Zdrowie Publiczne i Zarządzanie 2022; 20 (4): 148–153
https://www.ejournals.eu/czasopisma/zdrowie-publiczne-i-zarzadzanie, doi:10.4467/20842627OZ.22.022.19351

Informatyzacja systemu ochrony zdrowia – problemy i wyzwania. Część I

Artur Romaszewski https://orcid.org/0000-0003-3416-716X
Szczepan Jakubowski https://orcid.org/0000-0001-6419-9686
Mariusz Duplaga https://orcid.org/0000-0001-6963-8414

Zakład Promocji Zdrowia i e-Zdrowia, Instytut Zdrowia Publicznego, Wydział Nauk o Zdrowiu, Uniwersytet Jagielloński Collegium Medicum

Adres do korespondencji: Artur Romaszewski, Zakład Promocji Zdrowia i e-Zdrowia, Instytut Zdrowia Publicznego, ul. Skawińska 8, 31-066 Kraków, Polska, artur.romaszewski@uj.edu.pl

Abstract

Healthcare digitalisation – issues and challanges. Part I

The ongoing development of information and communications technology (ICT) is forcing the EU legislation to implement a modern legal framework (eIDAS 2.0) for emerging new services. In the case of trust services, neither electronic seals nor maintenance service for the electronic signatures and seals used to sign medical records in electronic format have been implemented in the Polish healthcare system so far. The European Digital Identity Wallet (EDIW) is expected to become a new European electronic identification method with potential in a cross-border healthcare. The integrated electronic identification method is intended to facilitate and streamline the identification process in different European countries, which is particularly important when using online services such as e-banking or e-government (in healthcare). Healthcare entities should ensure that procedures and tools for identifying individuals comply with current regulations and quality standards.

Słowa kluczowe: informatyzacja, ochrona zdrowia, usługi zaufania, eIDAS 2.0

Key words: computerization, healthcare, trust services, eIDAS 2.0

Wprowadzenie

Nowe technologie wdrażane w ochronie zdrowia mają na celu zarówno usprawnienie pracy podmiotów świadczących usługi zdrowotne, jak i ułatwienie korzystania z tych usług pacjentom. W ostatnich latach w odpowiedzi na rekomendacje Unii Europejskiej (UE) i przyjęte w ślad za nimi krajowe regulacje w Polsce wdrożono wiele nowych rozwiązań odnoszących się do korzystania z systemów informatycznych w ochronie zdrowia.

Ciągły rozwój technologii informacyjno-komunikacyjnych (*information and communications technology*, ICT) obliguje UE do ustanawiania nowoczesnych ram prawnych dla nowych rozwiązań wspomagających bezpieczną komunikację i wymianę danych między podmiotami uprawnionymi do otrzymywania danych o zrealizowanych świadczeniach zdrowotnych.

Przykładami wykorzystania takich rozwiązań implementowanych do polskiej ochrony zdrowia są usługi zaufania (*trust services*) – usługi elektroniczne o dedykowanym znaczeniu w identyfikacji elektronicznej. Możemy dostrzec ich zastosowanie w elektronicznej dokumentacji medycznej czy też ustalaniu tożsamości pacjentów poprzez logowanie do systemu Internetowego Konta Pacjenta. Logując się do IKP, można posłużyć się profilem zaufanym, stanowiącym jedną z metod elektronicznego potwierdzenia tożsamości [1].

Artykuł ten jest pierwszą z dwóch publikacji osadzonych w tematyce informatyzacji systemu ochrony zdrowia. Pierwszy artykuł poświęcony jest problematyce usług zaufania, np. tworzeniu, weryfikacji i walidacji podpisów i pieczęci elektronicznych [2]. Autorzy omawiają wybrane zagadnienia związane z wdrożeniem usług zaufania, wprawdzie od dawna uregulowanych, lecz nie w pełni

wykorzystywanych w praktyce, np. pieczęci elektronicznej. Omówione zostaną również nowe projekty UE zawarte w tzw. rozporządzeniu eIDAS (Electronic Identification, Authentication and Trust Services) 2.0 z szerszym opisaniem portfela cyfrowej tożsamości [3]. Natomiast w drugim artykule omówiona zostanie problematyka wykorzystania chmury obliczeniowej w ochronie zdrowia w aspekcie nowych regulacji UE, obowiązujące i przygotowywane regulacje dotyczące obszaru sztucznej inteligencji (*artificial intelligence*) oraz rozszerzone zadania rejestrów medycznych w kontekście regulacji dotyczących jakości w ochronie zdrowia.

