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

IDENTIFICATION AND AUTHENTICATION IN THE HEALTH CARE INFORMATION SYSTEM AFTER THE INTRODUCTION OF THE EU eIDAS REGULATION

1. Introduction

The digitization of the health care system is again in its starting point. It is unknown whether the scheme that was planned in the form regulated by the act will start functioning. As a result, it should be reconsidered whether the solutions that were developed several years ago should be implemented or perhaps current technological solutions make it possible to change, simplify and deformalize the scheme. Undoubtedly, the scheme that was based on the acquisition of information and data from patients, service providers and pharmacies had a basic drawback that made it impossible to start operating. The shortcoming resulted from the fact that there were no tools to identify the subjects (both service providers and the patients) in the e-signing scheme,

to share the documents or to authenticate the transactions and websites. None of the concepts concerning feasible solutions were finally implemented. That concerns the plans to implement ID cards with electronic chips, the medical specialist card (KSM), the administrative specialist card (KSA) or the patient card (eKUZ) [1].

At present the future of the ePUAP[2] (electronic Public Administration Service Platform) and the related signature that is confirmed by a trust profile is uncertain. In July 2016, the Act on electronic signature[3] expired just as the electronic signature that was regulated by the provisions of the Act and the so called secure e-signature that was used in the health care system and verified by means of a valid qualified certificate. (The secure e-signature had been recommended for many years and finally became obligatory in electronic medical record keeping)

It should be pointed out that the issue of identification and authentication is dealt with in the Directive 2011/24/EU of the European Parliament and the Council of Europe. It provides for the development of a network of national entities responsible for e-health care. In order to increase the security and continuity of cross-border healthcare, the network should develop the guidelines concerning the cross-border access to data and e-health services also by supporting *common identification and authentication means to facilitate transferability of data in cross-border healthcare.* The assurance of mutual recognition of e-identification and authentication is indispensable to introduce cross-border healthcare for EU citizens. When the citizens leave the country to start treatment, their medical data have to be available in the country where the treatment is conducted.

---

[1] Pursuant to Item 3, Paragraph 1 of the Ordinance of the Minister of Health of 25 March 2014 on the appointment of a team to implement eKUZ and KSM cards, the responsibilities of the team include: 1) the development of solutions as regards the functioning of the electronic eKUZ card and 2) KSM card and 3) the infrastructure of the National Health Fund (Public Key Infrastructure) and the service providers –secure readers that enable e-signing with the application of eKUZ and KSM (Official Journal of the Ministry of Law, No.2014.50,: 2014-03-26

- The draft act on the amendment of 30 April 2015 of the Act on the information system in health care of 28 April 2011 provided for 3 types of electronic cards and the related IT system:
1) health insurance card (KUZ)
2) medical specialist card (KSM),
3) administrative specialist card (KSA).

[2] See the statements of A.Streżyńska, the Minister of Digitization after subsequent breakdowns of the website http://www.dobreprogramy.pl/Po-kolejnej-awarii-ePUAP-moze-jednak-czas-zaorac-eadministracyjny-niewypal,News,72952.html

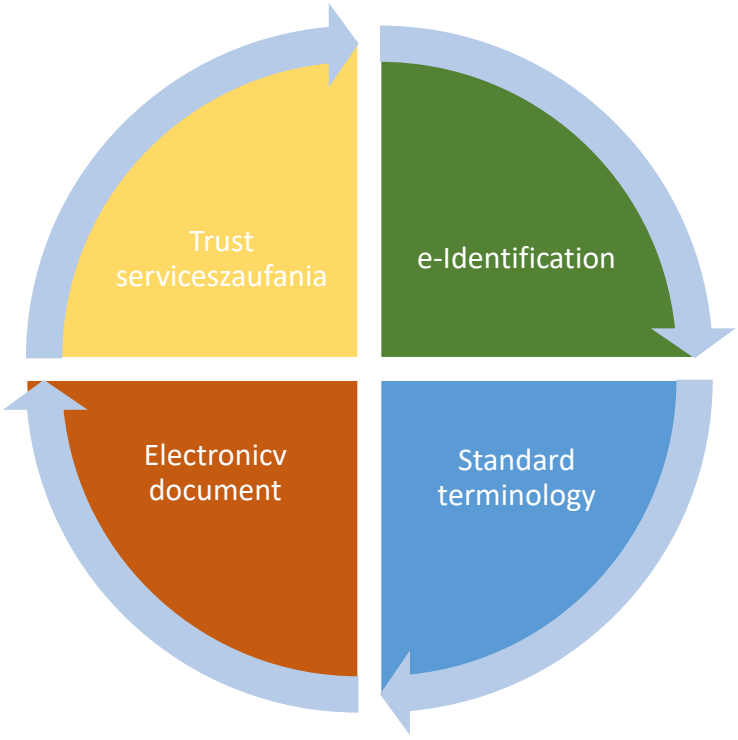
[3] It will be repealed by Art. 125 of the Act on Trust Services and Electronic Identification.

Consequently, a trustworthy, secure and credible framework of electronic identification is required.

Thus, one should find the answer to the question about the nearest future of the instruments for the identification and authentication of signatures and electronic seals as well as of other trust services necessary for running and processing medical e-documents, IT system management in the healthcare system and other services that apply IT systems and telecommunication networks, including the telemedicine services.

