DOI 10.5817/MUJLT2018-1-1

ENHANCED FUNCTIONALITY BRINGS NEW PRIVACY AND SECURITY ISSUES – AN ANALYSIS OF EID*

by

TAMÁS SZÁDECZKY**

As compared with traditional paper-based versions and the standard username--password login to e-Government services, the new electronic identity and travel documents have made on-site electronic and on-line authentication of citizen more comfortable and secure.

The biometric passport was introduced in Hungary in 2006. A decade later the electronic identity card (eID) was implemented. The reason for the improvement of such documents is twofold: enhancing security features and performing new functions. The development is certainly welcome, but it also generates new types of risks, with which governments and citizens must take into account.

In this paper, I will first analyze the most widespread technologies of data storage cards from the passive elements to the chipcards, including the biometric passport. The objective is to provide an overview of the technical development as a background to my paper. I will then proceed to an analysis of the relevant EU and national legal background, data elements, data protection and the functions (ePASS, eID, eSIGN) of the new Hungarian and German identity card, as well as the security risks and protection properties of the eID-type documents. The paper concludes with a summary of the lessons learned from and the risks involved in the current solutions in Hungary and Germany.

* The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled *„Public Service Development Establishing Good Governance"* in the Miklós Zrínyi Habilitation Program.

** szadeczky.tamas@uni-nke.hu, Associate Professor, Institute of E-Government, National University of Public Service, Hungary.

KEY WORDS

Chip Data Protection, E-Passport, Hungary eID, Protection of Government Issued Documents

1. INTRODUCTION

The primary technology used to manage physical access and identification of persons is the card, which is widely used as a means of possession-based authentication for several years now.

Such cards are designed to store data for identity or access purposes. These tools are categorized per the storage method and device type. Both the storage capacity, security, and usability depend on the technology of these devices.

The most straightforward data storage option is provided by passive solutions, such as punched cards, barcodes, and magnetic stripes, also used in bank cards. A later version includes memory chips for data storage, without the possibility of data processing, e.g. encryption. These solutions have been used for a long time for official documents, primarily to ensure efficient machine data processing.

2. DATA STORAGE ON CARDS

A well-known data card type is the magnetic card. Here the data carrier is a magnetic metal stripe, sealed on a plastic sheet. This medium requires contact between the card and the reader. The magnetic reader heads, known from the tape recorder, have to be in physical contact with the card. The technology is specified by several standards, such as the ISO 7811, ISO 7812, ISO 7813 and the ISO 4909. The amount of data stored is limited to about a hundred bytes. For example, in the case of a bank card, the same data is stored as shown on the surface, completed with a couple of control data.[1] Its use is still ongoing, due to its simplicity. It is also suitable for identification without supervision. Using a PIN code, you can increase security significantly. Its counterfeiting can be done by reading the magnetic stripe and magnetizing a blank card, so it does not require sophisticated knowledge. Consequently, visual identification is also

[1] See Visdómine, L. P. (2002) *Track format of magnetic stripe cards*. [online] Available from: http://www.gae.ucm.es/~padilla/extrawork/tracks.html [Accessed 10 September 2017].

essential here. For this reason, bank cards typically feature hologram document security elements.

One or two-dimensional barcode cards are also used for identification. The amount of data stored is smaller than on magnetic cards. In the case of one-dimensional (linear) barcode, capacity is a few bytes. The encoding is defined in international standards, widely used are EAN 8 or EAN 13, introduced in 1978. As a further development of the linear barcode, the square data matrix code appeared in the early 1990's. The black-and--white data matrix has a data storing capacity of up to 2335 alphanumeric characters.[2] Similar is the today's fashionable QR code, shown in Figure 1. It can also be read easily by mobile devices, thanks to its design.

Figure 1: QR code[3]

The drawback of these methods is that the barcode is readable for unauthorized persons, it can be copied, and it can be counterfeited. To prevent reading data out, the barcode may have a top coat which can only read by infrared light. By this method, counterfeiting can be significantly complicated.

Figure 2: An earlier version of the USA residency permit[4]

---

[2] See Eiler, E. (2008) Kódnyomtatás és nyomtatott vonalkód rendszerek (Code printing and printed barcode systems), *Magyar Grafika (Hungarian Graphic)*, 2008(5), p. 44.

[3] Kaywa AG. *Kaywa QR Code generator* [online] Available from: https://qrcode.kaywa.com [Accessed 20 August 2017].

[4] Department of Homeland Security. *U. S. Citizenship and Immigration Services: Acceptable Documents*. [online] Available from: https://www.uscis.gov/i-9-central/acceptable-documents/list-documents/form-i-9-acceptable-documents [Accessed 15 September 2017].

Because of its high cost, the laser card is a less popular method. A stripe like a compact disc is sealed on a hard-plastic data carrier, which a laser beam can read in a width of 1.6 to 3.5 cm. The amount of data that can be stored (from 1.1 MB to 2.8 MB) is far higher than the previous methods. In the top line of Figure 2 is a one-dimensional barcode, an optical (laser) data storage under it. At the bottom, there is an MRZ (Machine Readable Zone) code, which simplifies machine data reading.

The standard feature of the cards described so far is that it is not possible or it is very difficult to change their data content. They do not contain active elements, which would allow their safer use. If it is necessary to change the stored data, another method should be applied. A more reliable solution is the use of memory circuits, where data is stored in an electronically programmable non-volatile memory circuit (EEPROM). For convenience reasons, the memory chip is embedded in a larger plastic card. They are used, for example, in Hungarian phone cards. Counterfeiting in the case of commercial memory circuits is not excessively burdensome. The hacker should only attach the reader to a computer and emulate a memory card with credits available.

