislators payed attention to use definitions in regulation be different from terms in existing technological standards. This leads to the statement that a legal definition may related to multiple technological terms, namely signature creation data may be several private keys (e.g. RSA 1024, RSA 2048, RSA 4096 [9], ECDSA 128 [2]) and a set of biometric attributes also.

2.1 Technical definitions and a classification

We use the following terms in the technical meaning indicated below:

1. implementation of electronic signature: special electronic data attached to a document usually in connection with undertaking a commitment and used for the authentication of the signatory in order to enable accountability of the undertaking of the commitment.

2. human signature: a signature created by a given person by a specific tool (pen or pencil) or perhaps by a finger.

[4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

3. biometric electronic signature: signature created by a human signature produced on an electronic device capable to record and process biometric data in digital form.

4. electronically saved signature: a human signature which is captured and stored by a device electronically.

The most important difference between biometric electronic signature and electronically saved signature is that saved signature means only a recorded and reusable version of human signature, while biometric signature contains other biometric data characterized by the human signature, which can be processed and used for validation. In this aspect, signature of an autopen belongs to the class of electronically saved signatures. The relations between these definitions is shown below.

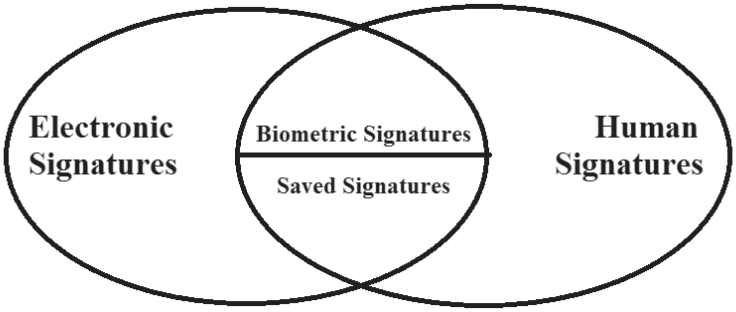

Figure 1. Electronic Signatures and Human Signatures (source: the Authors)

2.2 Legal definitions

After July 1 of 2016 the best starting point to analyse legal definitions of electronic signatures is the eIDAS Regulation in the European Union. eIDAS is the regulation for the electronic identification and trust services as issued on 23 July 2014. It repealed the Directive No. 1999/93/EC[5]. Between 1999 and mid of 2000 all Member States had created own slightly different legislation in national level, but all of them were replaced by eIDAS, which is mandatory for all Member States (and for all citizens) as an act. The eIDAS differentiates several levels of electronic signatures. We examine the following definitions of eIDAS:

1. electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

2. advanced electronic signature means an electronic signature which meets the requirements set out in Article 26". Article 26 contains four requirements: (a) it is uniquely linked to the signatory, (b) it is capable of identifying the signatory, (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

3. qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Similar definitions exist regarding to seals. In technological aspect, electronic seals and electronic signatures are the same, only the types of the subject are different. Signatory has been always a natural person, who is able to create electronic signature. A legal person can make only a seal according to the eIDAS terminology. Signing for legal persons is forbidden, sealing is allowed. However, Public Administration should be familiar with both concepts because public clerks and authorities may sign and seal documents, orders, decrees and any other electronic information in daily work processes, similarly to clients. As regards seals, biometric electronic signature can be created only by humans, and therefore the term of "biometric electronic seal" does not make sense. However, three different levels of electronic signatures are defined in eIDAS regardless the methods of implementation. Consequently, it should be noted that the definitions above are absolutely technology-neutral, i.e. independent from technologies. This means that the existence of advanced biometric electronic signature or qualified biometric electronic signature cannot be excluded theoretically, and it can be derived from law. On the other side, the content of biometric certificate has not been defined and standardized yet.

3. eIDAS in the EU

Why eIDAS is so important for Public Administration? There are two reasons. The eIDAS improves cooperation in the internal market by a commonly used and enforced legislation. In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognized by others. Mutually recognized electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities. One of the objectives of the eIDAS is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. It means that the first important aim of the Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.

The second important focus of the eIDAS is that the Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature. In the Member States authorities currently use different formats of advanced electronic signatures to sign their documents electronically. It seems to be necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically. Similarly, when competent authorities in the Member States use advanced electronic seals, it would be necessary to ensure that they support at least a number of advanced electronic seal formats. Consequently, according to the eIDAS, only such solutions can be used cross-border which are examined and accepted by affected Member States as it is defined by Article 27 and 37 of eIDAS. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognize advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and

qualified electronic signatures in at least the formats or using methods defined in the appropriate implementing acts[6]. Although the Commission has already defined the reference formats of advanced electronic signatures or reference methods where alternative formats are used by an implementing act[7], the biometric references are missing from these methods.

