International experiences in terms of electronic identification

(Doświadczenia międzynarodowe w zakresie systemu elektronicznej identyfikacji)

Sz Jakubowski [1,A,D], A Romaszewski [1,C,F], Z Kopański [1,E] , J Strychar [2,B] , M Liniarski [2,B], T Kilian [2,A,B]

Abstract – The authors have discussed the models of electronic identification systems used in the European countries and the USA. In many countries, the state has defined only the basic standards of functioning for the engaged institutions as part of safety and interoperability guarantee. The trust services market in Europe has been defined, while putting an emphasis on its diversity. The most common trust service offered by entrepreneurs or private and public institutions is the issuance of qualified certificates. On the other hand, the trust services providers very rarely undertake to create qualified electronically registered services, probably due to the complexity of the enterprise. Also the issues of electronic identification security undertaken by the EU states.

Key words - models of electronic identification systems, EU, USA.

Streszczenie – Autorzy mówili modele systemów identyfikacji elektronicznej stosowane w krajach europejskich i USA. W wielu krajach państwo w ramach zapewnienia bezpieczeństwa i interoperacyjności określiło jedynie podstawowe standardy funkcjonowania dla zaangażowanych instytucji. Scharakteryzowano rynek usług zaufania w Europie, podkreślając jego duże zróżnicowanie. Najczęstszą usługą zaufania oferowaną przed przedsiębiorców, instytucji prywatnych i publicznych jest wydawanie kwalifikowanych certyfikatów. Natomiast najrzadziej, prawdopodobnie ze względu na poziom skomplikowania przedsięwzięcia dostawcy usług zaufania podejmują się stworzenia kwalifikowanych usług, rejestrowanych elektronicznych doręczeń. Omówiono także kwestie bezpieczeństwa w elektronicznej identyfikacji podejmowane w państwa EU.

Słowa kluczowe - modele systemów identyfikacji elektronicznej, EU, USA.

Author Affiliations:

1. Faculty of Health Sciences, Collegium Medicum, Jagiellonian University
2. Collegium Masoviense – College of Health Sciences, Żyrardów

Authors' contributions to the article:

A. The idea and the planning of the study
B. Gathering and listing data
C. The data analysis and interpretation
D. Writing the article
E. Critical review of the article
F. Final approval of the article

Correspondence to:

Prof. Zbigniew Kopański MD PhD, Faculty of Health Sciences, Collegium Medicum, Jagiellonian University, P. Michałowskiego 12 Str., PL- 31-126 Kraków, Poland, e-mail: zkopanski@o2.pl

Accepted for publication: November 28, 2018.

I. THE MODELS OF ELECTRONIC IDENTIFICATION SYSTEMS

The electronic identification system emerging in Poland (also in the healthcare sector), together with the included authentication process, is based upon a federative model [1]. There are three basic models of electronic identification systems. The first one is a centralised scheme when the state is liable for the central management of its citizens' digital identity. It is acceptable to cooperate with private entities which may offer electronic identification and authentication services. However, in order to confirm the data, these entities shall need an access to a central state database the private institutions depend on. This system operates in Italy, Belgium, India or Pakistan. The second model, far more popular in Europe, is called federative and assumes cooperation between public and private institutions. The infrastructure of this scheme is defined e.g. by the legislator but it allows for the cooperation of a number of systems and tools of public and private identification. One of the first countries which successfully introduced this model is Estonia which makes a good example of a well-functioning system for the remaining countries. This system operates also in Finland, Norway and Great Britain. The third one is an open market model which allows for free cooperation of private and public entities in terms of accessibility of identification services and the used tools. This scheme works in the United States, where the government has defined only the basic standards of functioning for the engaged institutions as part of the process of ensuring security and interoperability [1].

Estonia is a country which has a big experience in the field of electronic identification and digital services. Nearly 100 percent of Estonian citizens have an access to electronic identification means through which they can realise most of public administration services in a digital manner. An ID card with electronic layer, identity confirmation performed by banking or IT systems are only a few examples of widely available electronic identification means [1].

According to Accenture report from 2017, about 300 thousand qualified certificates have been issued in Poland so far and they are used with qualified electronic signatures. Additionally, six entities have been operating within the trust services domain in Poland, offering 27 services in total. These institutions include: Unizeto Technologies S.A., Polska Wytwórnia Papierów Wartościowych [Polish Security Printing Works], Krajowa Izba Rozliczeniowa S.A. [National Clearing House], ENI GMA Systemy Ochrony Informacji [Information Security Systems], Eurocert and Asseco Data Systems [2].

