

**Mgr Szczepan Jakubowski**

Uniwersytet Jagielloński - Collegium Medicum, Wydział Nauk o Zdrowiu, Zakład  
Medycznych Systemów Informacyjnych  
szczepan.jakubowski@uj.edu.pl

**Dr Artur Romaszewski**

Uniwersytet Jagielloński - Collegium Medicum, Wydział Nauk o Zdrowiu, Zakład  
Medycznych Systemów Informacyjnych  
artur.romaszewski@uj.edu.pl

**Dr hab. Wojciech Trąbka**

Krakowska Akademia im. Andrzeja Frycza Modrzewskiego - Katedra Bioinformatyki  
i Zdrowia Publicznego, Wydział Lekarski i Nauk o Zdrowiu  
wojciech.trabka@uj.edu.pl

## **IDENTYFIKACJA I UWIERZYTELNIANIE PODMIOTÓW ORAZ DOKUMENTÓW ELEKTRONICZNYCH W OCHRONIE ZDROWIA JAKO NIEZBĘDNE ATRYBUTY BEZPIECZEŃSTWA DANYCH I INFORMACJI W OCHRONIE ZDROWIA**

### **Wprowadzenie**

Ostatnio pojawiło się wyjątkowo dużo publikacji dotyczących problemu ochrony danych, również w opiece zdrowotnej. Uwaga autorów tych publikacji koncentruje się głównie na przepisach RODO<sup>1</sup> oraz polskiej ustawie o ochronie danych<sup>2</sup>. Nie można tego samego powiedzieć o przepisach innego, nie mniej ważnego Rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do e-transakcji na rynku wewnętrznym (*Regulation of the European Parliament and of the Council on electronic identification and trust for electronic transactions in the internal market*) - (tzw. eIDAS)<sup>3</sup> oraz polskich przepisach, których zadaniem jest uzupełnienie i uszczegółowienie

---

<sup>1</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 Kwietnia 2016 r. w Sprawie Ochrony Osób Fizycznych w Związku z Przetwarzaniem Danych Osobowych i w Sprawie Swobodnego Przepływu Takich Danych Oraz Uchylenia Dyrektywy 95/46/WE (Ogólne Rozporządzenie o Ochronie Danych), p. 679 <<https://eur-lex.europa.eu>>.

<sup>2</sup> Ustawa z dnia 10 Maja 2018 r. o Ochronie Danych Osobowych (Dz.U. 2018 Poz. 1000) <<http://prawo.sejm.gov.pl>>.

<sup>3</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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 <<https://eur-lex.europa.eu>>.

regulacji UE w zakresie wskazanym w przepisach<sup>4</sup>. Niestety mało jest publikacji dotyczących rozwiązań zawartych w Rozporządzeniu (eIDAS) w odniesieniu do ochrony zdrowia<sup>5</sup>.

Rozporządzenie eIDAS jest jedną z ważniejszych regulacji, której rozwiązania są kluczowe dla systemu ochrony zdrowia. Jego podstawowym zadaniem jest zwiększenie zaufania do transakcji elektronicznych, przy zapewnieniu wspólnej podstawy bezpiecznych interakcji elektronicznych między obywatelami, przedsiębiorstwami i organami publicznymi. Jest to niezwykle ważne w sektorze zdrowia, gdzie następuje stała wymiana informacji między pacjentami, świadczeniodawcami, a podmiotami prawnie upoważnionymi do otrzymywania informacji zdrowotnych. Jedną z podstawowych kwestii w trakcie procesu wymiany informacji jest jej odpowiednie zabezpieczenie. Większość informacji gromadzona w zasobach elektronicznej dokumentacji medycznej zawiera dane o stanie zdrowia zaliczane do tzw. danych wrażliwych.

Polski system ochrony zdrowia przygotowuje się do wdrożenia przełomowych rozwiązań wprowadzających na rynek instytucję recepty elektronicznej, elektronicznego skierowania oraz finalizacji procesu wprowadzenia we wszystkich podmiotach świadczących usługi medyczne elektronicznej dokumentacji medycznej. Dodatkowo wprowadzono przepisy umożliwiające świadczenie usług z zakresu telemedycyny, które nie są jednak w pełni możliwe do wdrożenia w podmiotach leczniczych bez wprowadzenia powszechnego systemu identyfikacji świadczeniodawców i pacjentów. Należy również zwrócić uwagę na prace na szczeblu państwa nad rozwiązaniami bezpośrednio wynikającymi z Rozporządzenia eIDAS, których wdrożenie będzie odczuwalne w całym kraju w większości dziedzin życia, w tym w ochronie zdrowia. Mowa tutaj o usłudze zaufania e-Doręczenia, która może być przełomowa dla przekazywania dokumentów o stanie zdrowia oraz o nowym dowodzie osobistym. Należy mieć nadzieję, że prace nad tymi rozwiązaniami są skoordynowane na szczeblu ministerialnym.

W artykule zostaną przedstawione główne założenia i rozwiązania przyjęte w regulacjach, a więc zarówno uregulowania dotyczące identyfikacji podmiotów, jak i zastosowania usług zaufania w bieżącej pracy podmiotów leczniczych. Zostanie zwrócona uwaga na pewne „polskie aspekty” wdrażanych regulacji w świetle rozwiązań UE. Przede wszystkim należy podkreślić, że wprowadzono rozwiązanie wskazywane jako dopuszczalne przy prowadzeniu

---

<sup>4</sup> Ustawa z dnia 5 Września 2016 r. o Usługach Zaufania oraz Identyfikacji Elektronicznej (Dz.U. 2016 Poz. 1579) <<http://prawo.sejm.gov.pl>>.

<sup>5</sup> Sz. Jakubowski, *Identyfikacja i Uwierzytelnianie Podmiotów Oras Dokumentów Elektronicznych w Ochronie Zdrowia* (Praca wykonana w Zakładzie Medycznych Systemów Informacyjnych, Instytut Zdrowia Publicznego, UJ CM, 2018).

elektronicznej dokumentacji medycznej tj. podpis potwierdzony profilem zaufanym ePUAP, który nie jest w pełni kompatybilny z eIDAS. Jest on podpisem elektronicznym stosunkowo skomplikowanym w obsłudze i może być wykorzystywany tylko na terenie kraju. Zostanie poruszona również kwestia obecnie wdrażanej recepty elektronicznej oraz e-zwolnień, jako dokumentów elektronicznych, które muszą zachować zgodność z przepisami Rozporządzenia eIDAS.

Autorzy tego tekstu są orędownikami wdrażania wszystkich nowoczesnych rozwiązań, są jednak zdania, że wszelkie podejmowane kroki w zakresie ich realizacji, powinny być zgodne z rozwiązaniami przepisów rozporządzenia eIDAS. Środowisko medyczne powinno przed wdrożeniem tak dużych projektów zostać wyposażone w odpowiednie narzędzia, umożliwiające poprawne działania w tym zakresie. Dodatkowo korzystne byłby akcje edukacyjne przeprowadzane w tym obszarze.

