

Szczepan Jakubowski

Department of Medical IT systems, Institute of Public Health, Jagiellonian University Medical College in Krakow
szczepan.jakubowski@uj.edu.pl

Dr Artur Romaszewski

Department of Medical IT systems, Institute of Public Health, Jagiellonian University Medical College in Krakow
artur.romaszewski@uj.edu.pl

Dr Wojciech Trąbka

Department of Bioinformatics and Public Health, Faculty of Medicine and Health Science, Krakow Andrzej Frycz Modrzewski University
wojciech.trabka@uj.edu.pl

IDENTIFICATION AND AUTHENTICATION OF ENTITIES AND DIGITAL DOCUMENTS IN HEALTH CARE AS INDISPENSABLE ATTRIBUTES OF HEALTH CARE DATA AND INFORMATION SECURITY

Introduction

Numerous articles have been published recently that concern the issues of data protection, including data in health care. Their authors focus mainly on the GDPR¹ regulations and the Polish act on data protection². Unfortunately, this does not apply to the regulations of other documents that are equally important, i.e. the eIDAS regulation (*Regulation of the European Parliament and of the Council on electronic identification and trust for electronic transactions in the internal market*³ and Polish regulations whose objective is to supplement and detail the U regulations within the scope defined in the legislation⁴. Regrettably, very few publications concern the solutions included in eIDS with regard to health care⁵.

¹ 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), p. 679 <<https://eur-lex.europa.eu>>.

² Act of 10 May 2018 on Personal Data Protection (Journal of Laws 2018, item 1000), <<http://prawo.sejm.gov.pl>>

³ 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, <<https://eur-lex.europa.eu>>

⁴ Ustawa z dnia 5 Września 2016 r. o Usługach Zaufania oraz Identyfikacji Elektronicznej (Dz.U. 2016 Poz. 1579) <<http://prawo.sejm.gov.pl>>.

Act of 5 September 2016 on Trust Services and Electronic Identification, (Journal of Laws 2016, item 1579), <<http://prawo.sejm.gov.pl>>.

⁵ Sz. Jakubowski, *Identyfikacja i Uwierzytelnianie Podmiotów Oraz Dokumentów Elektronicznych w Ochronie Zdrowia* (Praca wykonana w Zakładzie Medycznych Systemów Informacyjnych, Instytut Zdrowia Publicznego, UJ CM, 2018).

eIDAS is one of the most important regulations whose solutions are crucial to the health care system. Its main task is to increase the trust to e-transactions and provide a common basis for secure electronic interactions among citizens, companies and public authorities. This is extremely important in the health sector where there is a constant exchange of information between patients, service providers and bodies that are legally authorized to obtain health information. Adequate security of the process of information exchange is one of the fundamental issues as most of medical e-resources contain health data which are considered sensitive.

The Polish health care system is preparing to implement breakthrough solutions that will help launch prescriptions and referrals onto the market electronic and is going to complete the process of introducing electronic medical documentation system to all medical service providers. Moreover, regulations have been introduced that enable the provision of tele-medical services, which – however – cannot be fully implemented in health care entities without the introduction of a widespread system of identification of service providers and patients. One should also mention the work at state-level on the solutions that result directly from the e-IDAS regulation. Their implementation will have an impact on the majority of areas, health care including, in the whole country. This concerns e-Delivery trust service, which may constitute a breakthrough in the transfer of health documents, and the new ID card. Hopefully, the work on these solutions will be coordinated at ministerial level.

The article presents the main assumptions and solutions included in the regulations, i.e. the regulations regarding the identification of entities and the application of trust services in everyday work of health entities. It focuses on certain “Polish aspects” of the regulations to be implemented in the light of EU solutions. First of all, it should be emphasized that when keeping electronic medical records, a signature confirmed by the ePUAP trusted profile has been introduced which is not fully compatible with eIDAS. This is an electronic signature which is comparatively complicated to use and can be applied only within the country. The article also discusses the issue of electronic prescription that is currently being implemented and electronic sick leaves as documents that have to comply with the eIDAS regulation.

The authors of the article are in favor of the implementation of the latest solutions. However, they think that all the measures that are taken should comply with the eIDAS regulations. Before the implementation of such significant projects, the medical environment should be equipped with tools that enable the new solutions to function properly. Moreover, it would be advisable to conduct educational operations in this area.

1. What are identification and authentication?

Identification in an electronic form is perceived as „a process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person” (art.3)⁶. According to the Polish Committee for Standardization, identification is a “process of automatic recognition of a particular user in the system due to the application of unique names”⁷. Person identification data are data that enable the assignment of a particular identity to a natural or legal person. A package of such data creates an identifier which can be placed in material or immaterial tools that are referred to as the means of electronic identification⁸.

