Trust services in the healthcare-related sector

(Usługi zaufania w sektorze ochrony zdrowia)

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 – Within the framework of this paper, the authors discuss the scope of the so-called trust services, with the focus being put especially on the healthcare-related sector. The role played by and the principles governing the process of putting one's electronic signature are discussed herein as well. The authors also touch upon the importance of the electronic seal as defined by both the European and domestic legal systems.

Key words **-** trust service, electronic signature, electronic seal, healthcare.

Streszczenie – Autorzy omówili zakres usługi zaufania, ze szczególnym uwzględnieniem sektora służby zdrowia. Scharakteryzowali rolę i warunki składania podpisu elektronicznego. Omówili znaczenie Pieczęć elektroniczna zdefiniowanej przez europejski i krajowy system prawny.

Słowa kluczowe **-** usługa zaufania, podpis elektroniczny, pieczęć elektroniczna, ochrona zdrowia.

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. INTRODUCTORY REMARKS

As specified by the legislator in the eIDAS ordinance, art. 3, point 16, trust service shall be understood as ,,a digital service typically provided for a remuneration and including [1]:

- creation, verification, and validation of electronic signatures, electronic seals, or electronic timestamps, digital registered delivery services, as well as certificates connected with such services; or
- creation, verification, and validation of website authorization certificates; or
- conservation of electronic signatures, seals, or certificates related to such services".

In the case of the healthcare-related sector, trust services can be further subdivided into open and closed ones, which makes it possible to specify the scope of supervisory undertakings and identify the requirements arising from the adoption of the eIDAS ordinance. Open trust services should be understood as a set of trust services created with the society (patients) in mind, which may have an impact on third parties. On the other hand, closed trust services are provided to a specified societal group without having an impact on third parties, and are based on the utilization of a closed IT system not governed by the eIDAS ordinance. Administrative workers of a hospital are a fitting example of a group taking advantage of closed trust services [1,2].

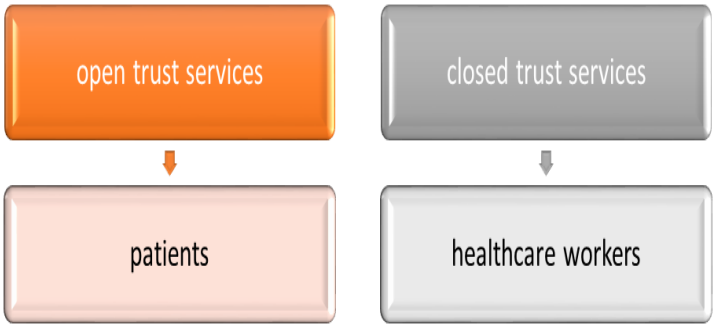

Figure 1. Division of trust services in the healthcare-related sector [own elaboration]

Potential advantages of utilizing trust services are as follows [3]:

- concluding employment agreements in an online manner (e.g. with doctors and nurses)
- concluding basic B2B contracts (e.g. hospital – wholesaler),
- proper security of digital formal correspondence exchanged between a citizen/patient and a public institution,
- automatic (free of any delays) issuing of certain certificates and attestations by public administration bodies (NHS, SII),
- limiting the scope of responsibilities of administrative bodies thanks to resorting to electronic delivery services,
- ability to provide services to the majority of the society thanks to the use of electronic services.

II. ELECTRONIC SIGNATURE

Electronic signature, understood as a trust service, should be understood as: „data in an electronic form that are attached to or logically connected with other electronic data and used as a signature" (*art. 3 point 10*). [1]
Basing on the eIDAS ordinance, one can distinguish 3 major types of electronic signatures [1]:

- Electronic signature,
- Advanced electronic signature,
- Qualified electronic signature.

The first type of digital signatures, namely – the electronic one, can be made only be a signatory being a natural person. Electronic signature is not to be used by legal persons, for they have to utilize the so-called electronic seal, which does not have the form of an electronic signature, but rather – of an authorization tool confirming the validity of certain data. It has to be indicated at this point that electronic signature cannot be utilized to identify a person or to authorize data, for separate identification and authorization-related systems are taken advantage of for the said purposes [2,4].

