ADVANCED BIOMETRIC ELECTRONIC SIGNATURE IN PRACTICE – LESSONS FOR THE PUBLIC ADMINISTRATION FROM A HUNGARIAN CASE STUDY

Péter Máté Erdősi[1]

DOI: 10.24989/ocg.v331.34

Abstract[2]

Signing documents is one of the most general requirements in our daily lives, including routines in Public Administration. After significant development of e-Administration, the question arose as to how the clients can sign documents electronically. The European Union legislated this question by the 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. This Regulation (henceforward: eIDAS) gives a technology-neutral and high-level framework for using electronic signatures in the EU, it refers several implementing acts and standards, records applicable concepts and definitions, and declares several obligations for all Member States. The Regulation does not contain strong provisions for advanced electronic signature, but it defines four requirements for it. All electronic signatures which fulfil these four requirements have to be considered as advanced electronic signatures. In most of the cases, creating an advanced signature is easier and more cost-effective than creating a qualified signature, therefore it may be an alternative solution for signing documents in Public Administration also. This paper intends to summarize the relating legal environment and it demonstrates an implemented solution of advanced biometric signature in the private sector. Finally, we discuss the technical conditions of the applicability of advanced biometric electronic signature in Public Administration by discovering similarities and differences of application and acceptability.

1. Legal background of advanced electronic signature

We found the ultimate answer to the question, whether human signature can be used for signing in Public Administration. It is "yes". But there were unknown methods and solutions to implement it. We needed further development and innovation for implementing biometric signatures which are able to fulfil all requirements of advanced electronic signature as required by eIDAS. Using new innovations in the private sector usually requires greater caution for reducing legal risks and business risks. Therefore, the legal background is essential in case of a novel innovation.

1.1. Advanced electronic signatures in and out of eIDAS

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

[1] National University of Public Service, Institute of e-Government, 1118 Budapest, Ménesi út 5., erdosi.peter.kdi@office.uni-nke.hu

[2] 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.

not recognized by others. Mutually recognized electronic identification will facilitate cross-border provision of numerous services in the internal market and enables businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities. One of the objectives of eIDAS is to remove existing barriers to cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. The European 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, organizations 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.

Consequently, according to the eIDAS, only such solutions can be used across borders which are examined and accepted by affected Member States as it is defined by Articles 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[3]. 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[4], the biometric references are still missing from these methods.

The eIDAS differentiates three levels of electronic signatures: normal, advanced and qualified. 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 (Article 3 (10)), advanced electronic signature means an electronic signature which meets the requirements set out in Article 26[5] ((Article 3 (11)) and 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 (Article 3 (12)). In the preamble of eIDAS, closed systems, background processes of Public Administration and contractual requirements are excluded from the scope. That is why we need to discuss the following questions. Many thanks to Balázs Kőnig for the long discussions of these legal questions.

- Question 1: What are the requirements for creating advanced electronic signature in connection with eIDAS? Creating advanced signature based on eIDAS is possible only with using public trust services. Definitions of eIDAS are not applicable in closed systems, agreements and background processes of the Public Administration.

[3] Article 27 (1) of eIDAS

[4] 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

[5] Article 26 contains four requirements: it is uniquely linked to the signatory, it is capable of identifying the signatory, it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

- Question 2: Is it possible to create advanced electronic signature based on eIDAS in closed systems and background processes of the Public Administration? It is not possible to create advanced electronic signature between participants of closed systems using only elements of closed systems. Closed systems, contracts and background processes of the Public Administration are excluded from the scope of eIDAS. If these solutions do not use publicly trusted services for signing, the creation of advanced electronic signature based on eIDAS will not be possible.

- Question 3: Is it conceivable to create advanced electronic signature based on eIDAS without a signing certificate? Advanced electronic signatures based on eIDAS require public trust services (for instance issuing certificate for the signatory), consequently it is unconceivable to create advanced electronic signature based on eIDAS without a signing certificate.