II. TRUST SERVICES MARKET IN EUROPE

The trust services market in Europe is quite diversified. In 2017 the market involved 29 engaged countries with 150 qualified trust services providers and about 1000 qualified trust services. The biggest number of companies offering trust services comes from Germany (72 providers) and Italy (70 providers) (Figure 8). Additionally, we can observe a tendency for some entities to provide their trust services locally within their countries, while others tend to work internationally [2].

The most common trust service offered by entrepreneurs and private or public institutions was the issuance of qualified certificates which constituted 75% of all services. The least common, on the other hand, probably due to the complexity of the enterprise, are the qualified services of registered electronic deliveries and as such they constitute only 1% of all trust services. [2].

In terms of security, we must remember about three things. First of all, every electronic system containing medical data should be protected by means of encryption controlled by the owner and enabling safe storage, transmission and access. Secondly, the process of setting up and maintaining the patient's documentation should preserve not only the contents authenticity, but also data integrity and configurable patient's privacy in the whole process of documentation integrity with other entities (including open and closed healthcare). Last but not least, it is important that providing access to medical documentation and sharing it ensures a comprehensive verification of resources through signatures and certification process against blind demands and unauthorised data alterations crucial for patients' health and users' contracts [3].

26 European countries use solutions based upon electronic identification of their citizens. The Ministry of Digitization and the Ministry of the Interior and Administration in Poland are currently making the second attempt to design such tool in the form of electronic ID. The first attempt made as part of the pl.ID project financed by EU fund was not completed in due time and the whole enterprise was abandoned. The second attempt assumes that the first electronic IDs shall be introduced by the end of March 2019. The proposed tool will be in the form of ID card with an electronic layer and will be used for the authentication purposes in digital services of public administration and healthcare, including signing electronic documents [4].

It is important that the designed electronic document provides a high-level authentication in case of an access to the patient's sensitive medical data, its approval or signing. Additionally, apart from electronic ID, another project coordinated by the Ministry of Health is planned and it involves the introduction of Medical Specialist Card [Karta Specjalisty Medycznego- KSM]. This useful tool will make easier for health professionals to create and send authorised electronic documents like e-sick leaves, e-prescriptions or e-referrals in a safe manner [4,5].

The primary concept of electronic ID has changed. Due to the eIDAS regulation, which added another type of signature (advanced electronic signature) and advised technological neutrality, a wider scale of action could be introduced. Thanks to it, an easier connection with Electronic Lines will be planned. Additionally, solutions based upon cloud computing such as a server signature or „on the fly" signature are being considered. [4].

The method of server signature involves storing the keys (encrypted data) necessary to identify the user on the side of the service provider, whereas the authentication process uses other mechanisms including tokens, one-time passwords, mobile devices and others [2]. This is a business-based solution with an entrepreneur offering his digital services to a public institution as part of a concluded agreement. The following types of sharing can be specified: software sharing (software-as-a-service), technical infrastructure sharing (infrastructure-as-a-service) or a combination of the two abovementioned types- full-functionality platform (platform-as-a-service). This method functions in Austria where the authentication process is performed by means of one-use SMS password [6].

Another technique of electronic signature, which could be considered for future use is the so-called "on the fly" signature. In this method the user's identity is confirmed by means of an electronic ID or special data used for appending signatures, certification or digital data destruction [2,7].) The „on the fly" signature service can be operated with mobile applications or web platforms using the Internet link and webpage mechanisms. The advantage of this method is the lack of obligation to store the key used for appending the user's signature as it has a temporary form. This method lowers the cost of the service operation due to the fact that appending the electronic signature is charged only once, you don't bear the costs of certificate validity extension for the following two years. The „on the fly service" provider makes the environment for appending signatures available to the user while informing him/her at the same time about the legal effects of electronic signatures and the contents of electronic document. The approval being made, the signatory starts the digital signature mechanism which generates temporary certificate on the basis of identifying data [2]. This method guarantees security in accordance with the eIDAS regulation.

