ZESZYT NAUKOWY
Wyższa Szkoła Zarządzania i Bankowości w Krakowie

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
Mariusz Kielar
Jagiellonian University Medical College
Faculty of Health Sciences
Medical Information Systems Department
mariusz.kielar@uj.edu.pl
Krzysztof Gajda
Jagiellonian University Medical College
Faculty of Health Sciences
Medical Information Systems Department
krzysztof.gajda@uj.edu

IDENTIFICATION AND AUTHENTICATION SYSTEMS IN POLISH HEALTHCARE SYSTEM – CURRENT SITUATION AND TRENDS

Introduction

At present, in 2017, the issues in the healthcare system concerning identification tools, the authentication of services in IT systems and signing medical documents (declaration of intention) have not been regulated[1]. Generally, a part of the environment that provides medical services uses tools that are provided by the providers of IT services, including the access to applications and the data that is generated in the course of the application of cloud computing. At present, there are no instruments provided by the state that would enable medical service providers and patients to be identified in the healthcare information system, to confirm the accomplished services, to be identified in the cases of telemedicine (teleconsultations) or to have access to various services that are necessary in the course of treatment, e.g. submitting consents for treatment or indicating authorized people to collect the data after the death of a patient. Despite the fact that telemedicine has been legalized, it is practically not possible to be

[1] Apart from the Medical Information system (SIM); Regulation of the Minister of Health of 11 April 2013 on identification methods of recipients of services, medical employees and service providers and the method and procedure of transferring the information about medical employees providing healthcare services by service providers

provided a telecommunication service due to the inability to confirm the identity and professional qualifications of the person that advertises his/her medical services on the Internet.

Signing electronic medical documents is conducted via the application of electronic signatures that were purchased by healthcare service providers and were issued when the act on electronic signature (the so called secure signature that was valid till the expiration of the certificate)) was in force (the act was repealed in 2016) and with electronic signatures regulated as trust services by eIDAS. However, electronic seals that are required by eIDAS and which should appear on the documents of all entities providing medical services (with the exception of sole-traders providing medical services and applying electronic signature) are not used. This is due to two reasons:

- the lack of information on the subject from the Ministry of Health,
- the lack of information on the possibilities to purchase the seal on the market

Undoubtedly, the present situation is the result of numerous changes of the concept in question and, consequently, of legal regulations regarding the information system in the healthcare system where the implementation of an electronic medical documentation was toobligatory in all healthcare entities. First, the idea of ID cards was rejected and then the same happened to the Medical Specialist Card (KSM), the Administrative Specialist Card (KSA) and finally to the electronic Health Insurance Card (eKUZ). KSM is an electronic document that makes it possible to identify and authenticate medical staff, to place electronic signatures on electronic medical documents as well to confirm the rights to practice medical profession.

The KUZ card was intended to be a single document in the form of an electronic card used to verify the insurance status of the authorized card holder. Moreover, it was to be a tool applied to express the agreement for sharing medical documentation, to authorize the benefits obtained and (optionally) to serve as a carrier of emergency medical data. At present, the introduction of the remaining tools mentioned before is not expected. A new document is going to take over some of the KUZ functionalities and be used in the healthcare system. The implementation of a document with an electronic layer (eID) was a part of the pl.ID project but it was not accomplished within a period agreed with the European Commission[2].

[2] This is the reason why the pl.ID project is given the status of a non-functioning project and in order to avoid the incurred eligible costs (i.e. 148 million zlotys) the project has to present results, that is it should facilitate the commencement of the issue of eIDS by the end of March 2019

At present, the concept of ID with an electronic layer has returned. The new electronic ID is going to confirm the holder's identity in a clear and incontestable way; it will also be used for authentication purposes in the e-services of public administration and signing documents in the cyberspace. What is more, it will also include the ICAO application (a travel document with a biometric face photo) and will confirm the visits in healthcare entities. At the same time, due to its range that is limited to one professional group and the desire for a prompt distribution, a separate KSM card will be issued[3].