It should be noted that these signatures and seals may correspond to the European definition of the digital signature[6] which is not a legal term. The American definition of digital signature is similar but a bit different in the NIST standard[7] [10]. The European standard allows a data appended to a data unit, which can prove the source and integrity of the data unit, as digital signature, but the American standard considers only data resulted by asymmetric cryptography as digital signature. Consequently, there is a legal question whether electronic signatures created in a closed system fulfil all requirements of advanced electronic signatures may be named as advanced electronic signature based on eIDAS or not. It seems to be that eIDAS does not extend to any trust services providing in closed systems[8]. It results that definitions of eIDAS are not applicable in any closed systems, agreements and background processes of Public Administration, therefore creating advanced signatures in such systems is also impossible only with internal elements. It would be a very interesting side effect of eIDAS, requiring exclusion of definitions instead of services. But if it is correct, we need to find further legal solutions at national level.

1.2. Advanced electronic signature in Hungarian laws

Hungary adopted the 93/1999 European Electronic Signature Directive by the Act 35 of 2001 and it was replaced after eIDAS by the Act 222 of 2015 defining general rules of electronic administration and providing trust services in Hungary. This Act (henceforward: Eübszt.) extends eIDAS. Two important sections can be cited: advanced electronic signature is a signature as defined by Article 3 (11) of eIDAS[9] and where a law refers to an electronic signature or an electronically signed document, an electronic seal or electronic document with a seal shall also be understood unless otherwise specified[10]. These sections result in three important consequences. The first is the general applicability of the definitions. The scope of this national Act is not restricted. Although it intends to regulate trust services and electronic administration, the definitions can be applied to closed systems, contracts and background processes of Public Administration as well. The second is the

[6] Digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient (ETSI EN 319 411-1, p.10.)
[7] Digital Signature: An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection (NIST 800-63-3, p.45.)
[8] See Article 2 (2) of eIDAS: This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.
[9] See Eübszt. Section 1 (22)
[10] See Eübszt. Section 99 (2)

signatory unification. Where a Hungarian law refers to an electronic signature or an electronically signed document, it can be signed by both natural and legal persons notwithstanding signatures do not equal to seals but both can be realized as a digital signature. The third is the cross-border inadmissibility. If these signatures are based on national law, cross-border acceptability can be ensured only by the similar extensions of national laws in all Member States. This governance method was defined by the Electronic Signature Directive, but it was obsoleted and repealed by eIDAS. It results that only electronic signatures based on eIDAS should be applied by cross-border closed systems, agreements and background processes of Public Administration, if legal effect is mandatory, until acceptance of these signatures enters into force in all Member States.

What can Hungarian financial institutes do if they want to eliminate paper-based documents and want to use only digital documents? There is an obvious answer, digitization should be implemented. But all processes of financial institutes are legislated by laws, thus digitization shall comply with all related legal provisions. The most important Act is the Act 237 of 2013, which prescribes numerous rules for credit institutions and financial enterprises. There is a special provision for contracting in Section 279 (1) according to a financial institution, with the exception of a single payment order and the derogation provided for in paragraphs (1a) and section 285, may only conclude a contract for financial and supplementary financial services in written form, including electronic documents signed with at least advanced electronic signatures[11]. Consequently, paper-based documents can be omitted if clients and the financial institute are able to sign documents with at least advanced electronic signatures. For fulfilling this requirement, further legal questions shall to be discussed in order to prove that advanced electronic signatures can be created both on the basis of eIDAS or national laws in Hungary.

- Question 4: Are the scope of eIDAS and Eübszt. different? Yes, eIDAS pertains to public trust services and Eübszt. describes additional rules for electronic administration and trust services at national level.

- Question 5: Can the definition of advanced electronic signature defined by Eübszt. be applied in closed systems, agreements and background processes of Public Administration? Definitely. Since Eübszt. is a part of the national law and its scope is not restricted generally, these definitions can be applied to interpreting concepts used by other national laws.

- Question 6: What kind of definition can be used if a national law refers the advanced electronic signature? European Regulations and Acts shall be applied primarily and national law should be used secondarily if there are no restrictions or it is not forbidden. Requirements for advanced electronic signatures are the same even the EU Regulation or Hungarian national law are applied.

