COMPARATIVE ANALYSIS AND MEASUREMENT OF ELECTRONIC SIGNATURES CREATED BY NOTARIES IN EUROPE

PÉTER MÁTÉ, ERDŐSI[1]

ABSTRACT

The eIDAS Regulation established the general acceptance of qualified signatures in the European Union and defines several Implementation Acts to support this goal. These rules are more general and there are numerous attributes of electronic signatures, which are not legislated, therefore several different electronic signatures can be created in legal way. The question arises whether these differences are meaningful or meaningless in case of qualified and non-qualified signatures, and how these differences can be measured. We use the Electronic Signature Dimension Model for the visualization of the distances between different electronic signatures and try to answer this question.

This paper provides a comparative analysis between electronic signatures used by notaries in Romania and in Hungary through examination of relevant dimensions in connection with electronic signatures and defines a potential calculus for the determination of numeric distance between different but real signatures. All knowing technological and legal aspects of electronic signatures are evaluated, which can be derivable from other laws, the practice and literature.

Finally, this paper tries to explain differences, in the other words, the meaning of distances between different electronic signatures and argues the measurement of conditions in accordance with cross-border acceptance of qualified electronic signatures in the European Union.

POINTS FOR PRACTITIONERS

This paper describes one of the usable methods for evaluating and measuring electronic signatures both from theoretical (in thesi) and practical (in praxi) aspects, which can be used for comparing national laws, national solutions and any types of electronic signatures with each other. Defining an appropriate order of dimensions, lower level limits and upper level limits can be declared in all areas of electronic signatures and helps in definition or evaluation of relevant conditions in connection with cross-border acceptance of the electronic signatures.

KEYWORDS: measurement, electronic signature, e-Administration, e-Government, notary

1. THE DEFINITION OF THE 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 systems of the concepts are more or less 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 (Rivest et. al., 1978) and ECDSA 128 (Lenstra, 1987)) also.

The best starting point to analyze 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, which repealed the Directive No. 1999/93/EC. The eIDAS differentiates three levels of electronic signatures. We examine the following definitions based on eIDAS:

Electronic signatures:
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,

[1] PhD candidate at Doctoral School of Public Administration, National University of Public Service, Budapest, Hungary

(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.
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.

Electronic seals:
4. electronic seal means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity,
5. advanced electronic seal means an electronic seal, which meets the requirements set out in Article 36, which contains the following requirements:
(a) it is uniquely linked to the creator of the seal,
(b) it is capable of identifying the creator of the seal,
(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation and
(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
6. qualified electronic seal means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.

The main difference between signatures and seals is the signatory, signatures can only be created by natural persons and seals can only be produced by legal persons. In case of notaries, the examined notaries signed the documents as natural persons, therefore we examine signatures in this context.

If we examine the used definitions of the electronic signature from a wider perspective, very similar definitions can be found. In the USA, the following definition is used: „Electronic signature. -- The term „electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[2] Processes might also be accepted as signatures beyond to data. The UNCITRAL Model Law contains the following definition: „"Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message"[3]. In China, we can read a corresponding definition: "„electronic signature means the data in electronic form contained in and attached to a data message to be used for identifying the identity of the signatory and for showing that the signatory recognizes what is in the message"[4].

2. DIMENSIONS AND VALUES OF ELECTRONIC SIGNATURES

Dimension means a set of attributes from which only one can belong to an electronic signature in a unique manner. If an electronic signature is defined exactly, all relevant dimensions will have to know and the appropriate value from each dimension will have to assign to the given signature. The complexity is grown by the fact that between certain dimensions may occur dependencies. The independent dimensions are called orthogonal. This model of dimensions can be used for measuring electronic signature and seal technology, which may become a very important part of measuring IT security (Muha, 2010).
The examined dimensions – our dimension model of electronic signature – are developed by examination of listed standards and mentioned documents above. Thirteen dimensions has already been identified, which are the following:

1. dimension: Formalization (CAdES: CMS based Advanced Electronic Signature, XAdES: XML-based Advanced Electronic Signature and PAdES: PDF-based based Advanced Electronic Signature
2. dimension: Type of Signature (normal, advanced and qualified)
3. dimension: Probative Force (evidence at court, full probative force)

[2] US Electronic Signatures in Global and National Commerce Act 2000, SEC. 106 (5).

