

Remigiusz Lewandowski
ORCID: [0000-0001-7353-9742](https://orcid.org/0000-0001-7353-9742)
Akademia Sztuki Wojennej w Warszawie

Analiza metod identyfikacji elektronicznej stosowanych w Polsce

<https://doi.org/10.19195/978-83-229-3843-0.13>

Abstrakt: Artykuł opiera się na analizie rozwiązań technologicznych stosowanych w Polsce w zakresie elektronicznej (zdalnej) identyfikacji. Rozwiązania te zostały przeanalizowane pod kątem różnych kryteriów, w tym: adekwatności do poszczególnych etapów procesu identyfikacji oraz posiadania różnego rodzaju funkcjonalności i cech, takich jak zakres wykorzystywanych danych, zakres zastosowań, wymagania wobec dostawców usług, a także przewidywana zgodność z eIDAS2. Artykuł prowadzi do wniosku, że Polska dysponuje bardzo rozwiniętymi i szeroko stosowanymi rozwiązaniami w zakresie identyfikacji elektronicznej. Co do zasady można je pogrupować na narzędzia wykorzystywane w celu wydania środka identyfikacji elektronicznej oraz narzędzia stosowane w etapach uwierzytelniania i autoryzacji. Ponadto istotną część analizowanych narzędzi znajduje swoje zastosowanie zarówno w kanale publicznym, jak i komercyjnym. Spośród wszystkich rozwiązań stanowiących przedmiot niniejszych badań największą użyteczność społeczną z punktu widzenia bezpieczeństwa i dostępności publicznej zapewniają: identyfikacja bazująca na tzw. tożsamości bankowej oraz weryfikacja wideo na podstawie warstwy elektronicznej dowodu osobistego.

Słowa kluczowe: eIDAS2, tożsamość, identyfikacja, środki identyfikacji elektronicznej.

Wstęp

We współczesnym świecie znaczna część aktywności społeczno-gospodarczych odbywa się w cyberprzestrzeni. Lockdowny spowodowane pandemią COVID-19 znacznie wzmocniły i zdynamizowały to zjawisko. Dobrym przykładem odbywającej się

migracji do cyberprzestrzeni jest szczególnie popularna bankowość internetowa, w ramach której wszystkie czynności bankowe mogą być wykonywane przez klienta on-line. Innym spektakularnym przykładem są wybory powszechne, które w niektórych państwach (np. w Estonii) odbywają się także w formie elektronicznej. Nie ulega wątpliwości, że wskazany trend będzie się rozwijał. Jednak wraz z rozwojem technologii pojawia się pytanie o bezpieczeństwo. W jakim stopniu nowe rozwiązania przenoszone do cyberprzestrzeni są zabezpieczone przed manipulacją? W tym obszarze największym wyzwaniem jest uzyskanie pewności co do tożsamości osób wykonujących określone czynności w cyberprzestrzeni. Jest to szczególnie ważne w kontekście prawnych i finansowych konsekwencji tych czynności. Na przykład otwierając rachunek bankowy, bank powinien mieć absolutną pewność co do tożsamości swojego klienta. Pewność należy zachować również w procesie jego obsługi, tzn. bank realizujący polecenie przelewu on-line powinien mieć również absolutną pewność, że przelew został zlecony przez osobę upoważnioną. Czy taką pewność zapewniają obecnie stosowane instrumenty w dziedzinie identyfikacji elektronicznej? Odpowiedź na to pytanie, oparta na analizie stanu faktycznego w Polsce, znajduje się w niniejszym artykule. Problem ten nie jest marginalny, ponieważ bezpieczeństwo tożsamości, a w szczególności weryfikacja tożsamości, jest wyzwaniem nawet w warunkach pozwalających na bezpośredni (fizyczny) kontakt z osobą, której tożsamość podlega weryfikacji¹.