## 1. Czym jest identyfikacja i uwierzytelnianie?

Identyfikacja w formie elektronicznej, rozumiana jest jako „proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną” (art. 3)<sup>6</sup>. Definicja według Polskiego Komitetu Normalizacyjnego określa identyfikację jako „proces zautomatyzowanego rozpoznania określonego użytkownika w systemie możliwy do zrealizowania dzięki zastosowaniu unikalnych nazw”<sup>7</sup>. Danymi identyfikującymi osobę są dane, które dają możliwość przypisania osobie fizycznej lub prawnej konkretnej tożsamości. Pakiet tych danych tworzy identyfikator, który może być zawarty na materialnym lub niematerialnym narzędziu nazywanym środkiem identyfikacji elektronicznej<sup>8</sup>.

W Polsce, w systemie informacji ochrony zdrowia wyróżnia się cztery identyfikatory, dla „usługobiorców, usługodawców, miejsc udzielenia świadczenia opieki zdrowotnej i

---

<sup>6</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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.

<sup>7</sup> A. Romaszewski et al., *Identyfikacja i Uwierzytelnienie w Systemie Informacyjnym Opieki Zdrowotnej Po Wprowadzeniu Rozporządzenia UE EIDAS*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2016, nr 42.

<sup>8</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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, p. 910.

pracowników medycznych” (art. 17c ust 1)<sup>9</sup>. Dla usługobiorcy, inaczej pacjenta jest to numer PESEL lub innego dokumentu tożsamości. Usługodawców dzieli się na trzy grupy. Pierwszą grupą są podmioty wykonujący działalność leczniczą a ich identyfikatorem jest kod, do stworzenia którego użyto znaków z systemu resortowego kodów identyfikacyjnych określonego przez Ministra Zdrowia. Drugą grupę stanowią apteki, których indywidualny kod pochodzi z Krajowego Rejestru Zezwoleń na Prowadzenie Aptek Ogólnodostępnych, Punktów Aptecznych oraz Rejestru Udzielonych Zgód na Prowadzenie Aptek Szpitalnych i Zakładowych. Natomiast trzecia grupa to podmioty, których działalność dotyczy zaopatrzenia w wyroby medyczne a identyfikatorem jest 9-znakowy numer REGON. Identyfikator miejsca udzielania świadczenia medycznego odrębny jest dla podmiotu wykonującego działalność leczniczą, aptek i podmiotów realizujących czynności z zakresu zaopatrzenia w wyroby medyczne, jednak zasada tworzenia identyfikatora jest taka sama jak przy ogólnym identyfikatorze usługobiorcy, jedyną różnicą jest to, że Narodowy Fundusz Zdrowia ustanawia indywidualny kod dla podmiotów zaopatrzenia w wyroby medyczne. Istnieją jeszcze identyfikatory pracowników medycznych, które stanowią numer prawa wykonywania zawodu lub PESEL w przypadku jego braku (opcjonalnie numer innego dozwolonego dokumentu np. paszportu)<sup>10</sup>. Podział identyfikatorów (pakietów danych przypisanych indywidualnie do jednostki) przedstawia Tabela 1.

**Tabela 1. Podział identyfikatorów w sektorze ochrony zdrowia**

<b>Identyfikatory w ochronie zdrowia:</b>		
1. Identyfikator usługobiorcy		
2. Identyfikator usługodawcy		
podmiotu wykonującego działalność leczniczą	aptek	podmiotów zaopatrzenia w wyroby medyczne
3. Identyfikator miejsca udzielania świadczenia medycznego		
podmiotu wykonującego działalność leczniczą	aptek	podmiotów zaopatrzenia w wyroby medyczne
4. Identyfikator pracownika medycznego		

Źródło: opracowanie własne na podstawie ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia<sup>11</sup>.

<sup>9</sup> Ustawa z dnia 28 Kwietnia 2011 r. o Systemie Informacji w Ochronie Zdrowia (Dz.U. 2011 Nr 113 Poz. 657) <<http://prawo.sejm.gov.pl>>.

<sup>10</sup> Ibidem.

<sup>11</sup> Ustawa z dnia 28 kwietnia 2011 r. o Systemie Informacji w Ochronie Zdrowia (Dz.U. 2011 Nr 113 Poz. 657) <<http://prawo.sejm.gov.pl>>.

Użytkownik chcąc potwierdzić swoją tożsamość przekazuje czynnik uwierzytelniania do systemu identyfikacji elektronicznej następnie, jeśli weryfikacja przebiegnie pomyślnie to środek identyfikacji elektronicznej jest uwolniony (odbezpieczony). Dodatkowo na wyższych poziomach bezpieczeństwa prócz weryfikacji środka elektronicznego sprawdzana jest za pomocą uwierzytelniania dynamicznego jego autentyczność<sup>12</sup>. W procesie uwierzytelniania zachodzi określenie czynnika uwierzytelniania, czyli czynnika przypisanego do danej osoby o potwierdzonym pochodzeniu i związku. Wyróżnia się trzy rodzaje czynników uwierzytelniania, a mianowicie:

- „czynnik uwierzytelniania na podstawie posiadania - oznacza czynnik uwierzytelniania, w przypadku którego, od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania jego posiadania;
- czynnik uwierzytelniania na podstawie wiedzy - oznacza czynnik uwierzytelniania, w przypadku, którego, od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania jego znajomości;
- czynnik uwierzytelniania na podstawie cech przyrodzonych - oznacza czynnik uwierzytelniania, który opiera się na rzeczywistym atrybucie osoby fizycznej, w którego przypadku od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania, że tę cechę fizyczną posiada”<sup>13</sup>.

Rodzaje czynników uwierzytelniania wraz z przykładami prezentuje Tabela 2.

**Tabela 2. Rodzaje czynników uwierzytelniania**

Czynnik uwierzytelniania na podstawie posiadania	Czynnik uwierzytelniania na podstawie wiedzy	Czynnik uwierzytelniania na podstawie cech przyrodzonych
sprzętowy token, karta elektroniczna (dowód osobisty z warstwą elektroniczną)	login, hasło, PIN, indywidualny numer jak PESEL, identyfikator lekarza	skan linii papilarnych, inne cechy biometryczne

Źródło: opracowanie własne na podstawie Komisja Unii Europejskiej, Załącznik *Specyfikacje Techniczne i Procedury Dotyczące Niskiego, Średniego i Wysokiego Poziomu Zaufania w Odniesieniu Do Środka Identyfikacji Elektronicznej Wydanego w Ramach Notyfikowanego Systemu Identyfikacji Elektronicznej* <<https://eur-lex.europa.eu>>.

<sup>12</sup> M. Marucha-Jaworska, *Rozporządzenie EIDAS : Zagadnienia Prawne i Techniczne*, Wyd. 1, Wolters Kluwer Polska, Warszawa 2017.