When it comes to advanced electronic signature, it is more complex in nature and has to meet certain criteria, namely: it has to be assigned exclusively to a signatory, make it possible to specify signatory's identity, as well as allow for safe and controlled document signing by resorting to data created for said purpose and be connected with data in such a way for any further data changes to be be easily traced and identified. In EU Member States, it is allowed to sign documents by utilizing various formats of advanced electronic signature. The level of security of the aforementioned signature is sufficient with regard to service provider – ordering party relations. Such a form of signature additionally incorporates a certificate which can be stored on a cryptographic card or assigned to a one-off password system based on SMS messages with personalized, one-off passwords being sent to the owner of the signature. [2,4]

The last signature type discussed within this paper is the so-called qualified digital signature, which is a digital signature incorporating qualified certificates, as well as made by using to a qualified device ensuring maximum security. Major requirements with regard to qualified certificates are as follows: data confirming the validity of certificate's origin, data allowing for signature validation, certificate validity period, identification code of the certificate, and others (Annex 1, eIDAS ordinance) [1]. Furthermore, within the borders of the European Union, the use of the qualified electronic signature results in identical legal consequences as signing documents by hand does [4].

Electronic signatures cannot have their legal effect limited or nullified only because they are digital in nature or fail to comply with certain standards (12). Electronic signatures are validated (by means of verification and authentication processes), which makes it possible to issue a validation report confirming the validity of a particular signature. Yet another important service is conservation performed by service providers, the aim of which is to ensure the validity of both electronic signature and electronic seal. It allows to prove that the certificate that has been used to verify a signature/seal has been valid at the moment of signing. [3,5]

Table 1. Specificity of electronic signatures basing on the provisions of the eIDAS ordinance [own elaboration]

Categories/ Signature name	Electronic signature	Advanced electronic signature	Qualified electronic signature
Scope of utilization	declaration of will of the signatory	service provider – ordering party relations	in cases typically requiring signing documents by hand
Users	natural persons only	natural persons only	natural persons only
Distinctive features	any set of electronic data utilized by the user to make a signature, signature available in a digital form only	similar to the ones specified for the standard electronic signature plus: ensures integrity with a document, unique for a given signatory, allows for identity specification, ensures the visibility of further changes made to a given document	identical to the ones of the advanced electronic signature
Conservation	recommendations unspecified	subject to conservation	subject to conservation
Certificate type	none or other	advanced certificate	qualified certificate
Signing method	arbitrariness of methods used	arbitrariness of methods used, recommended use of a cryptographic card or methods basing on cloud computing	qualified device only
Legal effects	warrant of recognisability	warrant of recognisability	warrant of recognisability, equivalent to making a signature by hand
Signature validation	not specified	required	obligatory
Signature conservation	not specified	required	obligatory

In the case of the Polish healthcare-related sector, a medical worker has three methods of electronic document signing at his or her disposal, namely – using a signature confirmed by an authorized ePUAP profile, qualified electronic signature, or taking advantage of a device made available by the IT system of the Social Insurance Institution. It allows such medical expert to sign [6]:

,,1) electronic medical documentation;

2) applications for the access to data allowing for downloading medical documentation or data pertaining to such documentation from SIM within the scope necessary to perform diagnostic examination, ensure the undisrupted course of treatment, or equipping ordering parties with healing products, specific foodstuffs, and medical products;

3) applications for the access to data processed within SIM, allowing for exchanging data included in medical documentation between service providers" (art. 17 point 3).

III. ELECTRONIC SEAL

Electronic seal was not defined or regulated in any way until the introduction of the eIDAS ordinance to European and domestic legal systems. According to the ordinance issued by the European Union: ,,electronic seal relates to electronic data compiled together with other data sets in a digital form or that logically connected with them and ensures the authenticity and integrity of the associated data (art. 3 point 25)" [1].

The main factor making the seal different from electronic signature is the fact that the former is addressed to legal persons, whereas the latter – to natural persons. It should also be taken into account that said seal is not a signature of a legal person. Technically speaking, similar tools have a different purpose and are addressed to different user groups [1].

