NATIONAL UNIVERSITY OF PUBLIC SERVICE

Doctoral School of Public Administration Sciences

THESIS

Evolution, Characteristics and Measurability of Electronic Signatures in Public Administration

Péter Máté, Erdősi

PhD Dissertation

Supervisor: Dr. Lajos Muha, College Professor

Budapest, 2020

1 Subject and Objective

The concept of electronic signature is widely used and has now infiltrated everyday practice and law in most countries around the world. Consistent use of this term is not aided by the fact that the interpretation of electronic signature has undergone a number of changes over the last four decades. Moreover, it is often confused with the notions of digital signature, identification, authentication, and authorization in the field of the information security as well as with the notions of trust, reliance, authenticity, and trustworthiness in everyday language. A lot of aspects of electronic signature have emerged in legislation and its application. For example, an advanced electronic signature or a qualified electronic signature can be used in electronic processes. However, it is not easy to answer the question of which of the electronic signatures has full probative force or which is suitable for satisfying the formal requirements of written form. Since this is essential for usability, it may be one of the reasons it has become less common. These issues have been present since the beginning. As early as 2000, prominent experts asked the question whether there was one "single right" structure for all electronic signature. Assessing the risks involved, it was also put forward if “this infrastructure is needed at all”. There has been no clear answer to this question. It is certainly not possible to use Internet technologies in a reliable way without the use of some authentication technology, as in general the content and sender of a simple e-mail cannot be trusted.[1] The conceptual confusion is well indicated by the fact that pre-written clauses that have been automatically inserted at the end of e-mails have been called signatures since the beginning. If it was not made for signature purpose, but the sender of the letter shared his favourite quote, it does not fulfil the requirements of electronic signature and it is completely different from the concept of digital signature based on cryptography.

Since 2014, the concept of electronic signature has been defined in the eIDAS Regulation in the European Union, according to which an electronic signature is an electronic data that is attached to another electronic data and used by the signatory for signature.2 The concept of a signature is therefore based on the activity of the person intending to sign and the process that serves it, as it means a natural person who is carrying out an activity with the intention of signing, i.e. who is signing.

[1] Bob Thomas from BBN-TENEX raised the following question in RFC 644 in July 1974: „How can the recipient of a network mail message be "certain" that the signature (e.g., the name in the "FROM" field) is authentic; that is, that the message is really from whom it claims to be?”

[2] eIDAS Regulation 910/2014/EU by the European Parliament and the European Council (23 July 2014)

With these in mind, the electronic signature raises the following implicit questions for the entity wishing to interpret the signature:

1. is the signatory a natural person? (question about the subject)
2. can the signature data be attached to another data? (question about the connection)
3. on what electronic data did the signatory create the signature? (question about the linked object)

Until 2014, the signatures of legal persons and natural persons were not separated at the level of definition in Hungary. Both entities were able to create electronic signatures. Following the entry into force of the eIDAS Regulation, the European Union has distinguished the signature of legal persons from the signature of natural persons and introduced a special concept for it. This concept is an electronic seal and its creator can only be a legal entity. There is a strong similarity between the concepts of electronic signature and seal. Consequently, the above three questions can also be applied to the electronic seal.

Given that electronic signatures are accompanied by numerous additional attributes, the question arises as to whether it is possible to dimension the attributes of electronic signatures and along what principles. By dimensioning we mean primarily the divisibility of the set of electronic signatures and we cover it by defining the dimensions and recording the sets of values of each dimension. For social purposes, it does not seem reasonable to use an inductive definition of dimension as it was created for topology and described by van Dalen in 2005. It is, however, obviously necessary to define some metric on the defined dimensions for measurability. After clarifying the concepts and clarifying the properties of electronic signatures, it becomes possible to define an Euclidean metric space for describing electronic signatures, where the distance between two electronic signatures is always non-negative, and the distance is zero if and only if both descriptions contain the same properties. It also follows that two electronic signatures will be at a distance of zero not only if they refer to the same document being signed by the same signatory at the same time, i.e. the identical binary copy of itself, but also if the signatures can be described with the same abstract properties. For information technology, i.e. in practical implementation, there will not necessarily be the same two electronic signatures described with the same properties. In fact, there will typically be different binary representations in the same place in this descriptive space. If it exists, only such a metric can provide a comprehensive discussion of electronic signatures in theory (in thesi) and in practice (in praxi), both in society and in the law that regulates society.

Finally, the question arises as to whether the dimensions suitable for the general description of electronic signatures can be used in electronic administration without any

change, i.e. whether it makes sense to distinguish between the general and administrative usage of electronic signatures. Indistinguishability would be conditional on the public administration being able to issue and receive electronic signatures and electronically signed content without requiring specific rules.