1.3. Biometric signature in Hungarian Law

Hungarian Act relating to governmental offices[12] was extended on 21-10-2016 with a new paragraph (20/J. §), which allows using biometric technology for Governmental Offices in capital and county from 01-01-2017. In Offices and in the Government Window, electronically captured electronic images and dynamic data of the customer's signature can be used for authentication tools

[11] Section 279 (1) of Hungarian Act No. 237 of 2013
[12] Hungarian Act CXXVI of 2010 on Government Offices in the Capital and the County as well as the amendments to the Act on the Establishment of Capital and County Government Offices, and Territorial Integration

of electronic documents. In case of implementing this service, the Governmental Offices appointed by a Government Decree shall develop and maintain a signature sample database containing the picture and other dynamic data of the signature (e.g. strength of pressure, speed of moving). This database may not contain other personal or biometric data in addition to the data required for the evaluation of signature samples. These data may be recorded only with the voluntary consent of the customer, clients shall not be obliged to use this authentication method. When a signature is created on a device regulated in accordance with this Act, only the conformity with the specimen can be verified and an electronic clause of the result shall be attached to the document. This clause shall to be issued by a certified system and the document identifier has to be included also. The clause may not contain any dynamic data of the signature or any sensitive personal data. The electronic document with the mentioned clause shall be considered a private document with full probative force. In this construction, the documents may contain only the picture of the client's signature. This signature should not be considered as advanced electronic signature according to the professional opinion of Hungarian Association for Electronic Signature [4]. In this public service, it is not necessary to fulfil requirements of advanced electronic signature, because the Governmental Offices are able to issue documents with the specified clause as private document with full probative force based on this statutory authorization. There is no more information about the implementation procedures of this provision at the moment of writing this paper.

2. A novel innovation – how to create advanced biometric electronic signatures in practice

2.1. Rationale

In the literature, numerous articles can be found, which addressed the problems of using biometric signatures. We should differentiate – as in eIDAS – the identification data from the signature data from legal aspect. Signature is a data which is connected to other data[13], identification is a process which uses data instead of connecting to other data[14]. Authentication is another process which enables the confirmation of a claimed identity of natural and legal persons or the origin and integrity of a data unit[15]. In the development of a signature, the method of connection seems to be the most important part beyond to identifying capability of the signatory. This part is missing from an authentication process, because only a matching result between the recorded and presented electronic data has to be confirmed or refused. The innovator company had to plan, develop and deploy such signature method which is capable to comply with the requirements of advanced electronic signature.

The customer is the OTP Bank Plc.[16] as the largest bank in Hungary by number of branches (about 350-400). The predecessor of OTP Bank called the National Savings Bank was established in 1949 as a nation-wide, state-owned, banking entity providing retail deposits and loans. OTP Bank's privatization began in 1995. As a result of public offers along with the introduction of the bank's shares into the Budapest Stock Exchange the state's ownership in the bank decreased to a single voting preference (golden) share. Currently the bank is characterized by dispersed ownership of

[13] See Article 3 (10) of eIDAS: '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;
[14] See Article 3 (1) of eIDAS: 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
[15] See Article 3 (5) of eIDAS: 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
[16] For more information see https://www.otpbank.hu webpage.

mostly private and institutional (financial) investors. After the realization of its own privatization process, OTP Bank started its international expansion targeting countries in CEE region, which offers more economic growth potential. Today OTP Group provides financial solutions to nearly 15.1 million customers through nearly 1,400 branches, agent networks and state-of-the-art electronic channels.

National University of Public Administration in Hungary issued a report named "Good State Report 2017" [5], which is based on a representative research (Report on Good State Survey, 2017 [2]) and covered several topics including preferred channels in Hungarian Public Administration. Having regard to the fact that the bank owned by the State formerly, correlation between usage of channels in the banking affairs and Public Administration can be assumed. Proving this assumption goes beyond the scope of this paper. Nevertheless, Hungarian people prefer channels in Public Administration as can be shown by the following table:

personal	postal services	call center	online	other
61.8%	5.8%	17.8%	14.7%	2.8%

Table 1: Preferred channels in Hungarian Public Administration (based on [5:169]

