

RULES FOR EID MANAGEMENT IN THE PUBLIC SECTOR (HUNGARY, 2018)

Alexandra Erzsébet Zámbo¹

DOI: 10.24989/ocg.v331.10

Abstract

The scope of the bodies providing e-governance services has significantly expanded in the past decade. Electronic identification has become an elementary obligation of the clients in e-procedures, as this is the starting point of any legal electronic transaction.

In Hungary, this legal issue is generally regulated by the Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions, and the related Government Decree 451/2016. (XII. 19.) on the details of electronic administration procedures. These national rules have been adjusted to the provisions of 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 (hereinafter: eIDAS Regulation).

The aim of the presentation is to summarize the legal possibilities and to evaluate their practical implementation.

1. Electronic ID: gate for e-administration

The electronic identification is a constant topic of discussions about electronic public services, especially because of the frequent transformations of this field. [8] The cause of the latest conversions and the development of the current system is that the European Union has recognized the main obstacle for a digital single market: “a perceived lack of legal certainty makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.” Therefore, the overall control of the electronic identification and trust services has become necessary at the level of an EU regulation. The recent Hungarian legal and organizational framework is the result of the obligatory harmonization of laws and the fulfilment of the targets set by the National Info-communication Strategy 2020.² The goals identified in the strategy related to the field of the digital state have been largely fulfilled in the past few years; at least the basic elements have been created. The Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions (hereinafter: E-Administration Act) and the related Government Decree 451/2016 (XII. 19.) on the details of electronic administration (hereinafter: E-Administration Decree) generally regulate the above mentioned field of e-administration.

Whenever we talk about e-governance in the EU, we can bump into the concept of CLBPS (Common List of Basic Public Services), issued in 2001: „Member States have agreed to a common

¹ Assistant Lecturer and PhD Student at the Group of ICT Law, Department of Administrative Law, Faculty of Law, University of Pécs. E-mail:zambo.alexandra@ajk.pte.hu

² Nemzeti Infokommunikációs Stratégia 2020,

http://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf [accessed 5 January 2018]

list of 20 basic public services, 12 for citizens and 8 for businesses. Progress in bringing these services online will be measured using a four stage framework: 1 posting of information online; 2 one-way interaction; 3 two-way interaction; and, 4 full online transactions including delivery and payment.”³ The real significance of the electronic ID is linked to the third and fourth levels of the CLBPS list. In the cases of the two-way interaction (third level) and the full online transactions (including delivery and payment – fourth level), the full and authentic identification of the client is inevitable at the very beginning of the legal process. As the E-Administration Act’s legal justification says: “The client must identify itself at the point of administration, where the data management makes this necessary. The regulations shall ensure that any of the electronic administration procedures could be done after the use of the electronic identification service.”

The aim of this study is to review and summarize electronic identification services granted by public sector bodies, to define the scope of these bodies and other organizations, and I also would like to sum up briefly the main legal provisions affecting clients. Since 1 July 2016, the national regulations have been adjusted to the supranational provisions of the EU. The starting point of this paper is the eIDAS Regulation. In the conclusion, I will evaluate the recent national solutions.

2. The provisions for electronic identification of the eIDAS Regulation

The Recital 12 of the eIDAS Regulation states that one objective is to remove existing barriers to the cross-border use of electronic identification means used in the Member States in order to authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States. The first step towards mutual recognition is to adapt the national identification systems to the conditions specified by the eIDAS Regulation and by the related Commission Implementing Regulations.⁴ According to Recital 13 of the eIDAS, Member States have the opportunity (and not the obligation) to notify their electronic identification schemes to the Commission. At least six months prior to this notification, the notifying Member State provides the other Member States a description of that scheme in accordance with the procedural arrangements established by the Commission Implementing Decision (EU) 2015/296 of 24 February 2015. On the other hand, if any Member State notifies the Commission, and this notification is published in the Official Journal of the European Union,⁵ all the other Member States shall apply the (mutual) recognition of the notified electronic identification system in their own public procedures where electronic authentication is needed.

