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

INTRODUCTION OF TRUST SERVICES PURSUANT TO EU eIDAS REGULATION WITH REGARD TO INFORMATION SYSTEMS IN HEALTHCARE (PART I)

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 require 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.

Trust services

At present work is underway on provisions that would facilitate the implementation of trust services[4]. As regards the principles of legal liability of trust service providers, the eIDAS regulation refers to the national law. The national law should ensure the introduction of new trust services to the law system Moreover, the conceptual framework that has been functioning in several legal regulations in Poland should be changed. Thus, new concepts should be added or eliminated. This also refers to institutions that are non-existent in the eIDAS regulation, e.g. a secure electronic signature (Figure 1).

Trust service means an electronic service normally provided for remuneration which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.[5]

Open and closed trust services

Trust services can be divided into:

- open trust services – i.e. set of trust services that are provided to the society and have an impact on third parties;
- Closed trust services – i.e. a set of trust services provided to a particular, well defined group of users and which have no impact on third parties. Their regulations do not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants. (see eIDAS Art.2 (2)

[4] Draft act of 3 June 2016 on trust services and electronic identification, Art. 4 :https://legislacja.rcl.gov.pl/projekt/12283556

[5] 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

The presented above division of services is significant as it facilitates the determination of a boundary between trust services that are subject to the supervision and requirements of the eIDAS regulation and the services that are not the subject to the above requirements (closed services)[6]. The division is of significance to the IT systems that are functioning in the healthcare system. That refers both to the schemes that operate on the national level and the schemes that are used in hospitals and outpatient care entities.

Services that are provided within the framework of hospital treatment are much cheaper than services that involve the application of procedures and standards required by law. A simple analysis does not always indicate which group of services is dealt with. Below examples are given of possible practical situations.

A commune provides trust services to the commune inhabitants with the use of certificates. The certificates are applied by the inhabitants to ensure the authentication of documents that are sent to the commune office. On the base of these documents the commune officials make decisions that may have an impact on third parties, e.g. inheritors who live out of the commune. Obviously, the inhabitants can be treated as a closed group, however the provision of trust services goes beyond the members of the group[7].

If a hospital issues certificates to its patients, the patients constitute an open group as they all can take advantage of the hospital's services. In this case, a group of patients is an open group since each patient can open an account in the hospital and apply the scheme while the results of their membership extend beyond this group (e.g. the results of an unlawful reception of data resulting from the application of a trust service may concern both the patients and the subjects from outside the group).

However, a scheme of hospital administration personnel that is used to manage internal documents generated and approved by various organization entities will be considered a closed scheme.

It could be implied from the proposals for the changes in the act on healthcare information system to be introduced in 2015 that qualified and unqualified certificates should be issued within the PKI infrastructure of the NFZ (National Security Fund). The certificate were

[6] Position of The Polish Post (Poczta Polska)
https://legislacja.rcl.gov.pl/docs//2/12283556/12343437/12343440/dokument216770.pdf
[7] 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