Perspektywa krajowa usług zaufania

Znaczna liczba usług medycznych świadczonych na rzecz pacjenta wymaga przygotowania odpowiednich procedur i narzędzi zapewniających prawidłową identyfikację podmiotów w nich uczestniczących. Dotyczy to zarówno komunikacji pracowników ochrony zdrowia z pacjentem, jak i korzystania z zasobów danych (m.in. rejestrów medycznych) w codziennej działalności podmiotów leczniczych. Prawidłowa identyfikacja musi być również zachowana przy przekazywaniu raportów do Narodowego Funduszu Zdrowia (NFZ), systemu informacyjnego w ochronie zdrowia oraz w trakcie przetwarzania danych pacjentów udostępnionych zgodnie z przepisami prawa w Systemie Informacji Medycznej [1].

Elektroniczne potwierdzanie tożsamości pacjenta (w tym użycie podpisu elektronicznego) może stanowić trudność dla systemów teleinformatycznych obsługujących szpitale i inne podmioty lecznicze, szczególnie w zakresie uzyskiwania wymaganych prawem zgód i oświadczeń pacjenta [4]. Dotyczy to m.in. podpisywania przez pacjentów dokumentów niezbędnych do przeprowadzania zabiegów operacyjnych oraz metod leczenia i diagnostyki stwarzających podwyższone ryzyko dla pacjenta [4]. W praktyce dokumenty te są często gromadzone tylko w postaci papierowej. Niedostępność postaci elektronicznej tych dokumentów koliduje z zasadami przewidzianymi w Rozporządzeniu o dokumentacji medycznej [5]. Obecnie Ministerstwo Zdrowia zapowiada pilotaż podpisu biometrycznego (tzw. tabletowego – z użyciem urządzenia mobilnego do składania podpisu), który ma przynieść przynajmniej częściowe rozwiązanie tego problemu [6].

Warto dodać, że istnieje możliwość podpisywania dokumentów elektronicznych za pomocą dowodu osobistego (wydanego po 2019 r.) z warstwą elektroniczną (chipem), natomiast wymaga to oprócz stosownego oprogramowania (aplikacja eDO App) wykupienia podpisu kwalifikowanego przez użytkownika. Nie ma prawnego obowiązku zapewniającego warunki do używania takich podpisów, więc lista instytucji, w tym podmiotów medycznych, stosujących tego typu rozwiązania jest ograniczona [7].

Ze względu na złożoność procesu rozwiązania techniczne umożliwiające ustalanie tożsamości osób tworzących dokumentację medyczną nie są łatwe w obsłudze. Wynika to w dużym stopniu z trudności w posługiwaniu się dopuszczonymi prawem podpisami elektronicznymi w sektorze ochrony zdrowia (kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych) [1].

W związku z tym nasuwa się pytanie, czy na etapie tworzenia, archiwizowania i przekazywania dokumentów w postaci elektronicznej można zastosować inne, alternatywne rozwiązania. Takim rozwiązaniem mogłoby być wykorzystanie wewnętrznych mechanizmów systemu teleinformatycznego[1]. Najczęściej wykorzystywane podpisy elektroniczne dostarczane są przez dostawców oprogramowania służącego do prowadzenia elektronicznej dokumentacji medycznej. Tak przygotowany podpis jest definiowany przez jego cechy *sine qua non*, tj. zapewnienie autentyczności wytworzonego dokumentu (podpis musi uniemożliwiać nieuprawnioną ingerencję w treść dokumentu) [8].