<sup>13</sup> Komisja Unii Europejskiej, Załącznik *Specyfikacje Techniczne i Procedury Dotyczące Niskiego, Średniego i Wysokiego Poziomu Zaufania w Odniesieniu Do Środka Identyfikacji Elektronicznej Wydanego w Ramach Notyfikowanego Systemu Identyfikacji Elektronicznej* <<https://eur-lex.europa.eu>>.



Elementem systemu identyfikacji jest system teleinformatyczny definiowany jako „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego” (art. 2 ust 3)<sup>14</sup>. Jeżeli użytkownicy systemu teleinformatycznego podmiotów pożytku publicznego (np. Samodzielnych Publicznych Zakładów Opieki Zdrowotnej – SP ZOZ) w Polsce chcą skorzystać z udostępnionych im usług online, uwierzytelnianie wymaga:

- 1) „użycia notyfikowanego środka identyfikacji elektronicznej, adekwatnie do poziomu bezpieczeństwa wymaganego dla usług świadczonych w ramach tych systemów, lub
- 2) profilu zaufanego ePUAP, lub
- 3) danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego” (art. 20a. 1)<sup>15</sup>.

## **2. System identyfikacji elektronicznej**

Krajowy schemat identyfikacji elektronicznej składa się z: węzła krajowego identyfikacji elektronicznej oraz węzła transgranicznego wykorzystywanych do uwierzytelniania osób w procesie dostępu do usług cyfrowych. W ramach standardowego węzła działają: system identyfikacji elektronicznej, przez który wydawane są środki identyfikacji elektronicznej oraz systemy teleinformatyczne udostępniające usługi online. Węzeł identyfikacji elektronicznej stanowi centralny element modelu identyfikacji elektronicznej i określamy nim system, który integruje w jednym miejscu systemy teleinformatyczne oraz systemy identyfikacji elektronicznej. Daje to możliwość skorzystania z usług online po wcześniejszym potwierdzeniu tożsamości użytkowników. Przyłączanie do węzła różnych systemów identyfikacji elektronicznej dostarcza wielu środków identyfikacji elektronicznej, dzięki którym użytkownicy przechodzą proces uwierzytelnienia<sup>16</sup>. Schemat projektowanego systemu Węzłów Identyfikacji Elektronicznej w Polsce przedstawia Rysunek 1.

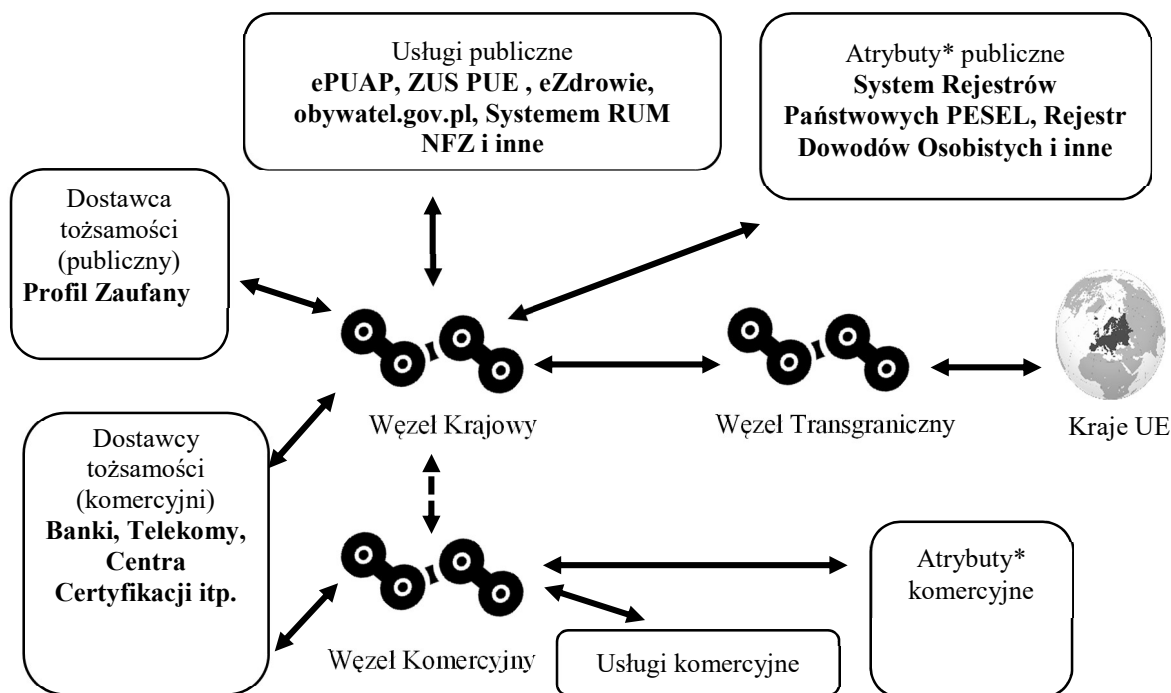
---

<sup>14</sup> Ustawa z dnia 18 Lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204).

<sup>15</sup> Ustawa z dnia 17 Lutego 2005 r. o Informatyzacji Działalności Podmiotów Realizujących Zadania Publiczne (Dz.U. 2005 Nr 64 Poz. 565) <<http://prawo.sejm.gov.pl>>.

<sup>16</sup> Projekt Ustawy o Zmianie Ustawy o Usługach Zaufania Oraz Identyfikacji Elektronicznej Oraz Niektórych Innych Ustaw (2018) <<https://legislacja.rcl.gov.pl>>.

Rysunek 1. Schemat planowanego systemu Węzłów Identyfikacji Elektronicznej



Źródło: opracowanie własne na podstawie: Ministerstwo Cyfryzacji i Centralny Ośrodek Informatyki; materiał konferencyjny<sup>17</sup> oraz Accenture, Obserwatorium.biz; *Raport EID 2017, Elektroniczna identyfikacja w Polsce*<sup>18</sup>.

\*Atrybuty - to nieobowiązkowe, indywidualne identyfikatory do weryfikacji tożsamości osoby fizycznej lub prawnej, ustalone zgodnie z prawem krajowym, które można stosować w kwalifikowanych certyfikatach, jeżeli nie zaburzają transgranicznej interoperacyjności<sup>19</sup>

Instytucja Węzła krajowego jest „rozwiązaniem organizacyjno-technicznym umożliwiającym uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego”<sup>20</sup>. Celem Krajowego Węzła Identyfikacji Elektronicznej jest upowszechnienie oraz ułatwienie korzystania z usług cyfrowych dla obywateli Polski przez

<sup>17</sup> D. Cabańska, K. Biniek, *Węzeł Krajowy*. Ministerstwo Cyfryzacji. Centralny Ośrodek Informatyki, <<https://www.gov.pl/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej>> (dostęp 06.2018).

<sup>18</sup> Accenture, Obserwatorium.biz, *Raport EID 2017, Elektroniczna Identyfikacja w Polsce 2017* <<https://www.accenture.com/pl-pl/event-eid-report-2017>> (dostęp 06.2018).

<sup>19</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 910/2014 z dnia 23 Lipca 2014 r. w sprawie Identyfikacji Elektronicznej i Usług Zaufania w Odniesieniu Do Transakcji Elektronicznych Na Rynku Wewnętrznym Orzaz Uchylające Dyrektywę 1999/93/WE, p. 2.