In Poland, the health care information system uses four identifiers for “service recipients, service providers, a place of health care service provision and for medical staff (Art.17c, item 1)⁹. In the case of a service recipient or a patient it is the number of PESEL or any other identity document. Service providers are divided into three groups: the group of entities that run health services whose identifier is the code that consists of characters from the identification code scheme defined by the Minister of Health, pharmacies whose individual code comes from the National Registry of Retail Pharmacies or the Registry of Hospital and Company Pharmacies, and finally, the entities that operate as suppliers of medical products for which a 9-character REGON number is used as the identifier. The identifiers of places where health services are provided, of the pharmacies and the entities that supply medical products are separate but the principle of creating them is the same as in the case of the service recipient identifier; the only difference is that the National Health Fund (NFZ) sets individual codes for medical product suppliers. Moreover, license numbers or (if non-existent) PESEL numbers (or – optionally – the numbers of any other legal documents, e.g. passports)¹⁰ serve as medical staff ID cards. The

⁶ 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

⁷ A. Romaszewski et al., *Identyfikacja i Uwierzytelnienie w Systemie Informacyjnym Opieki Zdrowotnej Po Wprowadzeniu Rozporządzenia UE EIDAS*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2016, No 42.

⁸ 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, p.910

⁹ Act of 28 April 2011 on healthcare information system, Journal of Laws 2011, No.113, item 657, <<http://prawo.sejm.gov.pl>>.

¹⁰ Ibidem.

division of identifiers (data packages that are assigned individually to entities) is given in Table 1.

Table 1. Division of identifiers in the health sector

Identifiers in health care		
1. Identifier of service recipient		
2. Identifier of service provider		
entities running medical services	pharmacies	medical product suppliers
3. Identifier of a place where medical service is provided		
entities running medical services	pharmacies	medical product suppliers
4. Medical staff ID card		

Source: Authors' research based on the Act of 28 April 2011 on information system in health care¹¹.

In order to confirm the identity, the user sends the authentication factor to the electronic identification scheme. Then, after a successful verification, the data can be released. Additionally, at higher security levels, apart from the verification of the electronic means, its authenticity is checked with the application of dynamic authentication¹². The authentication process involves the determination of the authentication factor, i.e. a factor confirmed as being bound to a person. There are three categories of authentication factors:

- 'possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it;
- 'knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it;
- 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute"¹³.

The types of authentication factors with examples are given in Table 2.

¹¹ Act of 28 April 2011 on healthcare information system, Journal of Laws 2011, No.113, item 657, <<http://prawo.sejm.gov.pl>>.

¹² M. Marucha-Jaworska, *Rozporządzenie EIDAS: Zagadnienia Prawne i Techniczne*, Edition 1, Wolters Kluwer Polska, Warszawa 2017.

¹³ EU Commission, Annex: **Technical specifications and procedures for assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme** <<https://eur-lex.europa.eu>>.

Table 2. Types of authentication factors

possession-based authentication factor	knowledge-based authentication factor	inherent authentication factor
hardware token, electronic card (ID with electronic layer)	login, password, PIN, individual identity number (e.g. PESEL), doctor's identifier	fingerprints scan, other biometric features

Source: Authors' research based on EU Commission, Annex: Technical specifications and procedures for assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme <<https://eur-lex.europa.eu>>.

One of the elements of the identification scheme is the ICT system which is defined as “a set of co-operating information devices and software ensuring processing and saving, and also transmitting and collecting data within telecommunications networks by means of a terminal appropriate for the kind of the given network” (art.2, item 3)¹⁴. Should the users of the ICT system of a public benefit purpose entity (e.g. SP ZOZ – Independent Public Health Care Units) wish to use the accessible online services, the authentication requires:

- 1) “the use of a notified means of electronic identification, adequately to the security level that is required for services provided within these systems or,
- 2) the ePUAP trusted profile or
- 3) data verified by a qualified electronic signature” (Art. 20a item 1)¹⁵.