The use of cards was revolutionized by the introduction of active cards, on which it is not only possible to write and read the data, but the card can do data processing and other mathematical operations. The microcontroller is the core element of the active tags. The microcontroller is a quasi--complete computer, practically made on an integrated circuit card (chip). It contains a processor, a non-volatile memory (ROM, FLASH), a random--access memory (RAM), input/output units (I/O), and other auxiliary elements (such as a real-time clock and similar). The microcontroller enables the implementation of the fourth-generation encryption systems, providing proactive protection for stored data and access. Depending on the type, its storing capacity may range from 1 to 256 kilobytes. Using a microcontroller, you can also create contact and contactless (touchless or proximity) data cards. Such contact data cards are the smart cards (chip cards). These were used in Hungary in the old type of higher education student ID cards, as well as on bank cards (EMV chip). Microcontrollers are also the primary means of storing the private key of the electronic signature (this is done on the SSCD, a secure electronic signature device). There are several international standards relating to chip cards, both from functionality and

security considerations,[5] for example, the ISO/IEC 7816. To read the data, the reader must have direct electronic contact with the microcontroller outlets. Apparently, this is the fastest and safest way of data transfer.

A contactless realization of the proximity card (RFID card) is the micro controller's active data card. The embedded microcontroller is substantially the same as the one used in smart cards. The main difference is that its connection to the reader is made at radio frequency. Its operating principle is that the data card has a large coil antenna, which is connected to the microcontroller. Per the basic design, the card does not contain a power source, but it takes the operating power of the electromagnetic field, generated by the reader. So, while the card is getting closer to the reader, it automatically turns on, and it emits a modulated signal. For example, the card sends an identification number. The reader will check if this identification number is included in its database and, depending on the result, it permits entry. The shortcoming of this system is easily recognizable since only the electromagnetic field of the given frequency is required to obtain the data. So the card reveals its identification number to any reader, including a malicious person's reader. He/she only writes this identification number to an empty card to maliciously copy the original one. To prevent this copying, the reader can also be combined with reader identification. At the time when the card reaches the electromagnetic space, it only indicates its presence, and the reader sends its identification code. The card will only reveal its identification number if the code is listed on the list of authorized readers stored in the card's memory. Data transfer can also be protected by encryption of data transfer, for example, using cryptography or a public key infrastructure (PKI) technology.[6] Because of the radio frequency transmission, the speed of communication and therefore the amount of stored data is also several orders of magnitude smaller than the ones of the contact smart cards. Usually, a length of the 26… 37-bit code is used. The standard reading distance of several centimeters can even be increased up to ten meters (long range proximity) with a built-in battery. Proximity technology is described in the ISO/IEC 14443 standard. In order for these cards to be used in public documents for authentication functions, cards must be improved and configured securely.

[5] See Hassler, V. (1995) *IT Security and Smart Card Standards. Graz*, Austria: Institutes for Information Processing Graz.

[6] Apparently, this is the case with e-Passport and eID solutions. The basic design shows only the security of proximity (RFID) card security.

3. BIOMETRIC IDENTIFICATION IN CARD TECHNOLOGY

The next generation of active cards is their combination with biometric security elements. The most characteristic feature of the human integument is the face, which, due to the underdevelopment of other senses of Homo Sapiens (e.g. smelling), is the primary means of identification of persons in addition to its socio-communication function. Its application is instinctive, and the human race applies it from the beginning. The first trace of using other biometric features was the use of fingerprint in China in the 14th Century, to identify children, which was recorded by the explorer, Joao de Barros.[7] In Europe, first Alphonse Bertillon, a Paris police officer introduced a body-size-based identification system in 1890, for identification of criminals. His method was not successful because of a mass occurrence of false positives. The fingerprint was first used for forensic aims by Richard Edward Henry, at Scotland Yard, based on Bertillon's work. In the 20th century, Karl Pearson at the University College of London, who dealt with applied mathematics, made significant discoveries in biometrics. In the 1960s, considerable progress was made in signature – dynamics analysis, which, however, remained in the military and national security applications. With the increasing threat of terror, the state enforcement of biometric identification in the United States and Western Europe has increased dramatically.

Currently the following biometric features are widely used for identification:

- fingerprint;
- hand geometry;
- palm print;
- vein pattern;
- grip dynamics recognition;
- skull thermal image;
- 2D facial features;
- 3D facial features;
- iris (iris diaphragm) recognition;
- retina (peripheral vein network) recognition;

[7] See Osborn, A. (2005) *Biometrics history. Looking at biometric technologies from the past to the present*. [online] Available from: http://ezinearticles.com/?Biometrics-History----Looking-at-Biometric-Technologies-from-Past-to-Present&id=91803 [Accessed 2 September 2017].

- voice recognition;
- signature dynamics;
- keystroke dynamics;
- DNA;
- recognition of posture.

They are applied to identify people with different success. By mathematical description and storage of biometric features, it is possible to make a more accurate identification, based on individual data.

In the history of travel documents, by the integration of data cards as complementary element and biometrics, as a higher degree of personal bound, a new generation was created, which means significantly higher reliability in the area of document security.