It can be stated that the Member States do not strive to ensure interoperability within the shortest possible time, and at present there is little interest in the facilities provided by the eIDAS Regulation, nevertheless, we can assume that all of the electronic identification systems of the Member States fulfil at least the criteria for *low* assurance levels. In Article 8 of the eIDAS Regulation, the electronic identification schemes are classified into 3 assurance levels: “low”, “substantial”, and/or “high”.

³ Communication from the Commission to the Council and the European Parliament - eEurope 2002: Impact and Priorities A communication to the Spring European Council in Stockholm, 23-24 March, 2001 /COM/2001/0140 final/ <http://eur-lex.europa.eu/legal-content/HU/TXT/?qid=1520937504379&uri=CELEX:52001DC0140> [accessed 5 January 2018]

⁴ Article 7 of the eIDAS Regulation and Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015, and Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

⁵ At present, it is only Germany that uses the opportunity of the eIDAS and has notified the Commission, OJ C 319. (26 of September 2017), p. 3.

The following table shows the most significant differences between each of the security levels:

Security level	Degree of confidence in the claimed or asserted identity of a person is:	Regarding risk of misuse or alteration of the identity, the purpose of the system is:
low	limited	decrease the risk
substantial	substantial	decrease substantially the risk
high	higher than substantial	prevent

It is important to note, that the eIDAS Regulation still remains on the ground of technology neutrality, and it only sets out a minimal number of technical specifications, standards and procedures, taking into account relevant international standards.

Furthermore, the eIDAS Regulation deals with questions of security breaches [Article 10], liability issues [Article 11] and the establishment of an interoperability framework [Article 12], but here I will not go into details as these questions are beyond the focus of this paper.

3. Organizational background of the Hungarian electronic administration

An old-new concept of e-governance has prevailed in Hungary since the E-administration Act came into force on 1 January 2016, for this comprehensive Act deals with every question of electronic procedures, instead of incorporating the rules for electronic administration into several other acts. This Act entirely replaces the previous chapters (II/A. and X.) of the Act CXL of 2004 on the General Rules of Administrative Proceedings and Services. The new code for public administrative law, the Act CL of 2016 on General Public Administration Procedures – which came into force on 1 January 2018 – refers already to the provisions of the E-administration Act when needed as General Rules on Communication [Section 26] and General Rules on the Delivery of Decisions [Section 85]. The legal framework for the *regulated electronic administration services* and for the necessary organizational background is also incorporated into the E-Administration Act.

The electronic administrative processes (within the electronic identification) assume on the one hand the client, and on the other hand the e-governance bodies interaction (or the interaction between the e-governance bodies). Those bodies providing e-governance services can perform their duties if they use *regulated electronic administration services* provided by a specified service provider(s). Electronic identification methods cannot work without authentic state registers in the background. In addition, it seems obvious to set up a supervisory body for the sake of compliance. In this section, I will briefly present the organs participating in the fairly complex process of electronic identification in the course of e-administration procedures.

3.1. Bodies providing e-governance services

According to the E-Administration Act, the bodies providing e-governance services are enumerated in Section 1 Point 17 of this Act.⁶ This overall list of 12 points has been barely changed since the

