● JOURNAL OF PUBLIC HEALTH, NURSING AND MEDICAL RESCUE ● No. 4/2018 (24-30) ●

Additional trust services

(Dodatkowe usługi zaufania)

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 other vital tools of trust services, including electronic time stamp, electronic registered delivery services and website authentication. The electronic time stamp was introduced due to the danger of time manipulation for electronic transactions. A trust service provider may use time stamps in order to prevent time shifting in the process of electronic transactions carried out between economic entities. The purpose of registered delivery service is to provide proof related to the handling of transmitted data, including proof of sending or receiving data, and to protect transmitted data against the risk of loss, theft, damage or any unauthorised alterations. On the other hand, an authenticated website ensures a visitor that a genuine and legitimate entity is held liable for it. Moreover, the forms of supervision over trust service providers have been discussed here.

Key words **-** electronic time stamp, electronic registered delivery services, website authentication.

Streszczenie – Autorzy omówili inne, ważne narzędzia usług zaufania jak elektroniczny znacznik czasu, usługi rejestrowanego doręczenia elektronicznego oraz uwierzytelnianie witryn internetowych. Narzędzie elektronicznego znacznika czasu wprowadzono ze względu na niebezpieczeństwo manipulacji czasem dla elektronicznych transakcji. Aby zapobiec zmianom czasu w procesie obrotu elektronicznego między podmiotami gospodarczymi, dostawca usług zaufania może użyć znaczników czasu. Usługa rejestrowanego doręczenia elektronicznego ma zapewnić dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chronić przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany. Z kolei uwierzytelniona witryna internetowa daje odwiedzającemu pewność, że za tę stronę jest odpowiedzialny prawdziwy i prawowity podmiot. Omówiono ponadto formy nadzór dostawców usług zaufania.

Słowa kluczowe **-** elektroniczny znacznik czasu, usługi rejestrowanego doręczenia elektronicznego, uwierzytelnianie witryn internetowych.

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. INTRODUCTION

Apart from major trust services including a signature and electronic stamp, there are some other equally important tools such as electronic time stamp, electronic registered delivery service and website authentication.

II. ELECTRONIC TIME STAMP

Electronic time stamp means : „electronic data which binds other electronic data to a particular time establishing evidence that this data existed in that particular time" (Art. 3 p. 33) [1].

The electronic time stamp was introduced because of danger of time manipulation in electronic transactions**.** A trust service provider may use time stamps in order to prevent time shifting in the process of electronic transactions carried out between economic entities. [2,3] We can single out a qualified time stamp, which due to its complexity, must fulfil the following standards: it must bind date and time with data in a manner that prevents any undetectable data alterations, it must be based upon accurate time source and be linked to a qualified signature or electronic stamp or, in some other way, be ensured by the trust services provider (Art. 42) [1]. Similarly as in the case of other trust services, the legal effect of electronic time stamp cannot be in any way limited or denied only due to the fact that the stamp is in electronic form or that at a specific moment it fails to comply with relevant standards. Moreover, the stamp tool uses the principle of time and date accuracy and should prove integrity with the data it was assigned to [1].

III. ELECTRONIC REGISTERED DELIVERY SERVICE

According to the EU legislator, the electronic registered delivery service means „a service that provides data transmission between third parties by electronic means and provides proof related to the handling of transmitted data, including proof of sending or receiving data and protecting transmitted data against the risk of loss, theft, damage or any unauthorised alterations (Art. 3 p. 36) [1].

A qualified electronic registered delivery service is encumbered with the following requirements [1]:

- it must be granted by at least one qualified trust service provider,
- it must provide undisputable identification of a sender,
- it must authorise an addressee prior to the data transmission,
- it must safeguard both sending and receiving data by means of an advanced electronic signature or electronic stamp, which prevents data manipulation,
- even a minimum data alteration requiring sending or receiving data must be clearly revealed to both parties of the data exchange process,
- the date of sending, receipt or any change of data must be indicated by a qualified time stamp (Art. 44 p.1).