Figure 3: e-Passport[8]

After the United States, the introduction of electronic Passports (e-Passports), shown in Figure 3, has also begun in the European Union. The main reasons for this are increasing the security of travel documents, as well as remaining in the US Visa Waiver Program, which means the visa--free regime of the EU states. For Hungary, the introduction of e-Passport aimed at getting into the program at that time. The e-Passport is an incorporation of a contactless chip card, described above, into the passport. First, saving only the data page, and then the fingerprint as well. E-Passport was first introduced in Sweden in October 2005 in Europe according to the Council of the European Union.[9] In Hungary, since August 2006, the full content of the data page was found in the storage

[8] Bundesamt für Sicherheit in der Informationstechnik. *The electronic passport*. [online] Available from: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/EPassport/epassport_node.htm [Accessed 20 June 2017].

element, together with the photo and signature as well. The fingerprint is also stored since 2008.

By the Council's decision, until 28th June 2009, all the EU states had to move on to apply e-Passports, also containing fingerprints, which triggered resistance of recognized data protection specialists in many EU countries. The new EU-level data protection legislation (GDPR) categorizes biometric data in special category of personal data.[10]

Security measures have been implemented to protect the stored data, but the exact control depends on the member country.[11] Apart from conventional document security procedures (embedded photo and signature, unique patterns, special paints), the electronic storage unit destroys the stored content because of a physical attack.[12] On the other hand, the chip is capable of active authentication, which is done by using the integrated PKI private key, and there is also the digital certificate of the passport publisher in it. For the access to the data page, the Basic Access Control (BAC) method is used. Its operation is as follows: similar to the ID card, the MRZ code can be found in the lower part of the passport data page. The MRZ code contains essential information about the document and its owner, which simplifies machine reading of data. Obtaining the passport number, the birth date and the validity period, the reader generates an access key. The e-Passport will only send stored data to the reader at radio frequency after getting this access key. The physical access to the card is proven this way. This method has insufficient security features. Breaking the key by using the brute force method, because of the approximately 50-bit entropy, is theoretically more than 35 years. However, some data analysis (choosing birth time intervals, tracing passport numbering) reduces entropy to 35-bit so that the key can be

[9] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal of the European Union* (L 385/1) 29 December. Available from: http://data.europa.eu/eli/reg/2004/2252/oj [Accessed 7 May 2018].

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (L 119/1) 4 May. Article 9 (1). Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 7 May 2018].

[11] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal of the European Union* (L 385/1) 29 December. Available from: http://data.europa.eu/eli/reg/2004/2252/oj [Accessed 7 May 2018].

[12] See Jóri, A.; Hegedűs, B.; Kerekes, Zs. (eds.) et al. (2010) *Adatvédelem és információszabadság a gyakorlatban. (Data protection and freedom of information in the practice).* Complex, Budapest.

broken within 3 hours.[13] It has been proven, that the communication, having Basic Protection (BAC), has been cracked in several cases and the data content has been accessed.[14] This encryption is unsuitable for protecting fingerprints, so a more secure procedure has been developed, which is called the Extended Access Control (EAC).[15] The EAC is based on ICAO Doc 9303, but it is not a uniform standard. Member States should also consider the change of numbering to a broader range, or random allocation within the field.

4. EID PROTECTION OPTIONS

In eID documents like in electronic passports a chip is embedded. The stored data can be accessed through a contact or radio interface. As this personal data can be potentially abused, countermeasures should be implemented. By radio interface cards remote reading is possible, by a directional antenna from up to several meters. Thus it is not enough to solve the security by physical protection alone. Under physical protection in this case we mean that we take care of the card and only give it to the one, with whom we want to share its full data content. The potential attack includes eavesdropping on the communication, the acquisition of saved data for example by skimming, as well as tracing. During tracing, the attacker prepares a profile of the target, following the geographic movement of the card. Unfortunately, the latter is allowed by the ISO 14443 standard, which requires the unique identification of the chip card, before communication.[16]

One of the most typical ways of protection is encryption, where the encryption algorithm is known by all compatible card readers, but with the symmetric encryption key, only readers, with whom we want to share the data, have the possibility of decryption. In this case, we encounter the key distribution problem, so if you have one hundred thousand readers, you either use the same password for all, and you cannot change

[13] Robroch, H. (2006) *ePassport Privacy Attack. Cards Asia Singapore.* [online] Available from: https://pdfs.semanticscholar.org/828a/70de925744617be3d2886442cd0e88058c25.pdf [Accessed 27 October 2017].

[14] See Papp, Z. (2010) Az új technológiák veszélyei: RFID és az elektronikus útlevél (Hazards of new technologies: RFID and e-Passport), *Hadmérnök (Military Engineer)*, 5(4), pp. 248–254.

[15] See Moses, T. (2010) *Protecting Biometric Data with Extended Access Control.* [online] Available from: https://www.entrust.com/wpcontent/uploads/2010/01/WP_Entrust_ePassport-Biometrics_Aug2014.pdf [Accessed 4 September 2017].

[16] See Naumann, I.; Hogben, G. (2008) Privacy features of European eID card specifications, *Network Security*, August.

the compromised keys, or each reader uses a separate password, but then passport management is challenging. The control of the readers' passwords on the issued cards is impossible from an organizational point of view. This method can only be applied in a closed system, for example, in the case of a corporate solution.

With authentication controls, we want to limit access to data. In this case, a short identification code should be provided from the reader's side, which can be called a PIN (Personal Identification Number), CAN (Card Access Number) or code. The reader device uses this piece of information to identify itself with the card. The card gives out the stored data only to the reader, which is determined in this way. The communication can optionally be encrypted, which can happen with a session key, used in the given connection, with a predetermined symmetric key, or the public key-secret key pair, used for asymmetric encryption. The latter may be, for example, supplied with a service provider certification, operated by the issuing authority. The memory of the card can be divided into several parts, according to the confidentiality of the data. The Spanish electronic identity card's memory is divided into three sections, for example, access to the public portion is not restricted, access to the secret area requires the PIN code of the card, while only public administration have access to the protected area.[17]

The plan of the electronic European Health Insurance Cards offers an exciting authentication option, which defines authentication between two smart cards. In doing so, health data, stored on the health insurance card (HIC) of the patient, can be accessed only with the health professional card (HPC) of the doctor, thus ensuring the protection of medical data.