⁶ a) government bodies, b) local authorities, c) other legal entities vested with administrative competence by an act or government decree, d) the Országos Bírósági Hivatal (National Office for the Judiciary) and courts, e) the commissioner of fundamental rights, f) the public prosecutor's office, g) notaries public, h) court bailiffs, i) public sector bodies, excluding appeal councils, j) public utility companies, k) legal entities with public service functions

adoption of the Act, although an amendment has been added an explanatory provision that specifies which of the listed bodies are regarded as *public entities required* to provide e-governance services. The bodies listed in the points from a) to k) are legal entities with public service functions or such providing public services. According to a presentation published by the National Info Communication Service Provider Private Limited Company (NISZ), there are approximately 1,2 million bodies in Hungary within the scope of this regulation that are regarded to be *public entities required* to provide e-governance services.⁷ [3] These legal entities shall ensure the availability of the means for electronic procedures in accordance with this Act as of 1 January 2018. (In practice, there may occur some difficulties in connection with the execution of this provision for some specific bodies, e.g. public sector bodies, court bailiffs, or local authorities, so we should consider this legal obligation as a developing process.) The merit of this unified list is that in the future, private legal entities – see point l) of the list – can voluntarily join and use the same services, and the same legal requirements shall refer to them as entities providing public services.

3.2. E-governance service providers

The E-Administration Act discusses the *regulated electronic administration services* separately (hereinafter referred to with the Hungarian abbreviation: SZEÜSZ) and the *centralized electronic administration services* (hereinafter referred to with the Hungarian abbreviation: KEÜSZ), although there can be considerable overlaps. The justification of the Act highlights the logic of the regulation, as it declares SZEÜSZ being left open for the private sector, while only state organs can provide the KEÜSZ. In addition to this dual system, another factor complicates the scheme apparently, as the E-Administration Act specifies the SZEÜSZ as services *provided by the Government on a compulsory basis* [Section 34], with services incorporated into the KEÜSZ services.

At present, there is no registered SZEÜSZ service provider in the private sector. KEÜSZ providers – designated by the 84/2012. (IV. 21.) Government decree – are the followings:

- a) NISZ National Info Communication Service Provider Private Limited Company (hereinafter referred to as NISZ),
- b) IdomSoft Ltd. (a subsidiary of NISZ), and
- c) Hungarian Postal Service Private Limited Company.

As a strategically important participant in Hungary, the NISZ has provided telecommunication, IT, and e-government services through its half century long history. Since 2005, the company has been fully state-owned, and the superior body of it is the Ministry of the Interior. According to the provisions of the 84/2012 (IV. 21.) Government Decree, the NISZ activities are based on the public service contract with the minister in charge of e-administration. Some projects of the NISZ (e.g. governmental hotline 1818, unified government file manager) have been carried out as the

or providing public services, and required to provide electronic administration services by an act or government decree, and l) legal entities, other than those covered under Paragraphs a)-k), who voluntarily agreed to provide means for electronic transactions under this Act in certain specific cases in compliance with the requirements set out in this Act, and who notifies the Supervisory Authority for Electronic Procedures thereof.

⁷http://www.kormanyhivatal.hu/download/0/0c/04000/Elektronikus%20%C3%BCgyint%C3%A9z%C3%A9s%202018%20janu%C3%A1r%201-t%C5%91%20_NISZ.pptx. [accessed 3 January 2018]

successor of the previous Central Office of Public Administration and Electronic Public Services (hereinafter referred to with the Hungarian abbreviation: KEKKH) since 1 January 2017.

3.3. The responsible bodies for central registries

After the termination of the KEKKH by succession on 31 December 2016, another successor of that central office is the Ministry of Interior, Deputy Undersecretary of State Responsible for the Registers (hereinafter referred to with the Hungarian abbreviation: BM NYHÁT), which is currently the competent authority for the undermentioned registers:

- a) the personal data and addresses records,
- b) the central address register,
- c) cross-referencing register,
- d) register of foreign persons relying upon an electronic identification or a trust service,
- e) Central Client Registration Database,
- f) register for official identification certificates,

and furthermore 12 registers for different purposes.⁸ The purpose and the legal basis of data processing are determinative for every register, and it is particularly prevalent for large state registries. The *central immigration register* also plays an important role in the process of electronic identification and it belongs to the authority of the Immigration and Asylum Office.