Ze względu na korzyści społeczne i gospodarcze wynikające z przenoszenia aktywności gospodarczych i społecznych do cyberprzestrzeni, identyfikacja elektroniczna podlega dynamicznemu rozwojowi. Rozwój ten wpływa zarówno na sektor prywatny, jak i publiczny. Trzeba jednak przyznać, że sektor bankowy odegrał niezwykle ważną rolę w upowszechnieniu identyfikacji elektronicznej praktycznie na całym świecie. Widząc korzyści ekonomiczne wynikające z upowszechnienia bankowości internetowej, banki opracowały system elektronicznej identyfikacji, który zapewnia bezpieczeństwo transakcji zdalnych. Jednocześnie rozwój ten i rosnące znaczenie zasady Know Your Customer (KYC) stymulowane były i są wymogami prawnymi związanymi z przeciwdziałaniem praniu pieniędzy.

1. Przegląd literatury przedmiotu

Zagadnienie nowoczesnych systemów identyfikacji w cyberprzestrzeni (tj. wykonywanych w warunkach zdalnych) w kontekście ich bezpieczeństwa i niezawodności

¹ W typowych warunkach bankowości oddziałowej pracownicy zazwyczaj nie mają wystarczających kompetencji do weryfikacji tożsamości na podstawie wizerunku twarzy (porównania twarzy na dokumencie tożsamości z twarzą klienta). W związku z tym aktualnym problemem pozostają np. oszustwa polegające na wykorzystaniu skradzionych dokumentów tożsamości.

nie jest zbyt szeroko omawiane w literaturze. Taki stan rzeczy wynika z charakterystyki procesu identyfikacji i potwierdzania tożsamości na podstawie etapu rejestracji, od wielu lat wymagającej najczęściej fizycznego kontaktu pomiędzy osobą identyfikowaną a osobą weryfikującą tożsamość. Ponadto ostatni etap procesu identyfikacji, czyli uwierzytelnianie, również opiera się w znacznej części przypadków na klasycznych środkach identyfikacji, takich jak login i hasła. Dopiero od niedawna widoczna jest ekspansja metod alternatywnych na większą skalę na wszystkich etapach weryfikacji tożsamości.

Znaczna część badań poświęconych bezpieczeństwu tożsamości w cyberprzestrzeni dotyczy zagadnień związanych z technologią. Raport techniczny ETSI², obejmujący m.in. przegląd technologii i wymagań prawnych w wybranych krajach europejskich w zakresie potwierdzania tożsamości na potrzeby usług zaufania, wskazuje, że uwierzytelnianie w trybie zdalnym może odbywać się przy zastosowaniu dwóch podstawowych metod: biometrii (automatycznie lub w obecności on-line osoby weryfikującej zgodność tożsamości) oraz na bazie transferu atrybutów tożsamości z innych zaufanych źródeł (takich jak system identyfikacji elektronicznej lub kwalifikowany podpis elektroniczny). Autorzy raportu stwierdzają, że zdalny proces identyfikacji jest problematyczny, ponieważ warunki równoważności identyfikacji zdalnej z fizyczną nie są dobrze zdefiniowane i brak jest wymagań co do jakości (fizycznych) dokumentów tożsamości, a także kompetencji lub procedur stosowanych w trakcie weryfikacji zdalnej.

Alan Goode wskazuje, że systemy biometryczne odgrywają kluczową rolę w świadczeniu usług weryfikacji tożsamości w warunkach on-line, ale istotnym wyzwaniem dla tych metod są ataki spoofingowe na tożsamość, w tym również bazujące na narzędziach sztucznej inteligencji³. Pomimo istniejących zagrożeń organizacje międzynarodowe, takie jak Bank Światowy, aktywnie uczestniczą w promocji rozwiązań opartych na tożsamości cyfrowej i wspierają kraje w procesie ich wdrażania⁴, a ONZ promuje stosowanie biometrycznej rejestracji uchodźców⁵. Obecnie wybrane państwa wdrożyły lub planują wdrożyć rozwiązania w zakresie identyfikacji elektronicznej oparte na biometrii i technologii *blockchain*. Wśród krajów UE swoje systemy identyfikacji elektronicznej zgłosiły do Komisji Europejskiej: Czechy, Estonia, Włochy, Holandia, Dania,

² *Technical Report TR 119 460 V1.1.1 (2021-02): Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects*, European Telecommunications Standards Institute ETSI 2021, https://www.etsi.org/deliver/etsi_tr/119400_119499/119460/01.01.01_60/tr_119460v010101p.pdf (dostęp: 13.09.2022).