This year, the European Parliament and Council of Europe Regulation on electronic identification and trust services for electronic transactions in the internal market No 910/2014 (later referred to as eIDAS) will enter into force (EU Official Journal, 28 August, 2014)[4]. This legal act will apply directly in EU and will not require the implementation of the national law (fig.1). Consequently, an act is being prepared on trust services, electronic identification and the amendment of certain acts.[5]

The aim of the article is to present the implications of the above regulations in the practical functioning of the healthcare system.**Figure 1. elDAS areas of regulation**



Source: Author' research

[4] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910
[5] https://legislacja.rcl.gov.pl/projekt/12283556, Draft act on trust services, electronic identification and the amendment of certain acts

e-Identification in healthcare in the light the elDAS Regulation and draft national provisions.

In line with the definition included in the Polish Standard[6], the identification is the process of automatic recognition of a particular user in the system due to the application of unique names.

At present, there is a constant need in the healthcare to identify both the patient and the person that provides the service. In the case of the patient, the verification of identity and eligibility are conducted by the identity card and through the EWUŚ (Electronic Verification of Rights of Beneficiaries) system which is done in the course of the patient's visit. The patient can also check in registries – among other things – the qualifications of the doctor[7] or the diagnostician[8] before or after the visit. Moreover, if the patient cannot do it, he or she can obtain the necessary information at the head of the entity that provides the service. The heads of healthcare institutions are obliged to check the qualifications of their employees and the patient can expect a qualified service provider[9].

Numerous services in the public service are conducted online. This also refers to the healthcare sector and such services – to a varying extent – are provided in several EU countries. The aim of the electronic identification for online services is to facilitate the holder of an electronic identification device that is issued in one country to use public online services in other member states. Numerous online services do not require the electronic signature; it is enough that a natural person presenting particular data that enable an explicit identification is well and without any doubt recognized by an IT system. Then such an individual – as a user authenticated by the system - can use several services that are provided within this system without the necessity to sign electronic document[10].

---

[6] PN-I-020003.1.031
[7] Act of 2 December 2009 on medical chambers, Article 50, paragraph 1 (Journal of Laws 2009, No.219, item 1708
[8] Laboratory Diagnostics Act of 27 July 2001 (Journal of Laws 2014, item 174)
[9] Act of 15 April 2011 on medical activity, Article 108, paragraph 2 (3) (Journal of Laws 2011, No.112, item 654)
[10] Justification of the draft act on trust services, electronic identification and the amendment of certain acts

In online healthcare services a correct identification of the subjects involved is actually the condition for their provision, e.g. in the case of the teleconsultation services. The patient must be convinced that the service is provided by an authorized person, a person who is not deprived of the right to practice the profession (the system should also recognize the status after the court sentence but before it becomes final and legally valid) and whether the authorized person is not using a stolen identity.

The identification of service providers that are not natural persons is also important. An identifier confirms whether the service provider provides services within the scope defined in an appropriate register and – consequently - is entitled to provide a particular healthcare service.

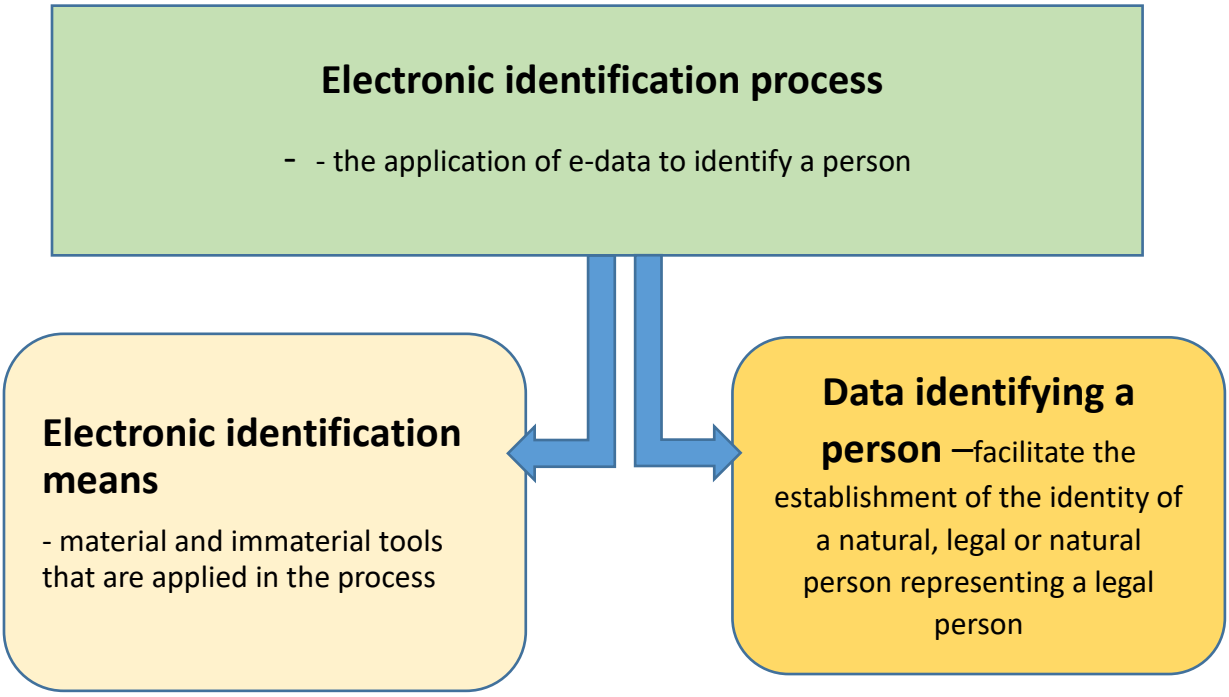
Moreover, a correct identification makes it possible for the patient to have online access, make appointments or verify particular information in registers, e.g. the information whether the services provider is registered and – as a result – can offer particular services.