Access to data may also be restricted by using an identifier. In this case, eID shares only a user ID (UID) with the service provider, who logs into a central database, to retrieve the data that can be accessed by him/her by the UID. However, public administration, regardless of all these, may have direct access to the data, stored on the card. This solution can also raise several questions, including data protection issues, affecting the use of a single identifier, a central database, accessible by market participants and similar problems.

[17] Sotirov, A. et al. (2009) Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. In: Halevi, S. (eds.) *CRYPTO, LNCS 5677*, pp. 55–69.

The protection of the privacy is more efficiently implemented by modifying the previous ID configuration method, with the use of hashes. A fingerprint is generated from an input data with a so-called hash function, which is a trapdoor function, which means, that performing it in one direction is simple, but in the other direction, it is a complicated mathematical task. This algorithm generates a constant amount of data (128–512 byte) from any amount of data. A change of a single bit in the input data set will change at least 50 percent of the output bits (this is the avalanche effect). The amount of data, applied as output, is called a fingerprint since it characterizes the input data amount nearly in a unique way. The input cannot be generated from the hash code. In practice, typically the SHA-256, SHA-512, SHA-3 or the Whirlpool, or the algorithms are encountered. The use of obsolete algorithms, like the MD5, SHA-1 or RIPEMD-160 is no longer secure for electronic signatures or similar purposes.[18] If the hash value is formed from the UID by a usage-dependent identifier, we make it harder for malicious providers to merge personal data, which are stored in various databases. Practically the decryption of the original (unified) UID from those is a mathematically impossible task.

An additional way of privacy protection is that the card does not provide personal data, stored on it, but only offers the possibility of comparison. In this case the reader optically reads the data and sends it to the chip. The chip only confirms that the sent data are the same as the data stored in the secure container. An example of this solution is the checking of the fingerprint pattern. The reading device reads the fingerprint of the person, who shows the identity document. The reader generates a digital model from the optical picture, which can be interpreted by the card. The card compares it with the fingerprint data, stored in its storage and provides a percentage-probability value to the reader, regarding the probability of the match. In this case, the reliability of the card is essential, so the card must provide the answer to the reader, not the attacker.

It is also possible to identify the user if the card is capable of electronic signature. One option is when the card creates a protected channel with the system, which requires the identification, using a key-exchange protocol (e.g. Diffie–Hellman Key Exchange). The other option is if the system

[18] Ibid.

requesting the authentication sends a generated (pseudo) random dataset and it is electronically signed and returned by the person to be identified. Although technically both solutions are right, misuse of the data is more likely in the latter case, if the data package to be signed is not random, but targeted generated data.

5. NEW IDENTITY CARD IN HUNGARY

Instead of the former paper-based identity card, the Government Decree No. 168 of 1999 (XI. 24.) issued a plastic card-based identity card from January 2000, shown in Figure 4. This step aligns with the initiative of the government to increase information security in e-governmental relations.[19] In addition, the ID1 (85.6 mm x 53.98 mm)[20] standard card size and water resistance are also favored by the cardholders. Its disadvantage or just property was that it did not contain the address, which was issued to the legitimate holder on a separate card (the same size) on the residence permit certificate. This document has undergone several minor updates.

Figure 4: Hungarian Identity Card between 2000–2015[21]

A significant change happened by introducing the electronic Personal Identification Card (eID or "eSzemélyi" in Hungarian), from 1st January 2016, shown in Figure 5, by the Government Decree No. 414 of 2015 (XII. 23.). In addition to the altered design and the new type of security features, the eID has introduced a contactless, active storage device,

[19] For detailed analysis of improving security legislation see Szádeczky, T. (2014): Information Security – Strategy, Codification and awareness. In: Nemeslaki, A. (ed.): *ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary*. Budapest, pp. 109–122.

[20] Defined in the ISO/IEC 7810 standard.

[21] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-03001.* [online] Available from: http://www.consilium.europa.eu/prado/en/HUN-BO-03001/index.html [Accessed 20 September 2017].

accessible via a radio interface, that is similar to the one that has already been used for a decade for electronic passports.

Figure 5: Hungarian Identity Card from 2016[22]

The visual content of the eID is practically the same as that of the old identity card. The optical and electronic data content of the new type of identity card is included in the relevant Hungarian Act.[23] These data have been edited in Table 1.

Information Contained	Visually[24]	In machine (MRZ) code	In storage device[25]
Name of the citizen	Yes	Yes	Yes
Name of citizen, in a minority language	At the request of the citizen, belonging to the minority[26]	N/A	N/A
Place of birth	Yes	N/A	Yes
Date of birth	Yes	Yes	Yes
Nationality	Yes	Yes	Yes
Mother's name	Yes	Yes	Yes
Gender	Yes	Yes	Yes

[22] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-05001.* [online] Available from: http://www.consilium.europa.eu/prado/en/HUN-BO-–05001/index.html [Accessed 20 September 2017].

[23] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 29.

[24] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 29. Paragraph 2.

[25] The document, "without deadlines", which is available for those, over 65 years old, is in fact a document, the validity of which is 60 years, and it does not contain any storage element, see *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 29/E. Paragraph 2.