The eIDAS Regulation has only partially obliged Member States to apply the general rules in public administration. For example, systems which support internal administrative procedures and use trust services should not be subject to the requirements of the eIDAS Regulation. However, all European regulations must be enforced for public trust services that are also available to third parties.

In Hungary, the client has the right to electronic administration if the governmental office developed and provides administration processes in electronic way, and electronic administration is a real alternative in matters of public authorities (see Ákr.) Except for life-threatening situations, the client can decide on the mode of the communication since 1 January 2018. The rules of electronic administration are defined by a separate decree. Government Decree 137/2016 (VI. 13.) covers organizations providing electronic administration, publishing, applicable trust services and the supervisory body (EüszR.). The Republic of Hungary has already exercised the right to define special regulations for the electronic management of administrative matters, which Hungary has been pursuing since 2012. This justifies the extension of our general-purpose investigations to the special regulations for public administration. Thus, in addition to the civic and private spheres, the public sector can also be involved in the analysis.

Taking a quick look at the authentication of constitutions, we find that the Magna Carta was signed by John I in England, the Golden Bull was authenticated with the gold seal of Andrew II in Hungary, and the Declaration of Independence was signed by each Founding Fathers with their own handwriting on page 4 of the document. Thus, signatures sometimes have special significance, and they are tied to place, time, and context. However, if it is not global, this significance can only prevail in the given society. From the point of view of the Hungarian public administration, the dissertation can be related to the following goals in "Zoltán Magyary Public Administration Development Program (MP 12.0) - for the salvation of the homeland and in the service of the public":

- Extension of e-government (3.2.3.1);
- Reducing administrative burdens (3.2.3.2).

2 Hypothesis, Objectives and Methods of the Research

Hypothesis: Electronic signatures can be measured by the attributes that describe them, and each type of signature can be univocally characterized in a suitable metric space.

A number of methodologies have recently been developed for measuring e-government. From the very beginning, the issue of the authenticity of electronic documents has played an important role in e-government, but we have had little information on the measurement or measurability of the solutions used.

The need to regulate electronic signatures also entailed the need for a precise definition of the concept. According to the definition introduced by eIDAS into the European law, an electronic signature is an electronic data that is attached to or logically associated with other electronic data and which is used by the signatory to sign. This definition does not automatically imply the measurability of electronic signatures (apart from trivial measurability), so the question can legitimately be raised whether it is possible to measure an electronic signature in a non-trivial way. In other words, is there one or more metrics that assigns a specific and unique value to each electronic signature and serves as a basis for comparing electronic signatures. The hypothesis can be accepted if there is at least one metric model in which all known electronic signatures can be placed and which assigns different values to different types of signatures. The hypothesis must be rejected if such a model cannot be created in theory or in practice. In this sense, my basic objective was not to demonstrate some kind of "goodness", but to be able to represent each electronic signature on the basis of its own characteristics in a suitable model that also allows to examine the differences between the various signature types.

In the course of the research, I reviewed the results and requirements for digital signatures, electronic signatures, and electronic authentications, from which I abstracted and defined the dimensions underlying the evaluation. Given that electronic signature is not a technical concept, but it is defined from technical content at social level, I also analysed the mechanisms necessary for the social embedding of technologies, together with the relevant legal background and social constructions. I also tracked its temporal appearances and changes as well as it conceptual (theoretical), technical (practical) and global (social) dissemination and usage. Having examined the spatial and temporal changes of electronic signature and the interactions of the changes, I came to the interpretation of the ontogenesis of electronic signature.

As the main method of my research I chose synthesis-based modelling. To determine the possible dimensions of the model, I surveyed the known and possible characteristics of electronic signatures, and then determined the elements that could be

taken into account as values in the dimensions summarizing each characteristic. To establish the measurability of the model, I defined a bijective mapping between the model and a finite part of a multidimensional Euclidean vector space and, to ensure measurability, I assigned numerical values to each element that could only be described as a categorical attribute. Next, I categorized the already recorded elements, named the categories as dimensions, and used statistical methods to examine the orthogonality of each dimension, i.e. its possible interdependence with other dimensions. Since the attributes are not continuous but discrete variables, and correlation between more than two variables had to be analysed, I chose CATPCA (Categorical Principal Components Analysis) as my statistical method.

Prior to the synthesis, I researched three sources to collect the elements to be used in the value set of the model:

- technical standards for the creation and verification of electronic signature,
- Hungarian, European and international legislation, and
- keyword based search in scientific databases and review of the results, highlighted certain attributes that appear in connection with the discussion of electronic signatures and seals, as well as some aspects of digital signatures.