IV. WEBSITE AUTHENTICATION

An authenticated website that was granted a certificate ensures a visitor that a genuine and legitimate entity is held liable for it. A website authentication service is voluntary. In order for a given web page to be granted a qualified certificate it must meet certain minimum requirements stipulated in the regulation [1]. It gives medical entities an opportunity to enhance the users'/patients' level of trust for their web pages and thus enables them to communicate important information. Experts from this field state that a qualified certificate for website authentication practically operates in a manner similar to SSL (Secure Socket Layer) certificate used by banks to confirm credibility [2].

V. SUPERVISION OVER TRUST SERVICE PROVIDERS

Each of the member states is intended to establish their own supervisory bodies over trust service providers. Their operating area is limited within the state borders. Despite the fact that each of the countries have received their separate supervision functions, they are subject to the same approved European standards and must follow similar procedures. Additionally, the rule of mutual assistance amongst different institutions has been accepted, which consists in mutual transfer of good practice and exchanging useful information, which may contribute to the efficiency enhancement. Apart from that, the state supervisory bodies are obliged to forward an annual activity report to the EU Commission and a report on any infringements of safety rules in a given country to a supervisory authority, i.e. the European Network and Information Security Agency (ENISA) [3,4].

The Minister of Digitization serves the role of supervisory body in Poland and according to the eIDAS regulation performs the following tasks [1]:

- undertakes supervision of qualified trust service providers established on the territory of the designating

member state in order to ensure that- by means of ex ante and ex post supervisory actions- the qualified trust services providers together with their qualified services meet the requirements laid down in this regulation;

- undertakes, if necessary, all the actions in relation to non-qualified trust service providers established on the territory of the designating member state- by means of ex post supervisory actions- when he finds out that the non-qualified service providers or their trust services allegedly do not satisfy the requirements stipulated in this requirement" (Art. 17 p. 3).

VI. TRUSTED PROFILE IN POLAND

The adoption of the Act on electronic signature in 2002 may be seen as the beginnings of implementing electronic identification and trust services in Poland. Since 2005, works on the eUPAP (the electronic public administration services platform) system have been performed, paying particular attention to the creation of electronic identification mechanisms and (qualified) electronic signature. In 2010 a new functionality was added to the platform, i.e. the Trusted Profile, which was meant to become an alternative tool for electronic signature and enabled settling administrative formalities such as filing applications, declarations or making payments via online services [5].

The Trusted Profile is seen as a set of reliable data related to a specific user. Data stored on the profile is encrypted and secured against theft and personating. Trusted profile makes it possible to confirm one's identity in online services or to sign electronic documents. The trusted profile can be set up by any person holding a PESEL (personal identification number) via bank account (electronic banking of selected banks excludes the need for a visit to an office), via qualified certificate (excludes the need for a visit to an office), or by online application (on ePUAP platform) which must be personally confirmed within 14 days in the nearest Place of Confirmation (Tax Office, Municipal Office or a bank- both in the country or abroad). Setting up the trusted profile is free of charge and instantly accessible and the account is valid for 3 years. Due to the trusted profiles one can use the services of the following portals, including: The Electronic Public Administration Services Platform (ePUAP), Electronic Services Platform of the Social Insurance Institution (PUE ZUS), or Business Activity Central Register and Information Record (CEIDG) [6]. Electronic signature, as part of the trusted ePUAP profile, does not meet all the technical requirements stipulated in the eIDAS regulation and therefore will not be valid in any administrative system other than Polish. It does, however, implement a significant scope of domestic services [6].

