ELECTRONIC SIGNATURE TECHNOLOGY IN HUNGARIAN GOVERNMENTAL IT PROJECTS IN 2010-2015

PÉTER MÁTÉ, ERDŐSI[1]

ABSTRACT

To improve Hungarian e-governance capabilities by developing new IT services, the Hungarian Government has spent more than one hundred million Euros since 2010. As the base pillars of the Hungarian Digital State, a number of Controlled Electronic Administration Services (CEAS) have been implemented. The usability of any digital system which can be linked to trust depends on the authenticity of stored and processed information. Using unauthentic information may result in fraudulent activities, which should be avoided in the Administration. Electronic signatures are methods of authentication as defined by the 93/1999 Directive, and tools of strong identification as specified by the new regulation.

The European Union enacted the Regulation (EU) No 910/2014 of the European Parliament and the Council called eIDAS. in September of 2014. eIDAS contains comprehensive and obligatory rules for applying electronic identification and electronic signature in Europe. It is the continuation of 93/1999 EU Directive, therefore addressing this topic is expected in IT projects in 2015.

The examination was performed on IT projects coordinated by the Hungarian Governmental – Information Technology Development Agency. The analysis focuses on three questions:

1. Is electronic signature technology applied in project administration?
2. Which electronic signature attributes appear in the final results of the projects?
3. What kind of electronic signature dimensions appear in the projects?

The presentation summarizes the main attributes of the examined projects, describes conceptual definitions of authenticity, gives a brief introduction into the electronic signature dimensions, and formulates conclusions about the success and lack of applying electronic signature elements in Hungarian Governmental IT projects.

INTRODUCTION TO AUTHENTICITY

EESSI Final Report (EESSI, 1999) stated that “an 'electronic signature' without being further qualified, is indeed an electronic authentication. The term 'authentication' itself is not defined nor explained in the recitals of the (93/1999 EU) Directive and thus leaves room for a broad interpretation. However, the term is usually defined as 'validation of a claimed identity'. Every type of electronic authentication will be regarded as an electronic signature, as long as it attached to or associated in a logical way with other electronic data.”. It is not a surprise that definition of electronic signature in 93/1999 EU Directive is the following: “data in electronic form which is attached to or logically associated with other data in electronic form and which serve as a method of authentication”. eIDAS Regulation (910/2014 EU Regulation) gives a very simple definition for it: “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”. This definition is not a technological dependent therefore several implementation has been deployed with different parameters. Consequently, implementing electronic signature systems requires deep and broad knowledge about dimensions and parameters of electronic signatures.

DIMENSIONS 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 known and the appropriate value from each dimension will have to assign to the given signature. Between relevant dimensions may occur dependencies. Dimension analysis should perform to define these interdependencies correctly. The independent dimensions are called orthogonal.

The examined dimensions are the following:

Dimension 1: Formalization (CAdES: CMS based Advanced Electronic Signature, XAdES: XML-based Advanced Electronic Signature and PAdES: PDF-based based Advanced Electronic Signature

Dimension 2: Type of Signature (normal, advanced and qualified

Dimension 3: Probative force (evidence at court, partial probative force, full probative force)

Dimension 4: Complexity (basic, extended policy based, timestamped, complex, extended, extended long, archive, long term valid)

Dimension 5: Validity Period (immediately, short time, long time)

Dimension 6: Certificate Standard (PGP, X509, other)

Dimension 7: Type of Certificate (qualified, non qualified, signature, seal, usable in Hungarian Public Administration)

Dimension 8: Type of Signatory (end entity including natural person, code signer, automaton, certificate authority including root, bridge, intermediate or certificate issuer, time-stamping authority, archiving authority, OCSP

[1] PhD student at Doctoral School of Public Administration Faculty at National University of Public Serice, Budapest, Hungary

provider etc.)

Dimension 9: Signature Algorithms (e.g. AES, TDEA, GOST, RSA, DSA, ECDSA)

Dimension 10: Length of Signature Creation Data (usually it is given in bits – 128, 256, 1024, 2048, 4096...)