The new e-ID will be developed in the cooperation of the Ministry of Digitization and the Ministry of Internal Affairs and Administration, while the KSM card will be the project of the Ministry of Health. The e-ID will make it possible to receive health care services and to express the agreement for the access to medical documentation. Originally, the above functions were planned for the KUZ card but the e-ID is to take over the functionalities as regards the confirmation of the healthcare service received by a patient. The purpose of such solution is to eliminate the cases when service providers claim payments from the National Health Fund (NFZ) for:

- services that were not provided to patients on a given day and consequently were not registered with the service provider,
- fictitious services to patients who received other , frequently "cheaper", service from the service provider[4].

However, such results will be obtained only after a mandatory use of the e-ID card is implemented, which is going to happen in 2029 in this version of the project. That is why the Ministry of Health and the Ministry of Digitization are working on an alternative provisional solution.

The proposed functionality of the new e-ID is crucial to the healthcare system:

- **Citizen identification and authentication:**

[3] A new implementation concept of a Polish ID card with an electronic layer: //mc.gov.pl/aktualnosci/nowa-koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna

[4] Concept: e-ID – follow-up of the pl.ID project and the development of related projects, Annex 1: Description of the pl.ID project status

  - in on-line information systems (PIN will be required), which will enable citizens the access to all public administration e-services on portals that use the national node for electronic identification (the node is planned to be implemented in 2017)
  - directly in the public administration and commercial information systems through the interface with the software that is responsible for the communication with the e-ID (in the cases where particular systems are adequately developed; the task is within the responsibilities of system maintainers)

- **Electronic signing of documents** by citizens in on-line processes with public administration and healthcare service (a server signature; PIN will be required for authentication before signing);

- **Confirmation of citizen's presence** in the processes with public administration, health service and other ones (without the PIN); in fact, it is the confirmation of the use of e-ID in an electronic transaction; the possible applications include: getting the access at security gates at workplaces, confirmation of the service received by a patient;

- **Possibility to read from the electronic layer the data that is included in the visual layer**– in order to collect the data necessary for the electronic process and to increase the document's security level (the forgery of data in the electronic layer is practically impossible); the access to the data will be protected against accidental read-out);

- **Possibility to store additional data for the purpose of a read-out of the data** other than the data included in the visual data to be used individually by a citizen (e.g. emergency contact);

- **Possibility to initiate a qualified server signature** from any service providers that are selected by a citizen (depending whether such option is offered by particular qualified signature providers); the e-ID (without the option of a qualified server signature) does not substitute a qualified signature and does not make it possible by law to make declarations of intention outside the public administration (unless commercial parties and the citizen express their agreement to do so);

- **There will be a few possibilities to use the e-ID** as in healthcare entities – to confirm the identity on a computer with an internal or external contactless card reader.

It is essential for the healthcare system to assume that the e-ID will:

- provide high level authentication – the electronic layer will include a certificate to authenticate (with PIN required) and to confirm the presence (PIN not required). The certificates will be issued by the Ministry of Internal Affairs and Administration and their validity will equal the document's validity, i.e. 10 years. The certificate will also be recognized by the Ministry of Health for the needs of the health service;
- make it possible to use the electronic signature in compliance with the eIDAS regulation regarding the advanced electronic signature. It is not assumed, however, that the signature should be a cross-border trust service – it will be legally anchored in the national regulations as regards contacts with the public administration. The signature will be confirmed by Trusted Profile (TP) and e-ID as the permitted identification tools.
- be a high security identification tool.

Numerous electronic services require the identification and authentication of the user; however, they do not need the same security levels. There are different requirements as regards the access to sensitive medical data and different for downloading official forms. Depending on the type of service and the required security level, adequate authentication methods and techniques should be applied with a particular level of credibility. As a result, every service should be assigned (on the basis of risk analysis) a credibility level that is required for the authentication. The credibility level determines the trust level that is acceptable with the consideration of losses that may be incurred due to false authentication[5].