[26] *Hungarian Government Decree No. 414 of 2015 (XII. 23.) on issuing of ID cards and collection of facial photo and signature.* Hungary. Section 33. Paragraph 1.

Facial Image	Yes	Yes	Yes
Signature	In case of literate person aged over 12 years	N/A	In case of literate person aged over 12 years
Validity	Yes	Yes	Yes
Document ID	Yes	Yes	Yes
Issue Date	Yes	Yes	Yes
Issuing Authority	Yes	Yes	Yes
Travel restrictions on traveling abroad	In specific cases and ways	N/A	In specific cases and ways
Code number (CAN), needed to start legitimate access to the data, recorded in the storage element	If there is a storage element	N/A	N/A
Fingerprint	N/A	N/A	In case of a person aged over 12 years, if he/she has not refused it, and if he/she is not physically unable to enroll
Data needed to create the electronic signature	N/A	N/A	At the request of the citizen
Social security identification number	N/A	N/A	Yes
Tax identification number	N/A	N/A	Yes
The electronic, unique identifier of the identity card	N/A	N/A	Yes
No more than two emergency phone numbers to be notified	N/A	N/A	At the request of the citizen

Table 1: Data content of the Hungarian eID[27]

The validity of the permanent identity card is three years, under the age of 18, and six years above that. Identity cards may be issued "without a deadline" for people aged above 65 years (the validity of which is in fact 60 years), and they do not contain any electronic storage element. The duration of the validity of the identification card, as a rule, fits the birth date of the eligible person.[28]

[27] Edited by the author, based on *Hungarian Act LXVI of 1992 on register of citizens' personal data and address*.

[28] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 29/E.

The identification card falls within the scope of national development competence, for which the European Union lays down security and functional requirements. As a document that can be used for proof of identity, the eID belongs to the highest document protection category.[29] According to the requirements, it must be protected against full or partial forgery. For protection methods, the chemical, physical, technical, technological and administrative procedures, and digital security methods shall be used together.[30] Specific protection solutions have been defined in the document protection plan, and they are not publicly available. However, the picture of the document and specific security elements of it are publicly available in the European Public Register of Authentic Travel and Identity Documents Online (PRADO) system.

According to the Regulation on the Protection of Security Documents, the electronic security document contains a data storage device, which is capable of storing the data. It is integrated into the material. In addition to the document protection categories, the law also names the document information security categories.[31]

In case of the eID, the following requirements apply:

- the stored data are encrypted, the encryption algorithm is at least RSA 2048;
- limitation of recording, writing and overwriting of the data;
- application of extended access protocol;
- protected communication channel between the data storage and the reader;
- manufacturer's certification of the data storage.

The storage element is an electronic data carrier unit,[32] which has a certificate (CC EAL5+) according to the Common Criteria for Information Technology Security Evaluation, and it is qualified as a secure signature creation device (SSCD).[33]

---

[29] *Hungarian Government Decree No. 86 of 1996. (VI. 14.) on the protection of security documents.* Hungary. Section 5/A (5)

[30] *Hungarian Government Decree No. 86 of 1996. (VI. 14.) on the protection of security documents.* Hungary.

[31] *Hungarian Government Decree No. 86 of 1996. (VI. 14.) on the protection of security documents.* Hungary. Appendix 2., II.

[32] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 19.

[33] See Szádeczky, T. (2010) Pillars of IT Security, *Studia Iuridica Auctoritate Universitatis Pécs Publicata*, 2010(147), pp. 247–268.

6. EID IN GERMANY AND IN EUROPE

A number of EU member states have already implemented an eID solution, but this does not mean that all are implementing eID functions to the National ID like Germany and Hungary. Here eID refers to the Electronic Identification (eID) function for using public and private services. Table 2 shows the form of the eID solution per country. As of today, 14 member states have implemented a national ID-based eID solution.

Member State	Form of the eID
Austria	other forms
Belgium	National ID
Bulgaria	National ID
Croatia	other forms
Cyprus	online
Czech Republic	National ID
Denmark	online
Estonia	National ID
Finland	other forms
France	online
Germany	National ID
Greece	online
Hungary	National ID
Ireland	online
Italy	National ID
Latvia	National ID
Lithuania	National ID
Luxembourg	National ID
Malta	National ID
Netherlands	National ID
Poland	N/A
Portugal	National ID
Romania	N/A

Slovakia	National ID
Slovenia	other forms
Spain	National ID
Sweeden	other forms
United Kingdom	other forms

Table 2: eID solutions in the EU[34]

The Hungarian eID solution is apparently[35] based on the German National Identity Card ("neue Personalauseis" in German) and the Electronic Residence Permit, shown in Figures 6 and 7.[36]

Figure 6: German identity card from 2011[37]

The German federal government introduced the new electronic identity card in 2011 to change the old paper-based ones.[38] The validity of the permanent document over 24 years is ten years. In contrast to the free Hungarian eID, the standard German eID (permanent, over 24 years) costs 28,80 Euro.[39]

---

[34] Edited by the author, based on PRADO and the data collected by the European Commission. Available from: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID [Accessed 6 February 2018].

[35] No official communication was found about a German–Hungarian cooperation on this topic but hardware, software and reader type shows that the German solution was the sample for the Hungarian government.

[36] Electronic identification schemes notified pursuant to Article 9(1) 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. *Official Journal of the European Union* (2017/C 319/3) 26 September. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2017.319.01.0003.01.ENG&toc=OJ:C:2017:319:TOC [Accessed 15 November 2017].

[37] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) DEU-BO-02001.* [online] Available from: http://www.consilium.europa.eu/prado/en/DEU-BO-02001/image-166166.html [Accessed 13 November 2017].