<sup>20</sup> Projekt Ustawy o Zmianie Ustawy o Usługach Zaufania Orzaz Identyfikacji Elektronicznej Orzaz Niektórych Innych Ustaw (2018) <<https://legislacja.rcl.gov.pl>>.

uproszczenie procedury logowania się do użycia uniwersalnego loginu oraz odpowiednio zabezpieczonego pakietu haseł. Węzeł docelowo będzie znajdował się pod adresem login.gov.pl. Krajowy Węzeł z założenia ma pośredniczyć w uwierzytelnianiu w obszarze krajowych usług online przy pomocy środków identyfikacji elektronicznej wydanych przez różne instytucje w obrębie systemów identyfikacji elektronicznej. Zgodę na przyłączenie systemu do Krajowego Węzła Identyfikacji Elektronicznej wydaje Minister Cyfryzacji. Decyzja ta oparta jest o spełnienie niezbędnych wymogów bezpieczeństwa rzetelnie udokumentowanych podmiotów zarówno publicznych jak i prywatnych<sup>21</sup>. Stworzenie węzła krajowego realizowane jest w ramach projektu finansowanego z budżetu państwa koordynowanego przez Ministerstwo Cyfryzacji we współpracy z Centralnym Ośrodkiem Informatyki<sup>22</sup>.

Cel, dla którego jest tworzony Transgraniczny Węzeł podobnie jak w przypadku Krajowego Węzła – ma poprawić dostępność do usług elektronicznych. Jednak zakres działania systemu będzie większy co pozwoli obywatelom Polski przy użyciu Profilu Zaufanego skorzystać z usług cyfrowych państw UE oraz obcokrajowcom krajów członkowskich na skorzystanie z polskich systemów usług elektronicznych (np. ePUAP, PUE ZUS) używając swojego loginu i hasła. Węzeł Transgraniczny będzie zintegrowany z pozostałymi systemami identyfikacji elektronicznej innych krajów Unii Europejskiej. Tylko notyfikowane (zatwierdzone pod względem bezpieczeństwa) systemy logowania będą dopuszczone do Węzła Transgranicznego<sup>23</sup>. W przypadku Polski jak dotąd jest to profil zaufany ePUAP. Instytucją prowadzącą projekt utworzenia Węzła Krajowego jest Ministerstwo Cyfryzacji przy współpracy z Państwowym Instytutem Badawczym NASK oraz Instytutem Maszyn Matematycznych<sup>24</sup>.

W Polsce równoległe z wdrażaniem Krajowego Węzła Identyfikacji Elektronicznej, prowadzone są prace nad Komercyjnym Węzłem Identyfikacji Elektronicznej tworzonym przez Krajową Izbę Rozliczeniową. Głównym zadaniem Węzła Komercyjnego będzie identyfikacja w komercyjnych usługach elektronicznych, natomiast dalsze plany przewidują integrację z

---

<sup>21</sup> Projekt Ustawy o Zmianie Ustawy o Usługach Zaufania Oraz Identyfikacji Elektronicznej Oraz Niektórych Innych Ustaw (2018) <<https://legislacja.rcl.gov.pl>>.

<sup>22</sup> Ministerstwo Cyfryzacji, *Budowa Krajowego Węzła Identyfikacji Elektronicznej* <<https://www.gov.pl/web/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej>> (dostęp 28.04.2018).

<sup>23</sup> Projekt Ustawy o Zmianie Ustawy o Usługach Zaufania Oraz Identyfikacji Elektronicznej Oraz Niektórych Innych Ustaw (2018) <<https://legislacja.rcl.gov.pl>>.

<sup>24</sup> Ministerstwo Cyfryzacji, *Budowa i wdrożenie Węzła Transgranicznego* <<https://www.gov.pl/web/cyfryzacja/budowa-i-wdrozenie-wezla-transgranicznego>> (dostęp 28.04.2018).



Krajowym Węzłem. Model, w którym do realizacji państwowych usług administracji publicznej dopuszczają się podmioty tworzące komercyjne Węzły lub jego elementy nazywany jest modelem federacyjnym. W procesie uwierzytelniania w usługach publicznych w pierwszej kolejności bierze udział węzeł krajowy, jednak dopuszczalny jest również węzeł komercyjny. Z kolei w usługach komercyjnych potwierdzenie tożsamości odbywa się wyłącznie za pomocą węzła komercyjnego. Takie rozwiązanie, nie powoduje niepotrzebnej konkurencji państwowych dostawców środków identyfikacji elektronicznej z komercyjnymi a dodatkowo w pewien (ograniczony) sposób państwo prowadzi kontrolę nad rynkiem dostawców usług komercyjnych<sup>25</sup>.

### 3. Usługi zaufania w ochronie zdrowia

W sektorze ochrony zdrowia usługi zaufania można podzielić na otwarte oraz zamknięte co umożliwia wytyczenie granicy działania nadzoru i wymagań wynikających z rozporządzenia eIDAS. Otwarte usługi zaufania rozumie się jako zestaw usług zaufania kierowanych do społeczeństwa (pacjentów), które mogą, ale nie muszą mieć wpływ na strony trzecie. Z kolei zamknięte usługi zaufania działają w obrębie określonej grupy, nie powodują skutków dla stron trzecich, oparte są o zamknięty system teleinformatyczny, poza nadzorem i mocą rozporządzenia eIDAS. Przykładem grupy stosującej zamknięte usługi zaufania są pracownicy administracji szpitala<sup>26,27</sup>. Potencjalne korzyści płynące z zastosowania usług zaufania:

- zawieranie umów o pracę przez środowisko online (np. z lekarzami, pielęgniarkami),
- podpisywanie nieskomplikowanych kontraktów na poziomie biznes – biznes (np. szpital – hurtownia),
- bezpieczeństwo formalnej korespondencji w wersji elektronicznej między obywatelem/pacjentem a instytucją publiczną,
- automatyczne (bez zbędnej zwłoki) wydawanie różnych zaświadczeń przez administrację publiczną (NFZ, ZUS),

<sup>25</sup> Accenture, Obserwatorium.biz, *Raport EID 2017, Elektroniczna Identyfikacja w Polsce 2017* <<https://www.accenture.com/pl-pl/event-eid-report-2017>> (dostęp 06.2018).

<sup>26</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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.

<sup>27</sup> A. Romaszewski et al., *Wprowadzenie usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej, część II*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2016, nr 42.

- odciążenie obecnej administracji dzięki usługom elektronicznego doręczenia,
- obsłużenie sporej części społeczeństwa za pomocą usług elektronicznych<sup>28</sup>.