³ A. Goode, *Digital identity: solving the problem of trust*, „Biometric Technology Today” 2019, vol. 2019, issue 10, s. 5–8.

⁴ *Technology Landscape for Digital Identification*, World Bank 2018, <https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf> (dostęp: 13.09.2022).

⁵ *Biometric identity management system*, United Nations High Commissioner for Refugees (UNHCR) 2018, <http://www.unhcr.org/550c304c9.html> (dostęp: 13.09.2022).

Hiszpania, Łotwa, Niemcy, Słowacja, Chorwacja, Belgia, Luksemburg, Litwa oraz Portugalia⁶.

Jednak procesu budowy systemów tożsamości cyfrowej nie można uznać za zakończony. Trwa on nadal i obejmuje zarówno te kraje, które zgłosiły swoje programy, jak i te, które jeszcze tego nie zrobiły (np. Polska). Co więcej, metody i narzędzia wykorzystywane w weryfikacji tożsamości podlegają ciągłej ewolucji. Ramy prawne w tym zakresie, w szczególności rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w zakresie transakcji elektronicznych na rynku wewnętrznym oraz uchylenia dyrektywy 1999/93/WE (dalej: eIDAS)⁷ pozostawiają państwom członkowskim znaczną swobodę w doborze środków identyfikacji i mechanizmów uwierzytelniania. Dlatego tak ważne są badania naukowe dotyczące metod stosowanych w poszczególnych krajach, aby móc przedstawić i zarekomendować optymalne rozwiązania.

Poza kwestiami technologicznymi przedmiotem badań jest również sam model zarządzania tożsamością. Na podstawie praktycznych problemów użytkowników z mnogością loginów i haseł oraz zagrożeń ze strony hakerów coraz częściej wysuwane są postulaty dotyczące tzw. suwerennej tożsamości cyfrowej. Christopher Allen zdefiniował suwerenną tożsamość jako „kolejny krok poza tożsamością zorientowaną na użytkownika [gdzie] użytkownik musi być centralnym elementem zarządzania tożsamością”⁸. Podejście to znacząco różni się od tradycyjnego zarządzania tożsamością, w którym, jak stwierdzają Kai Wagner i inni, „tożsamość użytkownika jest definiowana z perspektywy dostawcy w określonym celu i dlatego jest ważna tylko w domenie tego konkretnego dostawcy w ramach tego zakresu”⁹. Jak wskazują Kalman Toth i Alan Anderson-Priddy, suwerenna tożsamość cyfrowa może dać obywatelom wyraźne władztwo nad ich tożsamością w cyberprzestrzeni, zwiększyć prywatność obywateli i zmniejszyć poleganie na hasłach¹⁰. Ten nowy paradygmat zarządzania tożsamością cyfrową opiera się na założeniu, że to sam obywatel zarządza swoimi atrybutami tożsamości, wybierając w danym procesie identyfikacji te, które są do niego adekwatne. Wdrożenie suwerennej tożsamości cyfrowej wiąże się jednak tylko z fragmentem całego procesu potwierdzania tożsamości, a w szczególności z etapem uwierzytelnienia.

⁶ Digital Europe Programme, eID user community <https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS> (dostęp: 13.09.2022).

⁷ Dz. Urz. UE L 257 z 28.08.2014 r.

⁸ C. Allen, *The path to self-sovereign identity*, 2016, <https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/> (dostęp: 13.09.2022).

⁹ K. Wagner et al., *Self-sovereign identity. a position paper on blockchain enabled identity and the road ahead*, Blockchain Bundesverband, Berlin, Germany 2018, https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity-_Blockchain-Bundesverband-2018.pdf (dostęp: 13.09.2022).

¹⁰ K. Toth, A. Anderson-Priddy, *Self-sovereign digital identity: a paradigm shift for identity*, „IEEE Security & Privacy Magazine” 2019, 17(3), s. 17–20.