The features explored, collected and validated as dimensions during the above were systematized using an abstract model. I also examined attributes that are not closely related to electronic signatures and decided whether to include them in the model or not. I then applied the model to empirical samples and made conclusions based on the evaluation of the outputs of the model. With the help of clusters developed from the obtained results, I also give an example of the applicability of the results of the model.

In a dedicated chapter of my dissertation, I analyse the applicability of handwritten signatures and digital signatures in advanced security level by presenting the legal background and its consequences. This leads to the concept of advanced biometric electronic signature, which can be integrated into the model. I show the necessity of the existence of the concept by deduction, and its feasibility by an empirical description of a prototype.

To examine the social integration and the dissemination of innovation, I also discuss the knowledge required for the social use of technological innovation and the potential diffusion mechanisms of innovation. For that, I analyse digital certificate penetration in Hungarian electronic society and arrive at conclusions which can be drawn from the data.

3 The Structure of the Dissertation and the Description of the Analysis

The properties of electronic signatures and seals and their measurability are discussed in seven main chapters. The structure of the dissertation accurately reflects the duality of the analysis, i.e. the need to approach the issue from a social and technological perspective. Following the introductory thoughts, Chapter 2 reviews the social embedding of electronic signatures, through a historical analysis of authenticity, the evolutionary issue of societies, and its measurable effects on technology, exploring the relationship between trust and authenticity, including a description of time-varying dynamics of authenticity, too. The chapter's approach is technological. This chapter seeks to answer the question of how signature technologies have emerged at the social level. The description of the special rules developed by the Hungarian public administration cannot be omitted either, as e-administration has been the largest engine for the use of electronically signed documents in the recent past, and it has enriched e-administration processes with a lot of new elements related to electronic signatures or to some of their features. This chapter also addresses the problem of the distribution of a large number of digital certificates, if they have to be produced for the citizens, as Hungary did not have such experience before starting the Governmental Certification Authority. To investigate the problem, a simplified model (R.M.) was created. The functioning of the model probably cannot be described with an analytical formula. Administrative additions have highlighted that clerks' preference is still personal interaction in the administration, but the presence of electronic administration is permanent, and the use of electronic channels is increasing. Discussing security issues concludes Chapter 2.

Chapter 3 describes the change in the concept of electronic signature over time. The focus is on society, this chapter seeks to answer the question of how technology has been able to respond to problems at the societal level. For this, I primarily review the emergence of the need for authenticity and its connection with writing. To present the development, I have created a chronological list of the events in Hungary that I consider to be important in connection with electronic signatures. From this list a comprehensive picture of the temporality and succession of Hungarian events emerges. The legal background is an important social aspect. Another important factor in the trust in institutionalized technological systems is the degree of sanctioning misuse, i.e. the protection of the interests of legitimate users, which is also presented in Chapter 3.

In Chapter 4, I turn to the thematic discussion of the characteristics of electronic signatures and seals and select the possible dimensions. Exploring the independence or interdependence of the dimensions is an important feature of the model, so I present the identified dependencies in a table. After discussing the dimensions, the dimension model of the electronic signature is created. Examining the possible values and the clarity of the

representation, the following formula can be used to determine the value of an electronic signature (seal) in a way that gives the same value to the same type of signature:

$$V(ES) = \{D_1(ES); D_2(ES); \ldots, D_{14}(ES)\},$$

where ES is the electronic signature/seal, D_x is the 14 dimensions of the signature/seal, and Di (ES) is the value of the ES signature/seal for that dimension (i = 1, 2,…, 14), so V (ES) it will represent a vector of fourteen natural numbers in this model. The individual dimensions and the explanation of the values are shown in the table below. The value sets are described in detail in the dissertation.

D_i	Dimension	Description
D_1	Formalization	Designates the coding standard of the signature
D_2	Signature Type	Security level of the signature (basically Y/N)
D_3	Probative Force	Probative force of the signature
D_4	Complexity	Designates the details of the signature, including the policies, time, verification data and time stamps
D_5	Validity Period (days)	Indicates the period of time, expressed in days, for which the verification of the signature must be possible at any time
D_6	Certificate Standard	Specifies the format in which the certificate for the signature is created
D_7	Type of Signatory	Indicates the category of the signing entity
D_8	Signature Algorithm	Lists known and widely used cryptographic signing algorithms
D_9	Length of Signature Creation Data	The length of the signature-creation data in bits
D_{10}	Storage of Signature Creation Data	Specifies the location and method of storing the data used for signing
D_{11}	Relation of Signature	Describes the relative position of a signature for multiple signatures
D_{12}	Placement of Signature	Records the location of signatures relative to signed data
D_{13}	Certificate Authority	The type of certificate issuer
D_{14}	Special Attributes	Additional features (e.g. citizenship, which can be used in Hungarian public administration)

1. table: The electronic signature dimension model (source: own table)

In determining the values of the dimensions, I try to adhere to following three principles:

- PRINCIPLE 1: for different signatures, the model shall assign different values to the signatures (taking into account the types discussed above),

- PRINCIPLE 2: the distance between similar signatures should be such that they can be distinguished from very different signatures and from each other,
- PRINCIPLE 3: the similarities of near signatures should allow for the creation of clusters.