The eIDAS regulation defines three security levels as regards the electronic identification means:

- low security level,
- medium security level,

[5] Mielnicki T., Wołowski F., Grajek M., Popis P., Identyfikacja i uwierzytelnienie w usługach elektronicznych. https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf

- high security level

The tools of electronic identification that are applied (trusted profile ePUAP, the new e-ID) should be adequate to the needs and security targets of service providers who - on the basis of risk analysis - determine the means that are necessary to ensure the safety of their services

The Trusted Profile that at present is offered by the public administration as an electronic identification means is planned to be assigned the medium level. However, it is expected that for the scheduled health services (and also other services) a tool with a high trust level should be implemented; in that case the use of the Trusted Profile will not be possible and the e-ID will have to be applied.

An example of the service that requires such level is the service which enables pharmacies to sell medicines or a company board member to make a substantial transfer from the company bank account. In order to authenticate devices or systems (NPE – Non Person Entity), the use electronic certificates (e.g. X.509 or CVC)[6] is required. The Trusted Profile can be used only in digital services and is based on one-time authentication passwords via SMS, while the e-ID will be applied both in cyber and physical space and is based on a cryptographic card and PIN authentication.

The main problem in the implementation of the qualified signature on a card is the necessity to ensure the cooperation with any qualified entity that operates within the common market. Due to security requirements, a preliminary verification is necessary of the eligibility of entities that are qualified to introduce information on the card. Another solution is to give a permission to place a qualified signature in the e–ID only to a selected entity, which raises concerns as regards an unlawful support from the state or an abuse of free market principles.

There were concepts that e-ID should be combined with the KSM card. However, combining the functionalities of KSM and e-ID would result in a significant complication of the whole project and additional risk would be generated. Moreover, there is no objective justification to include the functionalities of KSM to e-ID and to neglect the needs of other professional groups. In the future – after the registers that include the information on professional qualifications are adjusted and integrated – the e-ID card may become a key to the

[6] The example for LoA 4 level in in the ISO 29115 standard in: Ibid.

registers and authenticate the return of suitable data. However, such solution is impossible until there are no integrated central qualification registers [7].

It was considered that the implementation of KSM is necessary to disseminate electronic exchange of medical information which would result in a significant increase in the effectiveness of health service.

The planned changes indicate that the lack of the KUZ and KSM cards does not pose an obstacle to a further development of project P1. From the very beginning both tasks (P1 and the cards) constituted separate projects although a part of the functions of the cards were intended to support P1 and also they played a critical role as regards the popularization and dissemination of the selected P1 functionalities. This concerns the option to place the electronic signature on Electronic Medical Documentation (EDM) by medical staff (the KSM function) and the patient's ability to express the consent for the access to his/her EDM (initially it was the KUZ function, while now it the e-ID function). The problem is that the implementation of EDM requires not only the introduction of an adequate obligation on the level of regulations but also the undertaking of appropriate measures as regards the technical readiness of stakeholders to fulfill the obligation in question (computerization of healthcare entities and the possession of e-signature tools).

KSM is an extremely necessary tool for the dissemination of medical documentation, including electronic leaves, prescriptions and referrals. KSM will be mainly used by medical staff to place electronic signatures on medical documents. Doctors, dentists and eventually the representatives of other medical professions will be issued KSM cards t for the purposes of identification and authentication of the card holders in ICT systems; moreover, KSM will confirm electronically the right to practice the profession and in the future it will facilitate the access to medical emergency data of a patient.

From a practical point of view it is planned that KSM as „the right to practice medical profession" and "the right to practice dental profession" (extended to other medical professions

[7] Koncepcja e-Dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych Załącznik 2 Opis planowanej funkcjonalności i architektury IT oraz otoczenie prawno-organizacyjne (Concept: e-ID – follow-up of the pl.ID project and the development of related projects, Annex 2: Description of the planned functionality and IT architecture and legal and organizational environment.)

in the future) should be available in two graphic (colour) versions: one for the staff during their postgraduate internships and the other for an unlimited period of time (with the assumption that at the beginning of the functioning of KSM, the access to the electronic layer will not be commonly available and KSM should include the following elements as a rule (to be modified or made more precise at the stage of the legislative work):

- the name of the document in Polish : *prawo wykonywania zawodu lekarza i odpowiednio lekarza dentysty;*
- the name of the document in English : *"the right to practice the profession of a physician (of a dentist)';*
- the number of the right to practice the profession of a physician;
- the date of obtaining the right to practice the profession of a physician;
- the name of the authority that granted the right to practice the profession of a physician;
- the first and the second name of the physician;
- the personal identity number (PESEL) or – if non-existent – the passport or other identity card number;
- professional title;
- the physician's photograph: bareheaded, without sunglasses and with a neutral expression;
- the signature of the physician.