2. Metodologia

Artykuł opiera się na analizie rozwiązań technologicznych stosowanych w Polsce w zakresie zdalnej identyfikacji. Rozwiązania te zostały przeanalizowane pod kątem różnych kryteriów, w tym adekwatności do poszczególnych etapów procesu identyfikacji oraz różnego rodzaju funkcjonalności i cech, takich jak zakres weryfikowanych danych, zakres zastosowań, wymagania wobec dostawców usług, a także gotowość do eIDAS2. W artykule wykorzystano dostępną literaturę przedmiotu oraz akty prawne regulujące identyfikację elektroniczną.

3. Pojęcie tożsamości

Bezpieczeństwo i komfort życia we współczesnych społeczeństwach zależą od poziomu rozwoju technologicznego. Jednym z najważniejszych aspektów bezpieczeństwa jest bezpieczeństwo tożsamości. Odnosi się ono do zagwarantowania pewności, czyli jednoznacznej wiedzy o tożsamości osoby. Angielski termin „tożsamość” pochodzi od łacińskiego słowa *idem*, które oznacza tożsamość i ciągłość. *Słownik Merriam-Webster* wskazuje cztery podstawowe znaczenia terminu „tożsamość”. W pierwszym znaczeniu to:

- wyróżniające cechy charakteru lub osobowość jednostki albo
- świadomość wspólnych cech określona przez psychologiczne identyfikowanie się.

W drugim znaczeniu słownik definiuje tożsamość jako stan bycia takim samym jak przedmiot opisu lub wskazania. Trzecie znaczenie omawianego terminu to:

- identyczność istotnej lub wtórnej cechy w różnych warunkach lub
- identyczność we wszystkim, co stanowi obiektywną rzeczywistość przedmiotu.

W czwartym znaczeniu *Słownik Merriam-Webster* wskazuje, że tożsamość jest równością dwóch wyrażen, która zachodzi dla wszystkich wartości występujących w niej zmiennych. Z kolei *Słownik języka polskiego* nadaje słowu „tożsamość” pięć znaczeń. W pierwszym znaczeniu termin ten oznacza identyczność. Jest to zatem rozumienie analogiczne do drugiej i trzeciej definicji pojęcia „tożsamość” zawartych w *Słowniku Merriam-Webster*. Drugie znaczenie, według *Słownika języka polskiego*, to samoświadomość w stosunku do jednostki. To znaczenie odpowiada pierwszej angielskiej definicji terminu „tożsamość”. Trzecie jego znaczenie w języku polskim to: fakty, cechy i dane osobowe pozwalające na identyfikację osoby. Czwarte polskie znaczenie w odniesieniu do wspólnoty to: świadomość cech wspólnych i poczucie jedności. Wreszcie piąte znaczenie omawianego terminu to definicja matematyczno-logiczna zgodna z jej angielskim rozumieniem tożsamości zawartym w czwartej definicji w *Słowniku Merriam-Webster*.

Na potrzeby tematyki niniejszej pracy proponuje się zdefiniowanie pojęcia „tożsamość” jako: faktów, cech i danych osobowych pozwalających na identyfikację osoby.

Choć jest to definicja słownikowa, a nie specjalistyczna i oparta na pogłębionych badaniach z zakresu socjologii, nauk prawnych czy nauk o bezpieczeństwie, to jest ona dość szeroka i kierunkowo prawidłowa, gdyż prowadzi do wniosku, że tożsamość jest powiązana z potrzebą identyfikacji danej osoby, czyli zweryfikowania, czy jest ona tą, za którą się podaje, lub tą, za którą ją uważamy.