Poważnym problemem, dotąd nierozwiązanym, jest brak wdrożenia w ochronie zdrowia zarówno pieczęci elektronicznych [9], jak i usługi konserwacji podpisów i pieczęci elektronicznych używanych przy podpisywaniu dokumentacji medycznej w postaci elektronicznej (opisanych w Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz.U. 2016 poz. 1579) [10]. Przykładowo, brakuje uregulowania sytuacji, w której lekarz nie przedłuży certyfikatu gwarantującego ważność podpisu elektronicznego po przejściu na emeryturę. Nie ma pewności, czy wtedy można posługiwać się taką dokumentacją. Brakuje też regulacji pozwalających na używanie pieczęci elektronicznej w dokumentacji medycznej. Takie rozwiązanie mogłoby zapewnić autentyczność wytworzonego dokumentu oraz usprawnić przekazywanie dokumentów tworzonych w podmiocie leczniczym do pacjentów i innych upoważnionych podmiotów. Pewne rozwiązania mogą się pojawić w najbliższym czasie w wyniku pracy grupy roboczej ds. rejestrów rozproszonych i *blockchain*, która podjęła się przygotowania koncepcji wykorzystania pieczęci elektronicznej [11].

Powszechne stosowanie usług zaufania, szczególnie w aspekcie identyfikacji elektronicznej, jeszcze bardziej zyska na znaczeniu w związku z wejściem w życie ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320) [12]. Przepisy prawne nałożą obowiązek wdrożenia, w stosunkowo krótkim czasie, rozwiązań umożliwiających przejście z korespondencji papierowej na bezpieczną i szybką korespondencję elektroniczną.

Perspektywa europejska: rozporządzenie eIDAS 2.0 oraz tożsamość cyfrowa

Rozporządzenie eIDAS 2.0

Wraz z rozwojem rynku cyfrowego o charakterze globalnym wzrasta zapotrzebowanie na nowe, **bezpieczne** i rozpoznawalne we wszystkich krajach UE rozwiązania identyfikacji elektronicznej osób oraz podmiotów [13]. Dlatego też w rozporządzeniu eIDAS 2.0 [3] (nowelizacja

eIDAS 1.0 z 2014 r. [2]) rozszerzono obecny wykaz usług zaufania o nowe kwalifikowane usługi[2]. Zaliczamy do nich: archiwizację elektroniczną, kwalifikowane rejestry elektroniczne oraz zarządzanie zdalnymi urządzeniami do składania podpisów elektronicznych i pieczęci [3].

Głównym celem nowych przepisów eIDAS 2.0 jest zapewnienie obywatelom uniwersalnego narzędzia umożliwiającego usprawnienie procesu identyfikacji elektronicznej na terenie UE. Ma to szczególne znaczenie w przypadku korzystania z usług online, takich jak e-bankowość czy e-administracja (także w ochronie zdrowia). Proponowanym rozwiązaniem mającym spełnić te oczekiwania jest Europejski Portfel Cyfrowej Tożsamości (*European digital identity wallet*, EDIW) [3].

Nowe przepisy w zakresie tożsamości cyfrowej oznaczają zharmonizowane podejście do proponowanych rozwiązań, oparte na wspólnej architekturze technicznej i normach, które mają powstać we współpracy między krajami członkowskimi. *Novum* jest wydawanie elektronicznych poświadczeń atrybutów (zestawu danych jednoznacznie reprezentujących osobę/podmiot) przez kwalifikowanych dostawców do tego upoważnionych [3].

Proces identyfikacji elektronicznej wpisuje się w program Komisji Europejskiej „Droga ku cyfrowej dekadzie" („The Digital Decade Policy Programme 2030") realizowany do 2030 r. [14, 15]. Wśród istotnych celów pozwalających osiągnąć europejską tożsamość cyfrową wskazano w nim dostępność wszystkich kluczowych usług publicznych online, w tym powszechny dostęp do elektronicznej dokumentacji medycznej. Ponadto przyjęto, że do 2030 r. 80% obywateli w wieku 16–74 lat powinno korzystać z identyfikacji elektronicznej [15]. W 2023 r. nastąpiła pierwsza – i jak do tej pory jedyna – ocena realizacji tego programu. W raporcie z ewaluacji znalazła się informacja, że posiadanie co najmniej jednego systemu identyfikacji elektronicznej zgodnego z rozporządzeniem eIDAS zgłosiło 21 państw UE. Ponadto poziom ucyfrowienia usług publicznych dla obywateli wyniósł 77 pkt. (na 100); natomiast wskaźnik dostępności do elektronicznej dokumentacji medycznej wyniósł 72 pkt. (na 100) [16].