[3] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, Article 2 (a)

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

4. dimension: Complexity (basic, extended policy based, timestamped, complex, extended, extended long, archive, long term validity)
5. dimension: Validity Period (immediately, short time, long time)
6. dimension: Certificate Standard (PGP: Pretty Good Privacy, X509, biometric, other)
7. dimension: Type of Certificate (qualified, nonqualified, signature, seal)
8. dimension: Type of Signatory (end entity including natural person or legal person, code signer, automaton, certificate authority including root, bridge, intermediate or certificate issuer, time-stamping authority, archiving authority, online certificate status provider etc.)
9. dimension: Signature Algorithm (e.g. AES, TDEA, GOST, RSA, DSA, ECDSA)
10. dimension: Length of Signature Creation Data (usually given in bit – 128, 256, 1024, 2048, 4096...)
11. dimension: Holder of Signature Creation Data (encrypted container file, hardware token including Hardware Security Module (HSM), Qualified Signature Creation Device (QSCD) or simple Signature Creation Device (SCD), file storage as SIM card or pen drive)
12. dimension: Placement of Signatures (single, multiple including sequential, parallel, countersign, embedding, embedded, detached or mixed)
13. dimension: Type of Certificate Authority (public, closed group, home-made)
14. dimension: Specialty (e.g. none, Citizen Certificate, required by Public Administration)

Quantum-safe algorithms have not included into the list yet, but it can be performed immediately as the situation will require (Buchanan, Woodward, 2017). This model is capable to measure the social construction of quantum technology also. In defining the values of dimensions, I tried to apply the following three principles:

> PRINCIPLE 1: For different signatures, the model shall assign different values to the different signatures (based on the dimensions discussed above),
> PRINCIPLE 2: The distance between similar signatures must be such different that they can be clearly distinguished from very distinct signatures and from each other,
> PRINCIPLE 3: The proximity of similar signatures should give the opportunity to create clusters.

Using these principles above, the following values may be defined for each dimension:

D_i	Dimension	Description	Set of Values
D_1	Formalization	Encoding standard of the signature	CMS: 100, XML: 200, PDF: 300
D_2	Type of Signature	Security level of the signature	Normal: 100, Advanced: 1000
D_3	Probative Force	Legal effect of the signature	None: 0, Evidence: 100, Written form: 1000, Full probative force: 10000
D_4	Complexity	How complex is the signature	B: 50, BES: 100, EPES: 500, T: 1000, C: 2000, X: 3000, X-Long: 3500, LT: 4000, LTA: 4500, LTV: 5000
D_5	Validity Period (daíys)	How long the validity of the signature should be verified	number of days: 1, 2, …, 365, …
D_6	Certificate Standard	How to encode the certificate for creating the signature	none: 0, PGP key block: 50, X.509v2 attribute certificate: 500, X.509v3 PKI certificate: 1000
D_7	Signatory	Who is the signatory	natural person: 100, legal person: 150, government entity: 200, commercial group without legal personality: 250, other: 300
D_8	Signature Algorithm	What kind of signature algorithms is used	None: 0, Schnorr: 25, DES: 50, 3DES: 75, GHOST: 100, ElGamal: 200, Blowfish: 300, DH: 950, RSA: 1000, ECDSA: 7600, DSA: 8000
D_9	Length of Signature Creation Data	How long is the signature creation data in bits	bit: 0, 64, 256, 384, 512, …, 1024, 2048, … 4096 etc.
D_{10}	Holder of Signature Creation Data	Where the signature creation data is placed	None: 0, File: 100, Personal certificate folder: 500, ALE / SCD: 5000, HSM: 15000, MALE / QSCD: 20000
D_{11}	Relation of Signature	What is the relative position of the signature	single signature: 0, sequential: 100, parallel: 200, countersigned: 300
D_{12}	Placement of Signatures	where the signature is placed compared to the document	enveloped: 100, enveloping: 150, detached: 200

D_i	Dimension	Description	Set of Values
D_{13}	Type of Certificate Authority	who is the issuer of the certificate	none: 0, self-signed: 50, CA in closed group: 100, EV: 250, public nonqualified: 500, public qualified: 1000
D_{14}	Specialities	any local attribute	none: 0, Hungarian Citizen: 1, Trusted by the Hungarian Public Administration: 2

Table 1: The Value Set of Dimensions (created by the Author)

In this Electronic Signature Dimension Model, the value of an electronic signature is defined by the following formula:

$$V(ES) = \{D1(ES); D2(ES); \ldots, D14(ES)\},$$

where ES means the electronic signature, D_x refers one of the dimensions between 1-14, $D_i(ES)$ means the value of the given electronic signature in the i^{th} dimension (i=1, 2, …, 14), consequently V(ES) means a 14-dimension vector in this model. Casola et. al. propagated a similar matrix-based model to evaluate the security features of the Certificate Practice Statements (Casola et. al., 2007).

In the next step, we define the difference and distance of the electronic signatures, which have different meanings. The difference of the electronic signatures is interpreted as the difference of the length of the electronic signature vectors but the distance of two electronic signature vectors means the length of the difference vector. The difference (K) and the distance (T) can be defined by the following formulas:

$$K(V(ES1);V(ES2)) = \left| \sqrt{(D_1(ES_1))^2 + ((D_2(ES_1))^2 + \cdots + ((D_{14}(ES_1))^2} - \sqrt{(D_1(ES_2))^2 + (D_2(ES_2))^2 + \cdots + (D_{14}(ES_2))^2} \right|$$

and

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

3. METHODOLOGY

This paper is developed by using multiple research technics. Identifying and delimiting legal environment required descriptive research method which was based on analyzing of legal and technological documents. For creating the model of dimensions, legal and technological concepts could be synthesized by deductive ways and defined abstract categories. Comparison of the signatures resulted empirical conclusions regarding to qualified electronic signatures in the European Union and provided several opportunities to make final statements.