Based on these three principles, the value sets of the dimensions are defined. Representing the "goodness" of each value is not intended.

In Chapter 5, I show how each signature/seal is represented in the electronic signature/seal dimension model, and what measurements can be made between different types of signatures and seals. I start the development of measurability with theoretical considerations, followed by a practical demonstration of the operation of the model on real examples. By the distance of two electronic signatures we mean the following value (the formula for the distance of the vectors is made based on the mathematical formula commonly used in n-dimensional Euclidean space):

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

denoted by T(V(ES1);V(ES2)). The absolute values of the vectors are used to interpret the differences. The difference between two electronic signatures is the following (absolute) value below (the formula was written in the n-dimensional Euclidean space based on the mathematical formula commonly used to calculate the length of vectors)

$$\left| \sqrt{(D_1(ES_1))^2 + ((D_2(ES_1))^2 + \cdots + ((D_{14}(ES_1))^2} - \sqrt{(D_1(ES_2))^2 + (D_2(ES_2))^2 + \cdots + (D_{14}(ES_2))^2} \right|$$

denoted by K(V(ES1);V(ES2)).

In addition to the length values of the vectors, the length of the difference vectors of the vectors can also be used to group electronic signatures, as it shows the similarities and differences from the vectors belonging to each signature in a slightly finer resolution.

Chapter 6 presents the technology independence of European regulation and, as a consequence, it interprets the concept of an enhanced biometric electronic signature based on the characteristics of biometric handwriting. The relevant standards define numerous technological solutions that meet the higher-level requirements for advanced electronic signatures based on the use of a cryptographic secret key. In the paper-based world, the signature is linked to the signatory's handwriting. Its acceptance has not been questioned since civil society. Methods and procedures have been developed for examining

questionable signatures. The question arises as to whether there is an electronic signature in the electronic world that is based on the signer's handwritten signature on the one hand and meets the higher-level requirements for the advanced electronic signature on the other. In response to this question, I present a practical example (prototype) used in the business world that was implemented in a banking environment. After discussing the advanced security signature, I determined a possible structure for the certificates that can be associated with such signatures. My conceptual proposal for the content of a non-qualified biometric signing certificate was created by mixing an X.509v3 signing certificate and an X.509v2 attribute certificate without a public key, taking into account the specialties of the biometric signature and its environment.

In Chapter 7, I briefly discuss existing, possible and recommended forms of knowledge transfer that facilitate the use of electronic signatures/seals. Assuming that at least the dissemination of knowledge needed to verify an electronic signature is desirable, one element of the problem is that signature techniques are not taught at the undergraduate level and user-level education is not widespread enough to reach critical mass. In other words, the education of electronic signature has been institutionalized at a low level in Hungary. The question is, how can the necessary knowledge be disseminated rapidly, which would result in effective use, if undergraduate courses are not or hardly available, and if voluntary forms of accredited trainings (ECDL) can only accommodate 20.000-40.000 candidates per year? I believe the answer is to be found in knowledge management tools.

4 Summary Conclusions

4.1 The Measurability of Electronic Signature

Ensuring the authenticity of electronic communications and data throughout their life cycle is essential for the functioning of the digital state in order to prevent disasters, pursue sustainable development into a new dimension, support the explosive development of the digital world, and manage change in the international security environment. The Estonian example has shown very emphatically that e-government based on a single technological solution is vulnerable, but the vulnerability can be significantly reduced by specifying coexisting alternatives. The condition of the equality of the coexisting solutions is that they have the same or similar values. The dimensional model of the electronic signature makes it possible to empirically examine economic/security aspects in the research of the institutional conditions of public management, focusing on the development of transactional security. Furthermore, the implementation and sustainability of security is essential, as well as a legal obligation both in Hungary and in the European Union, in the course of which trust plays a key role in the spread of hacktivism during the wars without a declaration of war. The use of an advanced electronic signature or equivalent technological solution is essential to ensure overall authenticity. Maintaining authenticity also requires preventive, detective, and corrective controls. The dimensional model of electronic signature may be considered a detective control for threats against the digital state and protection against cyber security disasters.