Entities conducting healthcare activity may use one of the two solutions (optionally a modification thereof) while processing the patients' data. The first solution involves data processing and safeguarding on the organisation's premises while performing legally imposed activities. The second solution is to transfer by contract the responsibility for IT systems and data security to a professional third-party. One of the positive aspects is the fact that a coalition of Cloud Infrastructure Services Providers in Europe (CISPE) has been established which specifies the standards of data processing, warehousing and securing in the form of a cloud computing infrastructure [8]. Additionally, the General Data Protection Regulation -GDPR- introduces the notion of the administrator's and processor's liability. In the health service sector it means that both the administrator (a healthcare centre) and the data processor (the service provider) outsourcing the data are held equally liable for the data safeguarding and processing [89]. Current identification and authentication methods used in healthcare centres aren't usually based on the cloud computing technology. The healthcare centres only use the users' names and passwords as a means of safeguarding sensitive data stored in internal electronic systems based upon local servers. It presents itself as a weak link in the structure of the patients' data security. Identity management performed in the cloud helps preserve security, identification and control and focuses particularly on the identity and access control [10]. A cloud signature used in the cloud computing is an electronic signature appended on a virtual device shared by the trust service provider. Cryptographic keys necessary for the authentication process are affixed to a certified device and only the user (owner of the keys) is granted an access to them in the process of strong identification. The signature affixed in this way does not require additional devices as the process takes place through a platform guaranteed by the service provider. The functionality of such signature is comparable to the ones used with cartographic cards and certificates [2].

There are a few types of electronic signatures which could be used for signing electronic documents. The source literature has defined so far 8 types of electronic signatures singled out on the basis of technologies used in them. These shall include: a keyboard signature, an e-mail signature, a handwritten signature, a manual signature, a biometric signature, a password signature, a mobile or cryptographic signature. A keyboard and e-mail signature, similar in nature, consist of signing a person's forename and surname on an electronic document with the use of a keyboard. Additionally, a scan of a handwritten signature is recognised as an e-mail signature. A manual signature includes data concerning the schemes of hand movements performed during a signature affixed with the use of a digital pen. The scheme of this action is also used by a handwritten biometric signature. Using a password (from a token or a scratch card) together with a sign-in ID constitute a password signature. Mobile devices (a smartphone or a tablet) are used for the purpose of a mobile signature, whereas a cryptographic signature requires encrypted data stored on real media or on remote cloud computing [11].

When it comes to the authentication issue, it worth noticing that there is a variety of authentication methods, including the ones based upon biometric mechanisms. The most commonly used is the biometrics of a handwritten signature (biometric signature) described above, however there are some other methods which include: fingerprints, face or voice biometrics. The fingerprint biometrics is used within the framework of solutions involving the collection of fingerprints on electronic cards, the so-called match-on-cards and the use of smartphone functionalities. In case of face biometrics, special three-dimensional cameras are used, potentially also smartphone cameras. Voice biometrics, on the other hand, collects unique audio recordings of the user's voice. Biometric methods used in the authentication process constitute only part of the process and do not provide full security. Therefore, additional safeguards based upon the user's knowledge or possession are required. A barrier for using this method is caused by the weak element of biometric sensor responsible for collecting biometric features and their verification since this process involves the risk of incorrect data processing or data manipulation [2].

The last proposed solution is the technology of blockchain which, according to experts, constitutes a safe manner of data sharing with the use of automatic cryptographic data coherence check. Data is stored in a digital account book including a connected transaction block. Blockchain is usually a decentralised system based upon a not very popular communication system where the entities have the same 'peer-to-peer' competing rights. In the last few years we could see an increasing interest in the blockchain technology as a new model of data sharing used e.g. in the banking or medical sector. An example of using this technology in healthcare sector is the Medical Chain platform. This platform stores data related to the patients' health and makes it available to doctors, hospitals, laboratories or pharmacists, whereas the health insurers can request for an access to medical documentation and use it for their own purposes [12].

The banking sector, on the other hand, is working on the implementation of the blockchain technology together with the qualified electronic stamp. An example of such technology could be the prototype of a web platform with a connection to selected banks on the principle of distributed data registers prototype. This technology is planned to be widely used in banks due to its good efficiency tests results and high security potential [13].