Dimension 11: Storage of Signature Creation Data (encrypted container file, hardware token including Hardware Security Module, Secure Signature Creation Device or simple Signature Creation Device, SIM card, pen drive)

Dimension 12: Placement of Signatures (single, multiple including sequential, parallel, countersign, embedding, embedded, detached or mixed)

Dimension 13: Type of Certificate Authority (public, closed group, home made)

Dimensions can be categorized by types of connections, some of them connect to signatures, others relate to certificates, in the other words, dimensions may be classified by functional point of view. Next figure visualises this picture:

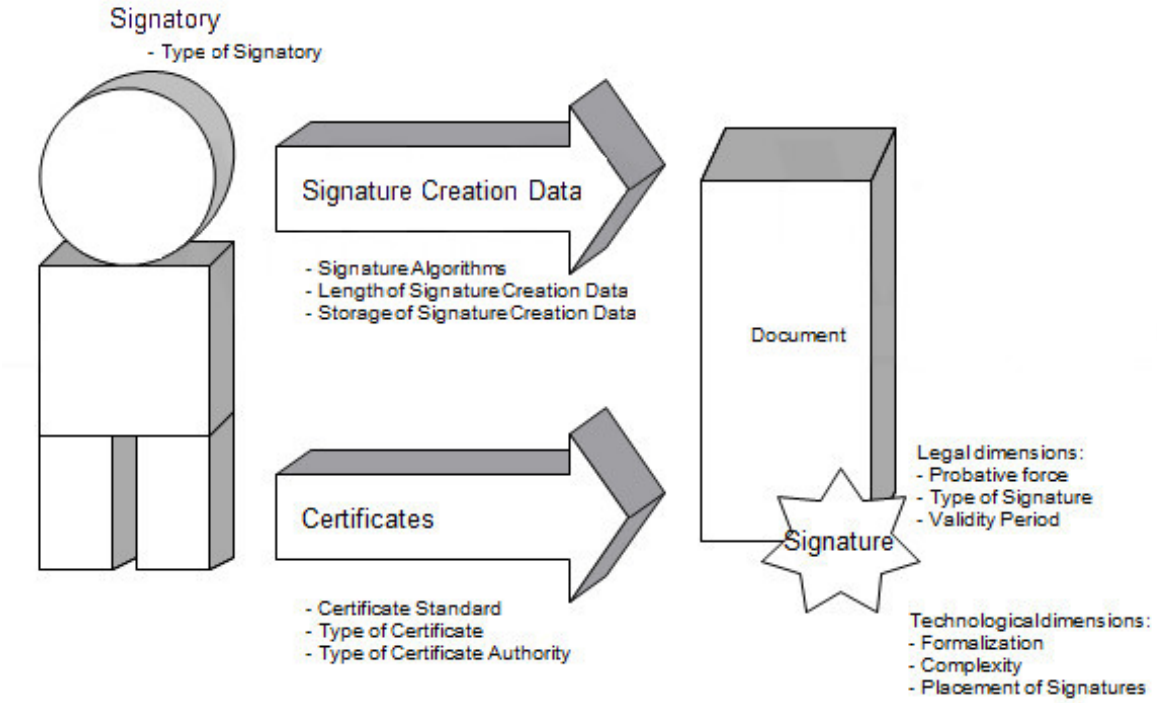

Figure 1: Classifying dimensions of electronic signature by functional aspects (created by author)

LIST OF PROJECTS

The Governmental IT Development Agency (GIDA) coordinates several IT projects in Hungarian Public Administration. The scope of this research contains 16 projects which started and performed between 2010 and 2014. Summarized budget of all examined projects was more than 38 billion Hungarian Forint (121 million Euros). It does not contain budgets of those IT projects which were coordinated by another governmental organization. The following information were gathered:

- Project code: short acronym created by first letters of words of project name
- Project name: short description of the project
- Project ID: Hungarian ID of project
- Started: The year when the project was initialized
- Finished: The year when the projects was deployed
- Budget (EUR): spent money in Euros

Details of the examined projects is listed in the next table**:**

	Project code	Project name	Project ID	Started	Finished	Budget (EUR)
1	**1AVAM**	Implementation of single customs administration	EKOP 1.2.2-07-2008-0001	2008	2010	7 692 000
2	**ACM**	Implementation of taxpayer-oriented data	EKOP 1.2.7-2008-0001	2009	2011	4 166 500