Z punktu widzenia rozważań na temat znaczenia rozporządzenia eIDAS 2.0 dla systemu ochrony zdrowia istotne znaczenie ma uruchomienie w kwietniu 2023 r. 4 projektów pilotażowych współfinansowanych w ramach Programu Cyfrowa Europa, mających na celu przetestowanie portfela cyfrowej tożsamości w wielu codziennych sytuacjach i jego integrację z krajowymi systemami identyfikacji elektronicznej w 26 państwach członkowskich oraz Islandii, Norwegii i Ukrainie [16].

W ramach projektu „Potential" [17] (jednego z czterech projektów pilotażowych) Grupa Deutsche[3] ma przeprowadzić testy tożsamości cyfrowej podczas aktywacji umowy z operatorem i bezpiecznego odblokowania karty SIM. Testy są zaplanowane w Niemczech, Francji, Austrii, Polsce, Holandii, Grecji, Ukrainie i potrwają do końca 2024 r. [18]. W podsumowaniu raportu znalazły się też zalecenia dotyczące zwiększenia liczby połączonych podmiotów świadczących opiekę zdrowotną, zakresu dostępnych danych oraz wykorzystania uwierzytelniania w usługach dostępu do danych zdrowotnych [16].

Koncepcja portfela cyfrowej tożsamości

Centralne przechowywanie danych umożliwiających identyfikację może być problematyczne, czyniąc dostawców tożsamości elektronicznej atrakcyjnym celem cyberataków [19]. Ryzyko to jest mniejsze w schemacie skoncentrowanym na użytkowniku. Zamiast przechowywać dane o tożsamości u jego dostawcy, dane te mogą być przechowywane na nośniku użytkownika, np. na karcie elektronicznej lub smartfonie. Gdy zajdzie taka potrzeba, wymagane informacje o tożsamości byłyby pobierane z tych nośników i przekazywane do żądającego dostawcy usług w procesie uwierzytelniania [19]. Posiadanie przez użytkownika pełnej fizycznej kontroli nad swoimi danymi daje temu schematowi przewagę pod względem prywatności [20]. Narzędziem spełniającym wymagania schematu skoncentrowanego na użytkowniku jest portfel cyfrowy (*digital wallets*). Pomimo że nie ma uniwersalnej definicji portfela cyfrowego [21], to może być on rozumiany jako aplikacja (oprogramowanie) umożliwiająca użytkownikom wygodne przechowywanie, zarządzanie i wykorzystywanie różnych zasobów cyfrowych, takich jak dane osobowe, informacje o płatnościach i dane uwierzytelniające [22]. W portfelach cyfrowych dostrzeżono potencjał rozwiązania kwestii zarządzania identyfikacją (*identity-management*, IdM) [23], tworząc z niego portfel cyfrowej tożsamości, który korzysta z modelu niezależnej tożsamości elektronicznej (*self-sovereign identity model*, SSI) [24]. Model ten zakłada autonomiczność i skoncentrowanie na użytkowniku. Zamiast polegać na scentralizowanym systemie służącym do uwierzytelnienia użytkowników, model SSI umożliwia zarejestrowanym na użycie środka identyfikacji elektronicznej[4] bezpośrednio i bez limitu [24]. Co więcej, model SSI pozwala użytkownikom samodzielne tworzyć nowe poświadczenia, np. przez dodanie samodzielnie elektronicznego dokumentu lub certyfikatu [24].

W przeglądzie systematycznym Podgorelec i wsp. [19] zbadali główne motywacje oraz funkcje portfeli cyfrowej tożsamości. Na podstawie uzyskanych danych zidentyfikowano 2 środowiska, w których działały portfele cyfrowe – lokalne i zdalne. W środowisku lokalnym użytkownik kontrolował i posiadał wymaganą infrastrukturę, np. urządzenie mobilne. Z kolei w środowisku zdalnym – zwanym również środowiskiem chmury (*cloud environment*) – infrastruktura portfela nie była własnością użytkownika i nie była zarządzana bezpośrednio przez niego, ale przez dostawcę zewnętrznego, np. firmę informatyczną. Najczęstszym IdM było SSI na urządzeniach mobilnych lub opartych na rozwiązaniach chmurowych, rzadziej użyte modele to: centralny, scentralizowany na użytkowaniu, federalny oraz jako usługa (*as a service*). Autorzy doszli do wniosku, że główną motywacją do zastosowania portfeli było uniknięcie centralizacji danych związanych z tożsamością cyfrową, zwiększenie bezpieczeństwa i prywatności danych, zapewnienie kontroli, ale i powierzenie odpowiedzialności użytkownikom oraz ułatwienie korzystania z tożsamości cyfrowych. We wszystkich badaniach użytych w przeglądzie zidentyfikowano następujące 3 główne cechy portfela cyfrowego dotyczące tożsamości cyfrowej: przechowywanie, zarządzanie i udostępnianie danych związanych

z tożsamością. Rzadziej pojawiające się cechy portfeli to: przechowywanie informacji kryptograficznych, łączenie danych związanych z tożsamością oraz możliwość odzyskiwania i tworzenia kopii zapasowych danych [19].