Na chwilę obecną pracownik medyczny dysponuje trzema metodami podpisywania elektronicznego, a mianowicie przy użyciu podpisu potwierdzonego profilem zaufanym ePUAP, kwalifikowanego podpisu elektronicznego lub dzięki narzędziu udostępnionemu przez system teleinformatyczny Zakładu Ubezpieczeń Społecznych. Daje to możliwość specjalistom medycznemu podpisu:

- „elektronicznej dokumentacji medycznej;
- wniosku o dostęp do danych umożliwiających pobranie z SIM (Systemu Informacji Medycznej) elektronicznej dokumentacji medycznej lub danych z tych dokumentów, w zakresie niezbędnym do wykonywania badań diagnostycznych, zapewnienia ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze, środki spożywcze specjalnego przeznaczenia żywieniowego i wyroby medyczne;
- wniosku o dostęp do danych przetwarzanych w SIM umożliwiających wymianę między usługodawcami danych zawartych w elektronicznej dokumentacji medycznej” (art. 17 pkt 3)<sup>29</sup>.

#### **4. Planowane działania w ochronie zdrowia**

Poniższe rozważania będą dotyczyć przede wszystkim planów wprowadzania elektronicznego dowodu (eID) oraz Karty Ubezpieczenia Zdrowotnego (KUZ) jako narzędzi uwierzytelniania i identyfikacji, elektronicznej recepty (e-Recepty), elektronicznego skierowania (e-Skierowania) oraz usługi elektronicznych doręczeń (e-Doręczeń). Wszystkie te elementy są bardzo ważne i potrzebne dla rozwoju rynku usług cyfrowych oraz bezpieczeństwa danych w sektorze ochrony zdrowia.

W 26 krajach europejskich stosuje się rozwiązania oparte o elektroniczną identyfikację obywateli. Ministerstwo Cyfryzacji oraz Ministerstwo Spraw Wewnętrznych i Administracji obecnie podejmuje się już drugiej próby stworzenia takiego narzędzia – elektronicznego dowodu (e-Dowodu) w Polsce. Pierwsza próba w ramach finansowanego przez fundusz UE projektu „pl.ID” nie została zrealizowana w terminie i przedsięwzięcie wstrzymano. Druga

---

<sup>28</sup> Accenture, Obserwatorium.biz, *Raport. Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce 2017* <<https://www.accenture.com/pl-pl/insight-breakthrough-online-services>> (dostęp 06.2018).

<sup>29</sup> Ustawa z dnia 28 Kwietnia 2011 r. o Systemie Informacji w Ochronie Zdrowia (Dz.U. 2011 Nr 113 Poz. 657).

próba zakłada wprowadzenie pierwszego elektronicznego dowodu do końca marca 2019 roku. Proponowane narzędzie ma mieć formę dowodu osobistego (karty) z warstwą elektroniczną oraz służyć do uwierzytelniania w usługach cyfrowych administracji publicznej i służbie zdrowia w tym do podpisywania dokumentów elektronicznych<sup>30</sup>. Pierwotna koncepcja elektronicznego dowodu uległa zmianie. Za sprawą rozporządzenia eIDAS, które dodało dodatkowy rodzaj podpisu (zaawansowany podpis elektroniczny) oraz zaleciło neutralność technologiczną spowodowało to otwarcie się na szerszy obszar działań. Dzięki temu planuje się łatwiejsze podłączenie do Węzłów Elektronicznych. Dodatkowo rozważa się rozwiązania oparte o chmury obliczeniowe (*ang. cloud computing*) takie jak podpis serwerowy czy podpis „w locie”<sup>31</sup>. Ważne, że projektowany elektroniczny dokument zapewni uwierzytelnianie na poziomie wysokim w przypadku dostępu, zatwierdzenia lub podpisania danych medycznych wrażliwych przez pacjenta.

Dodatkowo obok e-Dowodu planuje się realizację osobnego projektu, koordynowanego przez Ministerstwo Zdrowia dotyczącego stworzenia Karty Ubezpieczenia Zdrowotnego (KUZ). Narzędzie to ma służyć do „potwierdzania obecności świadczeniobiorcy w określonym czasie i miejscu w ramach wykonywanych świadczeń opieki zdrowotnej lub potwierdzania wykonania świadczenia opieki zdrowotnej” (art. 1 ust 2), ponadto przewiduje się wykorzystanie karty do identyfikacji i uwierzytelniania w systemach informatycznych ochrony zdrowia. KUZ będzie zawierała dane potrzebne do uwierzytelniania oraz certyfikaty, w tym o najwyższym stopniu bezpieczeństwa kwalifikowany certyfikat elektroniczny zgodny z rozporządzeniem eIDAS. Ustawodawca dopuszcza, pełnienie funkcji KUZ również przez inne narzędzia takie jak wspomniany dowód osobisty z warstwą elektroniczną lub przez publiczną aplikację mobilną (aplikację na telefon, w której będą dostępne dokumenty identyfikacyjne w formie elektroniczne np. dowód osobisty, prawo jazdy – plany stworzenia zawarte w ustawie dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne<sup>32</sup>). Wydawanie Kart Ubezpieczenia Zdrowotnego dla wszystkich obywateli będzie zadaniem

---

<sup>30</sup> Ministerstwo Cyfryzacji, *Koncepcja E-Dowód – Kontynuacja Projektu Pl.ID i Realizacja Projektów Powiązanych. Załącznik 1 Opis Statusu Projektu Pl.ID*, <<https://www.gov.pl/>> (dostęp 06.2018).

<sup>31</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 910/2014 z dnia 23 Lipca 2014 r. w sprawie Identyfikacji Elektronicznej i Usług Zaufania w Odniesieniu Do Transakcji Elektronicznych Na Rynku Wewnętrznym Orzaz Uchylające Dyrektywę 1999/93/WE.

<sup>32</sup> Ustawa z dnia 17 Lutego 2005 r. o Informatyzacji Działalności Podmiotów Realizujących Zadania Publiczne (Dz.U. 2005 Nr 64 Poz. 565).

Narodowego Funduszy Zdrowia i ma zostać zrealizowane nie później niż od 1 lipca 2020 roku<sup>33</sup>.

Warto wspomnieć, że w planach jest również stworzenie Karty Specjalisty Medycznego (KSM). To potrzebne narzędzie, które ułatwiłoby pracownikom medycznym bezpieczne tworzenie i autoryzowane przesyłanie dokumentów elektronicznych takich jak e-zwolnienia, e-recepty i e-skierowania<sup>34</sup>.

E-Recepta rozumiana jako elektroniczna dokumentacja medyczna jest jednym z wielu elementów Projektu P1 realizowanego przez CSIOZ (Centrum Systemów Informacyjnych Ochrony Zdrowia). Wdrożenie na poziomie krajowym zaplanowano do roku 2020. Obecnie trwa około 7 miesięczny (start od połowy lutego 2018) pilotaż systemu e-Recepty w Siedlcach (woj. mazowieckie) i Skierniewicach (woj. łódzkie) w celu sprawdzenia efektywności systemu elektronicznego oraz zebrania opinii użytkowników. Korzyści płynące z wdrożenia e-Recepty to poprawa czytelności recept, gromadzenie i wykorzystanie recept w procesie leczenia, dostęp do historii wystawionych recept dla pacjenta przez Internetowe Konto Pacjenta. Dodatkowo przewiduje się, że dla systemu ochrony zdrowia wprowadzenie e-Recept uszczelni system obrotu lekami i poprawi jego kontrolę<sup>35</sup>.