	Project code	Project name	Project ID	Started	Finished	Budget (EUR)
		model				
3	**ASP**	Initialization of a Centralized Application Service Provider Centre for Local Governments	EKOP 3.1.6-2012-2012-0001	2012	2015	8 333 500
4	**E-FIZ**	Implementation of central electronic payment system	EKOP 2.1.1-07-2008-0001	2008	2013	12 777 600
5	**EFER Conn**	Implementation of activities related to organizational connections with central electronic payment and settlement system (EFER)	EKOP-2.A.3-2013-2013-0002	2014	2014	320 500
6	**E-SZTENDERDEK**	Governmental standards for IT services and e-government functions	ÁROP 1.1.17-2012-2012-0001	2012	2013	641 0001
7	**ESR**	ESR-112 Single emergency calling system based on an emergency number	EKOP 2.1.12-2011-2012-0001	2012	2014	17 450 000
8	**FAIR**	Single IT support of the development policy	EKOP 1.2.12-2011-2011-0001	2011	2013	7 468 000
9	**GSM-R FEM**	GSM-R State supervising engineer	KÖZOP-6.1.1-11/K-2013-0001	2013	2015	2 404 000
10	**KGR**	Government budget management system	EKOP 1.2.1.-07-2008-001	2007	2013	14 263 500
11	**KKIR2**	Institutional Accounting Module (IKM-FI) subproject	EKOP-1.2.4-2013-2013-0001	2013	2014	961 500
12	**OTR**	Countrywide support monitoring system	EKOP-1.2.11-2013-2013-0001	2013	2014	2 564 250
13	**TÉBA**	Modernization of the payment of family benefits	EKOP 1.2.6-2008-0001	2009	2013	5 367 000
14	**INTÉZMÉNY-KÖZI**	IT systems development for centralized, inter-institutional data flow	TIOP 2.3.1.	2013	2014	8 880 750
15	**KATÉTER ÉS MÓNIKA**	Nationwide health monitoring and capacity map database and application development	TÁMOP 6.2.3/12-1-2012-0001	2013	2014	3 205 000
16	**KÖZHITELES**	Electronic public registers and sectoral portals	TIOP 2.3.2-12/1-2013-0001	2013	2014	6 730 500
17	**OEP**	Development of customer relationships in Health Insurance and implementing data management and identification integrated into health information systems	EKOP 2.3.7-2012-2012-0001	2013	2014	8 972 000
18	**EDR**	EDR development – Development of Single Digital Radiocommunication System (EDR)	EKOP 2.2.7-2013-2013-0001	2013	2014	9 612 750

Table 1: List of examined projects (created by author based on http://kifu.gov.hu webpage)

METHODOLOGY OF RESEARCH

There are couple of research regarded to Hungarian ICT projects. For instance ICT projects also examined by researchers focused on the policy objectives and project deliverables, not on execution and actual results (ARANYOSSI et. al., 2014). Security consideration of ICT projects is an other important aspect of examination.

Performing of my research includes two main direction, reviewing of projects documentation and interviewing with project managers and related professionals. I try to identify any PKI element in project documentation in designing phase and ask project managers about appearing these elements both in administration and in results of the projects (deploying phase). Measuring IT security is a complex task (MUHA, 2010) and needs some formalization. To formalize my results, research worksheet is specified for examining certificates, time stamps, signatures and archiving solutions. The worksheet contains the following elements:

1. **certificate**
   a) PGP signing certificate
   b) non-qualified signing certificate
   c) qualified signing certificate
   d) enciphering certificate
   e) authentication certificate
   f) SSL certificate
   g) qualified SSL certificate
   h) code signing certificate
2. **time stamp**
   a) qualified time stamp
   b) non-qualified time stamp
3. **signature**
   a) normal personal PKI signature
   b) advanced personal signature
   c) qualified personal signature
   d) normal seal
   e) advanced seal
   f) qualified seal
4. **archiving services**
   a) qualified archiving service
   b) non-qualified archiving service
   c) other archiving service

Main goal of this research is to identify used PKI elements of the examined IT projects because electronic signature appears as one of three basic functions of e-government in Hungary.

