ZESZYT NAUKOWY
Wyższa Szkoła Zarządzania i Bankowości w Krakowie

Mariusz Kielar
Jagiellonian University Medical College
Faculty of Health Sciences
Medical Information Systems Department
mariusz.kielar@uj.edu.pl

Dr Artur Romaszewski
Jagiellonian University Medical College
Faculty of Health Sciences
Medical Information Systems Department
artur.romaszewski@uj.edu.pl

Dr Wojciech Trąbka
Jagiellonian University Medical College
Faculty of Health Sciences
Medical Information Systems Department
wojciech.trabka@uj.edu.pl

Krzysztof Gajda
Jagiellonian University Medical College
Faculty of Health Sciences
Medical Information Systems Department
krzysztof.gajda@uj.edu

CONDITIONS FOR THE INTRODUCTION OF A UNIVERSAL ELECTRONIC IDENTIFICATION AND AUTHENTICATION SYSTEM IN THE HEALTHCARE INFORMATION SYSTEM

Introduction

The application of modern ICT in the information system of public administration in Poland should be conceived as a milestone in the development of the infrastructure that enables sharing the services of electronic identification and authentication in the healthcare system. It is crucial for correct functioning that the so called identification security should be guaranteed to all the users of such a system in the same sense as it is in the case of any information systems that process data based on electronic documentation and advanced solutions to verify the identity of particular user categories with a defined accessibility level to e-resources. Identification security implies smooth functioning of the state with respect to 1) correct authentication of the identity declared by the users, 2) verification of the allocation correctness of a particular individual and his/her identity to the rights related to the document they use, 3) legal and business transactions related to identity documents or particular rights, and also 4) the protection of citizens against identity theft[1] - See Fig. 1

The first steps to implement ICT solutions with the aim to provide identity security in the Polish healthcare system through the verification of the patient's security status and the authorization of services accomplished were made in the Silesia voivodeship in 2001 together with the opening of a local system of the so called e-KUZ card (electronic Health Insurance Card).

Electronic KUZ (e-KUZ) enabled first of all the verification in the Silesian health payer branch (previously Kasa Chorych, now NFZ –the National Health Fund) of the card user's security status and the authorization of the accomplished services within the contract with the Silesian branch. The card offered the possibility for doctors to print prescriptions and the healthcare entities could run a rational medicines policy by processing the data from prescriptions. Such solution resulted in tightening up the pharmaceuticals market and made it possible to discover more promptly the possible breaches of law in this respect[2].