2. Electronic identification scheme

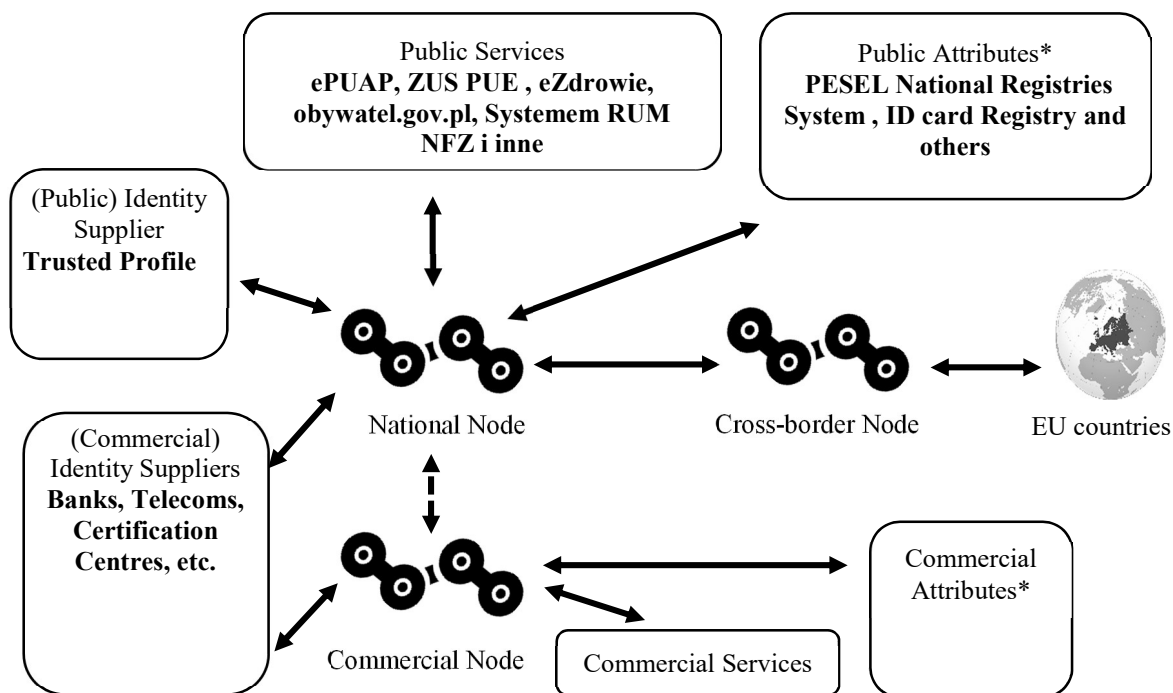
The national electronic identification scheme consists of a national electronic identification node and a cross-border node that are used to authenticate a person seeking the access to e-services. A standard node includes an electronic identification system which issues electronic identification means and ICT systems that provide online services. The electronic identification node is the central element of the electronic identification node and it is the system that integrates the ICT and electronic identification systems in one place. This enables the use of online services after the identity of users has been confirmed. Adding various electronic identification systems to the node provides numerous identification means which can be used in the user authentication process¹⁶. A diagram of the projected system of Electronic Identification Nodes in Poland is given in Figure 1.

¹⁴ Act of 18 July 2002 on Provision of e-services, (Journal of Laws 2002, No. 144 item 1204)

¹⁵ Act of 17 February 2005 on Informatization of Entities Performing Public Tasks, (Journal of Laws 2005, No. 64 item 565). <<http://prawo.sejm.gov.pl>>.

¹⁶ Draft Act on the amendment to the act on trust services and electronic identification and some other acts (2018) <<https://legislacja.rcl.gov.pl>>.

Figure 1. Diagram of the projected system of Electronic Identification Nodes



Source: Authors' research based on Ministry of Digitization and Center for Informatics Technology (COI), conference materials¹⁷ and Accenture, Obserwatorium.biz; *Raport EID 2017, Elektroniczna identyfikacja w Polsce*¹⁸.

*Attributes – non-mandatory, unique identifiers to verify the identity of natural and legal persons that comply with national law to be applied provided that they do not affect cross-border interoperability¹⁹

National Node is „an organizational and technical solution that enables the authentication of ICT users of online services with the application of an electronic identification means that is issued in the electronic identification system connected to the node either directly or through a cross-border node”²⁰. The objective of the National Electronic Identification Node is to disseminate and facilitate the use of digital services by Polish citizens by reducing the logging to the use of a universal login or adequately secured password packages. Eventually, the address

¹⁷ D. Cabańska, K. Biniek, *Węzeł Krajowy. Ministerstwo Cyfryzacji. Centralny Ośrodek Informatyki*, <<https://www.gov.pl/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej>> (Accessed: 06.2018).

¹⁸ Accenture, Obserwatorium.biz, *Raport EID 2017, Elektroniczna Identyfikacja w Polsce 2017* <<https://www.accenture.com/pl-pl/event-eid-report-2017>> (Accessed 06.2018).