Według planów wystawianie e-Skierowania będzie możliwe przez pracownika medycznego. Elektroniczne skierowanie będzie wysyłane przez podmiot wykonujący działalność leczniczą do Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych (platforma P1), pozostanie również możliwość wydruku skierowania przez danego usługodawcę. Działania możliwe w obrębie e-Skierowania to jego anulowanie, dodanie do dokumentacji medycznej, zmiana statusu realizacji oraz przeglądanie dokumentu zarówno przez pacjenta jak i usługodawcę. Świadczeniodawcy mają obowiązek wystawiania elektronicznych skierowań od 1 stycznia 2021 roku<sup>36</sup>.

<sup>33</sup> Projekt z dnia 1.06.2018 r. o Zmianie Ustawy o Świadczeniach Opieki Zdrowotnej Finansowanych Ze Środków Publicznych, p. 18 <<https://legislacja.rcl.gov.pl/projekt/12312303/katalog/12513763#12513763>>.

<sup>34</sup> A. Romaszewski, W. Trąbka, M. Kielar, K. Gajda, *Funkcjonowanie systemów identyfikacji i uwierzytelnienia w polskim systemie opieki zdrowotnej - stan obecny i kierunki zmian*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2017, nr 44.

<sup>35</sup> Centrum Systemów Informacyjnych Ochrony Zdrowia, *Pilotaż e-Recepty startuje w Siedlcach oraz Skierniewicach* <<https://www.csioz.gov.pl/aktualnosci/szczegoly/pilotaż-e-recepty-startuje-w-siedlcach-oraz-skierniewicach/>> (dostęp 28.04.2018).

<sup>36</sup> Centrum Systemów Informacyjnych Ochrony Zdrowia, *Opis Funkcjonalny Systemu P1 z Perspektywy Integracji Systemów Zewnętrznych*, Wyd. 1.1.2016 <[https://p1.csioz.gov.pl/fileadmin/user\\_upload/opis\\_funkcjonalny\\_systemu\\_p1\\_z\\_perspektywy\\_integracji\\_systemow\\_zew\\_5811ab8ee8e37.pdf](https://p1.csioz.gov.pl/fileadmin/user_upload/opis_funkcjonalny_systemu_p1_z_perspektywy_integracji_systemow_zew_5811ab8ee8e37.pdf)> (dostęp 06.2018).

Mając zapewnione narzędzia identyfikacji i uwierzytelniania (e-Dowód, KUZ), zaproponowane elektroniczne dokumenty, które będzie można przysyłać (e-Recepta, e-Skierowanie) potrzebna jest usługa gwarantująca bezpieczne dostarczenie informacji i skierowana do wszystkich zainteresowanych podmiotów – w tym obszarze planowana jest usługa elektronicznych doręczeń (e-Doręczeń).

Według unijnego ustawodawcy usługa rejestrowanego doręczenia elektronicznego (*ang. electronic registered delivery service*) „oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany (art. 3 pkt 36)<sup>37</sup>.

Kwalifikowana usługa rejestrowanego doręczenia elektronicznego obarczona jest następującym wymogami:

- świadczona przez minimum jednego kwalifikowanego dostawcę usług zaufania,
- zapewnia niepodważalną identyfikację nadawcy,
- uwierzytelnia adresata jeszcze przed przesłaniem danych,
- nadanie i otrzymanie danych jest zabezpieczone przez zaawansowany podpis lub pieczęć elektroniczną, co uniemożliwia manipulację danymi,
- nawet minimalna zmiana danych wymagająca wysłania lub otrzymania danych jest w sposób przejrzysty wskazana obu stronom procesy wymiany,
- cecha jak data i czas nadania, odbioru, zmiany są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu (art. 44 pkt 1)<sup>38</sup>.

W innych krajach europejskich pojawiły się już systemy informatyczne pełniące funkcję cyfrowej skrzynki pocztowej. Ciekawym rozwiązaniem w tym obszarze może się pochwalić Estonia. Każda osoba posiadająca estoński numer identyfikacyjny (odpowiednik PESEL) posiada możliwość założenia adresu e-mail w krajowym systemie, na który urzędy przesyłają swoim obywatelom ważne dokumenty poddane zaszyfrowaniu. Usługa ta jest uzupełniona o system DigiDoc służący do przechowywania, wymiany i podpisywania elektronicznych

---

<sup>37</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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.

<sup>38</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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.



dokumentów skierowany zarówno do obywateli, sektora prywatnego jak i publicznego. Zalogować się do systemu DigDoc można przy pomocy estońskiego dowodu osobistego z wbudowanym chipem lub mobilnego ID (obsługiwanego przez specjalną, dedykowaną kartę komórkową SIM). Użytkownicy mają możliwość wgrywania plików na serwer, podpisywania ich cyfrowo (przy pomocy karty) i wysłania (np. korzystając z narodowego adresu e-mail). Używanie podpisów elektronicznych daje Estonii oszczędność 2% PKB rocznie<sup>39</sup>.

Ministerstwo Cyfryzacji w ramach projektów indykatywnych Programu Operacyjnego Polska Cyfrowa przygotowało projekt stworzenia e-Doręczenia w okresie 2018-2020 roku jako uniwersalnej usługi zaufania świadczonej przez zaufaną stronę trzecią dostawcy usług rejestrowanego doręczenia elektronicznego (proponycja współpracy z platformą Envelo – Poczty Polskiej). Z e-Doręczeń będzie mógł skorzystać każdy: zarówno obywatel, jak i przedsiębiorca, którzy z dniem złożenia deklaracji przystąpienia do usługi e-Doręczenia będą mogli wymagać od podmiotów sektora publicznego komunikacji w postaci elektronicznej (również podmiotów wykonujących działalność publiczną w tym szpitali)<sup>40</sup>.

Korzyści z zastosowania e-Doręczenia to m.in., niższe koszty obsługi w porównaniu do tradycyjnej (papierowej) korespondencji, większy dostęp do usług (dostęp z każdego miejsca z połączeniem internetowym), bezpieczeństwo i pewność dostarczenia (szyfrowanie danych, archiwizacja dokumentów) oraz skutki prawne identyczne jak w przypadku oryginału wysłanego listem rejestrowanym<sup>41</sup>. Dodatkowo zaletą jest wysoka integralność dostarczanej treści i podpisywanie całej treści wiadomości dając gwarancję wiarygodności i bezpieczeństwa. Budowany w ten sposób standard doręczeń elektronicznych ma szansę przyczynić się do rozbudowy rynku dla dostawców usług zaufania<sup>42</sup>.