Jak wynika z badań potrzeb i preferencji użytkowników dotyczących portfela cyfrowej tożsamości, priorytetowo traktowana jest użyteczność, przedkładana nad bezpieczeństwo i prywatność [25]. Prosta i praktyczna aplikacja (oprogramowanie) była wskazywana jako ważna cecha portfela cyfrowej tożsamości. Okazało się również, że dla użytkowników ważne jest, aby narzędzia zapewniające bezpieczeństwo użytkowania, takie jak środki ochronne w przypadku nieautoryzowanego dostępu lub kradzieży informacji, były wbudowane w portfel. Eksperci objęci badaniem podkreślili, że różne warunki społeczno-kulturowe krajów i wynikający z nich poziom zaufania (do nowych technologii) może stanowić potencjalne wyzwania, jeśli chodzi o powszechne stosowanie portfela cyfrowej tożsamości w Europie [25].

Inni autorzy wskazali na potencjalne bariery w uruchomieniu portfeli cyfrowej tożsamości. Według nich brak odpowiednich standardów (np. wspólnych specyfikacji danych i standardów ich wymiany) oraz brak wspólnego, publiczno-prywatnego zarządzania (w przypadku braku wzajemnego zaufania tych dwóch sektorów) mogą stanowić główne przeszkody dla implementacji portfeli cyfrowej tożsamości [21].

W literaturze pojawiają się różne koncepcje portfeli cyfrowej tożsamości. Przykład takiego rozwiązania wraz z etapami dodania środka identyfikacji elektronicznej przedstawiono na rysunku 1.

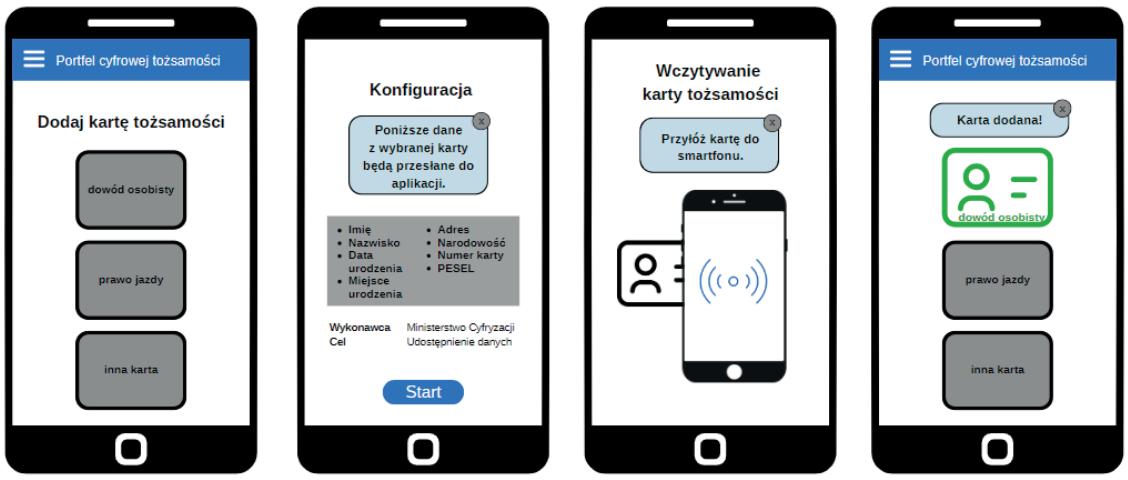
Europejski Portfel Cyfrowej Tożsamości

Europejski Portfel Cyfrowej Tożsamości wg eIDAS 2.0 ma stać się nowym europejskim środkiem identyfikacji elektronicznej. Wdrożenie EDIW w swoim założeniu ma:

- stanowić niezależny od obecnie stosowanych środek identyfikacji elektronicznej, do którego uznawania mają zostać zobowiązane nie tylko podmioty prywatne, ale także wszystkie podmioty publiczne,
- wprowadzić domniemanie, że kwalifikowane elektroniczne poświadczenie atrybutów (np. adresu, wieku, płci) posiada taki sam skutek prawny, jak legalnie wystawione poświadczenia w formie papierowej [27].