Electronic identificaton (eID)

According to eIDAS, electronic identification (eID) is the process where electronic data are applied that uniquely identify a natural, legal or a natural person representing a legal person[11]. This definition is expanded by the definition accepted for the needs of the STORK project[12]. Identification is the process of obtaining data from a declared identity (party) without the verification of the information[13].

[11] eIDAS Regulation, Art. 3 item 1
[12] Within the framework of the STORK project, general assumptions of electronic identity were developed: https://www.eid-stork.eu/index.php?optio
[13] STORK - D2.3 - *Quality authenticator scheme*

Figure 2. Elements of the electronic identification process under the eLDAS Regulation



Source: Authors' research

The process of identification includes the subject's declaration of identity. In order to facilitate the identification, material tools are issued: e.g. state-issued identity cards or company identification cards (Fig.2). At present, the old-fashioned ID cards or identification cards are replaced by the ones that enable an electronic identification.

The term *Electronic identification means* refers to a material and/or immaterial unit containing person identification data and which is used for authentication for an online service[14]. In other words, the means implemented in the identification process may be material (e.g. KUZ card) or immaterial (e.g. appropriate software in a smartphone or the electronic layer in an identification card). Identification means identify uniquely both a natural and legal person and constitutes the user's electronic identity. Thus, the identification itself makes it possible to state "what person is concerned" but it does not confirm whether the user of a particular e-service is in fact the person that was declared and identified. The confirmation is conducted by authentication which consists in presenting the evidence that the user is the identified person (and not a person who is

[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 (2).

pretending to be him/her) [15]. The regulation defines authentication as an electronic process that enables electronic identification of a natural or legal person, or the origin and integrity of electronic data to be confirmed[16].

According to the amendment to the Act of 17 February 2005 on the computerization of activities of entities performing public tasks[17], the authentication of the users of an IT system who use online services provided by entities performing tasks requires:

- the use of a notified means of electronic identification, adequately to the security level that is required for services provided within the systems or
- the ePUAP trust profile or
- the data that are verified by a qualified certificate of electronic signature.

All operations that involve the development of an electronic system of identification (used also in the healthcare system) should comply with the applicable legal provisions in a particular country. According to the authors, apart from the development and implementation of the identification means, all legally regulated services that can be provided online should be set in order and their list should be made available to all interested parties. That is due to the fact that the access to the services and their provision to the applicant must be done under the conditions that are provided by the provisions of a given country. Thus, for example, telemedical services can be provided in some EU countries in line with national regulations of particular countries (e.g. Norway[18])

Security and cross-borderism of eID

The assurance of the eID scheme security is a necessary condition when developing identifiers to be applied in processing medical data (the so called sensitive data) that will

[15] Mielnici 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

[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 3, item 5.

[17] Act of 17 February 2005 on the computerization of activities of entities performing public tasks (Journal of Laws 2005, No.64 item 565. The amendment is included in Article 95 on trust services and electronic identification, draf Act of 3 June amends Art. 20 a

[18] Zanaboni P., Knarvik U., Wootton R., *Adoption of routine telemedicine in Norway: the current Picture*, Glob Health Action 2014, **7:** 22801 - http://dx.doi.org/10.3402/gha.v7.22801

be included (among other places) in the electronic layer of the Health Insurance Card (KUZ); as system changes in the healthcare system are expected, the name of the identifier and its application are going to be changed.

At present, there is a necessity to develop a healthcare identification scheme that would also include identifiers which are notified in other EU countries and the possibility to apply identification tools for using healthcare information systems of these countries.

The objective of the proposed eID scheme is to ensure security to its users – particularly when it is used to process health data. The electronic identification scheme on the national level – including the level of the national healthcare system – should ensure the security of the identification subject. Thus, it should take into consideration:

- a correct verification of the declared identity,
- correctness verification of the assignment of a particular person and his/her identity to appropriate eligibilities resulting from the document possessed,
- legal and economic relations related to the use of documents that confirm identity or particular eligibility,
- the protection of citizens against the theft of identity.[19]

The issues of electronic identification are dealt with by chapter II of the eIDAS Regulation. Among other things, the regulations concern:

- mutual recognition and acceptance of electronic identification means;
- notification conditions of electronic identification schemes and the assurance of technical interoperability of the electronic identification schemes;
- security levels of the schemes;
- security breaches of the schemes;
- liability of the notifying member-state;
- cooperation of the member-states and the assurance of the interoperability framework.