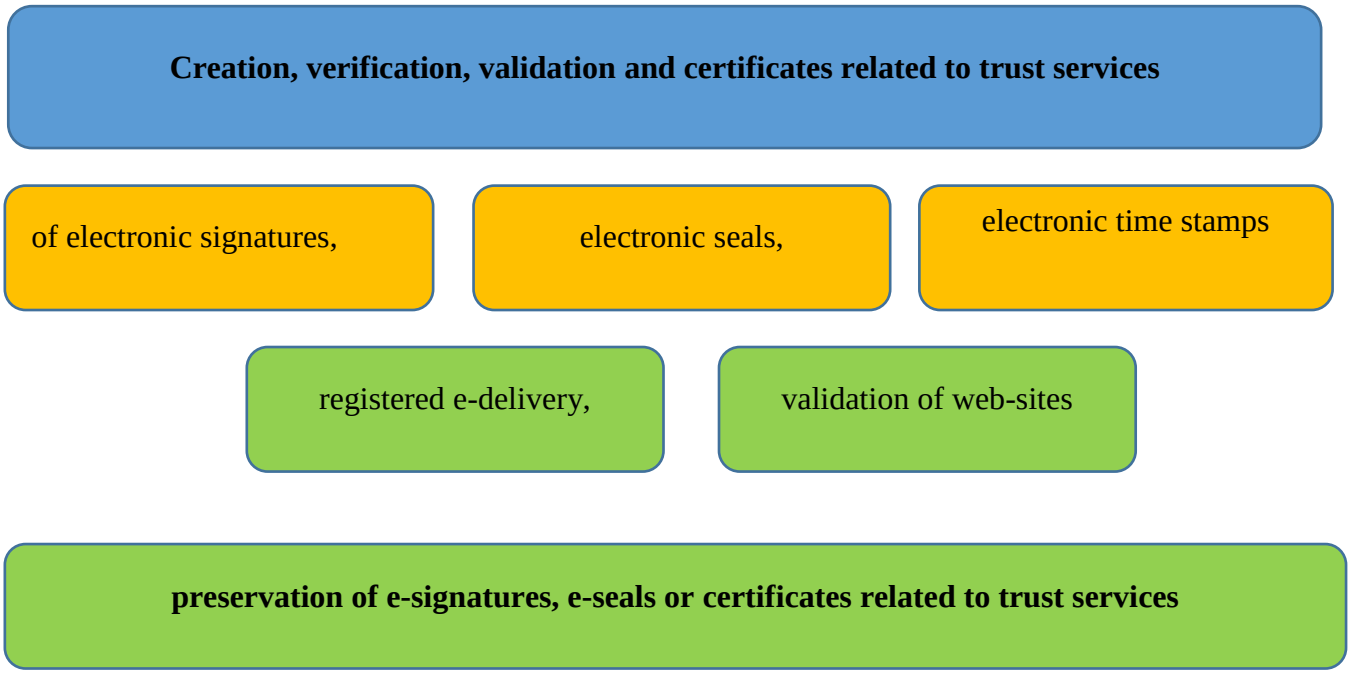
supposed to be installed in the eKUZ (EHIC) card, the KSM (Medical Specialist Card, and the KSA (Administrative Specialist Card). Thus, can one assume that the qualified trust services provided by the PKI of the NFZ are closed services? The analysis of the problem leads to the conclusion that such services belong to open services and, consequently, they are subject to the requirements given in the eIDAS regulation. Moreover, it should be assumed that these services should be provided through companies that will operate on commercial basis (this principle should also apply to unqualified services in the cases when the PKI of the NFZ does not provide them only for its own needs)[8].

The regulation introduces a general legal framework for the application of trust services. Their catalogue is also provided by the draft act. Member-states are free to define other types of trust services with the exception of the ones that are enumerated in the closed list of trust services. The member-states can leave or introduce national provisions on trust services that are in compliance to EU law as long as the services are not fully harmonized by a regulation (a draft act prepared in Poland). Trust services that meet the requirements of the regulation should be subject to free trade on the internal market. No technological solutions were imposed with regard to the introduced trust services. However, legal effects were defined that should be achieved by means of any technical solutions if the requirements of the eIDAS regulations are met.

Some of the above mentioned trust services have been regulated in Poland for several years, e.g. the electronic signature or time stamps. However, the new regulations introduce changes also to the services that were known before, and the changes are substantial. They mainly concern the electronic signature, time-stamping services and other services . At present, a new act is being developed with the aim to introduce institutions that are regulated in the eIDAS regulation to the Polish legal system. That refers both to the services that are known and regulated in Poland and the unknown ones, such as e-delivery, e-preservation, which will require a separate act.

[8] Ibid.

Figure 1. New regulations regarding trust services introduced by eIDAS



Source: Authors' research

Undoubtedly, both open and closed trust services will be widely used in the area of healthcare.

The draft regulation[9] defines the supervision over trust service providers. The supervision may be conducted by the minister competent for digitization and – with reference to the qualified trust service providers – the implementation includes:

- granting the permission for trust service providers to provide qualified trust services through the assignment of the status of a qualified trust service provider and the status of qualified trust services to the services provided by this provider;
- a verification whether the qualified trust services providers fulfil the requirements laid down in eIDAS[10]; the withdrawal of the status of a qualified trust service provider and the status of qualified trust services to the services provided by this provider;
- a demand to revoke immediately qualified certificates by a qualified trust service provider;

[9] Draft act of 3 June 2016 on trust services and electronic identification, Art. 4 :https://legislacja.rcl.gov.pl/projekt/12283556

[10] W sposób określony w art. 20 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

- a verification of service provision policies conformity to trust service regulations;
- the imposition of penalties as provided for by the act;
- a cooperation with other supervisory bodies at home and abroad and with the European Network and Information Security Agency.