4.2 The Applicability of Biometric Signatures

Recognizing the existence of an advanced biometric signature may also allow the creation of a qualified biometric signature (following the certification of the required signing device and the international standardization of the biometric signature certificate), which would enable the creation of electronic hand-writing equivalent to traditional hand-writing at the national level and in the EU. The presented solution, complemented by a qualified certificate and a certified signing tool, would already be able to provide a fully secure electronic signature in e-government for citizens without electronic signature. The solution could lead to a reduction or even disappearance of the impact of the digital divide, it could be independent of digital poverty and it could be applied at the national level in all areas of e-participation. By using an advanced biometric signature, all citizens, regardless of technology and knowledge, can be involved in e-government. Thus, based on a qualified electronic or handwritten signature, paperless e-government could be fully implemented.

5 New Scientific Findings

H1. Electronic signatures can be measured by the features that describe them, and each type of signature can be univocally characterized in a suitable metric space.

T1. In addition to the trivial measurability of an electronic signature (displaying them as binary numbers), a metric space, the dimensional model of the electronic signature, can be defined, which is based on abstract properties of electronic signatures and seals, and which makes electronic signatures and seals measurable in any environment. In the model, the measurement is based on the scalar representation of the value sets of the dimensions, which allows the numerical representation of the values assigned to each electronic signature. After the representation, the results can be used for algebraic operations, such as the calculation of the average, or the calculation of difference or distance. With the definition of the values, technologically different solutions may be evaluated.

If we wish to formulate the results of the model using a systematic approach, then the effects of electronic signatures in all related social systems can be expressed explicitly with the help of the model, but the value sets of dimensions applicable in each society should be developed from the bottom up. If we can fit every single value that any society uses into the model, then the result can be used globally. If we can include all historical values in the model, then the change in the values over time will also be displayed in the model. This means that our model provides a generalized tool that makes it possible to measure the connection points, depth, and nature of a system that can be defined by the abstract properties of electronic signatures as objects for all other systems involved. To explore the relationships, it is necessary to systematically examine the effect of signatures with social science tools (weak social construction, strong social construction, or technological determinism theories may be useful here). This is because the model needs categories and values within categories (such as the legal guarantees for different types of signatures in different societies). The electronic signature system or systems can be considered as systems or subsystems, which may raise questions in themselves, but from a social point of view it seems more important to examine how the electronic signature technology system is related to and affects other social systems and vice versa. and what social systems affect it and how. An example of the first is the public utility of e-government and all its relevant subsystems, while the second is a well-defined field of application of normative, administrative law. András Nemeslaki's suggestion thus seems valid also in the case of electronic signatures as a collaborative, ubiquitous ICT system. That means that examining the effects of signatures on the basis of social construction

theories can be of great help in building and maintaining an Internet of authentic things and tools that meet both scientific and pragmatic needs (IoT “Internet of Things”, IoD “Internet of Devices”). Here I think, for example, of deciding the question of who can be held liable if a transport drone causes an accident or if two devices attack each other and cause physical damage.

Another key issue of the social aspect is the digital divide, which also has an impact on electronic signatures. Intervention at all three levels of the digital divide, as summarized by Szilárd Molnár (access, use, quality of use), is needed to enable electronic signature techniques to be present in everyday life, especially in e-government. The conclusions of Mihály Csótó on information poverty are also relevant. According to Csótó, access to or the lack of access to technology has a significant impact on societal actors. Furthermore, technology increases inequalities rather than eliminates them. Finally, information poverty in general cannot be defined, it only makes sense to measure this concept in a specific context on the basis of a given system of norms. As a result, the use of electronic signatures can further deepen the digital divide. Information poverty can be interpreted in the context of electronic signatures, and the dimensions outlined above can help to map its contexts more accurately. The question is what is needed to reduce the number and proportion of the population in the negative half of the digital divide relative to the positive side. Unless significant user knowledge can be assumed, the use of biometric signatures can be a good choice, as it does not require knowledge or tools on the part of the user, yet the user can enter the digital world. Looking further ahead, undergraduate education is an excellent tool for introducing electronic signature technologies on both sides of the digital divide. By the quantitative distance between e-signature knowledge and e-administration needs, digital gap can also be measured. This argument shows that the evaluation of electronic signatures and seals, based on the developed model, can be applied in an automated way in public administration for regulatory, planning, implementation, educational and monitoring purposes.

