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

Mgr Mariusz Kielar
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
mariusz.kielar@uj.edu.pl

Mgr Krzysztof Gajda
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
krzysztof.gajda@uj.edu.pl

The article presents the concept of open and closed trust services and their types. It shows the idea of the national trust infrastructure and the national certification center. The eIDAS regulation, among other things, introduces changes in the existing services (e.g. in. the electronic signature). It also introduces such new services as electronic seal, authentication of websites and the preservation of electronic signatures, seals and certificates.

Introduction

The deadline for the introduction of trust services pursuant to the eIDAS regulation that are the topic of this article is 1 July 2016. This date is a precise moment after which the implementation of the trust service system is going to be commenced. With the consideration of several practical problems presented in the article and the changes being introduced pursuant to the new EU regulations, the fact that eIDAS is given by the legislator the form of a regulation and not of a directive seems to be crucial from the point of view of legal consequences. This is

because a EU regulation is a completely different legal act from a directive. While a EU directive is subject to implementation by member-states, the provisions of a directive are applied directly to national law systems. Moreover, the consequences of a regulation do not depend anyhow on national instruments that implement or introduce the regulation to national systems. The binding force of a regulation does not depend on the incorporation of its provisions to national law systems[1].

The form of a regulation excludes the possibility to change the provisions by member-states. However, the member-states have the right to make more precise or clarify the areas that were not defined by the legislator or that were directed to national law. Thus, it is acceptable to define the areas that remained "open" in the eIDAS regulation on the condition that the way it is done should not impede the achievement of the regulation objectives[2]. Currently, legal acts are being prepared in Poland that aim at the regulation of issues that were not regulated by eIDAS. The development should also include the principles and prerequisites of the civil liability of trust service providers as well as the methods and means of supervision, monitoring and control of these entities. The act should regulate the functioning principles of the trust service market by defining the conditions for the commencement and finalization of the operations of qualified service providers as well as the conditions for certificate suspension[3].

The above legal regulations will be of particular significance to Poland's systems of public administration, especially the healthcare IT systems. As regards the healthcare sector, the IT platforms that are developed within SIM (the Medical Information System) have not been completed and are not fully operational. Thus, an effective adoption of a varied model of trust services that are required by eIDAS may encounter several problems resulting from a substantial lack of adjustment of the Polish IT infrastructure to the regulations in question.

The article presents the concept of open and closed trust services and their types. It shows the idea of the national trust infrastructure and the national certification center. The eIDAS regulation, among other things, introduces changes in the existing services (e.g. in. the electronic signature). It also introduces such new services as electronic seal, authentication of websites and the preservation of electronic signatures, seals and certificates.

---

[1] Wróbel A., [in]: *Traktat o funkcjonowaniu Unii Europejskiej*. Komentarz. Volume III (ed.) D. Kornobis-Romanowska and J. Łacny, Warszawa 2012

[2] Mielnicki T. Wołowski F., Grajek M., Popis P. Łuczak P., Tabor M., Brakoniecki M., *Identyfikacja i uwierzytelnienie w usługach elektronicznych*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013

[3] Ibid.

Electronic seal

Electronic seal in trust services is a new solution in the Polish legal system. 'Electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity[4] (Figure 1).

Electronic seal is not an new concept – it has been functioning for over 15 years for example in the Czech Republic; moreover, the work on the act on the implementation of such instrument is being conducted in Belgium. It is worth mentioning that there were attempts to introduce electronic seal in Poland (e.g. there was an idea seven years ago to introduce it to the act on electronic signature) but finally the idea was withdrawn[5]. In fact, electronic seal was used in public administration offices for years but it was not defined directly in the provisions of law. Electronic seal was covered for the first time by a legal regulation when it appeared via the back door in the regulation on technical conditions for document delivery (ESP – electronic inbox). Such a regulation was necessary to implement ESP to enable issuing official document of receipt (UPO). Pursuant to the regulation, UPO was to be issued automatically by the system, without human intervention and with the application of an organization certificate, i.e. exactly contrary to qualified signature[6]. The definition of UPO that was included in the regulation as the attestation of the reception of "data attached to an electronic document" [7] functionally does not differ much from electronic seal but is restricted to the application in an inbox[8].