The supervisory body may undertake measures against an unqualified trust service provider when the unqualified trust service provider does not fulfil the eIDAS requirements – particularly in the cases of security risk or the risk of integrity loss of the service provided and the interest of trust service recipients is put to danger.

The national trust infrastructure

The supervisory body provides for the functioning of the national trust infrastructure that consists of:

- trusted list – which contains information on the qualified trust service providers
- national center for trust service certification – creation and issue of certificates to qualified trust service providers which are used to verify advanced e-signatures or e-seals; publication of data used to verify e-signatures and e-seals; publication of a list of revoked certificates
- registry of trust service providers.

In order to ensure a comparable security level of qualified trust services, all member-states should comply with common basic supervisory requirements. All member-states should accept comparable procedures and share the information on their supervisory measures and best practices in the area of security. All trust service providers should be subject to the regulation requirements, particularly to the requirements regarding security and liability so that due diligence, transparency and accountability of their operations and services are ensured. However, considering the kind of services provided by trust service providers, a distinction should be made as regards the requirements between qualified and unqualified service providers.

The establishment of a supervisory system for all trust service providers should result in equal security and accountability principles of their operations and services and, consequently, lead to the protection of the users and better functioning of the internal market.

Unqualified trust service providers should be subject to lenient and reactive ex post supervisory measures that are justified by the character of their services and operations. Thus, the supervisory body should not have a general obligation to supervise unqualified trust service providers. It should take measures only after being informed (e.g. by an unqualified trust service provider, another supervisory body, a user or business partner or as a result of its own investigation) that an unqualified trust service providers does not fulfil the requirements of the regulation.

In order to facilitate an efficient initiation process that should lead to the inclusion of qualified trust service providers and the trust services that they provide into trusted lists, preliminary interactions between potential qualified trust service providers and the competent supervising body should be encouraged . That should ensure the due diligence in the provision of qualified trust services. Trusted lists are an essential factor in the trust-building process among market operators as they indicate the qualified status of the service provider at the time of supervision.

Confidence in and convenience of online services are essential for users to fully benefit from e-services and rely on them. Thus, a EU trust mark should be developed to label qualified trust services that are provided by qualified trust service providers. Such a European mark would make it possible to differentiate qualified trust services from other trust services, which would result in the transparency of the market. The use of the EU sign by qualified trust service providers should be optional and should not result in any other requirements than the one provided by the regulation.

Electronic signature service

Currently, the literature on the subject differentiates eight types of e-signatures with regard to the technique and/or technology of the creation: keyboard signature, e-mail signature, manual signature, handwritten biometric manual signature, password signature, mobile signature, cryptographic signature and biometric signature. Keyboard signature consists in entering the first and the second name under a document with the use of a computer keyboard with the possibility of editing in any program. E-mail signature is considered to be the same kind of signature and, similarly, the scan of a digitized handwritten signature is treated as a

keyboard signature. A signature made by a digital pen that transfers specific spatial movements of the user's hand to computer memory results in the creation of a manual signature. Handwritten biometric signature belongs to the same category. A password signature is used when a non-reusable password is taken from a token or a scratch card and an identifier is applied to log into an IT system. Instead of a password from a token or a scratch card, a PIN can be used together with the number of the electronic card[11].

A separate category is defined by legal consequences of particular types of e-signatures. An e-signature with the most powerful legal effects (comparable to a written signature) is the secure e-signature that is verified by a valid qualified certificate. On the other hand, some types of e-signature do not involve any legal effects and the documents that are signed with them do not fulfil the conditions for a declaration of intention as there are no objective possibilities to identify precisely and unambiguously the person who signed the document i.e. submitted the declaration. A good example is the case when a document is send electronically by e-mail or SMS and the recipient is not able to verify the sender's authenticity.