One of the objectives of eIDAS is to remove – as regards public services – the existing barriers in the cross-border application of electronic identification means that

[19] Lewandowski R., *Elektroniczna karta ubepieczenia zdrowotnego - słabe i mocne strony projektowanego rozwiązania.* http://ww1.pwpw.pl/kwartalnik_archiwum.html?id=48&magCid=249

are used for authentication in member-states. A principle was accepted that there would be no interfering with electronic identity management systems and the related infrastructure located in member states. Freedom was left to apply or introduce means of access to online services for the sake of electronic identification and to make decisions whether private sector should be involved in providing such means. Nevertheless, in contrast to public trust services, the development and the service of electronic identification schemes was entrusted to the bodies of member states.

It is generally assumed that it is the state and not commercial companies that is considered to be a trustworthy entity to guarantee the correctness of – for example – certificates, the more so as it possesses a reliable and complete register of citizens[20]. A system of identity management should be based on digital certificates that are guaranteed by the state and – for example –included in new identity documents. Not all countries accepted this option. In some of them, the citizens are equipped with electronic IDs or other documents that enable identification only in the communication with state institutions; however this does not always work in all cases. Not everywhere do the new documents include biometric data and the digital signature is optional in most cases. Documents with biometric data (face/fingerprints) are used, for example, in Germany, the Netherlands and Spain. Documents that make it possible to apply biometric data in healthcare systems are used for example in Austria, Belgium and Portugal. In Estonia and Italy, cards facilitate the submission of electronic signature[21].

After a successful implementation of bank systems in the *Family 500+* project, it is possible that Poland will use bank systems[22] as they have been used and accepted for years by the citizens. In Estonia, the logging to the www.esti.ee website – the equivalent of the Polish ePUAP- is conducted either by means of an electronic ID or by a bank system. The user logs in in the same way as to the bank but the confidentiality is maintained, i.e. neither the bank nor the institution have the access to each other's data. A similar solution is being introduced in Denmark. This is due to an insignificant interest in the service based on trust profile: after many years of its operation only 20% of the

[20] Papińska-Kacperek J., *Usługi cyfrowe. Perspektywy wdrożenia i akceptacji cyfrowych usług administracji publicznej w Polsce*. Wydawnictwo Uniwersytetu Łódzkiego, 2013
[21] Ibid.

[22] 95% of applications were completed with the use of the „Rodzina 500+" systems of a dozen of banks; online applications were submitted mainly through banks, See the most common mistakes: http://www.polskieradio.pl/42/273/Artykul/1603800,Rodzina-500-wnioski-online-skladane-glownie-przez-banki-Zobacz-najczestsze-bledy.

citizens used it. Thus, the Danish government together with banks developed a central system of identification (NemID). The use of bank system is being implemented also in Canada and the United States. The *Canada's Cyber Authentication Renewal* applies authentication solutions that have been implemented by banks, credit card issuers, state institutions and bodies that provide healthcare services. The *Secure Key* authentication services facilitate the access to government services with the application of data necessary to log in to bank services or – with the banks permission – with the use of a microchip bank card. The *Secure- Key Credential Broker Service* (CBS) was implemented in the US in 2012. Perhaps such authentication method will be also used in our country.[23]

Identity management scheme

Recently, organizational and technical conditions have been regulated that should be complied with by a communication and information system that is used to authenticate users.[24] Features of identity management were defined and determined as well as the indispensable procedures that have to be performed when managing a scheme.

Identity management scheme is a communication and information system that processes the identity data of its users and is used by public bodies to authenticate the users by means other than certificates.

Identity management scheme:

- registers the users;
- confirms the identity of the users;
- stores and shares the identification data of users with eligible authentication systems;
- enables blocking user's account on his/her demand;
- provides accountability;
- ensures the integrity, authenticity and confidentiality of data that identify and authenticate the user;

[23] Papińska-Kacperek J., *Usługi cyfrowe. Perspektywy wdrożenia i akceptacji cyfrowych usług administracji publicznej w Polsce*. Wydawnictwo Uniwersytetu Łódzkiego, 2013

[24] Draft Ordinance of the Minister of Digitization on detailed organizational and technical conditions to be met by a IT user authentication scheme
https://legislacja.rcl.gov.pl/docs//522/12286305/12357434/12357435/dokument225309.pdf

- ensures the synchronization of the scheme time with the UTC (PL) time scale on a daily basis.

The administration of the identity management scheme involves the following :

- the assurance of the credibility of the user registration and identity authentication;
- the storage of data concerning the identity of the users for 20 years since 1 January of the next year after performing the latest operation with the application of identity;
- continual update of the scheme operational and technical documents, which guarantees its secure operation;
- the development and implementation of information security management policy.

The entities that decide to develop and implement the information security management policy in line with the security conditions that are defined by the Polish Standard meet the above requirements[25].

Authentication and certification scheme

Moreover, the authentication scheme was defined as an IT system that is used by a public entity and takes advantage of the certification or identity management systems to authenticate the user[26].

When identifying the user, the authentication scheme verifies the identity and stores the data that confirm the verification.

The data that confirm the verification should clearly make it possible to:

- identify the identification of the individual who performed an electronic operation;
- confirm the validity of the eligibility at the moment of the operation;

[25] PN ISO/IEC 27001:2007 or a more recent one, verified positively by an accredited certifying entity in line with the Act of 13 April 2016 on conformity assessment systems and market surveillance (Journal of Laws, 2016, item 542).