[38] *German Act on Identity Card 2009 (Personalausweisgesetz - PAuswG)*, BGBl. I S. 1346. Germany.

7. FUNCTIONALITY AND SECURITY

Both the German and the Hungarian electronic identity cards have three main functions:

1. Electronic Travel Document (ePASS) function;
2. Electronic Identification (eID) function;
3. Electronic Signature (eSIGN) function.

The purpose of the Electronic Travel Document (ePASS) is to ensure cross-border access as regulated in the Schengen Agreement. Therefore, in this aspect, it can only replace the passport just in specific cases.

The electronic identification function makes the usage of the e-government functions more efficient. It is also planned that cross--border service will be available later, the area also appears as the European Union Common List of Basic Public Services List (EU CLBPS, a Common List of Basic Public Services) or otherwise as a 12+8-list element.[40] The eID functions are defined in the electronic IDentification, Authentication and trust Services (eIDAS)[41] and in the Connecting Europe Facility (CEF).[42] Nonetheless, implementation in the Member States is slow and far from what is expected in both the degree of application and the content.[43] The cooperation between the EU member states is at a high level[44], and as of 29 September 2018, the recognition of notified eID solutions will

---

[39] *German Decree on Identity Card Price* (*Personalausweisgebührenverordnung, PauswGebV*) *2010,* BGBl. I S. 1477. Germany. § 1 (1) 2.

[40] See Szabó, A. B. (2016) Okmányvédelem és az elektronikus személyazonosító igazolvány (Document security and the electronic ID card), *Hadmérnök (Military Engineer)*, 11(1), pp. 13–17.

[41] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) 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. *Official Journal of the European Union* (L 53/14) 25 Febr. Available from: http://data.europa.eu/eli/dec_impl/2015/296/oj [Accessed 7 May 2018].

[42] Regulation (EU) No. 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No. 913/2010 and repealing Regulations (EC) No. 680/2007 and (EC) No. 67/2010. *Official Journal of the European Union* (L 348/129) 20 December. Available from: http://data.europa.eu /eli/reg/2013/1316/oj [Accessed 7 May 2018].

[43] See Siddhartha, A. (2008) National e-ID card schemes: A European overview, *Information Security Technical Report*, 2008(13), pp. 46–53.

[44] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) 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. *Official Journal of the European Union* (L 53/14) 25 Febr. Available from: http://data.europa.eu/eli/dec_impl/2015/296/oj [Accessed 7 May 2018].

become mandatory. The Hungarian eID itself, according to the available information, is ready to be notified. However, as of today, the only notified solution is the German National Identity Card and the Electronic Residence Permit.[45] In fact, the problem lies not with the issuer, but at the acceptance,[46] because member states are not yet ready to accept another member states' eID card.[47] The reason for that is hardware, firmware and software incompatibilty.

The electronic signature (eSIGN) function is, in contrast to the previous two features, entirely in the interest of the user. It is possible to create an electronic signature on any document with the embedded PKI key pair with S/MIME certificates. The process of creating an electronic signature is as follows: a specific hash function (e.g. SHA-256) generates a hash code (fingerprint) from the data. A PKI cryptographic private key (of the signer) encrypts this hash code, so we get the electronic signature, which will be a data packet, independent of the input document (but might be attached to it). The signed document and the electronic signature can be sent to a recipient via a public channel, such as an e-mail. The recipient deciphers the electronic signature with our public key, so he/she gets the hash code which we have created. In the meantime, he/she also produces the fingerprint from the document sent and compares these two. If they are the same, it shows that there is no change in the signed document, and, that the signature of the document was carried out by a specific key. However, this does not link the private key to a natural person, it does not prove that it has not been revoked, and it is not possible to determine the time of signature either. To solve these issues, additional functions should be used.

There are two ways to solve the problem of connecting a key to a person, i.e. to address the authenticity problem: on the one hand, by the web of trust

---

[45] Electronic identification schemes notified pursuant to Article 9(1) 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. *Official Journal of the European Union* (2017/C 319/3) 26 September. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2017.319.01.0003.01.ENG&toc=OJ:C:2017:319:TOC [Accessed 15 November 2017].

[46] Hornung, G. (2005) *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren (The digital identity. Legal problems of chipcard-IDs: digital national ID, electronic social security card, JobCard-process).* Nomos, Baden Baden, p. 379.

[47] See the current implementation report at CEF Digital. *Country overview: eIDAS-Node Implementation*. [online] Available from: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID [Accessed 15 November 2017].

method, used by PGP.[48] This way, each person's keys are signed by the persons, trusting each other. So if the recipient knows any person signing the sender's key or he/she can trace back the signatures to a trusted person, then this will also guarantee the reliability of the person. The disadvantage of this method is that it requires extensive trust networks, i.e. that two people who do not know each other have a common acquaintance. The other way is to use the S/MIME system. Here the reliability of the parties is certified by a third party, trusted by each side, through a certificate, which is an electronic data set including the public key as well. The third party is a Certificate Service Provider, CSP, considered as a trustworthy person by the government, who checks the association of the key and the key holder before issuing the certificate, for example by requiring to provide an identity card. These certification providers form a certification chain, with the highest certification authority (CA) at the top. These CAs are accepted by the public at large, and hence, the rest of the certification chain also becomes reliable.