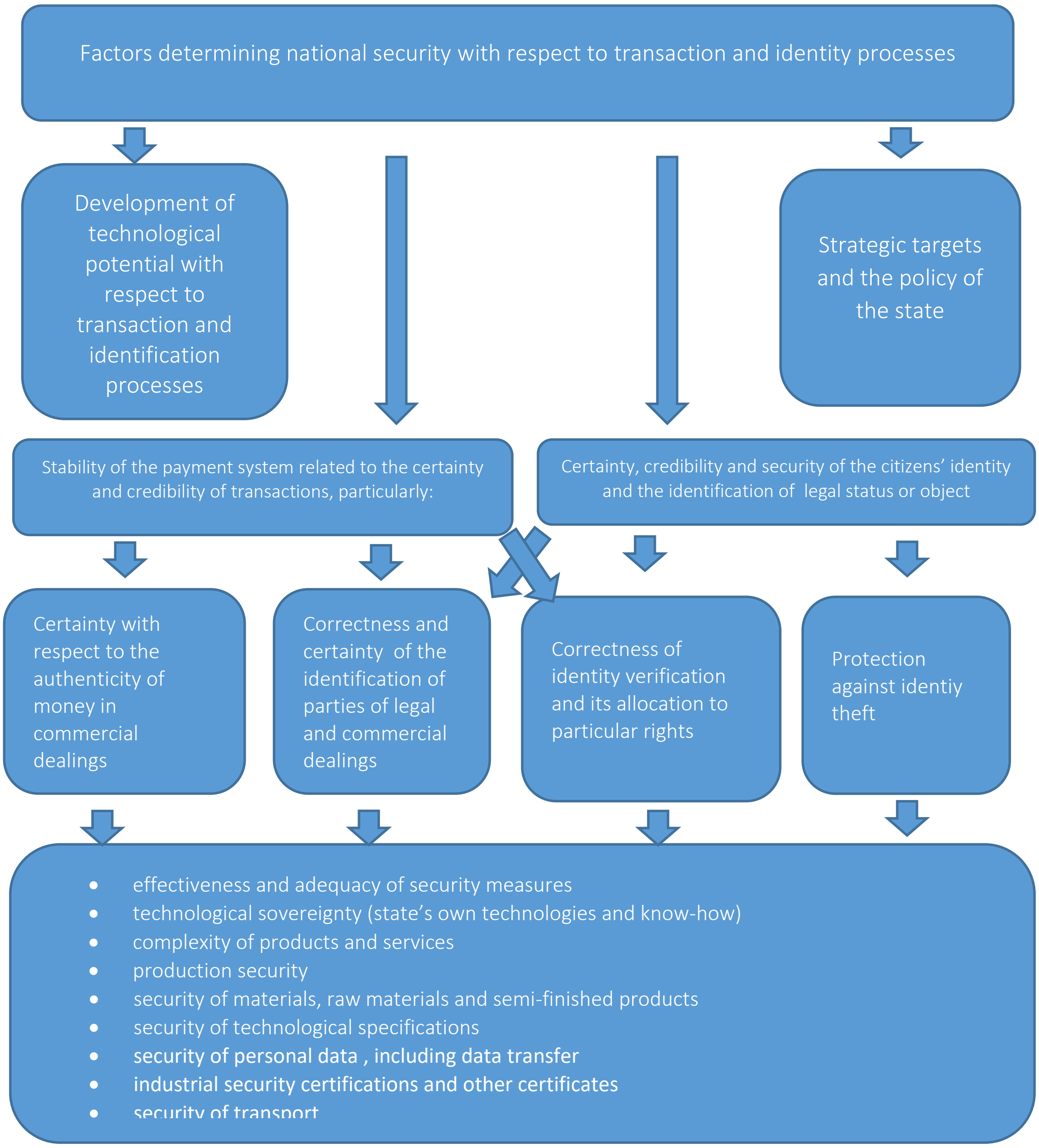
In 2007 the president of NFZ presented his point of view that health vouchers of a defined value should be introduced in order to activate the health insurance market and save on administration costs paid by the Social Insurance Institution ZUS. The concept, however, did not come into force[3].

[1] Lewandowski R., *Evaluation of legal and technical solutions with respect to new types of documents in the healthcare system – KUZ, KSM and KSA*, „Journal of Health Policy, Insurance and Management – Polityka Zdrowotna" 2015, nr 16, p. 77

[2] Lewandowski R., Karta Ubezpieczenia Zdrowotnego – zmiany. https://serwiszoz.pl/zarzadzanie/karta-ubezpieczenia-zdrowotnego-zmiany-3170.html, (Accessed: 09.05.2017)

[3] Ibid.

Fig. 1. National security with respect to identification credibility


Factors determining national security with respect to transaction and identity processes
Development of technological potential with respect to transaction and identification processes
Strategic targets and the policy of the state
Stability of the payment system related to the certainty and credibility of transactions, particularly:
Certainty, credibility and security of the citizens' identity and the identification of legal status or object
Certainty with respect to the authenticity of money in commercial dealings
Correctness and certainty of the identification of parties of legal and commercial dealings
Correctness of identity verification and its allocation to particular rights
Protection against identiy theft
effectiveness and adequacy of security measures
technological sovereignty (state's own technologies and know-how)
complexity of products and services
production security
security of materials, raw materials and semi-finished products
security of technological specifications
security of personal data , including data transfer
industrial security certifications and other certificates
security of transport

Source: Lewandowski R., *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów* w: Goc. M., Tomaszewski T., Lewandowski R., *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Volumina, Warszawa 2016, p. 289

In 2013 an Electronic Verification of Eligibility of Beneficiaries (eWUŚ) started operating in Poland and, as a result, there is a possibility of an immediate (in real time) confirmation of patient's eligibility to the public health care. The application significantly simplified and accelerated the verification of patients' security levels by service providers as it replaced the necessity to present the RMUA printouts or pensioner's cards[4]. In order to find more functional ITC solutions that would meet the requirements and conditions of the contemporary healthcare system, the identification measures that had so far had been used in the health sector were subject to revision. The drawbacks of the Silesian health insurance card included the local character of the application and a fairly limited functionality of such information carrier.