The main goal of the bank was to develop and use an electronic solution instead of paper-based documents which can be as similar to the paper-based process as possible and which fulfils legal requirements. Banking contracts shall be signed only in written form or with advanced electronic signature in Hungary. The main focus was on the contracting procedure between the bank and the clients. Extension of the process to signing other transactions and orders in branches by the clients or to signing documents in other back-office procedures by the officers or managers were expectable. Signing a paper-based document does not require much knowledge and many devices from the clients, only the paper and a pen shall be provided with the physical presence of the clients. In other words, the bank intended to redirect clients' signature to an electronic channel regardless of the clients' digital literacy in order to reduce number of paper based documents.

2.2. The Developed Signature Process

As the open procurement procedure resulted, the developer company was Cursor Insight Ltd. who won the competition of German on-line signature verification in 2015 [6]. The kick-off meeting was held in 11-03-2016. The development started in Q2 of 2016 and the pilot phase was deployed in Q1 of 2017. Currently more than one million documents (registration forms, contracts and involved orders) were signed by the clients in the branches of OTP with advanced biometric signatures using this method and the number of involved documents is growing continuously. The developer implemented the next procedure for creating advanced biometric signature in the branches. It can be divided into three parts: registration, signing and verification processes.

- Registration process
    - the identification and authentication of clients has to be performed, as required by law, using public records and official documents,
    - the client has to place several handwritten signatures in a registration form, which contains the natural identification data also.

- Signing process
    - the bank clerk has to identify the clients (as prescribed in the internal policies)
    - the bank clerk prepares the document which has to be signed
    - the bank places a qualified electronic seal and a qualified timestamp, which are issued by a public trust services, on the prepared document
    - the application sends the prepared document to the signing pad for signing
    - the client signs the document with moving a special pen17 on the signing pad
    - the signing pad connects the document and the client's biometric signature using its asymmetric private key which is certified by a public trust service provider
    - the bank places a qualified electronic seal and a qualified timestamp again on the whole document
    - the client gets the signed document through the internet banking system
- Verification process
    - the client requests a verification process on a given document
    - the bank provides a tool or data for performing the verification, including at least the following elements:
        - valid list of signing pads in the bank
        - valid certificates of signing pads
        - the client's registration form including handwritten signatures
    - the validity of qualified seals shall be checked
    - the validity of qualified timestamps shall be verified
    - the validity of non-qualified signature of the signing pad has to be determined
    - matching biometric signature(s) on the document with biometric signatures(s) on the registration form has to be evaluated.

The steps of the signature verification process can be derived from the following figure. All signatures should be verified and validated before the document is accepted. The relations between

[17] It is a battery-free pen using Eletromagnetic Resonance Technology. It means that the sensor is only responding to the pen. Output rate of the coordinates is 500 Hz consisting of x, y, time and pressure.

signatures are sequential from inside to outside. Outermost signature is needed by legal and archiving reasons.

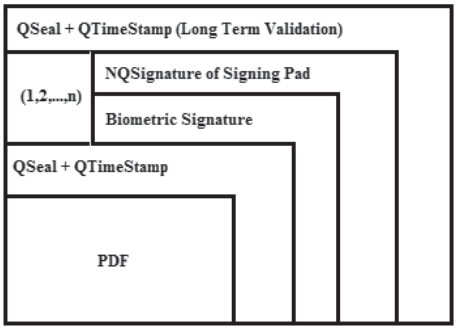

Figure 1: Internal structures of signed documents (Created by the Author)

It is very important that biometric data are used as signature instead of identification. The officer identifies clients by checking the presented identification documents (e.g. national ID card, passport, driving license or banking card with PIN code). This identification process always precedes the creation of biometric signature. Therefore, the bank focuses on verifying biometric signature created by an identified person instead of matching an unknown biometric signature to the one of the recorded biometric data. In January of 2018, IBM published a research material in connection with biometric authentication [8], which is based on a global survey with 3.977 answers, of which 1.976 came from the USA, 1.004 came from the EU and 997 answers came from Australia, India and Singapore. They found that the authentication methods perceived as most secure is the fingerprint usage (44%) and retinal (eye) scan (30%). Oher methods (facial recognition, handprint, voice and heartbeat recognitions) are used cumulatively less (32%) than fingerprint. Using handwritten signature as identification method may occur in less than 2% of responders.