With the consideration of the above, it is justified to conclude that electronic seal is a trust service for legal persons. This means that natural persons will not have the right to use electronic seal. Thus, an issue arises about the permissibility of electronic seal to be applied by

[4] Preamble, Art. 59
[5] Zwolińska A., Szostek D., *E-pieczęć uwierzytelni firmowe i urzędowe dokumenty,* Rzeczpospolita, 23.03.2016, http://www.rp.pl/Opinie/303239980-E-pieczec-uwierzytelni-firmowe-i-urzedowe-dokumenty.html
[6] Do czego posłuży pieczęć elektroniczna? https://ipsec.pl/kwalifikowany-podpis-elektroniczny/2010/do-czego-posluzy-pieczec-elektroniczna.html
[7] Repealed regulation of Prime Minister of 29 September 2005 on organizational and technical conditions for the delivery of electronic documents to public entities (Journal of Laws 2005, No.200 item 1651, paragraph 2 (4)
[8] *Do czego posłuży pieczęć elektroniczna?* https://ipsec.pl/kwalifikowany-podpis-elektroniczny/2010/do-czego-posluzy-pieczec-elektroniczna.html

organizational units without legal personality. At present, there is no rule in the legal system that would exclude such entities from the application of the provisions on electronic seal. It seems that the introduction of such regulation is not justified. Organizational units with legal capacity have some qualities of legal persons and they are separate legal entities as the act grants them legal capacity. Consequently, if the EU legislator recognized the legitimacy of legal persons to use electronic seal, in the opinion of several authors in the literature on the subject such a possibility should be granted to the so called persons without corporate status that are subject to Article 33 item 1 of the Civil Code and are not referred to in the European legislation.

Adequate application of the provisions on legal persons to the so called persons without corporate status is the basis that enables organizational entities with legal capacity but without legal personality a full scope use of electronic seal as it is the case with legal persons[9]. The Minister of Economy had several reservations as regards the concept of electronic seal, including its name which – according to him – brought associations with notarial or official seals[10].

The electronic seal implementation and application rules of a particular entity should be regulated on the level of internal documents of the entity and the entityshould be represented first of all by electronic seal. Analogically, as it is the case with a traditional seal, which is not used to represent a legal person, electronic seal should serve mainly to confirm authenticity and to ensure data integrity and not to represent an entity[11].

The regulations should ensure long-term preservation of information so that legal validity of electronic signatures and seals is ensured by extended periods and their validation in guaranteed regardless of future technological changes.

Electronic seals can not only be used to authenticate a document issued by a legal person but also to authenticate any digital assets of a legal person such as software code or the servers of the image diagnostics device. Electronic seal should serve as a proof that a document was issued by a particular legal person, which gives certainty as to the origin and integrity of the document.

---

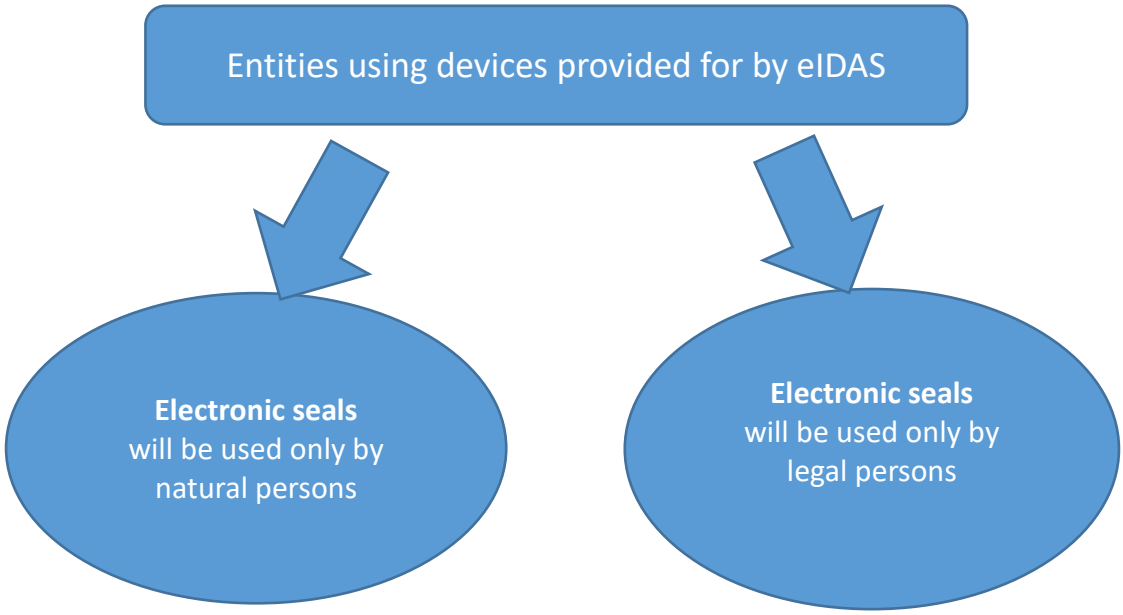
[9] Pejaś J., Szulga M.,Wagemann M., Stoliarowa-Myć A., Wiktorczyk P., *Wdrożenie rozporządzenia elDAS w Polsce – raport,* http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Główna-w.-4-2.pdf