The abovementioned registries (databases supervised by the state) are essential participants in the process of electronic identification because the authentic information stored in them is a reliable point of reference, in case the e-governance service providers check the identity alleged by a client. The E-administration Act contains some more details about this procedure, which will be mentioned in chapter 4.2.

3.4. Supervisory Authority for Electronic Procedures

The Supervisory Authority for Electronic Procedures (hereinafter “Authority”) shall mean a body designated by the Government for facilitating and supervising electronic administration procedures, for the cooperation and coordination of cooperating bodies, and it is tasked to carry out functions delegated in the E-administration Act and the E-administration Decree.⁹

The need for establishing a supervisory authority had emerged earlier than the present solution. There were some ineffectual attempts in 2013 [1], when the legal provisions regarding such authority were put into the Act CXL of 2004 on the General Rules of Administrative Proceedings and Services. The regulations according to the Authority were not only replaced on 1 January 2017 into the chapter IX of the E-administration Act, but the position of this supervisory body was also strengthened and its tasks were expanded.

⁸ <https://kozigazgatas.magyarorszag.hu/intezmenyek/450021/450094/450285/bmkanvh.html> [accessed 5 January 2018]

⁹ Section 1. 18., E-administration Act.

The Authority is more than the supervisory body of the SZEÜSZ and the KEÜSZ, it is a central body, as well, having coordinating, advisory, and regulatory powers in respect of the electronic administrative procedures. The Authority has extended inquiry legitimacy and shall order various sanctions.¹⁰ The Authority is also entitled to maintain a database on matters that can be processed by way of electronic means and on bodies providing e-governance services, and shall make this database available to the public.¹¹ This kind of database can facilitate the orientation of the clients tremendously, and can stimulate the willingness of using electronic public procedures.¹²

4. Basic rules for eID from the perspective of Clients

4.1. E-governance services as rights or obligations

The E-administration Act defines the concept of “client” broadly: “Client shall mean a person or other legal entity involved in matters falling within the powers and competence of a body providing e-governance services in the capacity of a client, party or a subject to the proceedings, or as a relying party or the representative thereof, where such person or other legal entity is not recognized as a body providing e-governance services and is not a member or employee of the competent body providing e-governance services.”¹³

From the point of view of a natural person, the client has an enacted *right*¹⁴ to grasp the opportunities of electronic public services, although in some exceptional cases, this right can be limited or even excluded by the act, like in the following cases:

- a) an act or government decree adopted in a vested legislative capacity creates an obligation for the physical presence of the client, or for the submission of documents that may not be obtained in any other way,
- b) for procedural steps where it is not applicable,
- c) for procedures or procedural steps where it is excluded by an international treaty or a directly applicable Community legislation that is binding in its entirety,
- d) in the case of any document, official instrument or other petition that contains classified information.

On the other hand, a natural person may be obliged to use electronic administration procedure only by an act.¹⁵ Nowadays it is still a very important legal guarantee because the whole population has not obtained all the ICT competencies and devices needed for e-procedures yet.

¹⁰ E-administration Act Section 48.

¹¹ E-administration Act Section 50.

¹² Unfortunately, at the closing time of the manuscript, there is no such database available on the website of the Authority, only a table about the KEÜSZ services <https://euf.gov.hu/eusz-tajekoztatok> [accessed 01.05.2018]. Those who are interested can find a lot of information about the electronic public procedures scattered on different websites.

¹³ Section 1, 48, E-Administration Act, furthermore, we find some additional interpretative provisions in the Subsections (3)-(4) Section 2.

¹⁴ Subsection (1) Section 8, E-administration Act: “Unless otherwise provided for by an act or government decree adopted in a vested legislative capacity, the client shall be entitled to take procedural actions before the body providing e-governance services electronically, and to make statements also by way of electronic means.”

¹⁵ Subsection (3) Section 9, E-Administration Act.