## 5. Problemy z nowymi rozwiązaniami

Już teraz w fazie prób wprowadzania nowych rozwiązań pojawiają się pewne bariery i problemy. W projekcie ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji

---

<sup>39</sup> Instytut Poczty, *Cyfryzacja Usług Publicznych w Europie, Rola Operatorów Poczty, Model Dla Polski* <[http://instytutpoczty.pl/files/raport\\_instytut\\_poczty.pdf](http://instytutpoczty.pl/files/raport_instytut_poczty.pdf)> (dostęp 06.2018).

<sup>40</sup> Ministerstwo Cyfryzacji, *e-Doręczenia - usługa rejestrowanego doręczenia elektronicznego w Polsce* <[/cyfryzacja/e-doreczenia-usluga-rejestrowanego-doreczenia-elektronicznego-w-polsce](#)> (dostęp 25.06.2018).

<sup>41</sup> K. Piskorski, *E-Skrzynka i e-Doręczenie, Możliwy Scenariusz Dla Polski*, Instytut Poczty, 2017.

<sup>42</sup> K. Okoński, *E-Doręczenia – Usługa Rejestrowanego Doręczenia Elektronicznego w Polsce*, Ministerstwo Cyfryzacji, 06.2018.

elektronicznej oraz niektórych innych ustaw (projekt 2018)<sup>43</sup>, ustawodawca chce dopuścić cyfrowe narzędzie Zakładu Ubezpieczeń Społecznych stosowane do podpisywania e-Zwolnień. Metoda ta funkcjonuje w zamkniętym systemie obiegu informacji do uwierzytelniania elektronicznej dokumentacji medycznej, natomiast w przypadku e-Recept mamy do czynienia z otwartym systemem. Tworzy się tym samym trzecia forma potwierdzania tożsamości obok profilu zaufanego ePUAP oraz Podpisu Kwalifikowanego. Różnica polega jednak na tym, że narzędzie uwierzytelniania ZUS nie spełnia wymogów bezpieczeństwa rozporządzenia eIDAS i nie powinno być stosowane jako powszechna metoda do podpisywania dokumentów elektronicznych, na zewnątrz instytucji, jak w przypadku e-recept.

Inny problem dotyczy tego, że w projekcie ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (projekt 2018) wyraźnie podkreślono, że podpis działający w ramach profilu zaufanego ePUAP nie jest zaawansowanym podpisem elektronicznym, zatem wymagania i kryteria rozporządzenia eIDAS nie są spełnione<sup>44</sup>. Oznacza to, że podpis potwierdzony profilem zaufanym ePUAP pomimo, że daje możliwość realizacji szerokiego zakresu krajowych usług administracyjnych to nie może być używany w usługach cyfrowych, publicznych poza Polskę<sup>45,46</sup>. Stwarza to barierę użycia polskich narzędzi podpisu elektronicznego w innych krajach członkowskich, ponieważ podpisane dokumenty elektronicznego przy użyciu publicznego klucza nie będą ważne. Powstaje zatem luka w usługach zaufania oferowanych przez instytucje publiczne, które są odpowiedzialne za stworzenie spełniającego standardy unijne narzędzia podpisu elektronicznego.

## Podsumowanie

Pomimo szeregu regulacji krajowych oraz międzynarodowych istnieje swoboda w procesie tworzenia systemów identyfikacji i usług zaufania głównie dzięki zasadzie neutralności technologicznej co z jednej strony mobilizuje do innowacyjności, ale z drugiej utrudnia koordynację systemów teleinformatycznych. W procesie tworzenia technik

---

<sup>43</sup> Projekt Ustawy o Zmianie Ustawy o Usługach Zaufania Oraz Identyfikacji Elektronicznej Oraz Niektórych Innych Ustaw (2018) <<https://legislacja.rcl.gov.pl>>.

<sup>44</sup> M. Marucha-Jaworska, *Rozporządzenie EIDAS: Zagadnienia Prawne i Techniczne*, Wyd. 1, Wolters Kluwer Polska, Warszawa 2017.

<sup>45</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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.

<sup>46</sup> Accenture, Obserwatorium.biz, *Raport. Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce 2017* <<https://www.accenture.com/pl-pl/insight-breakthrough-online-services>> (dostęp 06.2018).

identyfikacji i uwierzytelniania główną rolę odgrywa prawo międzynarodowe. Ramy otwartości stworzone przez prawodawcę mają za zadanie zachęcać prywatne firmy do współpracy z publicznymi instytucjami w zakresie metod, narzędzi i technik identyfikacji oraz uwierzytelniania w ochronie zdrowia. Dodatkowo istnieje potencjał otwarcia rynków krajów europejskich (również rynków medycznych) dzięki cyfryzacji usług. Niestety w Polsce w obszarze narzędzi identyfikacji i uwierzytelniania nadal nie ma jasno opracowanego jednolitego systemu funkcjonalnego a potencjał usług zaufania nie jest jeszcze w pełni wykorzystany w ochronie zdrowia. Polska powinna sugerować się dobrymi praktykami funkcjonowania systemów identyfikacji elektronicznej z innych krajach podczas tworzenia własnego modelu.

## Literatura

- [1] Accenture, Obserwatorium.biz, *Raport. Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce 2017* <<https://www.accenture.com/pl-pl/insight-breakthrough-online-services>> (dostęp 06.2018).
- [2] Accenture, Obserwatorium.biz, *Raport EID 2017, Elektroniczna Identyfikacja w Polsce 2017* <<https://www.accenture.com/pl-pl/event-eid-report-2017>> (dostęp 06.2018).
- [3] Accenture, Obserwatorium.biz, *Raport. Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce 2017* <<https://www.accenture.com/pl-pl/insight-breakthrough-online-services>> (dostęp 06.2018).
- [4] Cabańska D., Biniek K., *Węzeł Krajowy. Ministerstwo Cyfryzacji. Centralny Ośrodek Informatyki*, <<https://www.gov.pl/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej>> (dostęp 06.2018).
- [5] Centrum Systemów Informacyjnych Ochrony Zdrowia, *Opis Funkcjonalny Systemu P1 z Perspektywy Integracji Systemów Zewnętrznych*, Wyd. 1.1.2016 <[https://p1.csioz.gov.pl/fileadmin/user\\_upload/opis\\_funkcjonalny\\_systemu\\_p1\\_z\\_perspektywy\\_integracji\\_systemow\\_zew\\_5811ab8ee8e37.pdf](https://p1.csioz.gov.pl/fileadmin/user_upload/opis_funkcjonalny_systemu_p1_z_perspektywy_integracji_systemow_zew_5811ab8ee8e37.pdf)> (dostęp 06.2018).
- [6] Centrum Systemów Informacyjnych Ochrony Zdrowia, *Pilotaż e-Recepty startuje w Siedlcach oraz Skierniewicach* <<https://www.csioz.gov.pl/aktualnosci/szczegoly/pilotaz-e-recepty-startuje-w-siedlcach-oraz-skierniewicach/>> (dostęp 28.04.2018).
- [7] Instytut Poczty, *Cyfryzacja Usług Publicznych w Europie, Rola Operatorów Poczty, Model Dla Polski* <[http://instytutpoczty.pl/files/raport\\_instytut\\_poczty.pdf](http://instytutpoczty.pl/files/raport_instytut_poczty.pdf)> (dostęp 06.2018).
- [8] Jakubowski Sz., *Identyfikacja i Uwierzytelnianie Podmiotów Orzaz Dokumentów Elektronicznych w Ochronie Zdrowia* (Praca wykonana w Zakładzie Medycznych Systemów Informacyjnych, Instytut Zdrowia Publicznego, UJ CM, 2018).
- [9] Komisja Unii Europejskiej, *Załącznik Specyfikacje Techniczne i Procedury Dotyczące Niskiego, Średniego i Wysokiego Poziomu Zaufania w Odniesieniu Do Środka Identyfikacji Elektronicznej Wydanego w Ramach Notyfikowanego Systemu Identyfikacji Elektronicznej* <<https://eur-lex.europa.eu>>.