¹⁹ 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, p.2

²⁰ Draft Act on the amendment to the act on trust services and electronic identification and some other acts (2018) <<https://legislacja.rcl.gov.pl>>.

of the Node will be: login.gov.pl. The assumption is that National Node should act as a broker in authentication processes in the area of national online services with the use of electronic identification means that are issued by various institutions within the systems of electronic identification. The permission to add a system to the National Electronic Identification Node is issued by the Ministry of Digitization. The decision is made after the necessary security requirements are met of thoroughly documented public or private institutions²¹. The development of the National Node is conducted within the project financed from the state budget and coordinated by the Ministry of Digitization in cooperation with the Center for Informatics Technology (COI)²².

The purpose of the Cross-border Node is – as in the case of the National Node – to improve the access to e-services. However, the operation scope will be wider, which – with the application of the Trusted Profile - will enable the citizens of Poland to use e-services of EU countries and the citizens of non-EU countries to use Polish e-service systems (e.g. ePUAP, PUE ZUS) with their logins and passwords. Cross-border Node will be integrated with the remaining EU electronic identification systems. Only the notified (approved in terms of security) logging systems will be accepted by the Cross-border Node²³. At present, in Poland this concerns the ePUAP trusted profile. The institution responsible for the development of the National Node is the Ministry of Digitization in the cooperation with the NASK National Research Institute and the IMM institute²⁴.

Simultaneously with the implementation of the National Electronic Identification Node, work is conducted in Poland by the National Clearing House (KIR) on the development of the Commercial Electronic Identification Node. The main responsibility of the Commercial Node will be identification in commercial e-services; further plans include integration with the National Node. The model which will include entities forming commercial Nodes or their elements and provide the services of public administration is referred to as a federation model. As regards public services, the national node participates in authentication processes in the first order; however, commercial nodes are acceptable, too. In the case of commercial services, the

²¹ Draft Act on the amendment to the act on trust services and electronic identification and some other acts (2018) <<https://legislacja.rcl.gov.pl>>.

²² Ministerstwo Cyfryzacji, *Budowa Krajowego Węzła Identyfikacji Elektronicznej* <<https://www.gov.pl/web/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej>> (accessed: 28.04.2018).

²³ Draft Act on the amendment to the act on trust services and electronic identification and some other acts (2018) <<https://legislacja.rcl.gov.pl>>.

²⁴ Ministerstwo Cyfryzacji, *Budowa i wdrożenie Węzła Transgranicznego* <<https://www.gov.pl/web/cyfryzacja/budowa-i-wdrozenie-wezla-transgranicznego>> (accessed: 28.04.2018).

confirmation of identity is conducted solely with the use of a commercial node. Thanks to such solution the unnecessary competition is avoided between the state suppliers of electronic identification and the commercial ones. What is more, this results in some (limited) control of the state over the market of commercial services suppliers²⁵.

3. Trust services in health care

Trust services in the health care sector can be divided into open and closed trust services, which makes it possible to determine boundaries for the supervision and the requirements resulting from the eIDAS regulation. Open trust services are services that are provided to the public (to patients) and may – but do not have to – have an impact on third parties. Closed trust services are provided within a particular group, have no impact on third parties and are based on a closed ICT system beyond the supervision and powers of eIDAS. A good example of a group that applies closed trust services is hospital administration staff^{26,27}. Potential advantages of trust services are:

- online signing contracts of employment (e.g. with doctors or nurses),
- signing uncomplicated contracts at business-to-business level (e.g. hospital – warehouse),
- security of formal electronic correspondence between citizens/patients and public institutions,
- automatic (without undue delay) issuing of various certificates by public administration (NFZ, ZUS),
- reduced administrative burden thanks to e-delivery services,
- a substantial number of citizens served by e-services²⁸.

Currently, medical employees have three methods of electronic signing. They are: a signature confirmed by the ePUAP trusted profile, a qualified electronic signature or other means provided by the ICT system of ZUS. Thus, medical specialist can sign:

²⁵ Accenture, Obserwatorium.biz, *Raport EID 2017, Elektroniczna Identyfikacja w Polsce 2017* <<https://www.accenture.com/pl-pl/event-eid-report-2017>> (accessed: 06.2018).

²⁶ 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

²⁷ A. Romaszewski et al., *Wprowadzenie usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej, część II*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2016, No. 42.

²⁸ Accenture, Obserwatorium.biz, *Raport. Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce 2017* <<https://www.accenture.com/pl-pl/insight-breakthrough-online-services>> (accessed: 06.2018).

- „electronic medical documentation;
- request for the access to data that enable the download of electronic medical documentation or the data included there from the Medical Information System (SIM) in the scope necessary to perform diagnostic tests, to ensure the continuity of treatment and to supply service recipients with medical products, foods for particular nutritional uses and medical devices;
- requests for the access to data processed in SIM that enable sharing between service providers the data included in the electronic medical documentation” (Art. 17, item 3)²⁹.