The E-administration Act determines the scope of the clients for whom the electronic communication is *mandatory* in respect of all matters falling within the powers and responsibilities of the bodies providing e-governance services. The list of the obliged clients comes as follows:

- a) client economic operators;
- b) the legal counsels of clients;
- c) the followings when acting as clients:
 - ca) the State,
 - cb) municipal governments,
 - cc) budgetary agencies,
 - cd) the public prosecutor,
 - ce) notaries,
 - cf) public sector bodies,
 - cg) other administrative authorities not covered in Paragraphs cb)-cf).

Obviously, these are legal persons or their representatives, from whom the legislator can reasonably expect that they obtain the necessary instruments for electronic communication. Beyond the above listed legal persons, the client or his representative is obligated to use electronic administration procedure only where so prescribed by the law, and only if it is applicable to the given matter.

4.2. Obligation of electronic identification

According to the provisions of the E-administration Act Subsection (1) Section 18 “a client shall be entitled to communicate electronically *without electronic identification* if no personal identification data is required for carrying out the same procedural or administrative action or for making the same statement where communication is maintained by means other than electronic.” These cases are meant for a rather narrow path, but a typical example for this situation is when the client only wants to ask the administrative bodies for some general information.

In every other case, and that is more typical, the client must identify himself, and as the act declares in electronic administration procedures, the client shall have the option to identify himself:

- a) by way of electronic identification service;
- b) by way of electronic identification means under Article 6 (1) of the eIDAS Regulation; or
- c) by way of electronic identification service provided for in Subsections (3)-(4) Section 18 in the type of procedures and/or in respect of the procedural steps specified in the information published by the body providing e-governance services.

The core elements of the additional criteria referred to in point c) are:

- the client has to take specific procedural actions (registration), where physical presence is required,
- during this procedure it shall be provided to ascertain that the person claiming a particular identity is in fact the person to which that identity was assigned,
- this adequacy is met by a high degree of confidence if the data verified in the process correspond:
 - a) to that client's natural identification data shown in the personal data and address records, central immigration register, or in the register of foreign persons relying upon an electronic identification or a trust service;
 - b) to that client's natural identification data shown in the personal data and address records or central immigration register, or to data shown in the register of foreign persons relying upon an electronic identification or a trust service that can be verified directly through the cross-referencing register with a high degree of confidence;
 - c) to that client's identification data fixed in the administrative disposition; or
 - d) to that client's personal identification data held in the information systems of the body providing e-governance services, that enables the system to verify the identity claimed by the client by means of identity proofing and verification relying on data held in a public register.

The E-Administration Act Subsection (6) Section 18 offers another kind of opportunity when the client shall be entitled to take specific procedural actions or to make specific statements during electronic procedures if he is able to authenticate himself by means of electronic identification established previously in the client's physical presence. Where such identity provides assurance that the client's name and his other identification data are available, respectively, for the body providing e-governance services and to the electronic identification service provider.

5. The eID services available in Hungary

5.1. eID services provided by law

5.1.1. The electronic identification service

The legal guarantees for electronic identification services, which can be provided by private sector participants as SZEÜSZ, are regulated in the sections 30-33 of the E-Administration Act. In accordance with the regulations examined in the previous heading, it is essential that eID services of any type shall be useable only after a registration procedure, which is based on personal appearance. The Act contains details about the necessary progress of registration and the consequent content of the client registration database.

As the eIDAS Regulation is allowed to be used for public services – the eID management systems grant only “low” security level -, the E-Administration Decree declares that the “low” level security services are also suitable for clients.

5.1.2. Electronic identification services provided by the Government on a compulsory basis

The importance of the electronic identification KEÜSZ¹⁶ is shown by its highlighted place within the regulations of the E-Administration Act, as it has an own heading and the relating Section 35, which has several provisions providing legal guarantees for severe data control and for the prevention of profiling. Based on the Act, clients shall have access to the following electronic identification services provided by the Government on a compulsory basis:

- a) electronic identification services provided by way of a personal identification document with storage module;
- b) customer port of entry; and
- c) partial encoded phone identification.