In 2015, in the reaction to the above conclusions, the government presented a solution which consisted in the introduction of three electronic cards and the related ITC systems in the healthcare sector: 1) Health Insurance Card (KUZ), 2) Medical Specialist Card (KSM) and 3) Administrative Specialist Card (KSA). At first, the new information media and the related IT systems were to be regulated by the provisions of the amendments of the act of 29 April 2011 on the information system in healthcare. However, with time, the government abandoned its initiative due to legislative issues and its technical drawbacks that questioned the idea of patients' identification security.

At present, the original concept of e-KUZ is returning and its upgraded version is going to be introduced with the consideration of changes that would correct the limitations of the original version. Due to the key role of the e-KUZ as a public document with a strategic significance to the citizens' identity protection and authentication, its detailed technical specification and the applied IT solutions should meet the requirement of special regulatory supervision[5] - see Fig.2 Another issue to decide on is to select a target form of e-KUZ that would meet the statutory requirement of universality. At present, at least two possible options are taken into consideration; e-KUZ as a separate public document or the introduction of the e—KUZ functionality into a different common public document (i.e. the electronic ID, which as the only public document meets the requirement of universality) [6]. Controversies arise as to the concept of combining the e-KUZ card with a bank card as it is contrary to the ideas of the Minister of Digitization who presented in 2015 a strategic concept of the use of electronic ID

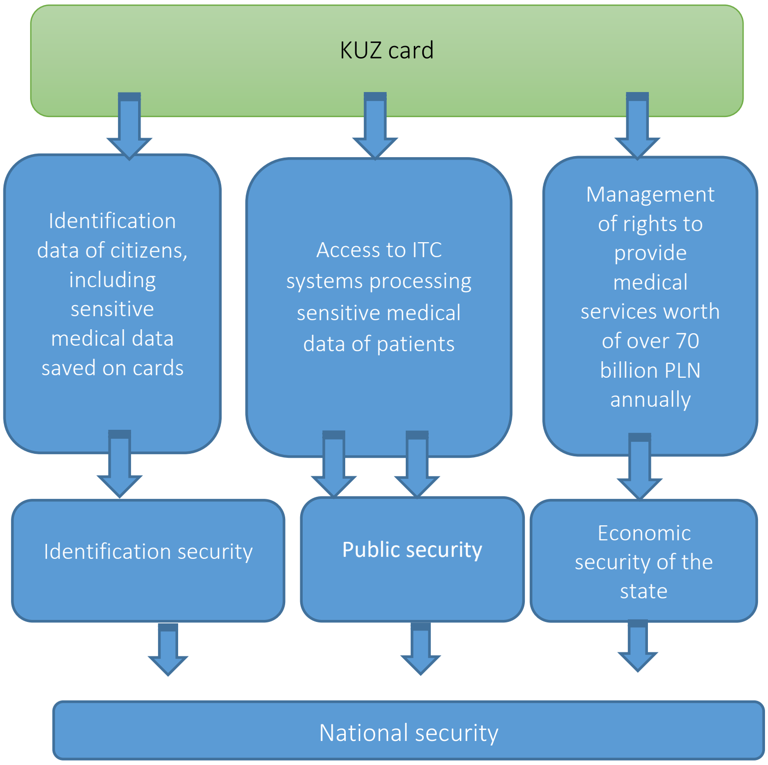
[4] Ibid.

[5] Lewandowski R, Miękina A. *Certyfikacja w zakresie Common Criteria – wstępna koncepcja budowy polskiego modelu*. Człowiek i Dokumenty. 2015;39:35.

[6] Lewandowski R., *Analiza nowej koncepcji elektronicznej karty ubezpieczenia zdrowotnego*, Polski Przegląd Nauk o Zdrowiu 3;(48): 2016

as a universal and common identification tool that would replace any other access cards for identification and authentication purposes[7].

Fig. 2. KUZ model with respect to national security


KUZ card
Identification data of citizens, including sensitive medical data saved on cards
Access to ITC systems processing sensitive medical data of patients
Management of rights to provide medical services worth of over 70 billion PLN annually
Identification security
Public security
Economic security of the state
National security

Source: Lewandowski R. *Evaluation of legal and technical solutions with respect to new types of documents in the healthcare system – KUZ, KSM and KSA.* Journal of Health Policy, Insurance and Management – Polityka Zdrowotna. 2015;16:75–84 w: Lewandowski R., *Analiza nowej koncepcji elektronicznej karty ubezpieczenia zdrowotnego*, Polski Przegląd Nauk o Zdrowiu 3;(48): 2016