Przytoczone powyżej znaczenie pojęcia „tożsamość” ze *Słownika języka polskiego* wiąże się z faktami, cechami i danymi osobowymi służącymi do weryfikacji i identyfikacji tożsamości. Cechy biometryczne należą do szerszej kategorii danych osobowych i są jednym z fundamentów identyfikacji lub weryfikacji tożsamości. Są one częścią szerszego katalogu danych osobowych, który obejmuje „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”¹¹. Tym samym katalog danych osobowych określonych przepisami prawa jest otwarty, a główną przesłanką w tym przypadku jest to, czy dana informacja umożliwia bezpośrednią lub pośrednią identyfikację konkretnej osoby. Takie rozumienie danych osobowych jest co do zasady zgodne ze słownikowym rozumieniem tożsamości jako faktów, cech i danych osobowych pozwalających na identyfikację osoby. Jest to jednak rozumienie zbyt wąskie i nie obejmuje specyficznego atrybutu tożsamości, tj. jestestwa człowieka, tego wszystkiego, co konstytuuje go jako jedną, niepowtarzalną w wymiarze fizycznym i umysłowym osobę. Jak wskazuje Olga Sakson-Obada, wymiar fizyczny jest ważny dla tożsamości, ponieważ ciało każdej osoby jest niepowtarzalne i zawiera unikalny zestaw możliwości, których nie ma żaden inny człowiek¹².

Literatura socjologiczna wskazuje, że tożsamość, w tym tożsamość pojedynczej osoby, jest zjawiskiem dynamicznym i w procesach interakcji społecznych podlega zmianom, choć jednocześnie tożsamość, zwłaszcza odnosząca się do grup społecznych, pozostaje czynnikiem zapewniającym trwałość, stabilizację i ciągłość. Dynamika tożsamości człowieka odnosi się nie tylko do wymiaru kulturowego i światopoglądowego, lecz także do wymiaru biologicznego, związanego np. z procesem starzenia. Człowiek

¹¹ Artykuł 4 rozporządzenia 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), Dz. U. UE L 119 z 4.05.2016 r.

¹² O. Sakson-Obada, *Rozwój ja cielesnego w kontekście wczesnej relacji z opiekunem*, „Roczniki Psychologiczne” 2008, 11(2), s. 29–31.

ulega zmianom w czasie. Czy zatem tożsamość ludzka jest zmienna i nietrwała? Jeśli tak, to „ten sam” – wydawałoby się – człowiek w perspektywie czasu nie będzie „tym samym” człowiekiem, ale kimś zupełnie innym. Jego szczególne czynniki określające fizyczną, fizjologiczną czy genetyczną tożsamość mogą przecież ulec zmianie. Nawet takie pozornie trwałe cechy biometryczne osoby, jak odcisk palca czy nawet DNA, mogą podlegać intencjonalnym lub nieintencjonalnym zmianom.

Dlatego zasadne jest zaproponowanie przez autora definicji tożsamości jako całokształtu cech fizycznych, fizjologicznych, genetycznych i psychicznych człowieka oraz identyfikatorów w postaci imienia, nazwiska i innych indywidualnie przypisanych mu atrybutów, które łącznie składają się na niepowtarzalność jego osoby. Zgodnie z powyższą definicją to nie jeden lub kilka czynników decyduje o tożsamości człowieka, ale ich całokształt. Jak wskazano w poprzednich przykładach, cechy fizyczne, fizjologiczne i genetyczne mogą ulec zmianie. Zmianie mogą ulec także cechy psychiczne, w tym nawet – w wyniku choroby – osobiste przekonanie o własnej tożsamości. Zmiany te nie skutkują jednak nową tożsamością, ponieważ nigdy nie zachodzą całościowo. Naturalny proces starzenia i choroba nie modyfikują wszystkich indywidualnych cech danej osoby. Nawet świadoma manipulacja tymi cechami, w tym interwencja medyczna, nie jest możliwa dla wszystkich tych cech „stanowiących indywidualność i niepowtarzalność” człowieka. Stosunkowo łatwa może być próba zmiany takich atrybutów, jak imię i nazwisko lub PESEL, aby uwierzytelnić się w systemach teleinformatycznych. Są to najczęściej występujące przykłady tzw. kradzieży tożsamości poprzez wykorzystanie cudzych danych osobowych przez nieuprawnioną osobę oraz wykorzystanie cudzych indywidualnych atrybutów. Jednak takie akty tylko stwarzają pozory nowej lub cudzej tożsamości. Przestępca posługujący się cudzym imieniem i nazwiskiem nie uzyskuje tożsamości prawowitego właściciela tych danych osobowych, ponieważ nie jest w stanie przejąć całości omawianych cech „stanowiących indywidualność i niepowtarzalność” drugiego człowieka. Dlatego Piotr Girdwoyń słusznie wskazuje, że „przypisanie jakiegokolwiek cesze (lub zespołowi cech) obiektu identyfikowanego waloru unikalności nie wydaje się możliwe, gdyż zawsze jej rzadkość, stanowiąca podstawową przesłankę indywidualności, jest odnoszona w najlepszym wypadku jedynie do klasy wszystkich przebadanych obiektów danego rodzaju i nie musi mieć waloru uniwersalnego”¹³. Dlatego należy raz jeszcze podkreślić, że pewności co do tożsamości osoby nie można opierać wyłącznie na jednej lub kilku jej cechach. Wymaganą pewność może zapewnić jedynie ogół tych cech i identyfikatorów, chociaż w praktyce, z powodów pragmatycznych, stosuje się pewność opartą na prawdopodobieństwie (jeśli dane zjawisko jest policzalne) lub tylko subiektywnym osądzie.