Authentication of the signing time is done by the Time Stamping Authority (TSA), who provides the exact time with their electronic signature, which the sender will incorporate into the electronic signature of the document. The application for the time stamp is carried out online via the Internet. The reliability of the TSA is ensured by its certificate, which can be traced back to a CA along the certification chain. The use of electronic signatures or certificates is usually limited. Typically, a key pair can only be used for electronic signature or encryption or setting up a secure link (SSL). If one wants to use several functions from these, more key pairs or certificates may be needed.

The e-signature and time stamping service, related to the new identity card, is provided by the NISZ National Infocommunications Service Company Ltd., as a government authentication service provider. The certification applied in the Hungarian eID corresponds to the requirements of the eIDAS Regulation[49], just like the German eID.[50]

---

[48] See Alfarez, A.-R. (1997) The PGP Trust Model. *EDI-Forum*, April.

[49] 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. *Official Journal of the European Union* (L 257/73) 28 August. Available from: http://data.europa.eu/eli/reg/2014/910/oj [Accessed 7 May 2018].

[50] Hornung, G.; Engemann, C. (2016) *Der digitale Bürger und seine Identität (The digital citizen and his identity).* Nomos, Baden Baden, p. 207.

The Hungarian eSzig Card Management Utility[51] can be used to activate and change the electronic PIN codes and to see e-signature certificates. It runs on the 7, 8, 8.1, 10 32 and 64-bit versions of the Microsoft Windows. It also supports the versions of the Apple Mac OS X Yosemite, El Capitan, Sierra, and some Linux distributions and versions (CentOS 7, Debian 8, SuSe 13.2, Ubuntu 14.04.5 LTS).[52] Its developer is ID&Trust Ltd., a small Hungarian business operating on the international chip card market.

The German desktop-based application is called "AusweisApp2". It has a different design, but similar functionality: the user may see the data stored on the card and may change the PIN code. There is also a function where the links to the available services are collected. The developer is Governikus GmbH & Co. KG. In both cases, the Ministry of Interior is responsible for the development and the operation. Both applications are lack of integrated functions. Thus the citizen does not need to use them regularly. But active usage is required for the acceptance of e-government services.[53]

8. CONCLUSION

With the development of card-based data storage technology and the increasing data storage and processing capacity of the cards, they can be used more and more efficiently for access and personal identification. With increasing complexity, the volume and quality of the stored data are also growing. Earlier, there was far less personal data printed on the card. The development in functionality, in addition, poses a new data protection risk.

From the functional side by the introduction of the electronic identity card (eID), the Hungarian government, similarly to some other EU governments, like Belgium, Estonia, and Germany, has made a considerable leap in e-government and it has opened up a number of widely available functions.

The electronic identification and electronic signature functions may revolutionize the e-government and electronic literacy, since the governments provide all the required elements. In Hungary, this means

[51] Hungarian Ministry of Interior. (2017) *eID thematic website.* [online] Available from: http://www.kekkh.gov.hu/Eszemelyi/ [Accessed 24 September 2017].

[52] Hungarian Ministry of Interior. (2017) *eID thematic website.* [online] Available from: http://www.kekkh.gov.hu/Eszemelyi/kartya_funkcioi/kartyaolvaso_alkalmazas [Accesed 24 September 2017].

[53] Bieler, F. Schwarting, G. (2007) *e-Government. Perspektive – Probleme – Lösungsansätze (Perspective, Problems, Solutions).* Erich Schmidt Verlag, Berlin, p. 271.

free access to both of above functions, which makes the critical element of the electronic literacy widely accessible. Using of "may" is due to the skepticism of the author: by the appearance of electronic signature in the 2000s and then the rapid legislation, made the professionals hope for a wide range of application, which eventually did not happen. In any case, the governments do indeed create at least the possibility of development by providing the new type of identity cards.

All new technologies and increasing complexity also generate new types of risks, which the governments and citizens must take into consideration. Cryptographic measures are effective against a lot of attacks, e.g. using well-known algorithms with large keys protects us from eavesdroppers. However, cryptography does not defend us in every case. The Estonian eID was using a well-known, certified chip, but the implementation was vulnerable to the Coppersmith attack for some years. Because of this, 750,000 valid Estonian eIDs became compromised, which is the worst nightmare of any issuers.[54] Nevertheless, in some cases, tracking is by design possible. In such cases, the citizen will need to apply additional technical and organizational measures.

LIST OF REFERENCES

[1] Alfarez, A.–R. (1997) The PGP Trust Model. *EDI-Forum*, April.

[2] Bieler, F. Schwarting, G. (2007) *e-Government. Perspektive – Probleme – Lösungsansätze (Perspective, Problems, Solutions)*. Erich Schmidt Verlag, Berlin.

[3] Bundesamt für Sicherheit in der Informationstechnik. *The electronic passport*. [online] Available from: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/EPassport/epassport_node.htm [Accessed 20 June 2017].

[4] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic Identification pursuant to Article 12(7) 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. *Official Journal of the European Union* (L 53/14) 25 February. Available from: http://data.europa.eu/eli/dec_impl/2015/296/oj [Accessed 7 May 2018].

[54] See Goodin, D. (2017) *Millions of high-security crypto keys crippled by newly discovered flaw, ars technica.* [online] Available from: https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/ [Accessed 16 November 2017].

[5] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal of the European Union* (L 385/1) 29 December. Available from: http://data.europa.eu/eli/reg/2004/2252/oj [Accessed 7 May 2018].

[6] Department of Homeland Security. *U. S. Citizenship and Immigration Services: Acceptable Documents*. [online] Available from: https://www.uscis.gov/i-9-central/acceptable-documents/list-documents/form-i-9-acceptable-documents [Accessed 15 September 2017].