[26] Draft Ordinance of the Minister of Digitization on detailed organizational and technical conditions to be met by an IT user authentication system, Paragraph 2, item 3 - https://legislacja.rcl.gov.pl/docs//522/12286305/12357434/12357435/dokument225309.pdf

- determine the moment when the operation was performed.

A certification scheme[27] was defined as an IT system that is used to issue certificates applied by public entities for user authentication. Moreover, its qualities were determined. Thus, a certification system:

- provides the services of an immediate annulment of a certificate;
- determines precisely the time of the certificate issue and annulment;
- confirms the identity of a person for whom the certificate is issued;
- meets the safety requirements of teleinformation security as defined by risk analysis;
- does not store nor copy the data that are used by the users to be identified by certificates.

The administration of the certification scheme involves the following operations:

- regular reviews of the efficiency of security measures as regards teleinformation security with the aim to introduce improvements;
- regular updates of the operational and technical documentation to ensure its safe operation;
- the assurance of organizational, technical and cryptographic security of the system operations;
- prevention against the falsification of certificates, including the assurance of confidentiality when generating data necessary to confirm the identity;
- the storage of information on the issued certificates for 20 years since 1 January of the next year after the issue;
- informing individuals who apply for certificates about the use conditions, particularly about the restrictions concerning their use and the procedures in case of complaints and disputes.

The above requirements can be met on the condition that an adequate certification policy[28] is implemented, appropriate organizational and technical conditions[29] are ensured and systems and products are used that comply with the standards.[30]

[27] Draft Ordinance of the Minister of Digitization on detailed organizational and technical conditions to be met by an IT user authentication system, Paragraph 2, item 1 – https://legislacja.rcl.gov.pl/docs//522/12286305/12357434/12357435/dokument225309.pdf

[28] In line with the requirements of the standard ETSI TS 102 042 , version 1.2.4. or more recent;

[29] According to standard CWA 14167-1or more recent as regards the provision of services other than issuing qualified certificates ;

[30] According to standard CWA 14167-2, 3 and 4 or more recent

Mutual recognition and EC notification

A principle of mutual recognition was introduced as regards electronic identification schemes that are notified by member-states which meet the conditions for notification published in the Official EU Journal. The principle of mutual recognition applies only to online service authentication.

There is no obligation to notify electronic identification schemes to the Commission. The decision was left to the member states whether to notify all, some or none of the schemes that are used within the country to obtain the access to public, online or specific services.

When, according to national law or national administration practices, the access to an online service provided by a public service in one member-state requires electronic identification with the use of electronic identification means or authentication, then – for the needs of cross-border authentication of the online service – one country recognizes the electronic identification means that is issued by the other member-state only if the following conditions are met:

- the electronic identification means is issued within the framework of the electronic identification scheme given in the list published by the Commission;
- the security level of the electronic identification means is equal or is higher than the security level required by an appropriate public sector entity for the access to a particular online service on the condition that the security level of this means equals the medium or high security level;
- the appropriate public sector entity uses a medium or high security level as regards the access to a given online service.

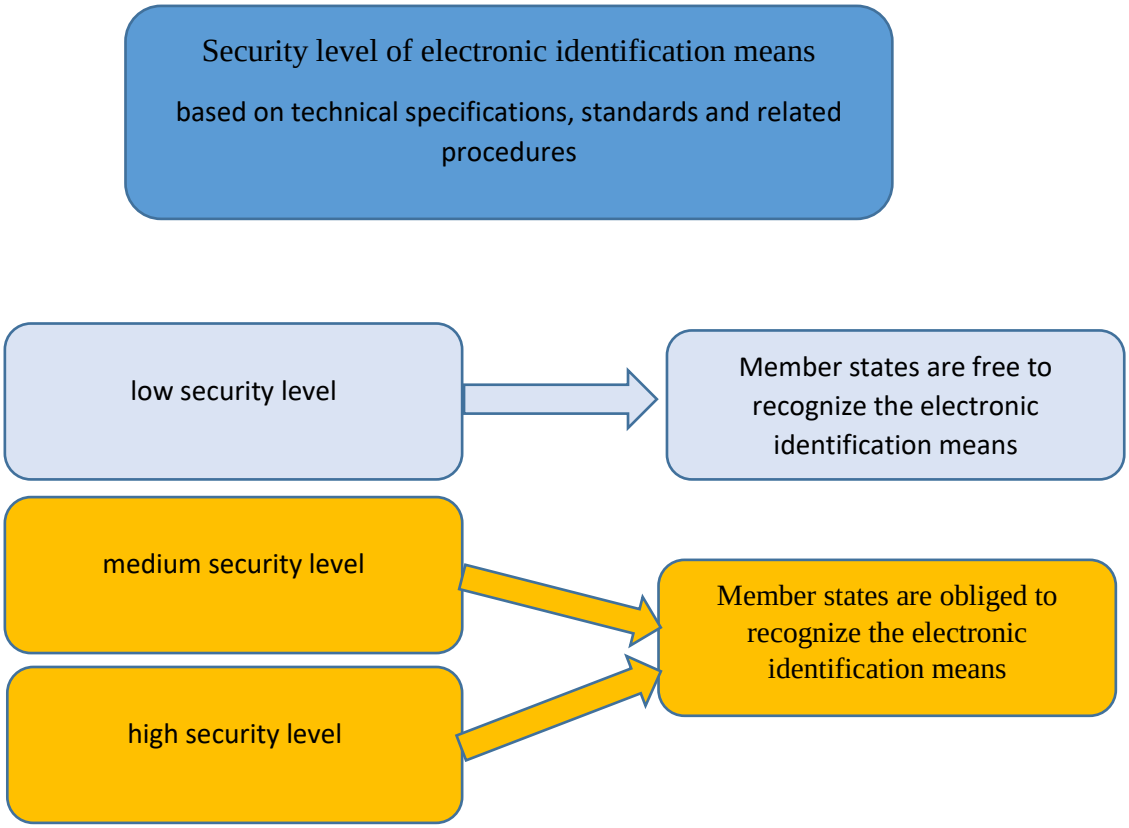
The obligation to recognize an electronic identification means should apply only to the means whose identity security level is equal to the level that is required to a particular online service or higher. Moreover, this obligation should be applied only in the cases when a given public sector entity uses "medium" or "high" security levels for the access to the online service in question.