Europejski Portfel Cyfrowej Tożsamości zaplanowany jest do użytku zarówno dla usług online, jak i bezpośrednio w formacie fizycznym do usług offline. Będzie on zapewniał wysoki poziom bezpieczeństwa[5] we wszystkich aspektach świadczenia usług w zakresie tożsamości cyfrowej, m.in. w zakresie infrastruktury służącej do gromadzenia, przechowywania i ujawniania tożsamości cyfrowej. Będzie to narzędzie bezpłatne dla osób fizycznych [3].

Dodatkowe funkcjonalności EDIW to możliwość przechowywania różnego rodzaju dokumentów oraz dokonywania płatności elektronicznych. Jedną z jego zalet jest również możliwość bezpłatnego składania podpisów elektronicznych przez osoby fizyczne. Dzięki temu użytkownicy portfela mogą bezproblemowo podpisywać dokumenty w formie elektronicznej, co przyspieszy procesy administracyjne i ułatwi załatwianie różnych spraw urzędowych. Warto zaznaczyć, że podpis elektroniczny może mieć



Etap 1
Wybór krajowego środka identyfikacji (karty tożsamości)

Etap 2
Widok ekranu konfiguracji z przepływem danych

Etap 3
Proces zapisywania danych przez zeskanowanie karty tożsamości

Etap 4
Dodana krajowa karta tożsamości na smartfonie

Rysunek 1. Przykład portfela cyfrowej tożsamości

Źródło: Opracowanie własne na podstawie [26].

taką samą moc prawną jak tradycyjny podpis odręczny, co oznacza, że jest on równie ważny i wiarygodny [28].

Wprowadzenie EDIW może mieć istotne znaczenie dla funkcjonowania systemu ochrony zdrowia także w wymiarze transgranicznym. Europejski Portfel Cyfrowej Tożsamości będzie mógł być wykorzystywany do dostępu do usług publicznych i prywatnych zapewnianych przez placówki medyczne, np. wydawania i uznawania zaświadczeń (w tym lekarskich), wydawania aktów urodzenia, podpisywania dokumentów związanych z realizacją świadczeń medycznych, a także przechowywania e-recept, z których będzie można korzystać w dowolnym kraju UE [3, 13]. Portfel „europejski" ma stanowić elektroniczne potwierdzenie posiadania kwalifikacji, tytułu i licencji edukacyjnej/zawodowej [3], co otwiera możliwość potwierdzenia prawa do wykonywania zawodu medycznego. Mogłoby to być z jednej strony korzystne dla profesjonalistów medycznych migrujących między krajami UE, którzy mieliby w łatwy sposób dostępne potwierdzenie prawa do wykonywania zawodu, a z drugiej dla pacjentów mogących sprawdzić, czy dany specjalista posiada odpowiednie kwalifikacje. Można dostrzec też potencjał cyfrowy w rozpoznawalnym międzynarodowo prawie do świadczeń zdrowotnych, obecnie funkcjonującym w formie fizycznej jako Europejska Karta Ubezpieczenia Zdrowotnego [29].

Przykładem wdrożonego rozwiązania cyfrowej tożsamości działającego na zasadach EDIW jest certyfikat szczepień przeciwko COVID-19 (Unijny Certyfikat COVID), uznawany w krajach członkowskich UE i umożliwiający elektroniczną identyfikację [16]. Krajowy przykład to portal mObywatel i jego narzędzia, np. e-recepta i elektroniczny dowód osobisty, które mogą być użyte w podmiotach medycznych [30]. Według porozumienia z UE mObywatel docelowo ma stać się jednym z EDIW. Jednak aby do tego doszło, sugerowane są zmiany dotyczące: decentralizacji platformy (braku centralnego punktu w kraju), zastosowania oprogramowania na zasadzie otwartego źródła (*open source*), dodanie bezpłatnych podpisów cyfrowych do użytku osobistego oraz możliwości logowania do Bardzo Dużych Platform Online (*Very Large Online Platforms*), np. Facebook, Booking.com [31].