4. DISCUSSION

Applying the Electronic Signature Dimension Model to the Hungarian and Romanian Notaries' signature, we get the following values:

V(HUN.NOTARY) = { 200, 1000, 10000, 4500, 365, 1000, 100, 1000, 2048, 20000, 0, 150, 1000, 0 }

V(ROM.NOTARY) = { 300, 1000, 10000, 5000, 365, 1000, 100, 1000, 2048, 20000, 0, 150, 1000, 0 }

It is assumed that both signatures should be validated for a year and there is no special attribute connected to the signatures. For comparing the Notaries' signature with other signatures, a PGP (Diffie, Landau, 2007) and a Hungarian Qualified Citizen signatures are inserted into the table 2.

V(PGP) = { 100, 100, 100, 50, 365, 50, 100, 1000, 1024, 100, 0, 200, 0, 0 }

V(HUN.CITIZEN) = { 300, 1000, 10000, 5000, 3650, 1000, 100, 7600, 256, 20000, 0, 100, 1000, 1 }

Using the formula defined above, we can compute the following lengths of each electronic signature:

Signature	Value of the ES
Hungarian Notary's signature	22 992,3907
Romanian Notary's signature	23 096,5372
PGP signature (RSA-1024)	1 508,9072
Hungarian Qualified Citizen Signature with Long Term Validation	24 479,7475

Table 2: The Values of The Electronic Signatures (created by the Author)

The table highlighted that the Hungarian Citizen Signature earned the most points which is resulted by the Long Term Validation and the ECC algorithm. The difference between the notaries' signature is 77,14, which means that these two signatures are very close to each other, but both are far away from the PGP signatures in this model.

The distances of the signatures (lengths of the difference vectors) are presented by the following table:

T()	ES1	ES2	ES3	ES4
ES1	X	509,90	22750,73792	7604,27
ES2	509,90	X	22854,45418	7587,159548
ES3	22750,74	22854,45418	X	24004,70891
ES4	7604,27	7587,159548	24004,70891	X

Table 3: The Distances of The Electronic Signatures (created by the Author)

5. CONCLUSION

Beyond the trivial measurement of electronic signatures (as a binary number), a metric space can be defined. It is named as the Electronic Signature Dimension Model, which is based on the abstracted properties of electronic signatures or stamps and makes it possible to measure electronic signatures and electronic stamps in any environment. In the model, the measurement is based on the scalar data of the value sets of the dimensions, which allows the numerical representation of the values assigned to each electronic signature. Following the numeric representation, algebraic operations can be performed with the results, for example, it becomes available to evaluate technologically different solutions based on the calculation of average computations, the predictability of the differences or the values of the distances.

Measurability of electronic signatures contributes to increase efficiency in the exercise of public authority and enables the development of further empirical studies in the fields of state governance, public administration, local governments with the development of opportunities to receive authenticated opinions or documents electronically. Given that measurability is not limited to technical elements but also applies to social constructions, the model can also be applied in the legislation (for example, the numerical definition of the minimum level and maximum level of electronic signatures that can be used in a given context). This can reduce the negative impact of the technology independence on legal certainty. The exact specification of the values, in the other word, the measurement eliminates significant uncertainty in the given situation regarding the acceptability of a given electronic signature.

This model can be used globally, it would be an interesting use case to compare all electronic signatures used by notaries in most countries of the World. The flexibility of the model makes it capable to measure and compare any electronic signatures globally, independently from the physical place or the society of the creation. The comparison seems to be necessary if we have no globally accepted electronic signatures and different societies use different electronic signatures in the Public Administration.

6. REFERENCES

William Buchanan, Alan Woodward. 2017. Will quantum computers be the end of public key encryption?, Journal of Cyber Security Technology, 1:1, 1-22, DOI: 10.1080/23742917.2016.1226650.

Valentina Casola, Antonino Mazzeo, Nicola Mazzocca, Valeria Vittorini. 2007. A policy-based methodology for security evaluation: A Security Metric for Public Key Infrastructures. Journal of Computer Security, (2007), vol. 15, no. 2, pp.197–229. DOI: 10.3233/JCS-2007-15201.

Whitfield Diffie, Susan Landau. 2007. Privacy on the Line. The Politics of Wiretapping and Encryption. Updated and Expanded Edition. The MIT Press, USA, England. ISBN 978 026 20 4240 6

Lajos, Muha. 2010. Measuring IT security (Az IT biztonság mérése). http://real.mtak.hu/12938/1/1278547.pdf (accessed April 10, 2019)

Hendrik Willem, Lenstra, Jr. 1987. Factoring Integers with Elliptic Curves, in: The Annals of Mathematics, 126/3 (1987), pp. 649-673

Ronald L., Rivest, Adi, Shamir, Leonard, Adleman. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, in: Communications of the ACM. 21/2 (1978), pp. 120–126