Electronic identification in the light of the selected European solutions

In 2014 the 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

[7] Lewandowski R., Karta Ubezpieczenia Zdrowotnego – zmiany.: https://serwiszoz.pl/zarzadzanie/karta-ubezpieczenia-zdrowotnego-zmiany-3170.html, (Accessed: 09.05.2017)

(Official Journal of EU, 28 August 2014) entered into force. The eIDAS regulation[8], as it is often referred to, applies directly in the European Union and does not have to be implemented in the local law of the member-states. However, despite this general principle, in some areas regulated by eIDAS some freedom was left to local legislators. Consequently, Polish authorities drafted an act on trust services, electronic identification and amendment of certain acts[9]. The eIDAS regulation creates basically some framework for the provision of mutual acceptance of the means of electronic identification and authentication, which enables actual functioning of cross-border health service for European citizens.

Austria is a good example of good practices conducted to adapt the country's legislative and organizational system to the eIDAS regulations. The coordination of both processes is carried out by the Austrian Chancellor's Office which is responsible for the computerization of the state with the cooperation with the Ministry of Justice (with regard to legislative work). The starting point of the harmonization process was the development by Austria of the open API specification, which is referred to as a *security layer*, to facilitate signing documents with mobile devices or citizen's cards. The MOCCA implementation is one of the solutions that is designed with the use of the above specification and is available free of charge to natural persons and business people. It is based on an open-source license and was developed in the cooperation between the Chancellor's Office and the Technical University in Graz. There are also three more applications which can be found on a dedicated website portal[10]. The API specification facilitates efficient integration of solutions in other applications (e.g. the workflow type systems). There are also applications for signing in PDF format[11]. The Austrian solutions were tested by the *European Telecommunications Standards Institute*, ETSI and Austrian signature obtained recognition in other member-states. However, in order to retain backward compatibility with older signature, a dedicated Internet portal is still operating[12].

[8] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910

[9] https://legislacja.rcl.gov.pl/projekt/12283556, Draft act on trust services, electronic identification and the amendment of certain acts

[10]https://www.buergerkarte.at/en/downloads-card.html, (Accessed: 19.05.2017)

[11] https://www.buergerkarte.at/en/pdf-signature-mobile.html, (Accessed: 19.05.2017)

[12] https:// www.signature-verification.gv.at, (Accessed:19.05.2017)

An interoperability model that was developed within the STORK project (*Secure Identity Across Borders Linked)* supplements the eIDAS regulations regarding the accepted principles of electronic identification and authentication with respect to the e-identification regulations that are in force in the member-states[13]. As in the case of eIDAS, the purpose of the STORK project was to develop universal methods of cross-border authentication and identification of citizens. Within the project, a PEPS (*Pan-European Proxy Services)* federation model of authentication and identification was set up as well as solutions applying cryptographic carriers as the source of information on citizens' identity (a middleware model). Such a solution aims at the facilitation of the functioning of a single European area of electronic identification and authentication that provides actual interoperability of eIDs (both for natural and legal persons) on the local and European level.

The concept of the model is relatively simple. The user's application for the access to the electronic identification and authentication system through his/her Web browser is transferred to the center of national authentication services where the identity of the user is confirmed by means of authentication. Then, the authenticated identity data can be sent to a service provider selected by the user[14]. In the complementary middleware model, the processes of authentication and reading of identity data are performed with the application of a cryptographic carrier through the middleware software installed on the user's station. The communication with the PEPS services is carried out through a virtual identity provider (V-IDP). In both cases the authenticated data is sent to the service provider[15].

In the search of effective solutions that would regulate a public scheme of electronic identification and trust services in Poland a comparative analysis of such schemes that operate in Austria and Switzerland leads to interesting conclusions. In Austria, a centralized and closed system makes it impossible for private entities to share identity. They can only provide particular identity carriers while the state takes responsibility for providing a complete infrastructure and it covers the investment and maintenance costs. It is crucial that the services provided within the Austrian system are free to the citizens and the state, apart from the identification and authentication services, provides the service of electronic signature. From the technical point of view, the infrastructure of the Austrian system and the binding model of

[13] https://www.eid-stork.eu
[14] Wachnik D., *Rozporządzenie eIDAS - na pograniczu technologii i prawa*. Elektronika 2/2014: 42-44

[15] Ibid.

integration with the trust services providers seem to be complicated and some of its elements depart from the current global standards in this area. Such approach results from the unique and restrictive legal regulations with regard to the identification of citizens (including the issue of privacy protection). It is interesting that even in such a well-organized system where practically every citizen is offered the possibility of electronic identification, the use of this functionality is not high (8.5 million citizens generate only 650 thousand transactions annually). The use of cards for electronic identification is also rather low. Some improvement in this field was noticed only after providing this functionality on mobile platforms.