DISCUSSING

Based on project documentation and performed interviews lack of PKI elements can be stated in most examined projects. Governmental Certificate Service Provider as a CEAS (henceforward: GOVCA) issued several certificates for the Governmental Agency, but most certificates (88,46%) were used for implementing only the central financial service (EFER). Detailed distribution of owners can be seen in the next table:

Certificate owner	**Count**
EFER project	115
Employees of Agency (12 authentication certificates + 1 signature certificate)	13
Developers (for testing purposes)	2
Total value:	**130**

Table 2: GOVCA issued certificates grouped by owners (created by author)

The intended usage of PKI element was an other interesting question of this research. It can be derived from the applied types of PKI elements. The questionnaire was prepared by eIDAS and Hungarian Electronic Signature Act. The interviewed persons and examined documentation give an early result which is conformed by issued certificates:

Type of Certificates	**Count**
organizational signing certificate (seal)	1
organizational mass signing certificate (automaton seal)	1
organizational authentication certificate	75
organizational SSL certificate (client and	26

server)	
organizational code signing certificate	27
Total value:	**130**

Table 3: GOVCA issued certificates grouped by types (created by author)

Note that this status was recorded at December 21, 2015 and each project manager have not interviewed yet.

CONCLUSIONS

Based on interviews and examined project documentation, it can be stated that there are no electronic signatures in any documentation of projects neither in creating nor in archiving phases. However, EFER project uses most certificates issued by GOVCA, because it has a commonly used financial part and electronic signature technology is an external requirement in electronic banking transactions nowadays. Furthermore digital certificates only use for authenticating and testing purposes typically according to the results of the current phase of the research. Based on project managers' general opinion and partial results of this research it is presumable that using electronic signature technology has not integrated into developing, performing, deploying and documenting Hungarian e-government projects yet, but more research need to prove it undoubtedly.

The reason of low intention to use electronic signatures in governmental IT projects requires further research, but it is known factors that the Governmental Certificate Authority started at the end of 2013 and a bit of employees have PKI engineering knowledge as PKI usage experiences both in public administration and commercial companies. Furthermore we can see from statistical data of National Media- and Infocommunications Authority that using PKI certificates is not typical among governmental players. The popular argumentation of electronic signature – it is more expensive and too complex – may result this behaviour in public administration but we cannot ignore its increasing usage in commercial sector during this time.

REFERENCES

European Electronic Signature Standardization Initiative (EESSI). 1999. Final Report of the EESSI Expert Team, 20th July 1999. http://cryptome.org/eessi.htm (accessed April 10, 2016.)

Márta Aranyossi, András Nemeslaki, Adrienn Fekó. 2014. Empirical Analyis of Public ICT Development Project Objectives in Hungary. *International Journal of Advanced Computer Science and Applications* 45. Vol. 5 No. 12. http://thesai.org/Publications/ViewPaper?Volume=5&Issue=12&Code=IJACSA&SerialNo=6 (accessed April 10, 2016.)

Lajos Muha. 2010. Measuring IT security. http://real.mtak.hu/12938/1/1278547.pdf (accessed April 10, 2016.)

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093 (accessed April 10, 2016.)

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. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463515865338&uri=CELEX:32014R0910 (accessed April 10, 2016.)

European Standard. 2016. ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf (accessed April 10, 2016.)

European Standard. 2016. ETSI EN 319 411-2 V2.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf (accessed April 10, 2016.)

European Standard. 2016. ETSI EN 319 411-3 V1.1.1 (2013-01). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates.
http://www.etsi.org/deliver/etsi_en/319400_319499/31941103/01.01.01_60/en_31941103v010101p.pdf (accessed April 10, 2016.)

European Standard. 2016. ETSI EN 319 422 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf (accessed April 10, 2016.)

Technical Specification. 2015. ETSI TS 119 122-1 V1.0.1 (2015-07). Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.
http://www.etsi.org/deliver/etsi_ts/119100_119199/11912201/01.00.01_60/ts_11912201v010001p.pdf (accessed April 10, 2016.)

Technical Specification 2015. ETSI TS 119 132-1 V1.0.1 (2015-07). Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures

http://www.etsi.org/deliver/etsi_ts/119100_119199/11913201/01.00.01_60/ts_11913201v010001p.pdf (accessed April 10, 2016.)
ETSI TS 119 142-1 V1.0.1 (2015-07). Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
http://www.etsi.org/deliver/etsi_ts/119100_119199/11914201/01.00.01_60/ts_11914201v010001p.pdf (accessed April 10, 2016.)