4. Projected actions in healthcare sector

The considerations below concern mainly the plans to introduce e-ID and the Health Insurance Card (KUZ) as the tools of authentication and identification, e-Prescription, e-Referral and e-Delivery. All these elements are very important and necessary to the development of e-service market and data security in the healthcare sector.

26 European countries apply solutions that are based on electronic identification of citizens. The Ministry of Digitization and the Ministry of Internal Affairs and Administration are currently taking a second attempt to develop an adequate tool, the e-ID, in Poland. The first attempt that was financed by EU funds within the *pl.ID* project was not completed in time and the project was stopped. The second attempt assumes that the introduction of the first e-ID will happen by the end of March 2019. The projected tool is to have the form of an identity card with an electronic layer and be used for authentication purposes in e-services of public administration and health sector, including the signing of electronic documents³⁰. The first concept of e-ID was subject to change. Due to the eIDAS regulation, which added a new kind of signature (the advanced electronic signature) and recommended technological neutrality, a wider area of operation has emerged. As a result, an easier connection to Electronic Nodes is planned. Moreover, new solutions based on cloud computing such as server signature or the fly signature scheme are taken into consideration³¹. It is important that the projected electronic

²⁹ Act of 28 April 2011 on healthcare information system, Journal of Laws 2011, No.113, item 657, <<http://prawo.sejm.gov.pl>>.

³⁰ Ministerstwo Cyfryzacji, *Koncepcja E-Dowód – Kontynuacja Projektu Pl.ID i Realizacja Projektów Powiązanych. Załącznik 1 Opis Statusu Projektu Pl.ID*, <<https://www.gov.pl>> (accessed: 06.2018).

³¹ 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.

document will ensure high quality authentication in the cases of accessing, confirming or signing sensitive medical data by the patient.

Apart from e-ID, there are plans to carry out a separate project that is coordinated by the Ministry of Health to develop the Health Insurance Card (KUZ). The purpose of this tool is to confirm within the framework of the provided health care services the presence of the service recipient at a given time and in a particular place or to confirm the completion of a healthcare service (Art.1, item 2). In addition, there are plans that the card will be used for identification and authentication purposes in the healthcare IT system. KUZ will include data that are necessary for authentication and certificates, including the qualified electronic certificate with the highest security level in compliance with eIDAS. It is accepted by the legislator that the functions of KUZ can be performed by other tools such as the mentioned before ID card with an electronic layer or a public mobile application (a mobile phone application where identification documents will be available in an electronic form, e.g. ID, a driving license – the plans are included in the Act of 17 February 2005 on Informatization of Entities Performing Public Tasks³²). According to the National Health Fund, the issue of KUZ cards to all citizens will start not later than of 1 July 2020³³.

It should be added that there are plans to develop a Medical Specialist Card (KSM). This will be a useful tool to enable medical staff to securely develop and send authenticated electronic documents such as e-sick leaves, e-prescriptions and e-referrals³⁴.

e-Prescription in the sense of electronic medical documentation is one of the numerous elements of the P1 Project that is run by the CSIOZ centre (the Centre for Healthcare Information Systems). The project implementation on the national level is planned by 2020. Currently, a 7-month pilot program (commencing in mid-February 2018) of the e-Receipt system is conducted in Siedlce (Mazowieckie voivodship) and Skierniewice (Łódź voivodship) to monitor the effectiveness of the electronic system and to collect user feedback. The benefits resulting from the implementation of e-Prescription include the improvement of the legibility of prescriptions, the savings and use of prescriptions in the course of treatment and patients'

³² Act of 17 February 2005 on Informatization of Entities Performing Public Tasks, (Journal of Laws 2005, No. 64, item 565).

³³ Draft act of 1 June on the amendment to the Act on Public Funding of Health Care Services, p. 18 <<https://legislacja.rcl.gov.pl/projekt/12312303/katalog/12513763#12513763>>.

³⁴ A. Romaszewski, W. Trąbka, M. Kielar, K. Gajda, *Funkcjonowanie systemów identyfikacji i uwierzytelnienia w polskim systemie opieki zdrowotnej - stan obecny i kierunki zmian*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2017, No. 44.

access to the history of prescriptions through the Internet Patient Account. Moreover, it is predicted that the introduction of e-Prescription will help control and improve medical trade³⁵.

It is planned that e-referrals will be given by medical staff. e-Referral will be sent by a healthcare provider to the Electronic Platform for Storage, Analysis and Sharing of Digital Resources Regarding Medical Events (P1 platform); there will also be an option for a printout of the e-Referral by a given service provider. Within the framework of the e-Referral system it will be possible to cancel the referral, change the execution status and browse the document both by the patient and the service provider. The obligation for service providers to give electronic referrals will come into force on 1 January 2021³⁶.