The Act sets down the steps of the client registration procedure, and it creates the legal basis for the inevitable background database as well, which is called in this case Central Client Registration Database (hereinafter referred to with the Hungarian abbreviation: KÜNY). The tasks and competences according to KÜNY belong to BM NYHÁT.

The exact methods how the client identifying himself with the above listed eID services takes place are specified in the E-Administration Decree as follows:

- ad a) through reading the identifying information from the internal storage of the eID card in addition with using a PIN code associated to the eID card,
- ad b) through user ID and password,
- ad c) through user ID and password (or additional elected secondary authentication factor).

Obviously, the most advanced and secure way of identification of these three methods is using the eID card [7], as it is a multifactor identification method, combining the possession based and the knowledge based proceedings. Since 2016, the new Hungarian personal identity card has had several new functions,¹⁷ the main functions are “ePASS”, “eID”, and “eSign”, which are supported by the internal storage (chip), however, there are few public service procedures still in practice where it can be used. [4]

¹⁶ *Electronic identification service available to natural person clients* is declared – by Subsection (1) a) Section 34, E-Administration Act – as a regulated electronic administration service, which shall be provided by the Government by way of a designated regulated provider of electronic administration services.

¹⁷ http://www.kekkh.gov.hu/Eszemelyi/in_english [accessed 5 January 2018]

5.1.3. Primary Identification Agency (KAŰ)

The E-Administration Act Chapter VII deals with the so-called KEŰSZ. According to the Act, the Government – by way of a service provider delegated by the relevant legislation – shall provide the *primary identification agency*.¹⁸ This authorized service provider, in particular, the NISZ – previously discussed in heading 3.2. – denominates this service as Central Client Authentication Agent (abbreviated: CCAA, Hungarian abbreviation: KAŰ). (For the sake of clarity, I will be using the abbreviation KAŰ when referring to this kind of KEŰSZ.)

Detailed rules for KAŰ are to be found in the E-Administration Decree Section 127, where the rules make clear that this service is a single point of access to all authentication services recognized by the state, and it shall provide the opportunity for the client to choose from among the accessible eID methods, at least from the followings:

- a) all of the electronic identification services provided by the Government on a compulsory basis, (at present these are the 3 services listed in the previous heading 5.1.2.),
- b) any electronic identification by SZEŰSZ (just in case any appears in the future provided by private sector participants),
- c) eID methods in compliance with the eIDAS Regulation (at present German eIDcard).

As we will see, this is a wider spectrum of possibilities offered by the law than the recent functioning of KAŰ can provide, but we can presume that there is no real need from clients for all of the above-mentioned possibilities yet.

5.2. eID services available in Hungary, 2018

At present, there is just one state-owned service provider granting eID services like KEŰSZ for the bodies providing e-governance services. We can rather think about it as an on-going process, as NISZ informs the clients about its e-public administration services: “The recent years have seen development projects making several e-services available for citizens, enterprises, and public authorities. However, the current range of services is yet to be extended and introduced to users.”¹⁹ NISZ has developed digital solutions of identification and authentication, as well as the digital signature, furthermore documents delivery for e-public administration infrastructure. In this paper, I only examine the services related to eID, and not even the digital signature, which is both an identification and a document authentication method.

5.2.1. Citizen’s Portal (or customer port of entry, or client gate)

There are three different English phrases for the service available at <https://ugyfelkapu.gov.hu/>, or <https://gate.gov.hu/>, respectively. The official translation of the E-Administration Act uses the phrase “customers port of entry”, the literature calls it “Client Gate” [4] and NISZ introduce this service on its English website as Citizen’s Portal.²⁰ In this paper, I will be using the Client Gate expression in the followings.

¹⁸ Subsection (1) j) Section 38, E-Administration Act.