[10] Reply of the Minister of Economy to the statement of Senator Ryszard Kronola on teh provisions of the act on electronic signature, Warsaw, 10 October 2013

[11] Ibid.

The eIDAS regulation provides for seals, advanced seals and qualified seals. It defines a certificate and a qualified certificate for electronic seal, a seal creation device and a qualified seal creation device.

Figure 1. Signatures and seals under eIDAS



Source: Authors' research

Pursuant to the eIDAS regulation qualified electronic seal should enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked[12].

Advanced electronic seal should meet the following requirements:

- it is uniquely linked to the creator of the seal;
- it is capable of identifying the creator of the seal;

[12] 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, Article 35, item 2

- it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
- it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

Electronic registered delivery service

It can be concluded from the definition of *trust service* that within the framework of this type of functionality, the following services can also be provided [13]:

- *creation of electronic registered delivery* perceived as the creation of proof resulting from the application of eIDAS services,
- *verification of electronic registered delivery* perceived as the verification of certificates that were used to create the proof for Electronic Delivery Service (EDS),
- *validation of electronic registered delivery* perceived as the validation of electronic evidence, i.e. such as the signature under EDS evidence, dates and times in such evidence, senders and addresses on the basis of the proof for EDS.

The eIDAS regulation includes also an explicit definition of *electronic registered delivery service* according to which it is 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[14].

The service in question will:

- transmit data,
- create evidence resulting from the use of the data (various proofs – not only the proofs of sending and receiving the data)\,
- create evidence of sending,
- create evidence of receiving and

[13] 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, Article 3, item 16

[14] 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, Article 3, item 36

- protect the transmitted data .

The evidence that is created in the course of the electronic registered delivery service includes:

- confirmation that the data was delivered for the service,
- confirmation that the information sender on the expected delivery was delivered to the addressee by the service,
- confirmation to the addressee that the data from the service was received,
- confirmation to the data sender that the delivery was received by the addressee, confirmation to the sender that the delivery was available at a given time and place to the addressee and could be received at a particular moment,
- confirmation to the sender about receiving (or the lack of receiving) of the delivery by the addressee at a particular time.

Other proofs that are required by business, administrative or court procedures may also be created (e.g. reports/attestations of certificate, signature or seal validation or verification, confirmations of reply before deadlines, evidence regarding the compliance of particular type of data with the requirements or "templates".

A minimum requirement for the above proofs should be the provided with electronic signature or seal of the electronic registered delivery service-provider as well as with non-repudiable information of the transmitted data, the dates of particular operations and the data that identify the senders and addressees.

The eIDAS regulation enumerates the requirements that are to be fulfilled by qualified electronic delivery services[15]:

- they are provided by one or more qualified trust service provider(s);
- they ensure with a high level of confidence the identification of the sender;
- they ensure the identification of the addressee before the receipt of the data;

[15] 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, Article 44, item 1

- 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;
- 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.

The above requirements will also certainly include a frequent – as practice shows – necessity to integrate with online payment systems or the payments that are carried out by services provided by telecommunication operators.