6 Practical Application of the Research Results

6.1 Measurability of the Electronic Signature

The measurability of electronic signatures contributes to increasing efficiency in the exercise of public administration, and by developing electronic means of expression, it enables further empirical research in the fields of science of state, public administration, local governments, national defence and law enforcement. Given that measurability is not limited to technical elements but also applies to social constructs, the model can be applied in legislation (for example, through the numerical definition of the minimum and maximum levels of electronic signatures that can be used in a given context). This will reduce the negative impact of technology independence on law, as the specification of a given value eliminates significant uncertainty about the acceptability of a given electronic signature in a given situation. The measurement of electronic signatures before their introduction into e-government services could be done already at the planning stage, e.g. as part of impact assessment, which could prevent in particular the high risk "weak technology - strong legal assurance" or the expensive "strong technology - weak legal assurance" situations.

Further development opportunities are offered by the extension of the model to different societies or countries and the potential aggregation of the extensions, which provides an opportunity for a unified global assessment. A possible extension is a historical analysis of different states over time, which also raises the possibility of plotting model values at different times and comparing them.

6.2 The Global Potential of Biometric Signatures

Biometric solutions also have numerous advantages in business and e-government. They do not require significant costs on the part of customers, they are efficient and do not require any training for customers. Their use may still be limited because the cross-border acceptance of such signatures requires an extension of national legislation. In Hungary an advanced electronic signature based on a qualified electronic certificate has full probative force, regardless of where the signature originated. In other Member States the legal effect can only be ascertained if the national law provides for it. In the absence of such a provision in the relevant national law, it is possible that the same signature will have different legal effects in different Member States.

There is no doubt that biometric electronic signatures will only be available at national level until the methods for creating and verifying enhanced security biometric signatures are standardized and widely accepted. On the basis of bilateral or multilateral agreements, cross-border acceptance is theoretically feasible, but in practice only generalization (such as “all secure electronic signatures based on qualified certificates

have full probative value in Hungary") can work until legislation at the regulation level. This may require a redefinition of the client's signature in the Hungarian public administration in order to avoid competition between the banking sector and the public administration and the negative consequences of the Finnish example. A good tool for this seems to be the establishment of validation authorities, proposed by Jon Ølnes and Leif Buene, which record, store and respond to the standardized verification requests of natural person signatories. If these answers could be implemented without territorial restrictions as to where the issue originates, this solution would allow the use of a handwritten signature on signature benches at a global level. No matter where the natural signatory signs, the signature would always be verified by a validation authority authorized by the person, so that on the one hand it is not necessary to store and keep a copy of the registration documents at all places of application and on the other hand local authorities should only deal with local signature habits, authentication options, and automatic signature verification problems, and not all the problems that may arise anywhere else. A global federated chain of validation authorities can provide global verifiability of biometric signatures to all human entities with registration documents, regardless of their current location. For cross-country acceptability, an additional step would be needed: non-copiable biometric signatures should be given independent and equal legal effect by all acceding countries, regardless of the legal effects of the current handwriting, qualified electronic signature or digital signature. Given that an advanced biometric signature meets European requirements for advanced electronic signatures and US requirements for digital signatures with legal effect, this idea would not overwhelm the current system. It would only add a new element to the existing elements, which would comply with the old rules and would not present problems in developing the global acceptability of PKI-based signatures.

Home and mobile use of the technology is also conceivable, especially in smart cities, when combined with a remote authentication process, e.g., video authentication, and when the security of the signing environment as well as the integrity of the software is ensured on the signature recording device. However, in the event of a shift in development needs in this direction, further innovation is likely to be needed, using the establishment and management of trust lists as a rather institutionalized technology for information security in the developed world, e.g. EU Trust List and Root CA programs.

6.3 Education Development

From an educational point of view, we found that the dissemination of electronic signature technologies requires some knowledge. Without related knowledge it can only spread through technological layers such as technology-savvy programmers and IT specialists. From there, due to the diversified nature and complexity of knowledge, the social transfer of the knowledge is unlikely. There are three, not completely equivalent

solutions in case the dissemination of knowledge required for the use of electronic signatures becomes a priority in Hungary:

1. Integration into primary and secondary education,

2. Introduction of a certificate from a non-undergraduate but widely supported education system (similar to existing examples), or

3. Enabling minimally invasive education.

The raison d'être of Option 3 is strengthened by the fact that, in addition to the trust elements of the National Core Curriculum, the area was not included in undergraduate education until January 2020. Further examination may be required as to whether there is an upper limit to the complexity of the knowledge that can be transferred through minimally invasive methods, including the extent of the knowledge or the duration required, and whether such a construct can be developed for adults.