4. Legal Effect of Biometric Signature

There is a most general legal effect regarding to all electronic signatures, the non-repudiation as evidence: "An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures."[8] All Member States are bound to give a qualified electronic signature an equivalent legal effect of a handwritten signature. It was proved that the biometric signature is a variety of electronic signature, therefore the most general legal effect is considered valid in this case. National legislations may contain further rules for applying different electronic signature. For instance, Hungarian Act 237 of 2013 for credit institutions and financial enterprises allows signing contracts between clients and institutions with at least advanced electronic signature also[9]. The specified standards in the referred implementation act state that all specified signature formats in standards[10] fulfill the requirements of advanced electronic signature and seal. eIDAS accepts that technologies may change from time to time and existing standards may not eligible in the near future especially in the field of security. Therefore, it declares that IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices, and it should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organizational solutions for qualified electronic signature creation devices for which security standards may not yet be available. The level of security of such devices could be evaluated by using alternative processes only where such security standards are not available. The applicable processes should be comparable to the standards for IT security certification as their security levels are equivalent. It means that comparable alternative processes may use to ensure the achievement of related requirements. So, an alternative evaluation method for advanced biometric signatures may exist and can be accepted widely. The question arises whether an open biometric signing methodology can be defined or not [3].

In any case, a Spanish trust service provider declared that they implemented a voice based advanced biometric signature system[11]. There are no more evidences for proving this statement but examining the related underpinning evidences will be interesting. It seems to be the case that electronic signatures and advanced electronic signatures may be created using biometric methods. But there is a lack of related standards and description of evaluation processes in aspect of electronic signatures. Numerous standards are available regarding to recording, transporting and storing different biometric data such as written sign, fingerprint and voice. Processing technology of biometric data

[6] Article 27 (1) of eIDAS
[7] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[8] Article 25 (1) of eIDAS
[9] Paragraph 279 (1) of Act No. 237 of 2013
[10] CAdES, PAdES and XAdES
[11] http://certifiedsignature.eu/2016/09/25/firvox-first-voice-based-certified-electronic-signature/

is developed and used widely as digital data. Connection between this data and electronic signatures is not fully developed yet [7], [8]. The Hungarian Association for Electronic Signature has issued a professional opinion of applying and using biometric signatures, which declares that most of biometric signatures do not fulfill the requirements of advanced electronic signatures, and therefore require additional measures [1]. Researchers developed combined methods, which combined public key cryptography (PKI) with biometric data and they stated that the combination of PKI and biometrics can offer a more secure mechanism, in that private keys can be generated directly from the biometric scan [5].

Finally, we should mention a method which we commonly used in the past and is still generally accepted as handwritten signature in case of quick authentication and signature for long distance. Of course, this is the facsimile, in brief fax, with several benefits and a number of security problems. But we have to distinguish between biometric signature (electronically captured and attached human signature) and the human signature which is scanned and stored in an electronic file. Fax is a good example for the second one. Both private and public sectors have accepted this method, in spite of the fact, that it is susceptible to fraud. The reasons of the acceptance were the rapidity and effectivity of the method. Security risks seem to be manageable in most of cases.

5. Conclusions

We have attempted to discuss biometric signatures in three dimensions: the legal, technical and business aspects were discussed theoretically. On the other hand, we have examined some existing solutions to find good or bad examples of advanced electronic signatures. We have inspected the implemented biometric signature solutions of Hungarian Post Office Logistic Company, T-points of Hungarian Telekom, Vodafone, Deutsche Post and DHL. None of them comply with the requirements of advanced electronic signature as defined by eIDAS. These solutions have several advantages on business side, because these are very cheap and efficient as well as do not require any tools on the client side, but the usage of these may be limited because there are not any known court practices in this field, and therefore certain legal risks may occur by owners in case of a legal dispute, a litigation.

The biometric electronic signature can be used as normal electronic signature until creation and validation methods of advanced biometric signatures will be standardized and widely accepted in the EU. Without cross-border acceptance procedures it may be used only at national level if related legislations will be developed for Pubic Administration. This solution can involve citizens without e-signature capabilities to e-Administration in an easy and effective way. Effectivity can be enhanced by integrating e-signature and biometric signature devices in Public Administration.

Finally, the ultimate answer to the question, whether human signature can be used for signing in Public Administration, is “yes”. But it still requires significant developments and additional cost-benefit analyses.

6. References

[1] HUNGARIAN ASSOCIATION FOR ELECTRONIC SIGNATURES, Issue Of Applying Biometric Electronic Signatures, Budapest, 2016.

[2] LENSTRA, H.W. Jr.: Factoring Integers with Elliptic Curves, in: The Annals of Mathematics, 126/3, 1987, pp. 649-673.

[3] MANN, D., GUPTA, S., SHARMA, A. and AKHTAR, S.: Digital Signature Using Biometrics, in: Proceedings of the World Congress on Engineering and Computer Science 2015 Vol I, San Francisco, USA, 2015.

[4] MCCARTHY, J. and WINCHESTER, J.: The Autopen, in: Journal of Forensic Sciences, 18/4 (1973), pp. 441-447.

[5] MOHHAMADI, S. and ABEDI, S.: ECC-BASED BIOMETRIC SIGNATURE: A NEW APPROACH IN ELECTRONIC BANKING SECURITY, In: International Symposium on Electronic Commerce and Security, 2008.

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

[7] ORVOS, P., SELENYI, E. and HORNYAK, Z.: Usage Of Biometric Identification For Creating Authentic Digital Signatures, in: Networkshop 2001 Conference, Sopron, 2001.

[8] ORVOS, P., SELENYI, E. and HORNYAK, Z.: Towards Biometric Digital Signatures, in: Networkshop 2002 Conference, Eger, 2002.

[9] RIVEST, R.L., SHAMIR, A. and ADLEMAN, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, in: Communications of the ACM. 21/2 (1978), pp. 120–126.