Podsumowanie

W sektorze ochrony zdrowia w Polsce są w użyciu niektóre z usług zaufanych, a inne (pieczęć elektroniczna, konserwacja podpisów i pieczęci) wciąż pozostają nieuregulowane. Ogranicza to możliwości użycia przez pacjenta elektronicznego podpisu w podmiotach leczniczych. Autorzy podkreślają potrzebę udostępnienia w Polsce narzędzia do bezpłatnego podpisywania dokumentów (zgód, oświadczeń) w systemach teleinformatycznych. Koncepcja portfela cyfrowej tożsamości jest wciąż mało znana i przebadana. Mimo to EDIW może mieć przełomowe znaczenie dla usprawnienia opieki transgranicznej pacjentów. Jednak aby do tego doszło, potrzebne jest większe zaangażowanie państw UE w rozwój i wdrożenie narzędzi cyfrowych w podmiotach medycznych, co powinny wspierać adekwatne normy.

Przypisy

1. Wówczas zgodnie z art. 2 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (eIDAS) nie ma ono zastosowania do świadczenia usług zaufania wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego, a za taki system należy uznać system ochrony zdrowia.
2. Wpływ eIDAS 1.0 na sektor ochrony zdrowia został opisany w poprzednich publikacjach [32–34].
3. Należą do niej: Telekom, T-Mobile Polska, o2 Telefónica, i Vodafone.
4. Środek identyfikacji elektronicznej (*electronic identification means*) jest sposobem, w jaki osoba może potwierdzić swoją tożsamość w Internecie, np. poprzez login i hasło lub certyfikat cyfrowy [2].
5. Najwyższy w skali trójstopniowej określonej w rozporządzeniu eIDAS 1.0 [2].

Piśmiennictwo

1. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2011 r. nr 113 poz. 657).
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (32014R0910).
3. Wniosek Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (52021PC0281), https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52021PC0281 (dostęp: 23.10.2023).
4. Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 1997 r. nr 28 poz. 152).
5. Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2020 r. poz. 666).
6. Ojczyk J., *Ministerstwo Zdrowia wdroży elektroniczny podpis dla pacjenta*, https://www.prawo.pl/zdrowie/elektroniczny-podpis-dla-pacjentow,515114.html (dostęp: 23.10.2023).