It should be noted that only such signing pads can be used in the bank, which are purchased, installed and configured by the bank, which have a valid X509v3 signing certificate from a public trust service provider listed in European Trust List for theirs on-board generated private keys, and which are not able to accept digital data beyond the signing surface. This condition ensures the validity of signatures. If an attacker tries to forge the signatures and repeat recorded biometric data or any variant of it, apparently real signatures may be created. The verification of these signatures may result in positive answer in a commonly used signature verification tool. In this system, this forgery can be detected, because the validity of the signature requires a valid signature on the document and the client's signature data from a valid signer pad also.

The elements and attributes of a client's signature in this closed system are the following:

- signature creation data: eventually, the signature creation data are the signs of a pencil which is moved by a natural person signatory's hand on the given signing pad. These analogue data are digitized for further processing. The digitized copy of the signature is not applicable for creating a valid signature again, it serves only verification purposes.

- signature validation data: digitized and stored instances of the natural person signatory's

handwritten signatures, which are recorded during the registration process, and the X509v3 certificate of the given signing pad where the signing process is performed.

- it is uniquely linked to the signatory, it ensures by the recorded biometric data and the performed identification process of the physically present client.
- it is capable of identifying the signatory, because digitized handwritten signature can identify the signer physically,
- it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control, hence the signature creation data – attributes of the pencil movements – cannot be digitalized, used or reproduced and injected to the signing pad without the signatory with a high level of confidence, and
- it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable, it guarantees a qualified seal on the unsigned document and a qualified seal with qualified timestamp on the entire document in order to enhance trust.

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

Table 2: Overview of biometric signing process (Created by the Author)

The data transferred between the signing pad and the officers' computer is protected by encryption. The signature and its biometric properties are resistant to any kind of surveillance or interference. The signature is placed in the document and protected against tampering. The encryption algorithms are accepted by the German Federal Network Agency also. Within the PDF, the signature cannot be manipulated or misused in any way. This has been independently confirmed by an Information Technology expert from TÜV Saarland (Technological Inspection Association) at the request of the manufacturer (general evidence). The whole process was audited by an internal IT and security professional, an eIDAS auditor, a judicial IT expert and it was certified by an accredited certification body in accordance to proving the fulfillment of eIDAS requirements for advanced electronic signatures (special evidences). The above facts prove with a high level of confidence that biometric signatures generated by the above method fulfil the requirements of advanced electronic signature.

3. Discussion and Conclusions

We have attempted to discuss biometric signatures in three dimensions: the legal, technical and business aspects were discussed theoretically, legally and practically. The biometric solutions have several advantages on business side and e-Administration side also, because these are cheap, efficient and using biometry does not require any tools on the client side, but the usage may be

limited because cross-border acceptance of such signatures requires the extension of national laws. Branches in other Member States can use this technology if the national legislation allows creating advanced electronic signature in closed systems. The court practices in this field have been unknown yet, therefore certain legal risks may occur in case of a litigation. It can be reduced by a professional opinion from an electronic signature expert, a legal opinion from a judicial IT expert and a certificate from an accredited certification body, which prove that the given solution fulfils all requirements of the advanced electronic signature. There is still a lack of standards and of the description of evaluation processes for advanced biometric electronic signatures. Numerous standards are available regarding the recording, transporting and storing of different biometric data such as written signature, fingerprint and voice for using these data in authentication procedures. Processing technology of biometric data is developed and used widely as digital data. 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 fulfil the requirements of advanced electronic signatures, therefore using such signatures in secure manner require additional measures [4]. Researchers developed mixed methods, which combined public key cryptography (PKI) with biometric data and they claimed that the combination of PKI and biometrics can offer a more secure mechanism, because private keys can be generated directly from the biometric scan [3], [11]. After a decade, this topic appears again [7]. Elliptic curves may also be combined with biometric data as digital signature [9]. The general problem of these ideas is the prevention of successful reusing of recorded biometric data. Other researchers proved that a biometric signature (more precisely the recorded digital data) can be modified and altered in such a way (e.g. combining data with Gaussian noise) that the verification procedure accepts the modified biometric signature as the original handwritten signature. The probability of a successful modification seems to be very low [12].