[7] Eiler, E. (2008) Kódnyomtatás és nyomtatott vonalkód rendszerek (Code printing and printed barcode systems), *Magyar Grafika (Hungarian Graphic)*, 2008(5), pp. 42–47.

[8] Electronic identification schemes notified pursuant to Article 9(1) 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. *Official Journal of the European Union* (2017/C 319/3) 26 September. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2017.319.01.0003.01.ENG&toc=OJ:C:2017:319:TOC

[9] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-03001.* [online] Available from: http://www.consilium.europa.eu/prado/en/HUN-BO-03001/index.html [Accessed 20 September 2017].

[10] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-05001.* [online] Available from: http://www.consilium.europa.eu/prado/en/HUN-BO-05001/index.html [Accessed 20 September 2017].

[11] *German Act on Identity Card 2009* (*Personalausweisgesetz – PauswG),* BGBl. I S. 1346. Germany.

[12] *German Decree on Identity Card Price (Personalausweisgebührenverordnung, PauswGebV) 2010,* BGBl. I S. 1477. Germany.

[13] Goodin, D. (2017) *Millions of high-security crypto keys crippled by newly discovered flaw, ars technica*. [online] Available from: https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys750kestonian-ids/ [Accessed 16 November 2017].

[14] Hassler, V. (1995) *IT Security and Smart Card Standards*. Graz, Austria: Institutes for Information Processing Graz.

[15] Hornung, G. (2005) *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren (The digital identity. Legal problems of chipcard-IDs: digital national ID, electronic social security card, jobCard-process)*. Nomos, Baden Baden.

[16] Hornung, G.; Engemann, C. (2016) *Der digitale Bürger und seine Identität (The digital citizen and his identity)*. Nomos, Baden Baden.

[17] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address*. Hungary.

[18] *Hungarian Government Decree No. 414 of 2015 (XII. 23.) on issuing of ID cards and collection of facial photo and signature*. Hungary.

[19] *Hungarian Government Decree No. 86 of 1996. (VI. 14.) on the protection of security documents.* Hungary.

[20] Hungarian Ministry of Interior. (2017) *eID thematic website.* [online] Available from: http://www.kekkh.gov.hu/Eszemelyi/ [Accessed 24 September 2017].

[21] Hungarian Ministry of Interior. (2017) *eID thematic website.* [online] Available from: http://www.kekkh.gov.hu/Eszemelyi/kartya_funkcioi/kartyaolvaso_alkalmazas [Accesed 24 September 2017].

[22] Jóri, A.; Hegedűs, B.; Kerekes, Zs. (eds.) et al. (2010) *Adatvédelem és információszabadság a gyakorlatban. (Data protection and freedom of information in the practice)*. Complex, Budapest.

[23] Kaywa AG. *Kaywa QR Code generator* [online] Available from: https://qrcode.kaywa.com [Accessed 20 August 2017].

[24] Moses, T. (2010) *Protecting Biometric Data with Extended Access Control.* [online] Available from: https://www.entrust.com/wp-content/uploads/2010/01/WP_Entrust_ePassport-Biometrics_Aug2014.pdf [Accessed 4 September 2017].

[25] Naumann, I.; Hogben, G. (2008) Privacy features of European eID card specifications, *Network Security*, August.

[26] Osborn, A. (2005) *Biometrics history. Looking at biometric technologies from the past to the present*. [online] Available from: http://ezinearticles.com/?Biometrics-History----Looking-at-Biometric-Technologies-from-Past-to-Present&id=91803 [Accessed 2 September 2017].

[27] Papp, Z. (2010) Az új technológiák veszélyei: RFID és az elektronikus útlevél (Hazards of new technologies: RFID and e-Passport), Hadmérnök (*Military Engineer),* 5(4), pp. 248–254.

[28] 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. *Official Journal of the European Union* (L 257/73) 28 August. Available from: http://data.europa.eu/eli/reg/2014/910oj [Accessed 7 May 2018].

[29] Regulation (EU) No. 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No. 913/2010 and repealing Regulations (EC) No. 680/2007 and (EC) No. 67/2010. O*fficial Journal of the European Union* (L 348/129) 20 December. Available from: http://data.europa.eu/eli/reg/2013/1316/oj [Accessed 7 May 2018].

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (L 119/1) 4 May. Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 7 May 2018].

[31] Robroch, H. (2006) *ePassport Privacy Attack. Cards Asia Singapore.* [online] Available from: https://pdfs.semanticscholar.org/828a/70de925744617be3d2886442cd0e88058c25.pdf [Accessed 27 October 2017].

[32] Siddhartha, A. (2008) National e-ID card schemes: A European overview, *Information Security Technical Report*, 2008 (13), pp. 46–53.

[33] Sotirov, A. et al. (2009) Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. In: Halevi, S. (eds.) *CRYPTO, LNCS 5677*, pp. 55–69.

[34] Szabó, A. B. (2016) Okmányvédelem és az elektronikus személyazonosító igazolvány (Document security and the electronic ID card), *Hadmérnök (Military Engineer),* 11 (1), pp. 13–17.

[35] Szádeczky, T. (2014): Information Security – Strategy, Codification and awareness. In: Nemeslaki, A. (Ed.): *ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary*. Budapest, pp. 109–122.

[36] Szádeczky, T. (2010) *Pillars of IT Security, Studia Iuridica Auctoritate Universitatis Pécs Publicata*, 2010 (147), pp. 247–268.

[37] Visdómine, L. P. (2002) *Track format of magnetic stripe cards*. [online] Available from: http://www.gae.ucm.es/~padilla/extrawork/tracks.html [Accessed 10 September 2017].