A signature confirmed by a trusted ePUAP profile is an electronic signature placed by the user of a given platform to which identifying information included in the trusted profile system is attached. Additionally, a signature placed via the trusted ePUAP profile must meet the following requirements[7]:

- it must expressly indicate the trusted ePUAP profile of a person who placed that signature,
- it must include information related to the time the signature was placed,
- it must expressly identify an ePUAP account of a person who placed that signature,
- it must be authorised by the user of the ePUAP account,
- it must be signed and protected with an electronic seal used in the ePUAP profile in order to ensure integrity and authenticity of the operations performed by the ePUAP system; (Art. 3 p. 15).

So far, the trusted profile is not widely used in health service either by the patients o by the medical personnel. The exception is with cases when entities performing their medical activities are related to public institutions and some of the issues can be handled by means of online services and with the use of electronic signature on the trusted profile. Additionally, a patient can fill in and send selected applications, for instance an application for EHIC card.

VII. DATA SECURITY

A few important international and state regulations play a key role in the area of personal data security, electronic documents and systems used in health service.

The basic standards used in the area of protection of the patients' personal data, are regulated, apart from legal requirements, by international standards such as: ISO/IEC 27001 (current version ISO/IEC 27018:2014), ISO/IEC 27002 and ISO/IEC 27018 [8]. The first ISO/IEC 27001 standard mentioned above refers to information security management, establishing a strategic model for information safeguarding based upon the standards and legal requirements of risk prevention. It is worth pointing out that the

standard also regulates the system elements such as cryptography, sensitive data encryption and access control. The ISO/IEC 27002 standard, on the other hand, discusses in a wider perspective the guidelines contained in the ISO/IEC 27001 standard and, in particular, the rules of implementing and monitoring the systems for information security. The last ISO/IEC 27018 standard functions in connection with the aforementioned standard and indicates specific requirements of secure personal data processing, including in cloud computing [8].

In Poland, Inspector General for the Protection of Personal Data, since May 2018 also referred to as the President of the Office of Personal Data Protection, holds the superior authority controlling data processing in accordance with applicable law. The institution's tasks involve carrying out planned and unannounced controls resulting from complaints or other disturbing signals. Apart from the domestic Office of Personal Data Protection, some other supervisory authorities from EU member states can be involved in the execution of control activities.

If the control reveals entity's unlawful activity, a warning, administrative order or a financial sanction can be imposed on such entity [9].

Additionally, the Bureau for the Office of Personal Data Protection issues certificates for enterprises which prove that the standards of personal data processing and protection are fulfilled. Moreover, the President of the Office of Personal Data Protection and the Polish Centre of Accreditation may grant accreditation to institutions having recognised expertise for issuing the abovementioned certificates. The entities are obliged to register their Data Protection Supervisors and their institutions processing personal data in the register of the Office of Personal Data Protection [10].

The amended *Act of 17 February 2005 on the computerisation of entities serving public functions (Journal of Laws of 2005, No 64, item 565)* plays a vital role in the area of supervision and security of ICT systems designed for performing public tasks of registering, collecting and sharing data or communicating with stakeholders [11]. In relation to the health sector, this Act involves mainly independent public healthcare institutions, companies conducting medical business within the meaning of healthcare regulations, National Health Fund, Health Insurance Company or the Agricultural Social Insurance Fund [7].

The President of the Office of Personal Data Protection acts mainly in accordance with legal regulations, including the international ones. These regulations shall involve: *Regulation No 2016/679 of the European Parliament and the EU Council of 27 April 2016 on the protection of individuals with regard to processing personal data and on the free movement of such data, and repealing Directive 95/46/EC*, commonly referred to as General Data Protection Regulation – GDPR (the Polish abbreviation- RODO). The GDPR was implemented in Poland by means of *the Act of 10 May 2018 on the protection of personal data (Journal of Laws of 2018, item 1000)* [11]. The objective of this regulation is the protection of personal data of individuals and the free movement of such data. It was decided that this objective could be achieved due to the establishment of standards for data protection and processing common for the EU member states and by ordering the design of data security systems managed by the Inspectors for the Protection of Personal Data employed by each entity that processes personal data. The provisions contained in the GDPR regulation gave the EU citizens a greater control over the data they entrusted to an entity and granted them the right to easier access, limitation or removal of collected data [10].