¹³ P. Girdwoyń, *Zarys kryminalistycznej taktyki obrony*, Zakamycze, Kraków 2004, s. 223.

4. Proces identyfikacji

Głównym wyzwaniem przy korzystaniu z identyfikacji elektronicznej jest proces weryfikacji tożsamości. Można go podzielić na siedem etapów:

- 1) rejestracja,
- 2) walidacja,
- 3) weryfikacja,
- 4) ocena ryzyka,
- 5) wydanie środka identyfikacji elektronicznej,
- 6) uwierzytelnienie,
- 7) autoryzacja.

Rejestracja to etap inicjujący identyfikację elektroniczną. Obejmuje dostarczenie przez osobę podlegającą identyfikacji dowodu potwierdzającego jej tożsamość. Najpopularniejszym rodzajem dowodu jest dowód osobisty lub paszport zawierający kluczowe dane umożliwiające identyfikację: imię, nazwisko, datę i miejsce urodzenia oraz zdjęcie twarzy. Dane te znajdują się w warstwie graficznej dokumentu tożsamości, a także – w przypadku wielu krajów – w warstwie cyfrowej. Ponadto w warstwie cyfrowej przechowywane są również inne dane (np. odciski palców).

Kolejnym etapem jest walidacja, w ramach której sprawdza się autentyczność, aktualność i kompletność podanych przez osobę informacji o jej tożsamości, w tym np. sprawdzenie autentyczności i ważności dokumentu tożsamości. W trzecim etapie, tj. weryfikacji, sprawdzeniu podlega, czy prezentowane dane identyfikujące konkretną osobę należą do tej osoby, która podlega procesowi identyfikacji. Tradycyjnie stosowaną metodą na tym etapie jest porównanie wizerunku twarzy osoby (w warunkach rzeczywistych) z wizerunkiem zapisanym lub wydrukowanym w dokumencie tożsamości. Porównanie to może być przeprowadzone na podstawie subiektywnego postrzegania osoby dokonującej weryfikacji lub z wykorzystaniem metod automatycznej weryfikacji tożsamości (z wykorzystaniem sztucznej inteligencji). Oprócz obrazu twarzy można również wykorzystać inne cechy biometryczne człowieka (np. odciski palców). Warunkiem koniecznym jest jednak obecność wzorowych cech biometrycznych w prezentowanych dokumentach tożsamości lub w innych źródłach danych (np. rejestrach publicznych) bezpośrednio związanych z danym dokumentem tożsamości i osobą, której dokument tożsamości dotyczy. Weryfikacja tożsamości na podstawie danych innych niż wizerunek twarzy odbywa się na ogół automatycznie (z wykorzystaniem specjalistycznych systemów informatycznych).

Ważnym elementem ustalania tożsamości jest analiza ryzyka związanego z osobą poddawaną identyfikacji. Zakres analizy jest bezpośrednio związany z celem, dla

którego przeprowadzana jest identyfikacja. Na przykład podczas identyfikacji w celu otwarcia rachunku bankowego i/lub uzyskania kredytu bankowego, ważne jest sprawdzenie historii finansowej klienta.