Electronic registered delivery service can already be used in the development of such solutions as:

- separate electronic inbox that serves a particular entity with a limited scope of defined documents that are sent to that entity; in this case separate proofs of receipt and sending are created,
- electronic inbox that serves several entities and numerous defined documents that are sent to these entities; in this case separate proofs of receipt and sending are created,
- electronic registered delivery service with a particular number of addressees and senders with the capacity to transfer both defined documents and any documents (e-mails, e-pictures; in this case multi-step chains of sending and receipt proofs are created,
- electronic registered delivery service with a particular number of addressees and senders with the capacity to transfer both defined documents and any other documents (e-mails, e-pictures) and with the capacity to use address lists of other electronic registered delivery service both in one or several countries; in this case multi-step chains of sending and receipt proofs are created,

Practically, in line with the doctrine of Polish law regarding delivery service, a citizen or an entity with a particular obligation that introduce documents directly to administration systems are adequately identified and authenticated. Besides, if such operations require particular templates or defined forms, the electronic registered delivery service provider should have the opportunity to use such templates or forms in the course of service provision.

In the course of administrative, tax, civil or criminal proceedings, a validation of electronic registered delivery services should be ensured to present evidence in a clear and generally comprehensible way.

After the eIDAS regulation comes into force, the sender of documents that uses a qualified delivery service (provided either by a national or other EU member-state provider) will have the capacity to introduce various kinds of data (e.g. letters, e-invoices) to any public administration mailbox that is publically accessible.

Moreover, the data that is introduced in this way should be dealt with on the basis of legal effects as defined in the eIDAS regulation[16]. Pursuant to the regulation data sent and received using an electronic registered delivery service cannot be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.

As in the case of electronic seal, data sent and received using a qualified electronic registered delivery service enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Currently, pursuant to the provisions on delivery rules in public administration and judicial system the delivery of an electronic document is carried out by services that are not provided by qualified service providers. Consequently, they are not provided as services complying with the eIDAS standards. Thus, they will not have a direct legal effect in other EU countries. Such legal effect will occur on the condition that the official confirmation of the receipt includes a qualified signature or a qualified seal.

The introduction of such tools as e-delivery, e-preservation and the creation, verification and validation of website authentication certificates requires new legal regulations.

[16] 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, Article 43

Website authentication services

Website authentication services[17] provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated.

The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, the regulation should lay down minimal security and liability obligations for the providers and their services.

The eIDAS regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognized as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded. (powyższe trzy akapity są dokładnie tekstem z pkt 67 Regulacji/preambuły)

The eIDAS regulation also defines the concept of *certificate for website authentication* as an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued. It also defines the requirements for qualified website authentication certificates[18].

The national legislation makes an attempt to define legal effects of website authentication by stating that a natural or legal person or an organizational entity without legal entity that is given legal capacity by the act to whom a website authentication certificate is issued are treated as the owners of the website to which an authentication certificate is issued that links the website to the person or the entity[19].

---

[17] Preamble, Article 67

[18] 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, Annex IV – Requirements for qualified certificates for website authentication

[19] Pejaś J., Szulga M.,Wagemann M., Stoliarowa-Myć A., Wiktorczyk P., *Wdrożenie rozporządzenia elDAS w Polsce – raport*, http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Główna-w.-4-2.pdf

Preservation services for electronic signatures, seals and certificates

This element of trust service aims at securing the nonrepudiation of the sender and the authenticity of the document that is signed by a qualified electronic signature at present and in the future. While a forgery of a paper document is fairly easy with the use of a thorough analysis of paper, seals, printing ink or handwriting, the verification of an electronic document may prove to be extremely difficult. This is why there is a necessity to preserve electronically signed documents, which in practice frequently comes to regular time stamping with the application of ever new cryptographic algorithms. Time stamps confirm that an electronic document existed in a given place and at a given moment, which makes it possible to secure it. The current Polish regulations require such stamping to be conducted every 10 years to consider the document trustworthy.

Pursuant to the eIDAS regulation a qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period[20]. The regulation states that its provisions "should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes" [21], and that "trust service means an electronic service normally provided for remuneration which consists of: (…) the preservation of electronic signatures, seals or certificates related to those services" [22].

It is worth noting that in the case of the preservation service for electronic signatures and seals a precise date of issue of implementing and delegated acts is not given. Moreover, the eIDAS regulation does not define the legal effects of the preservation service for the seal and electronic signature and, consequently differences between particular member-states may occur. Having analyzed the provisions in eIDAS on the preservation of qualified electronic signatures, seals and certificates, it can be concluded that they have one of the lowest precision

[20] 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, Article 34, item 1
[21] Preambule, Article 61
[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, Article 3, item 16

levels of legal regulations and such situation will certainly require further legislative and standardizing work.