The electronic layer of KSM should include:

- a data container[8] for qualified certificate to sign medical documents; the certificate will reveal in a dedicated box or boxes (the decision will be made at the stage of technical designing) the following additional information: the number of the right to practice the profession, title, profession and specialization (if applicable).
- a container for the CV certificate to communicate with the Patient's Card (which is scheduled for the future and is not included in the project in question),

[8] A data structure to store a set of data (objects) in an organized way. The container provides tolls of access, including adding, removing and searching data (objects) in the containers. Depending in the accepted organization, particular containers vary in the efficiency of particular operations. https://pl.wikipedia.org/wiki/Kontener_(programowanie)

- a container for the NFZ or the Ministry of Health identification and authentication to be used in the systems of medical entities.

The final range of data will be determined at the stage of technical designing and will depend on the regulations and possible differences resulting from the specific features of particular professions for which the KSM cards will be issued. The proposed solution will be supplemented by an IT system to issue KSM (card production and personalization system, a portal for processing the orders, a module to issue the certificates) and by card readers. The card will only have a contact interface.

The introduction to the identity cards with an electronic layer of the functionality of the medical service confirmation receipt and the agreement for the access to medical documentation as well as the issue of KSM will require amendments in several regulations in the healthcare system, including the act on healthcare services financed from public funds and the acts on particular medical professions.

One of the new solutions that patients should be able to use is the service of m-documents. It will facilitate the use of documents that patients (and other users) may need in situations when their ID is required or – in the nearest future in the Authors' opinion – a document that confirms particular rights, for example searching in registers for citizens with particular rights (blood donors, war veterans) with the use of mobile phones. Such service is an alternative to the presentation of a paper/plastic ID or other document[9.]

The solution under development does not substitute the traditional ID or other documents confirming entitlements; it only introduces an alternative way of confirming the identity by a citizen. Thus, current regulations in this area will only be supplemented by an alternative method of identity confirmation, i.e. by the application of the new e-service.

The citizens (including patients) will be entitled to use e-service after giving their consent taht may be withdrawn at any time[10]. The creators of the concept emphasize the fact that such a solution is not only convenient but also a safe one as no personal data will be transferred to a mobile phone. The new tool will only play the role of an access terminal to the data of a particular citizen. The access will be possible only on request of the entitled person.

The data will be fully reliable as they will be downloaded from authenticated bases (ID

[9] As in the new Art. 16c in the act of 17 February 2005 on the computerization of activities of entities performing public tasks

[10] Explanatory memorandum: https://legislacja.rcl.gov.pl/docs//2/12294950/12413452/12413453/dokument280559.pdf

Registry and other). Consequently, they will provide identification and confirmation possibilities to the same degree as it is done by traditional documents.

The confirmation of identity or entitlements with the use of m-documents will have the same significance and will enable the access to the same services as in the case of traditional documents. The data included in traditional documents are collected and stored in a public register – in the case of ID it is the ID Register (RDO). The information that will show on the tool of a public entity will be in a way a digital presentation of - for example - the id card and will be downloaded from RDO. It should be pointed out that the data presented in the new e-service will not be stored in the citizen's or public official's/officer's tools[11].

Due to the fact that new identification tools appear, the providers need a unique electronic identification within their systems in order to ensure the security of the services provided[12].

The information systems of public administration, to some extent also including the healthcare system, apply the following tools of the electronic identification of their users:

- mechanisms within the systems,
- the mechanism of the ePUAP trusted profile, which at present is– as regards public services – the only commonly used public means of electronic identification.

It is essential for the healthcare system to assign adequate rights both to the representatives of services providers and the patients, which involves the need to open accounts in the service providing systems. With regard to the kind of the on-line service, the electronic identification protects the service against an unauthorized takeover or the creation of false identity and, consequently, against potential damages that may affect both parties (the service recipient and its provider). For this reason, depending on the tasks that are performed in the healthcare system, various protection measures are implemented that are adequate to particular services provided.