Electronic signature is a concept that has been known in the Polish health care system for years[12]. The signature was used - although not very commonly - in the health care. This resulted from legal regulations that in some cases – especially in digitized medical documents – imposed the obligation to use e-signature in its qualified version, i.e. the secure signature that was verified by a qualified or unqualified certificate. However the trends in the regulations changed. The older ones pointed at particular steps of the creation of medical records and required particular types of signature. For example, although the type of e-signature was not specified for the development of medical records, s secure signature verified by a qualified certificate was required when the records were to be shared.[13]

IN the more recent regulations on medical records[14] the decision on the type of signature to be used is left to the head of a unit responsible for running medical records.

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

[12] Act of 18 September 2001 on electronic signature (Journal of Laws 2001, No. 130, item 1450)

[13] 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)

[14] 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)

Signing and authentication of documents

The differentiation of the notions *signing* and *authentication* is a positive change. Documents (applications) are simply signed and not authenticated. The quotation below explains the concepts of signing and authentication. *The document that I sign with an advanced electronic signature includes data that will make it possible to confirm its origin (authenticity) in the future and to confirm its integrity. However, as the objective is to deliver it to another person as the evidence in some proceedings, the integrity test of the signed document as well as the check of its origin will be the task of the person who is to undertake legal proceedings on the basis of the document in question, in other words is to trust the document. The process in which the document has to be entrusted by a relying party is the authentication which consists of the certificate verification, signature validation, the identification of the person who signed on the basis of the certificate and the integrity verification. The authentication is a process that is undertaken by the relying party itself or with the help of external services, i.e. verification, validation. E-signature, however, is the tool that enables a relying party to conduct this process as it provides the data that confirm the origin and help recognize changes in the signed data*[15].

A similar change concerns signing documents that grant the power of attorney. It was also indicated that this is the case of signing and not of authentication. However, this concept was left as regards the authentication of a document issued by a third party.[16] "Authentication" means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed[17].

Recently, new regulations on medical records[18] were introduced as well as the changes in the provisions on the healthcare information system. The act on healthcare information system imposed the obligation[19] on medical workers to apply a secure e-signature that is verified by a valid qualified certificate[20] or a signature confirmed by the ePUAP trusted profile[21] in order to sign:

- elektronicznej dokumentacji medycznej;

[15]M.Tabor; Uwierzytelnienie eIDAS to nie jest składanie podpisu elektronicznego http://notariat.pl/wiadomosci-notariat/374-uwierzytelnianie-w-eidas-to-nie-jest-skladanie-podpisu-elektronicznego
[16] Code of Administrative Procedure, Art. 33 (3a) and Art. 220; Tax Ordinance, Article. 138a (5) and Article 306d (3)
[17] 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 (5)
[18] Ordinance of the Minister of Health of 9 November 2015 on the types and scope of medical records and methods of their processing. (Journal of Laws) 2006 No. 247, item 1819
[19] Act of 28 April 2011 on healthcare information system (Journal of Laws 2011, No. 113 item 657)
[20] Within the meaning of the Act of 18 September 2001 electronic signature
[21] Within the meaning of the Act of 17 February 2005 on computerization of entities performing public tasks

- medical records;
- applications for the access to data that enable the download from the SIM of electronic medical records or the data from these records in the scope necessary to perform diagnostics, to ensure treatment continuity and to provide service providers with medicinal products, foodstuffs for particular nutritional uses and medical products;
- applications for the access to data processed in SIM that enable sharing the data in electronic medical records between service providers.

The above is in contrast to the provisions of the new regulation on the creation principles of electronic medical records. The provisions provide that in the creation of electronic medical records electronic signature is used that is verified with the application of internal mechanisms of the IT system. It seems that such solution is closer to the concept of eIDAS and the implementing provision regarding the act on patient rights[22], which includes basic regulations on medical records.

E-signature does not exist without an electronic document, which is the result of the technology of its creation. Consequently, the definition of an electronic document is extremely important. The eIDAS regulation defines electronic document as any content stored in electronic form, in particular text or sound, visual or audiovisual recording[23]. Thus, as regards healthcare, sound documents and images from medical imaging will be treated as documents. There is no requirement to record a document on a data carrier so there are obstacles as regards storing medical documents in the cloud.

An electronic document cannot be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form[24].

[22] Act of 6 November 2008 on patient rights and the Patient Ombudsman (Journal of LAws, 2009, No. 52 item 417, chapter 7)
[23] 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 (35)
[24] 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 46

Changes in e-signature introduced by eIDAS

A new definition of e-signature was introduced - '*electronic signature' means data in electronic form which are attached to or logically associated with other data in electronic form and which are used by the signatory to sign.*

The regulation provides for the introduction of e-signature, advanced e-signature and qualified e-signature.