Contrary to Austria, Sweden is an example of a market approach to the development of an electronic system of citizen identification. Its functioning does not involve only private companies from which the state purchases identification services for public digital services; a federalized model provides for the opportunity to include any economic entities that meet defined requirements. Such approach results in simple technical solutions and a widespread public use, which makes Sweden one of the top countries as regards the development of e-government sector and high level of the use of electronic identification means (9.5 million citizens generate over 300 million transactions per year). The above example shows an evident superiority of the Swedish federative model which is open to the autonomous (i.e. devoid of pressure from the state) development and integration of solutions provided by private companies. The citizens of Sweden use the means of electronic identification much more frequently in spite of the fact that these technologies are more widespread in Austria. This is due to the fact that Austrian solutions are more complicated and their flexibility depends on the development of the central infrastructure. That fact is significant with regard to the federative (i.e. similar to the Swedish approach) way of the development of private certification centers in Poland that issue qualification certificate recognized by public services[16].

Electronic registered delivery service (EDS/e-delivery)[17], which is commonly used in Scandinavia, is an extremely useful solution as regards the processing of electronic data. It is a digital equivalent of a traditional registered letter in which documents are signed electronically

[16] Draft act on the amendment of the act on trust services and electronic identification and the amendment of certain acts, Ministry of Digitization, 2017.

[17] Kawiński A., Sieradz A.[ed.], *Wyzwania informatyki bankowej*: material prepared on the basis of IT seminars organized by Gdańska Akademia Bankowa - Instytut Badań nad Gospodarką Rynkową in financial institutions, Gdańsk 2014

by citizens or companies and the proof of service is developed by the IT systems of the administration. Pursuant to Art.3 (36) of the eIDAS regulation "*electronic registered delivery service* means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations. In accordance to the definition of trust service (Art.3 16), it consists of the provision of *the creation of electronic registered delivery services* perceived as the creation of a proof resulting from the eIDAS service, the *verification of an electronic registered delivery* perceived as the verification of certificates that were used to create the proof, and *the validation of an electronic registered delivery* perceived as the validation of electronic documents, e.g. signatures, dates and time as stated in a e-delivery service proof, and the determination of senders and recipients on the basis of the proof of the service.

In Norway, for example, the entity that administers the system of e-delivery also manages the system of electronic identity and the communication between the citizens and public administration authorities is conducted electronically on regular basis. However, every citizen can decide on the return to a traditional way of communicating. Since 2011, in Germany, legal provisions have been in force that allow for the operating of the DE-Mail system which facilitates an electronic transfer of legally binding documents between the citizens and the public and private entities. In such cases, the role of the state is only to define the technical standards and legal basis for the functioning of the system without playing the role of a service provider.

The current functionality structure of the national ePUAP (electronic Platform for Public Administration Services) system provides a relatively simple implementation of the registered e-delivery service. If the electronic address is accepted as a registered address for official notifications and the e-PUAP box is shared with non-public entities, the adaptation to the technical standards with respect to eIDAS may result in a more common use of the ePUAP platform[18].

[18] Ibid.

Electronic identity card – a universal identification tool

The introduction of a system of electronic identity cards (ID cards with an electronic layer) is going to be an element of the basis of the state administration digital infrastructure. The system should facilitate, among other things, a common electronic identification and authentication of information about citizens in their relations with public administration offices. The universality and complexity of the future functionalities of e-ID cards will facilitate their application for the purposes of electronic identification in numerous sector information systems, including healthcare sector.

In compliance with the strategic plans of the Ministry of Digitization in the area of public service computerization e-ID card, as a basic and common identification document, is to be used as an authentication platform in ICT systems and as a register, including (among other information) the medical data of patients. Moreover, the ID card with an electronic layer that is currently used in 26 European countries can have other functionalities that improve the security of patient identification such as electronic signature, ICAO-compliant travel documents, or possibly emergency medical information and biometry[19].