Similarly to electronic signature, electronic seal can be further subdivided into three types [1]:

- electronic seal
- advanced electronic seal,
- qualified electronic seal (art. 3, points 25 to 27).

The basic purpose of electronic seal is to secure a proof relating to a given electronic transaction. Said seal can be understood as a deed of issuing a document by an economic entity that ensures its authenticity. The European legislator, by expanding the function of electronic seal, made it possible to utilize such a tool to access and verify digital resources (e.g. programming code, server) [4,5].

Analogously to advanced electronic signature, advanced electronic seal has to be: uniquely assigned to a signatory and allow for the specification of his or her identity, make it possible to safely and efficiently use the seal by utilizing proper data, as well as make correlations between data sets to ensure the visibility of changes made. The manner of exercising supervision over data utilized while taking advantage of the seal in question is left to the signatory[4].

One can also draw analogies with regard to qualified electronic signature and qualified electronic seal. Said seal has to incorporate a qualified certificate and be made by

using a qualified device ensuring data safety. If qualified electronic seal is required to finalize a particular transaction, the legislator allows for using the qualified electronic signature of a legal person. What is more, the providers of trust services issuing advanced electronic seal-related certificates are obliged to utilize devices and tools allowing for the identification of natural persons representing legal persons, especially if it is required for administrative and judicial purposes at a domestic level [4].

Electronic seals cannot have their legal effect limited or nullified only because they are digital in nature or fail to comply with certain standards [1]. Both electronic seal and electronic signature are subject to validation, within the scope of which it is possible to issue a validation repot confirming the validity of the seal [3]. The aim of electronic seal is to automate certain electronic processes. It is used, among others, to: confirm agreement conclusion, issue electronic invoices (e.g. in the case of private medical treatment), issue administrative.

Table 2. Specificity of electronic seals basing on the provisions of the eIDAS ordinance [own elaboration]

Categories / Seal name	Electronic seal	Advanced electronic seal	Qualified electronic seal
Users	legal persons only (companies, agencies, or organizations)	legal persons only (companies, agencies, or organizations)	legal persons only (companies, agencies, or organizations)
Distinctive features	is not equivalent to electronic signature, ensures the authenticity of data, protects electronic transaction-related deeds, used to authorize electronic documents and digital resources	similar to the ones specified for the standard electronic seal plus: seal is unique for a specific entity, makes it possible to specify its identity, is required to use the seal safely, and ensures the visibility of amendments introduced to a document	similar to the ones specified for the advanced electronic seal plus: required to identify natural persons representing legal persons at a national level, possibility of using qualified electronic signature for transactions requiring qualified electronic seal to be utilized
Supervision	unspecified	arbitrariness of methods of supervising the validity of seal-related data	obligatory
Certificate type	none or other	advanced certificate	qualified certificate
Signing methods	arbitrariness of methods used	arbitrariness of methods used	qualified device only
Legal effects	warrant of recognisability	warrant of recognisability	warrant of recognisability
Seal validation	applies	applies	applies

IV. REFERENCES

[1] Ordinance of the European Parliament and Council (EU) 910/2014 of 23rd July 2014 on digital identification and trust services in relation to electronic transaction on the internal market repealing the 1999/93/WE Directive. [online] [cited 2018 Apr 28] Available from: URL: https://eur-lex.europa.eu

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

[3] Accenture, Obserwatorium.biz.: Raport. Przełom w usługach online. Rozwój usług zaufania w Polsce 2017. [cited 2018 Apr 28] Available from: URL: https://www.accenture.com/pl-pl/insight-breakthrough-online-services

[4] Marucha-Jaworska M. Rozporządzenie eIDAS : zagadnienia prawne i techniczne. 1. wyd. Warszawa; Wolters Kluwer Polska, 2017.

[5] Pejaś J, Szulga M, Wagemann M, Stoliarowa-Myć A, Wiktorczyk P. Wdrożenie rozporządzenia eIDAS w Polsce. Raport Wersja 4.2. 2014.

[6] Act of 28th April 2011 on information-related system in healthcare (The Journal of Laws 2011 no. 113 pos. 657). [cited 2018 Apr 28] Available from: URL: http://prawo.sejm.gov.pl