The existence of numerous electronic systems already poses a problem. Thus, it seems reasonable that the users should aim at applying a similar or identical set of identification data within the range of various services. Consequently, measures were taken that should result in

[11] Information about the reasons and the need to introduce solutions as planned in the project, https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/prace-legislacyjne-rm-i/prace-legislacyjne-rady/wykaz-prac-legislacyjny/rejestr4819738125,dok.html?czas=1487930400

[12] https://legislacja.rcl.gov.pl/projekt/12297458

the development of a common electronic identification and authentication system to be managed by a separate entity appointed solely for this purpose.

A public scheme of electronic identification as an institutional solution is under development. It is meant to facilitate the delivery of public services that are available in public ICT systems that require authentication. The scheme will consist of:

- a national node and
- electronic identification systems connected to the node within which electronic identification tools (identity providers) will be issued, ICT systems that will include data to describe and identify citizens, particularly public registers (attribute providers) and ICT system and ICT systems where public services will be available (service providers).

The national node will facilitate authentication for service delivery with the application of the electronic identification tools that are issued by the electronic identification system connected to the node. It is meant to serve as an organizational and technical solution that connects the **platforms** on which services are available, the systems that provide **additional data to identify a citizen** and **electronic identification systems within which free identification tools will be issued**[13]**.**

The important duty of the entity responsible for the e-identification system that is connected to the node will be to provide the accountability and undeniability of the operations of the users of particular e-identification tools.

It is essential for healthcare protection to assume that the provider of the e-identification tools should supply a possibly wide range of attributes from the minimum and the wide data sets[14]. In the cases when the provider of the e-identification tool does not possess all the required attributes from the wide set of identification data, they are supplemented from the attribute provider in the course of the e-identification process. The transfer of additional attributes must always be conducted with knowledge and consent of the data subject. It is assumed that the

[13] Draft amendment of the act on trust services, electronic identification and other acts– explanatory memorandum: https://legislacja.rcl.gov.pl/projekt/12297458

[14] See the Annex to Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework.

attribute providers will be eventually connected to a public e-identification scheme through the Platform of Service and Data Integration[15] that is under development.

Bibliography

[1.] https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/prace-legislacyjne-rm-i/prace-legislacyjne-rady/wykaz-prac-legislacyjny/rejestr4819738125,dok.html?czas=1487930400

[2.] https://legislacja.rcl.gov.pl/docs//2/12294950/12413452/12413453/dokument280559.pdf

[3.] https://legislacja.rcl.gov.pl/projekt/12297458

[4.] https://mc.gov.pl/aktualnosci/nowa-koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna

[5.] *Koncepcja e-dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych* Załącznik 2 Opis planowanej funkcjonalności i architektury IT oraz otoczenie prawno-organizacyjne (Concept: e-ID – follow-up of the pl.ID project and the development of related projects, Annex 2: Description of the planned functionality and IT architecture and legal and organizational environment.)

[6.] *Koncepcja: e-Dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych*, Annex 1: Opis statusu projektu pl.ID (Concept: e-ID – follow-up of the pl.ID project and the development of related projects, Annex 1: Description of the pl.ID project status)

[7.] Mielnicki T., Wołowski F., Grajek M., Popis P., *Identyfikacja i uwierzytelnienie w usługach elektronicznych.* https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf

[8.] Draft amendment of the act on trust services and electronic identification and other acts https://legislacja.rcl.gov.pl/projekt/12297458

[9.] Regulation of the Minister of Health of 11 April 2013 on identification methods of recipients of services, medical employees and service providers and the method and procedure of transferring the information about medical employees providing healthcare services by service providers

Abstract

The article discusses present issues regarding the identification and authentication services in information systems and the signing of medical documents (the declaration of

[15] Draft amendment of the act on trust services and electronic identification and other acts, https://bip.kprm.gov.pl/kpr/form/rejestr14180691990456,dok.html?cza

intention) in the healthcare sector. It points at the trends in the present model of the information security of the healthcare system stakeholders in Poland.