¹⁹ <http://www.nisz.hu/en/services> [accessed 05. 01. 2018]

²⁰ <http://www.nisz.hu/en/services> [accessed 05.01.2018]

The Client Gate had been the first e-governance application that spread widely among clients. Despite the fact that it is a one-factor, only knowledge based (and therefore considered to be a “low” security level method) eID system, it had a central role and was legally the favoured option during the third era (2009 to 2012) of electronic public administration. [2]

However, it is still the most popular and easiest way to get in touch with the bodies providing e-governance services. According to the latest statistical data at the end of 2017, more than 3 million registered clients had a Client Gate.²¹ According to the NISZ English website information: “For those who login to the Citizen’s Portal, some 300 e-services become accessible, the most popular being tax and social insurance declarations, university applications, personal document related services, land registry enquiries, and requests for a Certificate of No Criminal Record.” Any natural person can register personally for this service, even online, if they have a Hungarian eID card issued after 1 January 2016.

There have been some important differences in the operation of the Client Gate service since the beginning of this year. One of them is that the Client Gate has to cooperate with KAÜ, as this central portal mediates the eID process by the Client Gate to several e-administration services. Another alteration is that the storage service – connected to every user – has been moved to a new portal, the legal expression for it is “personalized communication platform” (abbreviated in Hungarian: SZÜF).²² This platform is accessible after (at present double) login with the login name and user ID of the Client Gate, and finally, the client can find its legal documents at the new website at <https://tarhely.gov.hu/>.

5.2.2. Partial Encoded Phone Identification

The legal ground of this service can also be found in the E-Administration Act, but we can find the details of this service only in the General Terms and Conditions²³ of this service granted by the NISZ. This e-service was introduced in 2017 and the main conditions are unchanged. [4]

It is important to emphasize that this service also requires a registration procedure when a preliminary full identification is carried out in the presence of the client by the correlation of the personal documents displayed by the client and the authenticated data gained from the registries. At the same time, there is no natural identity data stored in the registry of Partial Encoded Phone Identification, during the identification process; an encrypted access code will serve for authentication later on. Just as the Client Gate, this type of eID can also be considered as a “low” level security system because it is also based on a knowledge based method.

5.2.3. Central Client Authentication Agent (KAÜ)

The KAÜ operated by the NISZ is to accomplish in a way that government and market identity services (if they appear later on the scene) shall be handled on equal terms. Until this year February, the KAÜ had only provided the choice between the Client Gate and the Partial Encoded Phone Identification eID methods. As I stated earlier in the heading 5.1.3., the E-Administration Act expects to activate the possibility of electronic identification by eID card as well, as it was planned to be incorporated

²¹ The source of the number of registered clients of Client Gate from: https://segitseg.magyarorszag.hu/segitseg/portal/latogatottsagi_adatok.html [accessed 5 January 2018]

²² Subsection (1) k) Section 38, E-Administration Act.

²³ http://www.nisz.hu/sites/default/files/altalanos_szerzodesi_feltetelek_0.pdf [accessed 5 January 2018]

from the start of this service. [4] This feasibility became available at last on 31 January 2018.²⁴ This service was devoted to develop, modernize, and simplify the process of the eID, but it still needs some efforts in order to serve these aims properly, and not only by broadening the optional eID methods, but by strengthening the communication security of the portal as well. [6]

6. Conclusions

Constructing a well-functioning e-administration has not only been started, but to formulate it in a more optimistic way, we can say that we are on the right path with it. There have been some encouraging achievements that can serve as a good basis for the ongoing developments. First of all, it seems to be a good choice that the principal service provider (NISZ) for the public sector is a state-owned Ltd. which has the financial, technical, and professional background for high quality ICT services. Another good item of news is that the Authority could start its operation on a well-based legal ground.