When the identification and authentication tools of identification (e-ID, KUZ) are provided and there are electronic documents to be sent (e-Prescription, e-Referral), there is a need for a service that is offered to all stakeholders and ensures secure information delivery. In this is the area the service of electronic delivery (s-Delivery) is planned.

According to the EU legislator 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means, provides evidence related to the handling of transmitted data, including the proof of sending and receiving the data, and protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations (Art.3, item 36)³⁷.

Qualified electronic registered delivery services should meet the following requirements:

- they are provided by one or more qualified trust service provider(s);
- they ensure the identification of the sender with a high level of confidence;
- they ensure the identification of the addressee before the delivery of data;
- the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;

³⁵ Centrum Systemów Informacyjnych Ochrony Zdrowia, *Pilotaż e-Recepty startuje w Siedlcach oraz Skierniewicach* <<https://www.csioz.gov.pl/aktualnosci/szczegoly/pilotaz-e-recepty-startuje-w-siedlcach-oraz-skierniewicach/>> (accessed: 28.04.2018).

³⁶ Centrum Systemów Informacyjnych Ochrony Zdrowia, *Opis Funkcjonalny Systemu P1 z Perspektywy Integracji Systemów Zewnętrznych*, Edition 1, 1.1.2016 <https://p1.csioz.gov.pl/fileadmin/user_upload/opis_funkcjonalny_systemu_p1_z_perspektywy_integracji_systemow_zew_5811ab8ee8e37.pdf> (accessed: 06.2018).

³⁷ 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.

- any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;
- the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp (Art. 44, item 1)³⁸.

Other European countries have already implemented IT systems that play the function of electronic mailboxes. Estonia, for example, uses an interesting solution. Every person with the Estonian identification number (the equivalent of the Polish PESESL) has the possibility to set up an e-mail address in the national system to which the authorities send important encrypted documents. The service is supplemented by the DigiDoc system which is used to save, share and sign electronic documents and is provided both to the citizens and private and public sectors. Logging to the DigiDoc system can be done through the Estonian ID card with a built-in chip or with the use of a mobile ID (with a special dedicated SIM card). The users can upload files to the server, sign them digitally (using the card) and send (e.g. with the use of the national e-mail address). The use of electronic signatures helps Estonia save 2 percent of its GDP per year³⁹.

Within the indicative projects of the Polska Cyfrowa Operational Program, the Ministry of Digitization prepared a plan for developing e-Delivery in 2018-2020 as a universal trust service that is provided by a trusted third party of a registered electronic delivery service provider (the cooperation with the Envelo platform of Polish Post is suggested). e-Delivery is to be available to everybody: a citizen or an entrepreneur will be entitled to electronic communication with public sector institutions (also with public activity bodies, hospitals including) after declaring their accession to e-Delivery service⁴⁰.

The benefits of e-Delivery include lower service costs in comparison to traditional (paper-based) correspondence, an easier access to services (the access from any place with an Internet connection), the security and reliability of delivery (data encryption, documentation archiving) and similar legal effects as in the case of sending the first copy by a registered post⁴¹. Moreover, a high integrity of the contents delivered is an advantage and the possibility to sign the whole

³⁸ 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.

³⁹ Instytut Poczty, *Cyfryzacja Usług Publicznych w Europie, Rola Operatorów Poczty, Model Dla Polski* <http://instytutpoczty.pl/files/raport_instytut_poczty.pdf> (Accessed: 06.2018).

⁴⁰ Ministry of Digitization, *e-Doręczenia - usługa rejestrowanego doręczenia elektronicznego w Polsce* <cyfryzacja/e-doreczenia-usluga-rejestrowanego-doreczenia-elektronicznego-w-polsce> (Accessed: 25.06.2018).

⁴¹ K. Piskorski, *E-Skrzynka i e-Doręczenie, Możliwy Scenariusz Dla Polski*, Instytut Poczty, 2017.

content of the message gives the assurance of credibility and security. The development of such a standard of electronic delivery may result in the growth of the market for trust service providers⁴².

5. Problems with new solutions

Certain barriers and problems appear already in the trial stage. The draft Act on the amendment to the act on trust services and electronic identification and some other acts (2018)⁴³, provides for the use of the digital tool of ZUS that is applied to sign electronic leaves. The method is used in a closed system of information flow to authenticate medical electronic documentation while in the case of e-Prescriptions this is an open system. Thus, a third form of identity confirmation is developed apart from the ePUAP trusted profile and the Qualified Signature. However, the difference is that the ZUS authentication tool does not meet the eIDAS regulation security requirements and it should not be used as a common method to sign electronic documents outside an institution as it is the case with e-Prescriptions.