They will replace the existing electronic signature, secure electronic signature and the secure electronic signature verified by a qualified certificate[25]. The changes in meaning make it necessary to amend provisions on "secure electronic signature verified by a valid qualified certificate", which results in the use of the equivalent notion of "qualified electronic signature". In the draft act the term "secure electronic signature" is replaced by "qualified electronic signature" as the closest – although not equal - in meaning. This term refers to an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures[26].

The advanced electronic signature under eIDAS does not have to be created by the so called secure electronic signature creation devices. The following requirements for advanced electronic signature were defined:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

[25] Draft act on trust services and electronic identification (3.06.2016), Article 134
[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, Article 3 (12)

Another kind of e-signature is the e-signature confirmed by the ePUAP trusted profile. According to the definition, e-signature confirmed by the ePUAP trusted profile is a signature created by a user of the ePUAP[27] account to which identifying data are attached that are included in the ePUAP trusted profile. Moreover, the signature:

- points unambiguously at the ePUAP trusted profile of the signatory,
- includes the information when the signature was created,
- identifies unambiguously the ePUAP account of the person who created the signature,
- is authorized by the ePUAP account user,
- bears and is protected by the electronic seal that is used by ePUAP to ensure the integrity and authenticity of the ePUAP operation.

Legal effects of data in an electronic form with e-signature that is confirmed by the ePUAP trusted profile are equivalent to the ones of a document with a handwritten signature unless separate provisions state otherwise. The validity and effectiveness of an e-signature that is confirmed by the ePUAP trusted profile cannot be denied on the grounds that it is in an electronic form or that changes were made other than the ones that confirm the trusted profile[28]. The signature that is confirmed by the ePUAP trusted profile is not an advanced electronic signature[29].

What is more, when adjusting the provisions to the eIDAS regulation in order to ensure the integrity and authenticity of operations by ePUAP and to attach an e-signature confirmed by the ePUAP trusted profile, it was indicated that an electronic seal defined in ePUAP should be used instead of "the ePUAP signature"

At present the EU member-states apply various formats of advanced e-signatures to sign electronic documents. The member-states should ensure technical possibilities to use at least a few formats of advanced e-signatures when receiving electronically signed documents. This requirement is referred to as the non-discrimination rule for qualified services. Consequently, a

[27] Act of 17 February 2005 on computerization of entities performing public tasks Article 3 (15) (Journal of Laws 2014, item 1114)

[28] Act of 17 February 2005 on computerization of entities performing public tasks Article 20b (Journal of Laws 2014, item 1114)

[29] Justification of the draft act on trust services and electronic identification

qualified electronic signature based on a qualified certificate issued in one member state is recognized as a qualified electronic signature in all other member-states. [30].

A similar approach was taken as regards electronic seal[31]. A qualified electronic seal based on a qualified certificate issued in one member state is recognized as a qualified electronic seal in all other member-states.

Creation of remote electronic signatures

The creation of a remote electronic signature is becoming increasingly more common. In such cases, the environment of e-signature is managed by the service provider on behalf of the signatory. The service providers of remote e-signature should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. In the case of a qualified electronic signature created by a remote e-signature creation device, the requirements applicable to qualified trust service providers set out in the eIDAS regulation should apply. The signatory should have access to qualified electronic signature creation devices to have sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.

The rule is accepted that electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. It is for national law to define the legal effect of electronic signatures so that a qualified electronic signature should have the equivalent legal effect of a handwritten signature.

[30] 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 25 (3)
[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, Article 35 (3)

Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.

Chyba wypadałoby dac odnośnik,bo powyższy akapit jest żywcem wzięty z **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 punkt 54 (reszta podrozdziału dotycząca podpisu na odległość też w większości odnosi się do tego dokumentu a nie ma odnośnika, moim skromnym zdaniem)**

IT security certification, including electronic signature creation device, is based on international standards such as ISO 15408

IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is ongoing. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to the standards for IT security certification insofar as their security levels are equivalent. Those processes could be facilitated by a peer review. (a to w całości punkt 55 Regulacji)

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.

The article is continued in the second part where the whole bibliography is presented.