7. eDO App, *Twoja elektroniczna tożsamość*, https://www.edoapp.pl/ (dostęp: 23.10.2023).
8. Ustawa z dnia 13 lipca 2023 r. o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz ustawy o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz.U. z 2023 r. poz. 1733).
9. Rozporządzenie Ministra Zdrowia z dnia 14 września 2018 r. w sprawie minimalnych wymagań organizacyjno-technicznych dla Zintegrowanego Systemu Monitorowania Obrotu Produktami Leczniczymi (Dz.U. z 2018 r. poz. 1821).
10. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r. poz. 1579).
11. Ministerstwo Cyfryzacji, *Grupa robocza ds. rejestrów rozproszonych i blockchain*, https://www.gov.pl/web/cyfryzacja/blockchain (dostęp: 23.10.2023).
12. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. z 2020 r. poz. 2320).
13. Mędrala W., Sanok S., *Unijna tożsamość cyfrowa. Rozporządzenie eIDAS 2.0*, https://www.parp.gov.pl/component/content/article/76093:unijna-tozsamosc-cyfrowa-rozporzadzenie-eidas-2-0 (dostęp: 23.10.2023).
14. Komisja Europejska, *Cyfrowa dekada Europy: cele cyfrowe na 2030 r.*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pl (dostęp: 23.10.2023).
15. Wniosek Decyzja Parlamentu Europejskiego i Rady ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r. (52021PC0574), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0574 (dostęp: 2.11.2023).
16. Komisja Europejska, *2030 Digital Decade – Report on the State of the Digital Decade 2023*, 2023. doi: 10.2759/999709.
17. *Potential – For European Digital Identity*, https://www.digital-identity-wallet.eu/ (dostęp: 23.10.2023).
18. Tkaczyk M., *Cyfrowa tożsamość: Grupa Deutsche Telekom z T-Mobile Polska, o2 Telefónica i Vodafone testują ją w ramach inicjatywy UE*, https://firma.t-mobile.pl/dla-mediow/aktualnosci/informacja-prasowa/2023/07/cyfrowa-tozsamosc-o2-telefonica--telekom-i-vodafone-testuja-ja-w-ramach-inicjatywy-ue.html (dostęp: 23.10.2023).
19. Podgorelec B., Alber L., Zefferer T., *What is a (Digital) Identity Wallet? A Systematic Literature Review*, Proceedings – 2022 IEEE 46th Annual Computers, Software, and Applications Conference, COMPSAC 2022: 809–818, doi: 10.1109/COMPSAC54236.2022.00131.
20. Zwattendorfer B., Zefferer T., Stranacher K., *An Overview of Cloud Identity Management-Models*, WEBIST 2014 – Proceedings of the 10th International Conference on Web Information Systems and Technologies, 2014, t. 1: 82–92, doi: 10.5220/0004946400820092.
21. Lukkien B., Bharosa N., de Reuver M., *Barriers for Developing and Launching Digital Identity Wallets*, ACM International Conference Proceeding Series 2023*:* 289–299. doi: 10.1145/3598469.3598501.
22. Stodt F., Reich C., *A Review on Digital Wallets and Federated Service for Future of Cloud Services Identity Management*, Service Computation 2023: The Fifteenth International Conference on Advanced Service Computing, June 26, 2023 to June 30, Nicea 2023, s. 16–20, na: https://opus.hs-furtwangen.de/frontdoor/index/index/docId/9725 (dostęp: 3.11 2023).
23. Malik R, Kataria A., Nandal N., *Analysis of Digital Wallets for Sustainability: A Comparative Analysis Between Retailers and Customers*, "International Journal of Management" 2020; 11 (7): 358–370. doi: 10.34218/IJM.11.7.2020.035.
24. Naghmouchi M., Laurent M., Levallois-Barth C. et al., *Comparative Analysis of Technical and Legal Frameworks of Various National Digial Identity Solutions*, https://arxiv.org/abs/2310.01006v1 (dostęp: 2.11.2023).
25. Sjöholm M., *Designing a Trustworthy EU Digital Identity Wallet:* A *study of user needs and preferences*, https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-504761 (dostęp: 23.10.2023).
26. Kostic S., Poikela M., *Do Users Want to Use Digital Identities? A Study of a Concept of an Identity Wallet*, https://www.usenix.org/conference/soups2022/presentation/kostic-poster (dostęp: 23.10.2023).
27. Szczepania S., *Metropolie: Opinia do nowego projektu rozporządzenia UE tzw. eIDAS 2*, https://metropolie.pl/artykul/opinia--do-nowego-projektu-rozporzadzenia-ue-tzw-eidas-2 (dostęp: 23.10.2023).
28. Rada Unii Europejskiej, *Europejska tożsamość cyfrowa: Rada porozumiała się z Parlamentem – Consilium*, https://www.consilium.europa.eu/pl/press/press-releases/2023/06/29/council-and-parliament-strike-a-deal-on-a-european-digital-identity-eid/ (dostęp: 23.10.2023).
29. Centrum e-Zdrowia, *Europejska Karta Ubezpieczenia Zdrowotnego (EKUZ)*, https://pacjent.gov.pl/ekuz (dostęp: 23.10.2023).
30. mObywatel, https://info.mobywatel.gov.pl/ (dostęp: 23.10.2023).
31. European Commission, *Final Agreement on EU Digital Identity Wallet*, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651 (dostęp: 13.11.2023).
32. Romaszewski A., Trąbka W., Kielar M. et al., *Wprowadzenie usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej (część I)*, „Zeszyt Naukowy.pl / Wyższa Szkoła Zarządzania i Bankowości w Krakowie" 2016; 42: 24–40.
33. Jakubowski S., Romaszewski A., Trąbka W., *Identyfikacja i uwierzytelnianie podmiotów oraz dokumentów elektronicznych w ochronie zdrowia jako niezbędne atrybuty bezpieczeństwa danych i informacji w ochronie zdrowia*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2018; 49: 60–77.
34. Romaszewski A., Kielar M., Jakubowski S. et al., *Część II – Dane o stanie zdrowia w świetle nowych wyzwań technicznych, prawnych i organizacyjnych – wybrane zagadnienia*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2021; 58: 13–25.