The General Regulation on the Protection of Personal Data is amended with an „e- Privacy" regulation on privacy and electronic communication with the full name as follows: *Regulation of the European Parliament and the EU Council on the respect for private life and protection of personal data in electronic communication, repealing Directive 2002/58/EC.*

The objective of this regulation is to enhance the safety level for the users of the so called terminal equipment, including computers, telephones and other mobile devices). This regulation focuses primarily on data deriving from electronic communication services (e.g. e-mails) and on metadata (detailed data, residual data), including the data sent automatically between devices when the exchange takes place on the device- to- device level [12]. An example of data exchange from the device- to-device level is sending medical tests results from medical devices such as a computer-assisted tomograph to the medical specialist's computer via Internet. According to „ePrivacy" regulation, also the data collected by the user's devices, including metadata sent from a portable electrocardiograph to a web platform via Internet should be safeguarded- such solution is based on the Internet of Things (IoT) approach [13].

Apart from the abovementioned regulations, there some other key documents related to cyber security, i.e. the NIS (Network and Information Systems Directive) and a Polish directive which is being prepared in connection with the NIS- *an Act on the State cyber security system (a draft law from 2018)*. A Directive with the full name of: *Directive 2016/1148 of the European Parliament and the EU Coun-*

cil of 6 July 2016 on the measures for the common high level of network and IT systems security on the EU territory is addressed mainly to the key service providers (banking, health care and others) and to the digital service providers (e.g. web browsers, cloud computing services) in order to achieve a higher level of cyber security in particularly sensitive sectors, susceptible to data loss. In order to succeed, the following actions must be taken: setting the security standards, designing procedures for reporting incidents in the key sectors, approving domestic standards from the area of the network and IT systems security and finally building a network of Computer Security Incident Response Teams (CSIRT) [14]. In Poland, works on the Act on the network security are in progress in response to the EU regulation. The draft law on the state cyber security stipulates the achievement of high level security of the IT systems, vital for the state and the economy (including healthcare sector) [15]. The draft law provides for the implementation of an IT system by 2021 and will facilitate reporting, servicing and assessment of incidents involving breach of data security standards and preventing potential threats. The key actor working in this area is the Ministry of Digitization which is devising the State Cyber Security Strategy and reporting on the condition of the state IT security systems to the EU institutions [16]. The European Union Agency for Network and Information Security – ENISA, set up in 2004, is an authority and the centre of expertise on cyber security in central Europe [17].

VIII. BARRIERS TO THE IMPLEMENTATION OF IDENTIFICATION SOLUTIONS IN HEALTH CARE

Devising an effective system of information exchange in health care, based upon the elements of identification and authentication, meets various obstacles.

The Supreme Audit Office (NIK) has controlled entities carrying out medical activity and assessed the process of setting up electronic medical documentation, safeguarding the records and making them available. The report results revealed key problems with abiding the rules and standards as regards electronic medical documentation. None of the controlled entities had a reliable IT system working in compliance with the abiding law [18]. Therefore, despite all the IT tools implemented on the state level, the model of trust services practically meets a lot of obstacles on the territory of Poland, which results mainly from „a huge non-compliance of IT infrastructure" with said regulations [19].

The proposed system of making up and filling prescriptions could look as the one on the scheme presented below.