There is no doubt that the biometric electronic signature can be used as normal electronic signature nationwide until creation and validation methods of advanced biometric signatures will be standardized and widely accepted in the EU. Without cross-border acceptance advanced biometric signature may be used only at national level. It requires the partial extension of related legislations for Pubic Administration (e.g. redefining the client's signature in Hungarian Public Administration). The presented solution can provide advanced electronic signature with full probative force for citizens without e-signature capabilities in e-Administration. This solution can make the digital gap disappear [14], and it is also independent from digital poverty [1] as well as it can be applied in all areas of e-Participation [13] at national level. Effectivity can be enhanced by integrating e-signature devices (e.g. card readers) and biometric signature devices (e.g. signing pads) in Public Administration until remote signature applications are developed. Home and mobile use of this technology is also conceivable, if it is combined with a remote identification procedure (e.g. video identification), and if the security of the signing environment as well as the integrity of the software on the signature capturing device is ensured. For this, however, further innovation will be necessary in the near future.

4. References

[1] CSÓTÓ, M., Aki (információ)szegény, az a legszegényebb? Az információs szegénység megjelenési formái, (Is the poorest the one who is (information) poor? Forms of information poverty), Információs Társadalom, XVII. évf. (2017) 2. szám, 8-29. old. http://dx.doi.org/10.22503/inftars.XVII.2017.2.1, 2017.

[2] Eds. DEMETER, E., PETÉNYI, S., Jelentés a Jó Állam Véleményfelmérésről (Report on the Good State Survey), Nordex Nonprofit – Dialóg Campus, 2017.

[3] FENG, H., WAH, C. C., Private key generation from on-line handwritten signatures, Information Management & Computer Security, 2002 10(4) pp.159-164.

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

[5] Ed. KAISER, T., Jó Állam Jelentés 2017 (Good State Report 2017), Dialóg Campus, 2017.

[6] 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.

[7] 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.

[8] KESSEM, L., Future of Identity Study – Consumer perspectives on authentication: Moving beyond the password. IBM Security, Cambridge, USA. 2018.

[9] MOHAMMADI, S., ABEDI, S., ECC-Based Biometric Signature: A New Approach in Electronic Banking Security, In: International Symposium on Electronic Commerce and Security, 2008.

[10] NIST, Special Publication 800-63-3, Digital Identity Guidelines, USA, 2017.

[11] ORVOS, P., SELÉNYI, E., HORNYÁK, Z., Towards Biometric Digital Signatures, in: Networkshop 2002 Conference, Eger, Hungary, 2002.

[12] PARZIALE, A., DIAZ, M., FERRER, M. A., MARCELLI, A., Do synthetic generated signatures reflect the subject motor programs? A pilot study, Proceedings of 18th IGS Conference, June 2017, Gaeta, Italy, (pp. 119-122.), 2017.

[13] PINTERIČ, U., Limitations of the e-Participation, In Hendrik Hansen, Robert Müller-Török, András Nemeslaki, Johannes Pichler, Alexander Prosser, Dona Scloa (eds.), CEE e|Dem and e|Gov Days 2017, Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment? Proceedings of the Central and Eastern

Eurpoean e|Dem and e|Gov Days 2017 May 4-5 Budapest (pp. 89-96), Austrian Computer Society, Vienna, Austria, 2017.

[14] SORIN DAN, S., Digital Divide in the EU countries from the Danube Region, In Hendrik Hansen, Robert Müller-Török, András Nemeslaki, Johannes Pichler, Alexander Prosser, Dona Scloa (eds.), CEE e|Dem and e|Gov Days 2017, Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment? Proceedings of the Central and Eastern Eurpoean e|Dem and e|Gov Days 2017 May 4-5 Budapest (pp. 79-86), Austrian Computer Society, Vienna, Austria, 2017.