Conclusion

At present, work on the adaptation of national legal regulations on authentication and authorization of documents to eIDAS standards is conducted in Poland within ARIADNA (Adaptation of Trust Profile to EU Requirements of the eIDAS Regualtion) and HELIOS (Integration of Public Registries with the application KSU – National Service Network) projects[23]. In the view of the experts, the first quarter of 2019 is the earliest possible time when a standard concerning trust service of qualified electronic signatures and seals will be developed.

A project *From Paper to Digital Poland* is under development and it ivolves several particular operations together with a schedule of their realization. It assumes a digitization of key public services, the growth in non-cash transactions and the implementation of the eID initiative.

Digitization may constitute the basis for a successful realization of the government's Responsible Development Plan. It is also consistent with the plan's particular development pillars and the potential of the digital sector is a prerequisite for the innovativeness and competitiveness of the Polish economy[24].

Bibliography

1. Marucha-Jaworska M., *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym.* Wydawnictwo Lex, Warszawa 2015

[23] Internet source: https://mac.gov.pl/aktualnosci/publiczna-prezentacja-zalozen-kolejnych-projektow-w-ramach-popc-21

[24] http://telewizjarepublika.pl/dowod-osobisty-aplikacja-na-smartfon-morawiecki-zapowiada-koniec-quotpapierowej-polskiquot,34815.html

2. Mielnicki T. Wołowski F., Grajek M., Popis P. Łuczak P., Tabor M., Brakoniecki M., *Identyfikacja i uwierzytelnienie w usługach elektronicznych*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013
3. Pejaś J., Szulga M.,Wagemann M., Stoliarowa-Myć A., Wiktorczyk P., *Wdrożenie rozporządzenia eIDAS w Polsce – raport*, http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Główna-w.-4-2.pdf
4. Draft act of 3 June 2016 on trust services, electronic identification:https://legislacja.rcl.gov.pl/projekt/12283556
5. Draft act of 3 June 2016 on trust services and electronic identification, Art. 4: https://legislacja.rcl.gov.pl/projekt/12283556
6. Draft act on trust services and electronic identification (3.06.2016)
7. Ordinance of the Minister of Health of 21 December 2006 on the types and scope of medical records in health care entities and methods of their processing (Journal of Laws 2006 No. 247, item 1819)
8. Ordinance of the Minister of Health of 21 December 2010 on the types and scope of medical records and methods of their processing (Journal of Laws 2010 No. 252, item 1697)
9. Ordinance of the Minister of Health of 9 November 2015 on the types and scope of medical records and methods of their processing. Dz.U. (Journal of Laws) 2006 No. 247, item 1819
10. 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
11. Position of The Polish Post (Poczta Polska) https://legislacja.rcl.gov.pl/docs//2/12283556/12343437/12343440/dokument216770.pdf
12. Act of 14 June 1960 Code of Administrative Procedure, (Journal of LAws No.30, item 168
13. Act of 17 February 2005 on computerization of entities performing public tasks (Journal of Laws 2005, No. 64 item 565)
14. Act of 18 September 2001 on electronic signature (Journal of Laws 2001, No. 130, item 1450
15. Act of 28 April 2011 on healthcare information system (Journal of Laws 2011, No. 113 item 657)
16. Act of 29 August 1997 – Tax Ordinance (Journal of Laws 1997, No. 137, item 926)
17. Act of 6 November 2008 on patient rights and the Patient Ombudsman (Journal of Laws 2009, No. 52, item 417)
18. Wróbel A., [in]: *Traktat o funkcjonowaniu Unii Europejskiej*. Komentarz. Volume III (ed.). D. Kornobis-Romanowska and J. Łacny, Warszawa 2012
19. Internet source: http://notariat.pl/wiadomosci-notariat/374-uwierzytelnianie-w-eidas-to-nie-jest-skladanie-podpisu-elektronicznego

Abstract

The article discusses the concept of open and closed trust services and their types. It presents the idea of the national trust infrastructure and the national center for trust services certification.

The eIDAS regulation , among other things, introduces changes in the existing services (e.g. in. the electronic signature) and such new services as electronic seal, authentication of websites and the preservation of electronic signatures, seals and certificates.