Belgium is an interesting example as regards the solutions in the area discussed. Electronic ID cards were implemented there to facilitate the identification of the citizens both online and conventionally. The Belgian solutions are based on three different typologies of identity cards that are assigned to particular user categories and enable the access to precisely defined types of services.

The first category is the eID, i.e. a card that is issued only to the citizens of Belgium. It functions in a similar way as a typical ATM card with a PIN. It includes a microprocessor with the citizen electronic identification data and digital certificates. The user can confirm his/her identity with the card and consequently can travel across EU. Additionally, the card can be used to confirm the identity on the Internet, to complete official documents or forms and also to confirm the identity in such places as a public library or trusted computer network. All procedures can be conducted with only one electronic signature.

[19] Program of Integrated State Computerization, Ministry of Digitization, Warszawa 2016. https://mc.gov.pl/files/program_zintegrowanej_informatyzacji_panstwa_1.pdf, (Accessed: 06.05.2017)

The second category of the e-ID card is referred to as the kids-ID. It is designed for children under the age of 12 and the possession is not mandatory. However, the kids-ID is obligatory when a child intends to travel in EU. The architecture of the kids-ID card resembles the one of the eID discussed above. A narrower range of permissions of the "small" ID card makes it easier to apply in the pilot tests of its new functionalities, e.g. the registration of children in schools or sports clubs. It can also include up to seven contact numbers in the cases of emergency. The third category is an e-ID issued to foreigners and it replaces a permit to stay in Belgium. Consequently, the user is given the access to the services of Belgian electronic administration and can sign official documents electronically.

Similarly, as in the case of the Belgian e-ID card, the Italian electronic identity cards enable both online and offline identification of citizens. Two types of identification cards are commonly used that provide an online access to public services: EIC - descriptive electronic identity cards and CNS (*Carta Nazionale dei Servizi*) i.e. cards including electronic signatures that were applied prior to the introduction of electronic identity cards. Originally, CNS was supposed to be abolished by the end of 2007 but the decisions were changed and it remains active and will be added some new functionalities[20].

Electronic identification and authentication system – Polish experiences

The provision and maintenance of high standards of information processing and the quality of public administration services are the key condition for the development of an effective state. The implementation of modern IT solutions in this area supports the integrity of the state information system by offering the users the access to the completely new functionalities of a digital domain. The improvement of the public administration digitization process was one of the postulates of the draft Plan of the State Digitization for 2011-2015[21] that was developed in 2011. The priorities included three main areas within which the implementation process of electronic public services was to be coordinated: the computerization of offices, e-administration and e-society. However, a critical attitude to the

[20] Perkowski B., *Elektroniczny dowód osobisty jako element informatyzacji służby zdrowia*. Studia Oeconomica Posnaniensia 2013, Vol. 1, No. 2 (251): 133-151

[21] Smoktunowicz U., *Plan Informatyzacji Państwa na lata 2011-2015*. https://www.crn.pl/rynek/plan-informatyzacji-panstwa-na-lata-2011-2013-2015, (Accessed: 06.05.2017)

assumptions that were presented in the draft plan resulted in its rejection. Thus, an upgraded and updated version was developed – the State Integrated Digitization Program (PZIP) [22]. The strategic aim of the new document is to increase the volume of high quality electronic public services in Poland. The percentage of people (private and business people) that use these services was the indicator of the accomplishment of the target. In the opinion of the authors of the document, the strategic target can be achieved by the provision of the interoperability of the existing and the new public administration IT systems through ,among other elements, the removal of redundancies in their functionalities. Such approach is to result in the construction of a coherent State Information System that should provide the citizens with key services in an effective way[23].

The current availability level of digital services in Poland is insufficient both with respect to the citizen's demand for information and with the capacity of the contemporary ICT solutions. The restrictions concerning the use of the present methods of electronic identification and authentication in the public systems which provide digital public services are the most significant reasons of such state of affairs. In the era of a dynamic development of online service sector, the possibility to conduct electronic identification and authentication is necessary for citizens to use securely various types of digital applications. At present, electronic identification and authentication in public administration IT systems is carried out in two ways: with the application of mechanisms that operate within the administrative institution (i.e. its own IT systems) or the ePUAP trusted profile mechanism[24]. The requirement of universality with respect to the means of electronic identification is met only by the ePUAP trusted profile; however, its accessibility and the application range is still limited. It is estimated that the number of users in the whole country who have and use their own ePUAP trusted profile

[22] State Integrated Digitization Program. Ministry of Digitization, Warszawa 2016. https://mc.gov.pl/files/program_zintegrowanej_informatyzacji_panstwa_1.pdf, (Accessed: 06.05.2017)

[23] MAiC 2012, Państwo 2.0 – Nowy start dla e-administracji, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.