The member states are free to recognize electronic identification means with lower security levels.

Security level

Low, medium or high security levels are assigned to an electronic identification scheme with regard to the electronic identification means used within the system. Security levels should define the degree of trust to the identification means that is applied when determining the identity of an individual. They depend on the degree of trust to the identification means as regards the confirmation, verification and authentication of individual's identity, management operations (the entity that issues the means and the procedures that are implemented) and technical security measures.

Figure 3. Security levels of an electronic identification means



Source: Authors' research

The security level depends on the type of the accessible data. Adequate methods and authentication techniques with specified reliability should be applied with regard to

the kind of service and the required security level. As a result, an adequate (based on risk analysis) credibility level required for authentication should be assigned to every service. The credibility level determines the acceptable degree of confidence with the consideration of possible loss in the case of faulty authentication. In order to facilitate the comparison of the authentication services and methods and to achieve interoperability, various classifications were developed to standardize the levels of credibility and their interpretations together with the requirements regarding the identification and authentication processes and techniques[31]. Standard ISO 29115 was developed to determine the above processes. It describes four credibility levels (Figure 3) Ale wg tłumacza rysunek 3 podaje tylko trzy poziomy wiarygodności (bezpieczeństwa) !!!

The access of the private sector to identification schemes

The identification scheme is developed mainly for the public sector. However, there are no obstacles for the private sector to use it freely when identification in necessary for online services or electronic transactions.

In Poland changes are introduced[32] that meet the above recommendations. The draft Ordinance of the Minister of Digitization on the scope and conditions for the use of electronic platform in public administration services provides for a free of charge organizational and technical application in the ePUAP platform of electronic identification means that are used for authentication in the IT system of a national bank or other employer. The application in ePUAP of electronic identification means to authenticate a non-public entity in an IT system will be performed by an agreement between the minister and a non-public entity.

Jednak wykorzystanie w ePUAP środków identyfikacji elektronicznej, stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, wymaga:

[31] 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

[32] Draft Ordinance of the Minister of Digitization of 03.06.2016 on the scope and conditions for the use of electronic platform in public administration services

However, the use in the ePUAP platform of the electronic identification means to authenticate a non-public entity in an IT system will by possible if the non-public entity:

- implements security measures of at least medium credibility level[33],
- develops and sets out, implements and applies, monitors and reviews as well as maintains and improves the information security management scheme;
- is subject to an audit that checks the fulfillment of the requirements by an independent third party at least once a year;
- confirms the identity of the individual who has the access to electronic identification means that are applied in the authentication process in its IT system on the basis of:
    - the presentation of the ID or passport with the PESEL identification number upon personal appearance,
    - the data that are obtained after a correct verification of the qualified electronic signature used by the individual to sign an electronic document in which it is stated that he/she is aware of the conditions and recommended trust means that are related to the use electronic identification scheme and, he/she agrees to be given the status of the scheme user and accepts the application of the shared electronic identification means in the ePUAP platform.

The ePUAP platform can share the information with other IT schemes of entities that perform public tasks and the schemes of non-public entities. The opportunity is provided to obtain a certificate for an IT scheme at the request of a non-public entity.

In order to facilitate the cross-border use of such electronic identification schemes by the private sector, the possibility ensured by any member-state to authenticate should be accessible to the relying parties[34] in the private sector that are located outside the member-state on the same conditions as for the relying parties from the private sector inside the member-state in question. The member-state has the right to define the access conditions to the authentication means and to inform whether the authentication means