An old drawback of this issue is, however, that it is still very complicated to ensure a good legal basis for these services and procedures. The relating legal rules are not the easiest reading, not even for researchers, as they have become extremely complex, introducing a lot of new phrases, and sometimes iterative rules deteriorate the structure. The principle of technological neutrality is also a big challenge from the legislators' point of view. As this legal field is intended to regulate big state registries containing a huge amount of personal data, the legislation cannot avoid to deal with questions of data protection and to strictly determine the access rights either. [5]

At the same time, we can say that the recent EU and domestic regulations are a little bit ahead of the practical solutions. Member States shall make efforts in order to fill-in the interoperability framework with content, and e-service providers (like NISZ) have to develop and to extend the current range of services. It would be welcomed if the eID card and the electronic signature could gain a more important role, as these are the most secure methods of electronic communication.

In Hungary, the wide range of bodies providing e-governance services now cover all the fields where e-governance services can be expected. The legal basis has been elaborated in the past few years, from this year on, all the affected bodies must become familiar with these regulations. This progress requires not only instrumental (proper hardware and software utilities) development, but organizational and procedural reformation within the above mentioned bodies as well.

According to the three main eID methods available for citizens provided by the KAÜ, it can be established that the most popular solution is still the Client Gate, regardless the fact that it is still the most vulnerable in terms of security. Since there has not been any significant precedent of abuse in the past years, clients prefer (and also get used to) this easily and quickly usable feasibility. The opportunity of using the new eID card for electronic identification from the security point of view is the best choice, however, it is still unusual and a brand new way for most of the public. Another obstacle for the eID card application to become more common is that the potential users have to gain special devices for operating it.

As regards the clients, there is also lot to be done, particularly in order to improve their ICT competences and their knowledge about the already available options. As we consider this

²⁴ <https://hirlevel.egov.hu/2018/02/04/elerhetove-valt-az-eszemelyi-eszig-kartya-a-kormanyzati-kau-kozponti-azonositasi-ugynok-szolgalatas-mogott/> [accessed 1 March 2018]

development for the future, I suppose that the most useful way to inform and to prepare the prospect clients is to start educating them on the subject of e-governance as early as in the elementary school.

7. References

- [1] CZÉKMANN, Zs. CSEH, G., Elektronikus közszolgáltatások a SZEÜSZ-ök tükrében [Electronic public services in the mirror of SZEÜSZ], Publicationes Universitatis Miskolciensis Sectio Juridica et Politica, Tomus Vol. XXII. 2014 pp. 135-145.
- [2] KISS, A., KÖNIG, B., Electronic identification and authorization with focus on public administration in Hungary in: CEE e|Dem and e|Gov Days 2015, Austrian Computer Society 2015.
- [3] NÉMETH, Á. M., Elektronikus ügyintézés 2018. január 1-től – kötelezettségek, lehetőségek, tapasztalatok [Electronic transactions from 1 January 2018 – obligations, possibilities, experiences]:http://www.kormanyhivatal.hu/download/0/0c/04000/Elektronikus%20%C3%B0gyint%C3%A9z%C3%A9s%202018%20janu%C3%A1r%201-t%C5%91%20_NISZ.pptx. [accessed 1 March 2018]
- [4] ORBÁN, A., BELÁZ, A., eIdentification – Renewable Regulated Electronic Administration Services in: HANSEN, H., et al. (eds.) CEE e|Dem and e|Gov Days 2017, Austrian Computer Society 2017.
- [5] POLYÁK, G. SZŐKE, G. L., Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére [Technological determinism and legislation, in particular the development of Data Protection Law], Pro Publico Bono Vol 1/2015.
- [6] SZÁDECZKY, T.: Communication security of e-government services. Hadmérnök Vol. XII. No. 2, 2017.
- [7] SZÁDECZKY, T.: Data protection and data security of electronic identification documents. Hadmérnök, Vol. XII. „KÖFOP” Issue 2017.
- [8] VESZPRÉMI, B: Személyazonosítás az elektronikus közigazgatásban [Identification in electronic administration]. Infokommunikáció és Jog, 2009/34.