[24] Explanatory memorandum to the act on the amendment of the act on trust service,: https://legislacja.rcl.gov.pl/docs//2/12297458/12427868/12427869/dokument284778.docx, (Accessed: 06.05.2017

amounts only to approx.. 700 thousand per year[25]. The number did not change basically after the corrections introduced in the last quarter of 2016 and which introduced the option to confirm and authenticate the ePUAP trusted model with, among other tools, a system of bank certificates. Thus, a limited use of the ePUAP trusted model results in the continuation of the practice that internal identification systems are financed separately at every service provider. Paradoxically, there is a solution that meets the universality requirement of the electronic identification means but its insufficient dissemination results in the necessity to develop autonomous and dispersed identification means in the public administration institutions where the digitization of services is in fact determined by the functioning of a common and widespread electronic identification and authentication of the users of services provided by administrative authorities.

Due to the situation presented above, the necessity arises to share and assign adequate permissions to particular users (i.e. to set up individual accounts) in the system that provides particular type of services. This requirement involves additional problems for the users of the currently available systems of electronic identification – the users of digital services provided by different entities have to learn and remember various identification methods in different systems that are managed by different service providers. The drawback results from the lack of a single coherent security policy in the IT systems of digital service providers which would regulate in detail the principles regarding password sharing and using (with respect to, for example, the required length of the password, the number of alphanumeric signs, etc.). Thus, the existence of numerous systems of electronic identification constitutes a practical problem for the users. What is more, in every institution the way and range of electronic identification depend on the scope and type of the service that has to be secured against unauthorized breach or use of false identity. In theory, there is some justification: the security levels should be diversified in relation to the status of the information that is processed by the system and the profile of the service. This, however, leads to an even more significant dispersion of electronic identification and authentication in the state information system that strives for coherence.

Because of the above inconveniences a question arises how the current troublesome and complicated electronic identification and authentication system should be changed so that it is

[25] Draft act on the amendment of the act on trust services and electronic identification and the amendment of other acts, Ministry of Digitization, 2017.

more convenient for the citizen in the first place. From the point of view of the users of the present systems it seems that the optimal solution would be to have a similar (or identical) set of identifying data for various services. The implementation of such flexibility should be conducted in the environment of identification systems that are trusted by the users on a larger scale. Some support may come from the informative awareness of our society that has been developed in the course of the use of commercial digital services that are fairly commonly used by the institutions of the banking, ICT – and in some cases – healthcare sectors. It seems that competent informative activities that refer to the mechanisms of electronic identification and authentication in the areas of e-banking or telecommunication services that are well-known and used on a daily basis by the majority of citizens should be a good starting point towards a much more common use of the digital services provided by public administration institutions.

Such a significant simplification of the method of electronic citizen identification and authentication will be beneficial also to the public administration entities that provide digital services; if their operations can be supported by a functional and credible system of electronic identification and authentication, a further management of their own systems with the same functions will not be necessary. In order to implement sustainably the solutions in question so that our citizens are guaranteed universal and secure means of electronic identification and authentication, the following rights, responsibilities and targets should be provided on a statutory level[26]:

- to have a significant number of users of electronic identification means, which will additionally make it easier to develop and share new digital services;
- to develop a reliable electronic architecture that is open to private sector and innovations and guarantees electronic identification, which will result in the creation of a positive image of e-administration;
- to provide adequate diversification of electronic identification means with a particular emphasis on the provision of public – made available by the State – means of electronic identification on all security levels maintaining the clarity of the system and of the citizen identification methods that are offered;

[26] Explanatory memorandum to the act on the amendment of the act on trust services. https://legislacja.rcl.gov.pl/docs//2/12297458/12427868/12427869/dokument284778.docx, (Accessed: 06.05.2017)

- to disseminate the electronic identification means, which will provide a common access to the existing digital services of public administration;
- to provide high flexibility and growth potentials to the market of digital services of public administration and commercial entities;
- to provide a high level of citizen data security.