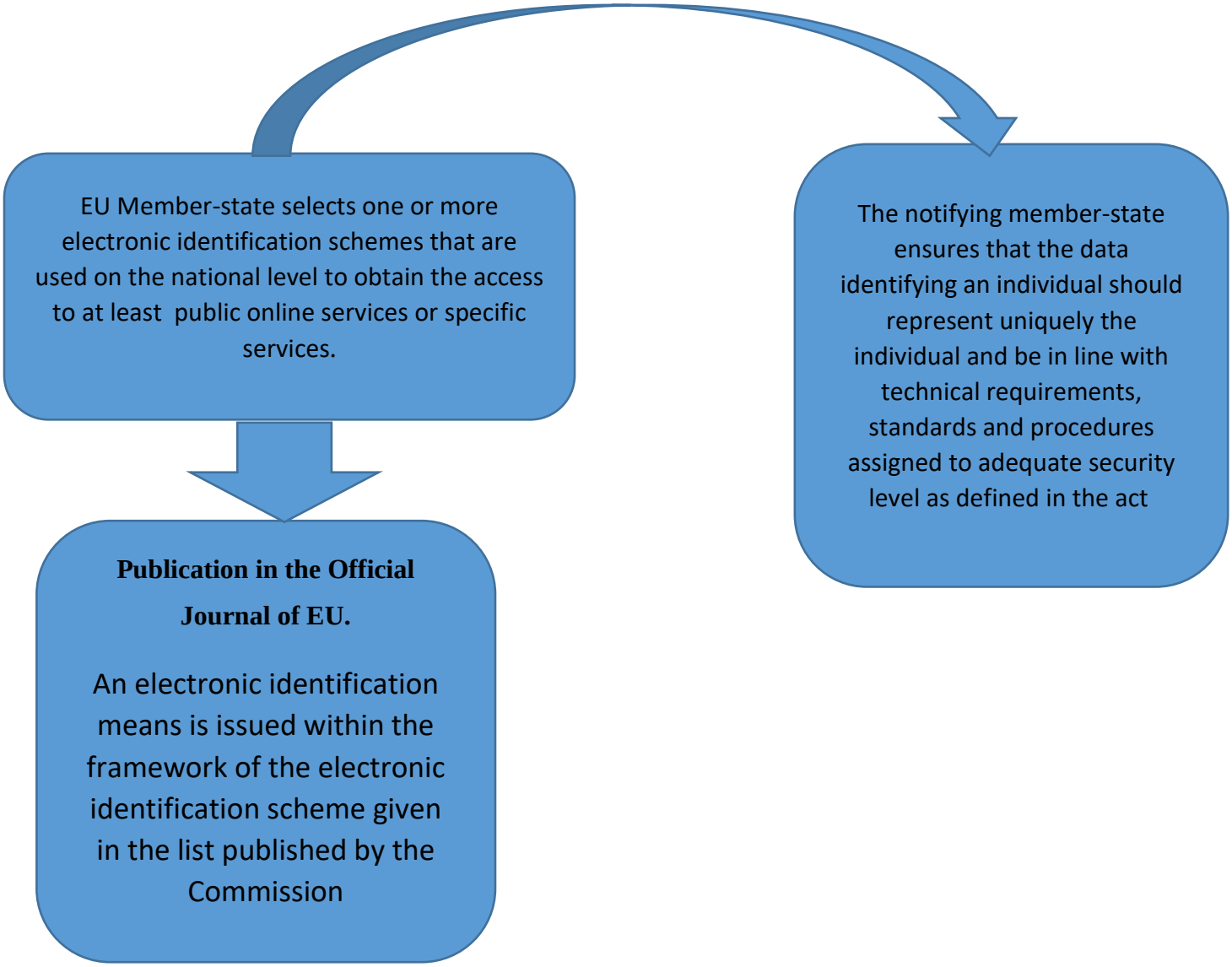
[33] As required by the Commission implementing regulation (EU)2015/1501 of 8 September 2015 on setting out minimum technical requirements and procedures for assurance levels for electronic identification means in electronic transactions

[34] i.e. a natural or legal person that is subject to electronic identification or trust service;

that are related to the notification system are currently available to the relying parties in the private sector.

The electronic identification means that is issued within the framework of the electronic identification scheme which is given on the list published by the Commission and corresponds to the low security level may be accepted by public sector entities for the needs of the cross-border authentication in online services provided by them (fig.4)

Figure 4. Electronic identification scheme in EU



Source: Authors' research

At present, conceptual work is being conducted on the development of a national identifier. The term *national identifier* refers to an identifier that is:

- commonly accessible to the citizens, potentially to all adults,
- commonly possessed,
- issued or recognized (when issued by commercial issuers) by the state,
- accessible for public and commercial e-services,
- credible ("safe"),
- interoperable.

Initially, there were plans in Poland to introduce an electronic ID (pl.ID project). When that concept was rejected, two projects of Trust Profile under eIDAS were considered for notification. Another scheme that is planned by Poland for notification is the KUZ health insurance card. The preparations were conducted under the *Ariadna* project. The main aim of the project is to implement the eIDAS regulation with the consideration of the national achievements in the area of internal administration, i.e. the ePUAP , Trust Profile and other trust services in public administration. The project assumes the use of ePUAP, Trust Profile and other existing IT solutions that are already available and would facilitate the achievement of the objective in question. A dedicated Trust Profile will provide the mechanisms of identity confirmation and authentication of Polish citizens after the notification process is completed. The Trust Profile will be communicated (in both directions) with the nationwide PEPS service from which it will receive identification requests and to which it will send the confirmations of identity[35].