Pomyślna realizacja powyższych kroków prowadzi do wydania środka identyfikacji elektronicznej, tj. materialnej i/lub niematerialnej jednostki zawierającej dane identyfikujące osobę, która służy do uwierzytelnienia się w usługach on-line. Często spotykanym środkiem identyfikacji elektronicznej jest indywidualnie przypisany do klienta login do systemów teleinformatycznych wraz z hasłem. Stosunkowo nowym (materialnym) środkiem identyfikacji są elektroniczne dowody osobiste (wyposażone w warstwę elektroniczną, czyli mikroprocesory), służące do uwierzytelniania posiadacza w systemach teleinformatycznych w celu korzystania z usług elektronicznych.

Opisywane powyżej etapy procesu identyfikacji mają charakter jednorazowy. Wydanie środka identyfikacji elektronicznej pozwala na realizację kolejnych etapów, które mają charakter powtarzalny. Po wydaniu środka identyfikacji elektronicznej możliwe jest logowanie się do systemu internetowego (np. za pomocą indywidualnego loginu i nadanego hasła), tj. uwierzytelnienie przy każdym dostępie internetowym do danego systemu teleinformatycznego. Uwierzytelnianie – w przypadku korzystania ze środków identyfikacji elektronicznej – jest procesem, który umożliwia elektroniczne potwierdzenie pochodzenia i integralności zweryfikowanych danych użytkownika.

Wyrażenie zgody na wykonanie określonej czynności w internetowym systemie teleinformatycznym, tj. autoryzacja, może odbywać się przy użyciu różnych narzędzi, w tym także przy użyciu środka identyfikacji elektronicznej. Możliwe jest jednoczesne użycie więcej niż jednego rozwiązania. Typowe rozwiązania stosowane na etapie autoryzacji to:

- 1) jednorazowe hasło SMS,
- 2) hasło jednorazowe na karcie kodów (TAN),
- 3) kod w aplikacji systemu teleinformatycznego (danej usługi wymagającej identyfikacji),
- 4) rozwiązania biometryczne (np. wizerunek twarzy),
- 5) token,
- 6) kwalifikowany podpis elektroniczny.

5. Rozwiązania stosowane w identyfikacji elektronicznej w Polsce

Sprawne i skuteczne wdrożenie identyfikacji elektronicznej wymaga wsparcia specjalistycznymi narzędziami informatycznymi. Narzędzia te skupiają się przede wszystkim na obsłudze wybranych lub wszystkich etapów identyfikacji elektronicznej. Stosowane są głównie w sektorach, w których potwierdzenie tożsamości i niektórych

atributów tożsamości (np. wieku) jest wymagane prawem, a także jest ważne z punktu widzenia bezpieczeństwa i interesów użytkownika oraz dostawcy usług internetowych. W konsekwencji w Polsce do sektorów, w których identyfikacja elektroniczna jest najbardziej rozwinięta i rozpowszechniona technologicznie, należą (w odniesieniu do usług internetowych):

- 1) sektor finansowy, zwłaszcza bankowy,
- 2) sektor gier hazardowych,
- 3) sektor użyteczności publicznej,
- 4) sektor usług publicznych,
- 5) sektor sprzedaży detalicznej napojów alkoholowych.

Analiza procesów identyfikacji elektronicznej stosowanych w praktyce w Polsce wskazuje na szereg różnych rozwiązań technologicznych, których zakres – w odniesieniu do poszczególnych elementów procesu identyfikacji – jest jednak różny, co przedstawia tabela 1.

W tabeli 1 przedstawiono płaszczyznę zastosowania różnych rozwiązań technologicznych na poszczególnych etapach procesu identyfikacji. Wynika z niej, że tylko nieliczne z analizowanych rozwiązań można zastosować na wszystkich etapach tego procesu. Co do zasady narzędzia używane w procesie identyfikacji wyspecjalizowane są w zakresie:

- 1) przeprowadzenia niezbędnych czynności pozwalających na wydanie środka identyfikacji elektronicznej,
- 2) prowadzenia dalszych etapów procesu identyfikacji, tj. uwierzytelnienia i autoryzacji.