According to Petrenko *et.al*., the blockchain technology is a realistic solution to one of the major requirements of IT systems used in healthcare, i.e. data security. The purpose of blockchain technologies is to assure that the patient's data shall be encrypted by a trusted cryptographic algorithm and shall be stored and shared on distributed servers providing security and reducing the accessibility problems. The most important feature of this solution is the constancy of the data registered on a blockchain. Moreover, this solution provides the patients with an access to their own information with a simultaneous utmost respect for the protection of privacy, while at the same time allowing all the interested parties to use anonymous data for research and medical purposes [14]. However, there are limitations caused by the lack of proper regulations which could acknowledge the data signed in the form of a blockchain as legally binding. There are some grounds implying that in the future this technology could replace the currently used solutions of the Public Key Infrastructure (PKI), i.e. the procedures and computer systems used for the purposes of entity authentication and identification or data security based on private and public key cryptography together with electronic certificates used e.g. in trust services. Additionally, the combination of blockchain functionality with trusted services could make an innovative solution [2].

III. REFERENCES

[1] Accenture, Obserwatorium.biz. Raport eID 2017. Elektroniczna identyfikacja w Polsce. [online] [cited 2018 Mar 18] Available from: URL: https://www.accenture.com/pl-pl/event-eid-report-2017

[2] Accenture, Obserwatorium.biz. Raport. Przełom w usługach online. Rozwój usług zaufania w Polsce 2017. [online] [cited 2018 Mar 18] Available from: URL: https://www.accenture.com/pl-pl/insight-breakthrough-online-services

[3] Zhang R, Liu L. Security Models and Requirements for Healthcare Application Clouds. W 2010: 268–75.

[4] Ministerstwo Cyfryzacji. Koncepcja e-Dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych. Załącznik 1 Opis statusu projektu pl.ID. [online] [cited 2018 Mar 18] Available from: URL: https://www.gov.pl/

[5] Romaszewski A, Trąbka W, Kielar M, Gajda K. Funkcjonowanie systemów identyfikacji i uwierzytelnienia w polskim systemie opieki zdrowotnej - stan obecny i kierunki zmian. Zesz Nauk Wyższa Szk Zarządzania Bank w Krakowie. 2017;44:46–58.

[6] Siwik L, Mozgowoj Ł. Biotrustis Biometric Trust Information Systems,. Serwerowy system podpisu elektronicznego z uwierzytelnianiem biometrycznym. [online] [cited 2018 Mar 18] Available from: URL: https://www.researchgate.net/publication/263651892_Serwerowy_system_podpisu_elektronicznego_z_uwierzytelnianiem_biometrycznym

[7] Okamoto T, Tada M, Miyaji A. Efficient "on the Fly" Signature Schemes Based on Integer Factoring. [W:] Progress in Cryptology — INDOCRYPT 2001. Berlin, Heidelberg Springer, 2001: 275–86. [online] [cited 2018 Mar 18] Available from: URL: https://link.springer.com/chapter/10.1007/3-540-45311-3_26

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). [online] [cited 2018 Mar 18] Available from: URL: https://eur-lex.europa.eu

[9] Romaszewski A, Trąbka W, Kielar M, Gajda K. Elektroniczna dokumentacja medyczna - przetwarzanie danych o stanie zdrowia poza miejscem świadczenia usług zdrowotnych. Zesz Nauk Wyższa Szk Zarządzania Bank w Krakowie. 2017; 44:14–27.

[10] Romaszewski A, Trąbka W, Kielar M, Gajda K. Wprowadzenie Usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej (część I). Zesz Nauk Wyższa Szk Zarządzania Bank w Krakowie. 2016; 42:24–40.

[11] Mehraeen E, Ghazisaeedi M, Farzi J, Mirshekari S. Security Challenges in Healthcare Cloud Computing: A Systematic Review. Glob J Health Sci 2016;9:157-162.

[12] Mannaro K, Baralla G, Pinna A, Ibba S. A Blockchain Approach Applied to a Teledermatology Platform in the Sardinian Region (Italy). 2018;9,2 :44.

[13] Krajowa Izba Rozliczeniowa. KIR opracował prototypowe rozwiązania dla trwałego nośnika informacji / KIR opracował prototypowe rozwiązania dla trwałego nośnika informacji. [online] [cited 2018 May 30] Available from: URL: https://www.kir.pl/o-nas/aktualnosci/kir-opracowal-prototypowe-rozwiazania-dla-trwalego-nosnika-informacji,219.html

[14] Petrenko A, Kyslyi R, Pysmennyi I. Blockchain as a service for medical records. Syst Res Inf Technol 2017;1:7–11.