The Draft Act on trust services, electronic identification and amendment of certain acts provides for setting up a national elDAS node[36], i.e. a hub that makes it possible to connect the national electronic identification infrastructure in Poland with the infrastructures of other EU countries. The national elDAS node will play a double role:

[35] Annex 8 to the *Ariadna* project feasibility study - Dostosowanie Profilu Zaufanego do unijnych wymogów rozporządzenia elDAS,
https://mac.gov.pl/files/zalacznik_nr_8_kopia_protokolu_z_prezentacji_publicznej_ariadna.pdf

[36] In the Commision Implementing Regulation (EU) 2015/1502 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of the elDAS draft regulation on identification and trust services, the minister competent for digitization ensures the functioning of a national node of eIDAS identification

- it will be an intermediary in the authentication of the holders of foreign electronic identification means that are issued within the framework of notified identification schemes in national online services,
- it will be an intermediary in the authentication of the holders of national electronic identification means in foreign online services in the cases when the identification scheme within which the means were issued will be notified to electronic identification of other member-states[37].

In conclusion, the national elDAS node will constitute an indispensable basis for the notification of the Polish electronic identification scheme irrespectively of the fact what scheme is going to be selected.

Bibliography:

1. Papińska-Kacperek J., *Usługi cyfrowe. Perspektywy wdrożenia i akceptacji cyfrowych usług administracji publicznej w Polsce*. Wydawnictwo Uniwersytetu Łódzkiego, 2013
2. Lewandowski R., *Elektroniczna karta ubezpieczenia zdrowotnego - słabe i mocne strony projektowanego rozwiązania*. Internet source: http://ww1.pwpw.pl/kwartalnik_archiwum.html?id=48&magCid=249
3. 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
4. PN ISO/IEC 27001:2007
5. PN-I-020003.1.031
6. Draft Ordinance of the Minister of Digitization on detailed organizational and technical conditions to be met by a IT user authentication system - Internet source: https://legislacja.rcl.gov.pl/docs//522/12286305/12357434/12357435/dokument225309.pdf
7. Draft act on trust services, electronic identification and the amendment of certain acts – Internet source:https://legislacja.rcl.gov.pl/projekt/12283556
8. Draft Act of 28 April 2011 on the amendment of the Act of 30 April 2015 on information system in health care
9. Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework - Internet source: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32015R1501

[37] Draft Act on trust services, electronic identification and the amendment of certain acts – Internet source : https://legislacja.rcl.gov.pl/projekt/12283556

10. Commision Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means and trust services for electronic transactions – Internet source: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32015R1501
11. 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
12. CWA 14167-1 standard regarding the provision of services other than issuing qualified certificates
13. ETSI TS 102 042 standard, version 1.2.4.
14. STORK - D2.3 - *Quality authenticator scheme*
15. Act of 13 April 2016 on conformity assessment systems and market surveillance (Journal of Laws, 2016, item 542)
16. Act of 15 April 2011 on medical activity, (Journal of Laws 2011, No.112, item 654)
17. Act of 17 February 2005 on the computerization of activities of entities performing public tasks (Journal of Laws 2005, No.64 item 565.
18. Act of 2 December 2009 on medical chambers, (Journal of Laws 2009, No.219, item 1708
19. Laboratory Diagnostics Act of 27 July 2001 (Journal of Laws 2014, item 174)
20. Annex No.8 to the feasibility study of the *Ariadna* project: Adjustment of Trust Profile to EU requirements of eIDASRregulation - https://mac.gov.pl/files/zalacznik_nr_8_kopia_protokolu_z_prezentacji_publicznej_ariadna.pdf
21. Zanaboni P., Knarvik U., Wootton R, *Adoption of routine telemedicine in Norway: the current Picture*, Glob Health Action 2014, **7:** 22801 - http://dx.doi.org/10.3402/gha.v7.22801
22. Ordinance of the Minister of Health of 25 March 2014 on the appointment of a team to implement eKUZ and KSM cards (Official Journal of the Ministry of Health, 2014.50 published: 2014.03.26
23. Internet source: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910
24. Internet source: http://www.dobreprogramy.pl/Po-kolejnej-awarii-ePUAP-moze-jednak-czas-zaorac-eadministracyjny-niewypal,News,72952.html
25. Internet source: http://www.polskieradio.pl/42/273/Artykul/1603800,Rodzina-500-wnioski-online-skladane-glownie-przez-banki-Zobacz-najczestsze-bledy.
26. Internet source: https://legislacja.rcl.gov.pl/projekt/12283556, Draft Act on trust services, electronic identification and amendment of certain acts

Abstract:

The digitization of the healthcare system is again in its starting point. It is unknown, whether the scheme that was planned in the form regulated by the act will start functioning. As a result, it should be reconsidered whether the solutions that were developed several years ago should be implemented or perhaps current technological solutions make it possible to change, simplify and deformalize the scheme.

Thus, one should find the answer to the question about the nearest future of the instruments for the identification and authentication of signatures and electronic seals as well as of other trust services necessary for running and processing medical e-documents, the national scheme solutions and other services that apply IT systems and telecommunication networks, including the telemedicine services.

In 2016, the European Parliament and Council of Europe Regulation on electronic identification and trust services for electronic transactions in the internal market No 910/2014 (eIDAS) will enter into force (EU Official Journal, 28 August, 2014). This legal act will be applied directly in EU and will not require the implementation of the national law. Consequently, an act is being prepared on trust services, electronic identification and the amendment of certain acts.

The aim of the article is to present the implications of the above regulations in the practical functioning of the healthcare system