Conclusions

The aim of the draft act of April 2017 on the amendment of the act on trust services and electronic identification and the amendment of certain acts that was prepared by the Ministry of Digitization is to implement an effective electronic identification system in Poland on the basis of commonly available, clear and secure organizational and technical solutions. The solutions presented in the draft act are to provide the possibility to use in the public on-line services the electronic identification means that are issued by various entities as well as to use the existing ones that are applied in the on-line services provided by private entities (e.g. banks and telecoms).

The legislator assumes that this concept will result in a prompt removal of the barrier of the lack of the common access to electronic identification means. The draft act also presents a public scheme of electronic identification which is dispersed (federation) in character and operates on the basis of numerous means of electronic identification. They can be issued by various entities, including commercial providers. The National Electronic Identification Node (KWIE) will be the central element of the scheme and will coordinate the operations between commercial nodes, cross-border nodes, service and attribute providers.

It is assumed that KWIE will be integrated with the IT systems that provide public electronic services and with the suppliers of the means of electronic identification by 31 December 2013. By the end of the next year a mandatory migration should be conducted of all portals that are integrated with the Trusted Profile as at 31 January 2017, and by 31 December 2020 the migration of websites with separate login systems should be completed.

Bibliography:

[1] Goc. M., Tomaszewski T., Lewandowski R., *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Volumina, Warszawa 2016, p. 289

[2] Kawiński A., Sieradz A.[ed.], *Wyzwania informatyki bankowej*: materiał przygotowany na podstawie seminariów IT w instytucjach finansowych organizowanych przez Gdańską Akademię Bankową Instytut Badań nad Gospodarką Rynkową, Gdańsk 2014

[3] Lewandowski R, Miękina A. *Certyfikacja w zakresie Common Criteria – wstępna koncepcja budowy polskiego modelu*. Człowiek i Dokumenty. 2015;39:35.

[4] Lewandowski R. *Evaluation of legal and technical solutions with respect to new types of documents in the healthcare system – KUZ, KSM and KSA.* Journal of Health Policy, Insurance and Management – Polityka Zdrowotna. 2015;16:75–84

[5] Lewandowski R., *Analiza nowej koncepcji elektronicznej karty ubezpieczenia zdrowotnego*, Polski Przegląd Nauk o Zdrowiu 3;(48): 2016

[6] Lewandowski R., *Evaluation of legal and technical solutions with respect to new types of documents in the healthcare system – KUZ, KSM and KSA*, „Journal of Health Policy, Insurance and Management – Polityka Zdrowotna" 2015, No. 16, p. 77

[7] Lewandowski R., Karta Ubezpieczenia Zdrowotnego – zmiany. https://serwiszoz.pl/zarzadzanie/karta-ubezpieczenia-zdrowotnego-zmiany-3170.html, (Accessed: 09.05.2017)

[8] MAiC 2012, Państwo 2.0 – Nowy start dla e-administracji, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.

[9] Perkowski B., *Elektroniczny dowód osobisty jako element informatyzacji służby zdrowia*. Studia Oeconomica Posnaniensia 2013, Vol. 1, No. 2 (251): 133-151

[10] Program of Integrated State Computerization, Ministry of Digitization, Warszawa 2016. https://mc.gov.pl/files/program_zintegrowanej_informatyzacji_panstwa_1.pdf, (Accessed: 06.05.2017)

[11] Draft act on the amendment of the act on trust services and electronic identification and the amendment of other acts, Ministry of Digitization, 2017.

[12] Smoktunowicz U., *Plan Informatyzacji Państwa na lata 2011-2015*. https://www.crn.pl/rynek/plan-informatyzacji-panstwa-na-lata-2011-2013-2015, (Accessed: 06.05.2017)

[13] Explanatory memorandum to the act on the amendment of the act on trust services. https://legislacja.rcl.gov.pl/docs//2/12297458/12427868/12427869/dokument284778.docx, (Accessed: 06.05.2017)

[14] Wachnik D., *Rozporządzenie eIDAS - na pograniczu technologii i prawa*. Elektronika 2/2014: 42-44

[15] https://www.buergerkarte.at/en/downloads-card.html, (Accessed: 19.05.2017)

[16] https://www.buergerkarte.at/en/pdf-signature-mobile.html, (Accessed: 19.05.2017)

[17] https://www.signature-verification.gv.at, (Accessed: 19.05.2017)

Abstract

The article presents current conditions for the implementation of the services of electronic identification and authentication with the application of modern ICT systems that can be used in the healthcare system. Their implementation is both a milestone and a condition for the provision of real information security to patients and healthcare sector employees.