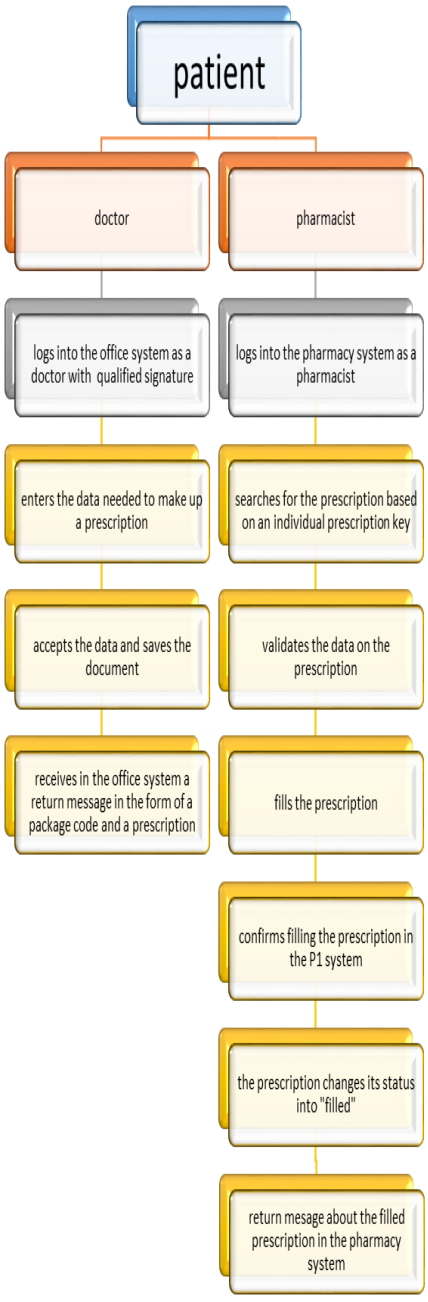

Figure 1. A proposed scheme of making up and filling e-Prescriptions
[own study based on: Test Scenarios, e-Prescription Projectathon, CSIOZ:20]

The problem arising in this area is the fact that in *the draft law of the amended Act on trust services and elec-*

tronic identification and some other Acts (draft law 2018) [20], the legislator plans to approve a ZUS (Social Insurance Institution) tool used for signing electronic sick-leaves, which functions in a closed system of information sharing, and to implement it into the system authenticating electronic medical documentation, in this case e-prescriptions included in the open system. Thus, the third means of identity confirmation, apart from the ePUAP profile and Qualified Signature, shall be created.

The difference is that the ZUS authentication tool does not meet the requirements of the eIDAS regulation and as such should not be commonly used as a tool for signing electronic documents (e-prescriptions) outside institution, i.e. in the open system.

The draft law of *the amended Act on trust services and electronic identification and some other Acts (draft law 2018)* clearly states that a signature operating within the framework of the trusted ePUAP profile is not an advanced electronic signature, therefore the requirements and criteria of the eIDAS regulation are not fulfilled [3]. It means that a signature authenticated by the trusted ePUAP profile gives the possibility of realizing a wide scope of administrative services. However, it cannot be used in public online services outside Poland [1,2]. It creates a barrier for the use of Polish electronic signature tools in other EU member states as the documents signed by means of a public key shall be invalid. Therefore a gap arises in the trust services offered by public institutions which are responsible for devising an electronic signature tool that would meet the EU standards.

The current concept of electronic medical documentation assumes that it will be created from scratch in a medical healthcare entity with the patient's confirmation of an appointment. Next, the confirmed data should be sent to the Medical Information System (MIS) [20]. The problem is that neither the tools for patient or medical Staff identification nor the electronic health cards preventing it have been prepared .

IX. REFERENCES

[1] Regulation of the European Parliament and the European Council 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [online] [cited 2018 Apr 28] Available from: URL: https://eur-lex.europa.eu

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

[3] Marucha-Jaworska M. Rozporządzenie eIDAS : zagadnienia prawne i techniczne [eIDAS regulation: legal and technical issues].
1. ed. Warsaw; Wolters Kluwer, Poland, 2017.

[4] Pejaś J, Szulga M, Wagemann M, Stoliarowa-Myć P, Wiktorczyk P. Wdrożenie rozporządzenia eIDAS w Polsce. [Implementation of the eIDAS regulation in Poland] Report Version 4.2. 2014.