Another problem concerns the fact that Draft Act on the amendment to the act on trust services and electronic identification and some other acts (2018) points out clearly that the signature within the ePUAP trusted profile is not an advanced electronic signature and, consequently, the requirements and criteria regulations of eIDAS are not met in this case⁴⁴. As a result, the signature that is confirmed by the ePUAP trusted profile, despite the fact that it provides wide the opportunity to be used in national administration services, cannot be applied in public digital services outside Poland^{45 46}. This creates a barrier for the use of Polish tools of electronic signature in other member-states as the documents that are signed with the public electronic key are not valid. Thus, a gap emerges in the trust services that are provided by public institutions which are responsible for the development of electronic signature that should meet EU standards.

⁴² K. Okoński, *E-Doręczenia – Usługa Rejestrowanego Doręczenia Elektronicznego w Polsce*, Ministerstwo Cyfryzacji, 06.2018.

⁴³ Draft Act on the amendment to the act on trust services and electronic identification and some other acts (2018) <<https://legislacja.rcl.gov.pl>>.

⁴⁴ M. Marucha-Jaworska, *Rozporządzenie EIDAS: Zagadnienia Prawne i Techniczne*, Edition 1, Wolters Kluwer Polska, Warszawa 2017.

⁴⁵ 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,

⁴⁶ Accenture, Obserwatorium.biz, *Raport. Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce 2017* <<https://www.accenture.com/pl-pl/insight-breakthrough-online-services>> (accessed: 06.2018).

Conclusions

Despite several national and international regulations, there is some freedom as regards the development of identification and trusted service systems, which is mainly due to the principle of technological neutrality. This encourages innovativeness on the one hand, but on the other hand it makes the coordination of ICT systems more difficult. International law plays a major role in the development of identification and authentication technology. The freedom of operations that is offered by legislators aims at encouraging private business to cooperate with public institutions in the field of identification and authentication methods, tools and technology in healthcare. What is more, there is a chance for opening European markets (medical markets including) thanks to the digitization of services. Unfortunately, with regard to identification and authentication tools, Poland has no clear and uniform functional system and the potential of trusted services is not fully implemented in the healthcare sector. When developing its own model, Poland should follow good practices of electronic identification systems of other countries.

Bibliography

- [1] Accenture, Obserwatorium.biz, *Raport. Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce 2017* <<https://www.accenture.com/pl-pl/insight-breakthrough-online-services>> (accessed: 06.2018).
- [2] Accenture, Obserwatorium.biz, *Raport EID 2017, Elektroniczna Identyfikacja w Polsce 2017* <<https://www.accenture.com/pl-pl/event-eid-report-2017>> (accessed: 06.2018).
- [3] Accenture, Obserwatorium.biz, *Raport. Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce 2017* <<https://www.accenture.com/pl-pl/insight-breakthrough-online-services>> (accessed: 06.2018).
- [4] Cabańska D., Biniek K., *Węzeł Krajowy. Ministerstwo Cyfryzacji. Centralny Ośrodek Informatyki*, <<https://www.gov.pl/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej>> (accessed 06.2018).
- [5] Centrum Systemów Informacyjnych Ochrony Zdrowia, *Opis Funkcjonalny Systemu P1 z Perspektywy Integracji Systemów Zewnętrznych*, Edition 1.1.2016 <https://p1.csioz.gov.pl/fileadmin/user_upload/opis_funkcjonalny_systemu_p1_z_perspektywy_integracji_systemow_zew_5811ab8ee8e37.pdf> (accessed: 06.2018).
- [6] Centrum Systemów Informacyjnych Ochrony Zdrowia, *Pilotaż e-Recepty startuje w Siedlcach oraz Skierniewicach* <<https://www.csioz.gov.pl/aktualnosci/szczegoly/pilotaz-e-recepty-startuje-w-siedlcach-oraz-skierniewicach/>> (accessed: 28.04.2018).
- [7] Instytut Poczty, *Cyfryzacja Usług Publicznych w Europie, Rola Operatorów Poczty, Model Dla Polski* <http://instytutpoczty.pl/files/raport_instytut_poczty.pdf> (accessed: 06.2018).