- [10] Marucha-Jaworska M., *Rozporządzenie EIDAS: Zagadnienia Prawne i Techniczne*, Wyd. 1, Wolters Kluwer Polska, Warszawa 2017.
- [11] Ministerstwo Cyfryzacji, *Budowa Krajowego Węzła Identyfikacji Elektronicznej* <<https://www.gov.pl/web/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej>>.
- [12] Ministerstwo Cyfryzacji, *Budowa i wdrożenie Węzła Transgranicznego* <<https://www.gov.pl/web/cyfryzacja/budowa-i-wdrozenie-wezla-transgranicznego>>.
- [13] Ministerstwo Cyfryzacji, *e-Doręczenia - usługa rejestrowanego doręczenia elektronicznego w Polsce* </cyfryzacja/e-doreczenia-usluga-rejestrowanego-doreczenia-elektronicznego-w-polsce> (dostęp 25.06.2018).
- [14] Ministerstwo Cyfryzacji, *Koncepcja E-Dowód – Kontynuacja Projektu Pl.ID i Realizacja Projektów Powiązanych. Załącznik 1 Opis Statusu Projektu Pl.ID*, <<https://www.gov.pl/>> (dostęp 06.2018).
- [15] Okoński K., *E-Doręczenia – Usługa Rejestrowanego Doręczenia Elektronicznego w Polsce*, Ministerstwo Cyfryzacji, 06.2018.
- [16] Piskorski K., *E-Skrzynka i e-Doręczenie, Możliwy Scenariusz Dla Polski*, Instytut Poczty, 2017.
- [17] Projekt Ustawy o Zmianie Ustawy o Usługach Zaufania Oraz Identyfikacji Elektronicznej Oraz Niektórych Innych Ustaw (2018) <<https://legislacja.rcl.gov.pl/>>.
- [18] Projekt z dnia 1.06.2018 r. o Zmianie Ustawy o Świadczeniach Opieki Zdrowotnej Finansowanych Ze Środków Publicznych, p. 18 <<https://legislacja.rcl.gov.pl/projekt/12312303/katalog/12513763#12513763>>.
- [19] Romaszewski A. et al., *Identyfikacja i Uwierzytelnienie w Systemie Informacyjnym Opieki Zdrowotnej Po Wprowadzeniu Rozporządzenia UE EIDAS*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2016, nr 42.
- [20] Romaszewski A. et al., *Wprowadzenie usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej, część II*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2016, nr 42.
- [21] Romaszewski A., Trąbka W., Kielar M., Gajda K., *Funkcjonowanie systemów identyfikacji i uwierzytelnienia w polskim systemie opieki zdrowotnej - stan obecny i kierunki zmian*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie” 2017, nr 44.
- [22] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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.
- [23] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 Kwietnia 2016 r. w Sprawie Ochrony Osób Fizycznych w Związku z Przetwarzaniem Danych Osobowych i w Sprawie Swobodnego Przepływu Takich Danych Oraz Uchylenia Dyrektywy 95/46/WE (Ogólne Rozporządzenie o Ochronie Danych), p. 679 <<https://eur-lex.europa.eu>>.
- [24] Ustawa z dnia 5 Września 2016 r. o Usługach Zaufania oraz Identyfikacji Elektronicznej (Dz.U. 2016 Poz. 1579) <<http://prawo.sejm.gov.pl>>.
- [25] Ustawa z dnia 10 Maja 2018 r. o Ochronie Danych Osobowych (Dz.U. 2018 Poz. 1000) <<http://prawo.sejm.gov.pl>>.
- [26] Ustawa z dnia 17 Lutego 2005 r. o Informatyzacji Działalności Podmiotów Realizujących Zadania Publiczne (Dz.U. 2005 Nr 64 Poz. 565) <<http://prawo.sejm.gov.pl>>.



- [27] Ustawa z dnia 18 Lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204).
- [28] Ustawa z dnia 28 Kwietnia 2011 r. o Systemie Informacji w Ochronie Zdrowia (Dz.U. 2011 Nr 113 Poz. 657) <<http://prawo.sejm.gov.pl>>.
- [29] Ustawa z dnia 17 Lutego 2005 r. o Informatyzacji Działalności Podmiotów Realizujących Zadania Publiczne (Dz.U. 2005 Nr 64 Poz. 565).

### ***Streszczenie***

Rozporządzenie eIDAS jest jedną z ważniejszych regulacji, której rozwiązania są kluczowe dla systemu ochrony zdrowia. Jego podstawowym zadaniem jest zwiększenie zaufania do transakcji elektronicznych, przy zapewnieniu wspólnej podstawy bezpiecznych interakcji elektronicznych między obywatelami, przedsiębiorstwami i organami publicznymi. Jest to niezwykle ważne w ochronie zdrowia, gdzie następuje stała wymiana informacji między pacjentami, świadczeniodawcami, a podmiotami prawnie upoważnionymi do otrzymywania informacji zdrowotnych.

Przedstawiono główne założenia i rozwiązania przyjęte w regulacjach, a więc zarówno uregulowania dotyczące identyfikacji podmiotów, jak i zastosowania usług zaufania w bieżącej pracy podmiotów leczniczych.

Mając zapewnione narzędzia identyfikacji i uwierzytelniania (e-Dowód), zaproponowane elektroniczne dokumenty, które będzie można przysyłać (e-Recepta, e-Skierowanie) potrzebna jest usługa gwarantująca bezpieczne dostarczenie informacji i skierowana do wszystkich zainteresowanych podmiotów – w tym obszarze planowana jest usługa elektronicznych doręczeń (e-Doręczeń).

Pomimo szeregu regulacji krajowych oraz międzynarodowych istnieje swoboda w procesie tworzenia systemów identyfikacji i usług zaufania głównie dzięki zasadzie neutralności technologicznej co z jednej strony mobilizuje do innowacyjności, ale z drugiej utrudnia koordynację systemów teleinformatycznych. W procesie tworzenia technik identyfikacji i uwierzytelniania główną rolę odgrywa prawo międzynarodowe.

### ***Słowa kluczowe***

eIDAS, identyfikacja elektroniczna, uwierzytelnienie, usługi zaufania, krajowy schemat identyfikacji elektronicznej, ochrona zdrowia