The ECDL module has been available since 2010, but its success was limited. According to NJSZT ECDL Office, 205 certificates were issued between 1 January 2011 and 1 January 2019. So, it may be necessary to look at new methods to facilitate dissemination, because training is of great importance, as confirmed by Vrabie, too.

Vrabie also highlighted that there is a strong correlation between good e-government and IT education, which means that in addition to new innovative solutions, the existence of “smart citizens” is also a necessary condition for the existence of quality e-government. The e-signature dimension model is also suitable for use in education, as the Hamming distances of the electronic signatures used in the given field and the ubiquitous zero-value signature (null vector) precisely indicate the knowledge elements required for the use of the given electronic signature. This would be the basis of the required educational, which would explicitly discuss topics that may have been hidden so far.

7 Main Publications

1. ERDŐSI Péter Máté: *Fokozott biztonságú biometrikus aláírások alkalmazhatósági és szabályozási kérdései a közigazgatásban*.
   - In. dr. POLGÁR Miklós tű. százados (szerk.): A társadalom szolgálatában – felkészülés és felkészítés a katasztrófavédelmi kihívások tükrében. - Pécs: Baranya Megyei Katasztrófavédelmi Igazgatóság, 2019. - p. 63-68.

2. ERDŐSI Péter Máté: *Az elektronikus aláírás fogalmának megjelenése és változása.*
   - In. Információs Társadalom. Társadalomtudományi Folyóirat, 2019. XIX. évf. 1. szám. - p. 66-91.

3. ERDŐSI Péter Máté: Elektronikus aláírás e-közigazgatási használatához kapcsolódó tudás szétosztási megoldásainak összehasonlító elemzése biztonsági aspektusból.
   - In. Társadalom és Honvédelem, 2018. 2016. évf. 2. szám. p. 31-40.

4. Dr. HORVÁTH Attila, ERDŐSI Péter Máté: *Rosszindulatú számítógépes fertőződés vizsgálatának lehetséges kérdései és indokai a közigazgatásban.*
   - In. KISS Ferenc, HORVÁTH Attila (szerk.): IT és hálózati sérülékenységek társadalmi-gazdasági hatásai. - Budapest: Információs Társadalomért Alapítvány, 2016. - p. 31-48.

5. ERDŐSI Péter Máté: *A 2013. évi L. törvény végrehajtásának tapasztalatai kettes szintű közös önkormányzati hivatalok esetében.*
   - In. KERESZTES Gábor (szerk.): Tavaszi Szél 2016 = Spring Wind 2016. Tanulmánykötet. III. kötet. - Budapest: Doktoranduszok Országos Szövetsége, 2016. - p. 34-40.

6. ERDŐSI Péter Máté: *Elektronikus aláírások ortogonális dimenzionálása*.
   - In. KISS Natália, NAGY Bálint, NÉMETH István Péter (szerk.): Tudományos terek, Dunaújváros, Magyarország: DUF Press, 2014. - p. 57-64.

7. ERDŐSI Péter Máté: *Magyar bizalmi szolgáltatások felügyeletének összehasonlító elemzése.*
   - In. Műszaki Katonai Közlöny, 2014. 2014. évf. 1. szám. - p. 200-212.

8. ERDŐSI Péter Máté: *Elektronikus írásbeliség a magyar jogban.*
   - In. Társadalom és Honvédelem, 2013. 2013. évf. 3-4 szám. - p. 589-595.

9. ERDŐSI Péter Máté: *Az információ hitelessége.*
   - In. KALOTAY Balázs, KOVÁCS Zoltán, ERDŐSI Péter Máté, KOVÁCS Árpád, OZSVÁR Ferenc, KANCSÁR Attila (szerk.): E-Government Tanulmányok

V. Elektronikus rendszerek a közigazgatásban. - Budapest: E-government Alapítvány, 2011. - p. 37-47.

10. EGERSZEGI Krisztián, ERDŐSI Péter: *Problems in the Implementation of the Electronic Signature.*
    - In. Periodica Polytechnica - Social And Management Sciences, 2003. Volume 11. Issue 1. - p. 67-82.

11. ERDŐSI Péter: *Az elektronikus aláírás alkalmazásának háttere.*
    - In. Híradástechnika: Hírközlés-Informatika, 2002. LVII. évf. 9 szám. - p. 41-44.

12. ERDŐSI Péter: *A hazai informatikai biztonsági helyzet és az elektronikus aláírás.*
    - In. EGERSZEGI Krisztián, KISS Ferenc, GELLÉRI Péter, RÁCZ Csaba (szerk.): Intelligens rendszerek, hatékony alkalmazások. - Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem, 2001. - p. 119-131.