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

[6] Ministerstwo Cyfryzacji. Czym jest profil zaufany i jak go założyć [the Ministry of Digitization. What is a trusted profile and how to establish it?] [Internet]. obywatel.gov.pl. [online] [cited 2018 Apr 28] Available from: URL: https://obywatel.gov.pl/zaloz-profil-zaufany#scenariusz-przez-internet

[7] Act of 17 February 2005 r. on computerisation of the activity of entities performing public tasks (Journal of Laws, 2005 No 64 item 565). [online] [cited 2018 Apr 28] Available from: URL: http://prawo.sejm.gov.pl

[8] Domański Zakrzewski P, Najbuk P, *and partners.* Cyberbezpieczeństwo w sektorze ochrony zdrowia. [Cyber security in the healthcare sector] [online] [cited 2018 Mar 18] Available from: URL: www.dzp.pl

[9] Generalny Inspektor Ochrony Danych Osobowych. Zadania i kompetencje - GIODO [General Inspector for the Protection of Personal Data. Tasks and competences] [Internet]. [online] [cited 2018 May 28] Available from: URL: https://giodo.gov.pl/pl/537

[10] Regulation 2016/679 of the European Parliament and the EU Council (UE) of 27 April 2016 on the protection of individuals with the regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC

[11] (general regulation on the data protection). [online] [cited 2018 Apr 18] Available from: URL: https://eur-lex.europa.eu

[12] The Act of 10 May 2018 on the protection of personal data (Journal of Laws of 2018, item 1000) [online] [cited 2018 May 18] Available from: URL: http://prawo.sejm.gov.pl

[13] Regulation of the European Parliament and the EU Council on the respect for private life and protection of personal data in electronic communication and repealing Directive 2002/58/EC (regulation on privacy and electronic communication). [online] [cited 2018 Mar 18] Available from: URL: https://eur-lex.europa.eu

[14] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener Comput Syst. 1 wrzesień 2013; 29, 7:1645–60.

[15] Directive 2016/1148 of the European Parliament and the EU Council of 6 July 2016 on the measures for the common high level of network and IT systems security on the EU territory [online] [cited 2018 Mar 18] Available from: URL: https://eur-lex.europa.eu

[16] Draft law of the state cyber security system. [online] [cited 2018 Mar 18] Available from: URL: http://www.sejm.gov.pl/sejm8.nsf/agent.xsp?symbol=RPL&Id=RM-10-64-18

[17] The Ministry of Digitization, Dominika Waligórska.: Draft law of the state cyber security system. [online] [cited 2018 May 30] Available from: URL: /cyfryzacja/projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa

[18] The European Union.: The European Union Agency for Network and Information Security (ENISA) - EUROPA. [online] [cited 2018 May 30] Available from: URL: https://europa.eu/european-union/about-eu/agencies/enisa_pl

[19] Romaszewski A, Trąbka W, Kielar M, Gajda K. Wprowadzenie Usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej [Implementation of trust services in compatible with the EU eIDAS regulation in the ascpect of healthcare information system (part I). Zesz Nauk Wyższa Szk Zarządzania Bank W Krakowie [Cracow University, Department of Management and Banking]. 2016;(No 42):24–40. Centrum Systemów Informacyjnych Ochrony Zdrowia [Healthcare Information Systems Centre].: Test scenarios, Projectathon e-prescriptions. [online] [cited 2018 May 30] Available from: URL: https://www.csioz.gov.pl/fileadmin/user_upload/projectathon_e_recepty_scenariusze_testowe_5ace11f79d0ef.pdf

[20] The draft law of the amended Act on trust services and electronic identification and some other Acts. [online] [cited 2018 May 31] Available from: URL: https://www.premier.gov.pl/

[21] The Act of 28 April 2011 . on IT systems in hdealthcare (Journal of Laws of 2011, No 113, item. 657). [online] [cited 2018 Nay 31] Available from: URL: http://prawo.sejm.gov.pl