- [8] Jakubowski Sz., *Identyfikacja i Uwierzytelnianie Podmiotów Oraz Dokumentów Elektronicznych w Ochronie Zdrowia* (Praca wykonana w Zakładzie Medycznych Systemów Informacyjnych, Instytut Zdrowia Publicznego, UJ CM, 2018).
- [9] EU Commission, **Annex: Technical specifications and procedures for assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme** <<https://eur-lex.europa.eu>>.
- [10] Marucha-Jaworska M., *Rozporządzenie EIDAS: Zagadnienia Prawne i Techniczne*, Wyd. 1, Wolters Kluwer Polska, Warszawa 2017.
- [11] Ministerstwo Cyfryzacji, *Budowa Krajowego Węzła Identyfikacji Elektronicznej* <<https://www.gov.pl/web/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej>>.
- [12] Ministerstwo Cyfryzacji, *Budowa i wdrożenie Węzła Transgranicznego* <<https://www.gov.pl/web/cyfryzacja/budowa-i-wdrozenie-wezla-transgranicznego>>.
- [13] Ministerstwo Cyfryzacji, *e-Doręczenia - usługa rejestrowanego doręczenia elektronicznego w Polsce* </cyfryzacja/e-doreczenia-usluga-rejestrowanego-doreczenia-elektronicznego-w-polsce> (Accessed: 25.06.2018).
- [14] Ministerstwo Cyfryzacji, *Koncepcja E-Dowód – Kontynuacja Projektu Pl.ID i Realizacja Projektów Powiązanych. Załącznik 1 Opis Statusu Projektu Pl.ID*, <<https://www.gov.pl/>> (Accessed: 06.2018).
- [15] Okoński K., *E-Doręczenia – Usługa Rejestrowanego Doręczenia Elektronicznego w Polsce*, Ministerstwo Cyfryzacji, 06.2018.
- [16] Piskorski K., *E-Skrzynka i e-Doręczenie, Możliwy Scenariusz Dla Polski*, Instytut Poczty, 2017.
- [17] Draft Act on the Amendment of Act on Trust Services and Electronic Identification and some other acts (2018, <<https://legislacja.rcl.gov.pl>>).
- [18] Draft act 1 June on the amendment to the Act on Public Funding of Health Care Services , p. 18 <<https://legislacja.rcl.gov.pl/projekt/12312303/katalog/12513763#12513763>>.
- [19] Romaszewski A. et al., *Identyfikacja i Uwierzytelnienie w Systemie Informacyjnym Opieki Zdrowotnej Po Wprowadzeniu Rozporządzenia UE EIDAS*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2016, No 42.
- [20] Romaszewski A. et al., *Wprowadzenie usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej, część II*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2016, No 42.
- [21] Romaszewski A., Trąbka W., Kielar M., Gajda K., *Funkcjonowanie systemów identyfikacji i uwierzytelnienia w polskim systemie opieki zdrowotnej - stan obecny i kierunki zmian*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2017, No 44.
- [22] 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
- [23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EU (General Data Protection Regulation), p. 679 <<https://eur-lex.europa.eu>>.
- [24] Act of 5 September 2016 on Trust Services and Electronic Identification, (Journal of Laws 2016, item 1579), <<http://prawo.sejm.gov.pl>>.
- [25] Act of 10 May 2018 on Personal Data Protection (Journal of Laws 2018, item 1000), <<http://prawo.sejm.gov.pl>>.

- [26] Act of 17 February 2005 on Informatization of Entities Performing Public Tasks, (Journal of Laws 2005, No. 64 item 565).
- [27] Act of 18 July 2002 on Provision of e-services, (Journal of Laws 2002, No. 144 item 1204)
- [28] Act of 28 April 2011 on healthcare information system, Journal of Laws 2011, No.113, item 657, <<http://prawo.sejm.gov.pl>>.

Abstract

The eIDAS regulation is one of the most significant regulations whose provisions are crucial to health care system. Its basic task is to increase the trust to electronic transactions together with the provision of a common basis for secure electronic interactions between citizens, companies and public institutions. This is extremely important in health care where there is a constant exchange of information between, patients, service providers and entities that are legally authorized to receive health information.

The article presents the main assumptions and solutions of the regulations that concern both the identification of entities and the application of trust services in the present-day operations of health care institutions.

With the existing identification and authentication (e-ID card) tools and the suggested e-documents to be sent (e-Prescription, e-Referral), a service is needed that would ensure the delivery of information to all entities in question – for such purposes e-Delivery is planned.

Despite several national and international regulations there is some freedom as regards the development of identification systems and trust services, which is mainly due to the principle of technological neutrality. This encourages innovativeness on the one hand but on the other hand it makes the coordination of teleinformatic systems more difficult. A major role in the development of identification and authentication techniques is played by international law.

Key words

eIDAS, electronic identification, authentication, trust services, national electronic identification scheme, health care