7.1 Most Important Conference Papers

13. ERDŐSI Péter Máté: Comparative Analysis and Measurement of Electronic Signatures Created by Notaries In Europe.
    - In. From Policy Design to Policy Practice. e-Proceedings of the 27th NISPAcee Annual Conference. May 24-26, 2019 Prague, Czech Republic. - NISPAcee Press, 2019. - ISBN 978-80-89013-99-9

14. ERDŐSI Péter Máté: Advanced Biometric Electronic Signature in Practice: Lessons for the Public Administration from a Hungarian Case Study.
    In. HANSEN, Hendrik, MÜLLER-TÖRÖK, Robert, NEMESLAKI András, PROSSER, Alexander, SCOLA, Dona, SZÁDECZKY Tamás (eds.): Central and Eastern European e|Dem¸ and e|Gov Days 2018. Conference proceedings. - Wien, Ausztria: Facultas Verlags- und Buchhandels AG, 2018. - p. 407-418.

15. ERDŐSI Péter Máté: Digitális tanúsítvány kiosztási modelljének elemzése különböző regisztrációs feltételek mentén.
    - In. CSISZÁR Imre, KŐMÍVES Péter Miklós (szerk.): Tavaszi Szél 2014 / Spring Wind 2014: I. kötet Közgazdaságtudomány, Debrecen: Doktoranduszok Országos Szövetsége, 2014. - p. 141-150.

16. ERDŐSI Péter Máté: The Integration of Electronic Signature into the Information Society in Hungary.
    In. TARGAMADZÉ Aleksandras, BUTLERIS, Rimantas, BUTKIENÉ, Rita (eds.): Conference Proceedings of 14th International Conference on Information and Software Technologies. - Kaunas, Lithuania: Kaunas University of Technology, 2008. - p. 241-248.

8 Curriculum Vitae

Name: Péter Máté, ERDŐSI

Date of Birth: June 19, 1969.

Education:

2013/09 – 2016/07 Doctoral School of Public Administration Sciences, National University of Public Service, Budapest, Hungary

PhD studies

1988/09 – 1994/07 Faculty of Science and Technology, Lajos Kossuth University, Debrecen, Hungary

Teacher of Mathematics and Computing Sciences

Languages: English (C1), German (B1), Hungarian (native)

Péter Máté ERDŐSI completed his higher education at Kossuth Lajos University, Debrecen between 1988 and 1994, during which he listened a total of 28 semesters in four disciplines (Mathematics, Physics, Computing Sciences, General and Applied Linguistics). His essay "Representing a Fragment of a Natural Language in an Intensional Logic Framework" finished fourth in the social sciences section of the XXII. OTDK conference. He graduated as a Secondary Teacher of Mathematics and Computer Sciences.

After graduation he worked as Assistant Research Fellow at the Center for Informatics and Computing of Lajos Kossuth University, Debrecen. He began to work intensively on the problems and educational issues of electronic signatures in 2000. Lots of his publications discuss this topic. He joined the Information Security Management Research Group established at the Department of Information and Knowledge Management of the Budapest University of Technology and Economics in 2001, and he actively participated in the work of the research group and created several publications. After the Foundation for Information Society took over the research tasks, he worked there as a Researcher between May 2005 and October 2006.

He gained professional experience as a Registered Electronic Signature Expert from July 3, 2002. He issued several expert opinions in connection with the annual supervision of the Hungarian qualified and non-qualified certification service providers. He has been an external eIDAS Auditor of the German TÜViT and TÜV TRUST IT conformity assessment bodies. He also manages WebTrust audit work at the international audit firm, Crowe. Since October 2019, he has contributed to the digitization work in the Government Office of the Capital City Budapest on a part-time basis as an Electronic Public Administration Professional.

In 2013, he was admitted to the Doctoral School of Public Administration Sciences of the National University of Public Service, which was launched as the first such program in the country, and researched the topic of increasing security of electronic information systems in Public Administration. He obtained a pre-degree certificate stating that all course-units have been completed on July 6, 2016. During his doctoral studies, he authored 28 scientific publications. As an author of a university publication and co-author of an ECDL module book, he also contributed to the development of the field of the education. His presentation at the Spring Wind National Scientific Conference won first place in the public administration section in 2016. As a PhD student, he also participated in the OTKA research entitled "The effects of IT and network vulnerabilities on economy and society" conducted under number PD 109740, which resulted in 7 scientific publications and a scientific database.

He served as a Committee Member in the Military and Law Enforcement Section of the XXXIV. OTDK. As a member of the Public Administration Science Section of the Association of Hungarian PhD and DLA Candidates, he helped the work of the section with his ideas and thoughts from the very beginning.