Różnice pomiędzy analizowanymi rozwiązaniami dotyczą także ich innych cech funkcjonalnych, które przedstawiono w tabeli 2. Z analizy porównawczej wyłączono jednak rozwiązania służące jedynie etapom uwierzytelnienia oraz autoryzacji (hasło SMS, hasło w aplikacji, karta TAN, wideoweryfikacja na podstawie wzorca zapisanego w smartfonie lub innym urządzeniu oraz weryfikacja na podstawie wzorca odcisku palca zapisanego w smartfonie lub innym urządzeniu) z uwagi na ich bardzo wąski zakres funkcjonalny.

Tabela 1. Rozwiązania technologiczne stosowane w Polsce na różnych etapach identyfikacji elektronicznej

Rozwiązania technologiczne	Etapy procesu identyfikacji		Rejestracja	Walidacja	Weryfikacja	Analiza ryzyka	Wydanie środka identyfikacji elektronicznej	Uwierzytelnienie	Autoryzacja
Automatyczna wideoweryfikacja na podstawie warstwy graficznej dowodu osobistego		Tak	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Tak	Nie	Nie
Wideoveryfikacja na podstawie warstwy graficznej dowodu osobistego z udziałem operatora		Tak	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Tak	Nie	Nie
Automatyczna wideoweryfikacja na podstawie warstwy elektronicznej dowodu osobistego		Tak	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Tak	Nie	Nie
Wideoveryfikacja na podstawie warstwy elektronicznej dowodu osobistego z udziałem operatora		Tak	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Tak	Nie	Nie
Rozwiązanie bazujące na tożsamości bankowej		Tak	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Tak	Możliwe, ale rzadkie	Możliwa, ale rzadka
AIS		Tak	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Tak	Nie	Nie
Przelew weryfikacyjny		Tak	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Możliwe, ale niestosowane	Możliwe, ale niestosowane	Możliwa, ale niestosowana
Kwalifikowany podpis elektroniczny		Tak	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Możliwe	Tak	Tak

Etapy procesu rozwiązania identyfikacji technologiczne	Rejestracja	Walidacja	Weryfikacja	Analiza ryzyka	Wydanie środka identyfikacji elektronicznej	Uwierzytelnienie	Autoryzacja
Profil osobisty	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Tak	Tak	Tak
Profil zaufany	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Tak	Tak	Tak
mObywatel	Tak	Tak	Tak	Możliwa do wdrożenia przez dostawcę usług*	Możliwe, ale niestosowane	Możliwe, ale rzadkie	Możliwa, ale rzadka
Hasło SMS	Nie	Nie	Nie	Nie	Nie	Tak	Tak
Hasło w aplikacji	Nie	Nie	Nie	Nie	Nie	Tak	Tak
Karta TAN	Nie	Nie	Nie	Nie	Nie	Tak	Tak
Token	Nie	Nie	Nie	Nie	Nie	Tak	Tak
Wideoweryfikacja na podstawie wzorca zapisanego w smartfonie lub innym urządzeniu	Nie	Nie	Nie	Nie	Nie	Tak	Tak
Weryfikacja na podstawie wzorca odcisku palca zapisanego w smartfonie lub innym urządzeniu	Nie	Nie	Nie	Nie	Nie	Tak	Tak

* Usługodawca – podmiot świadczący usługi wymagające realizacji procesu identyfikacji elektronicznej.

Źródło: opracowanie własne.

Tabela 2. Funkcjonalności wybranych rozwiązań identyfikacyjnych

Rozwiązanie – funkcjonalności	Zakres danych	Zakres zastosowań	Dodatkowe funkcjonalności	Wymagania dla dostawców usług	Kanały rynkowe	Potencjał użytkowników	Gotowość na eIDAS2
Automatyczna i wspomagana operatorem wideoweryfikacja na podstawie warstwy graficznej dowodu osobistego	Dane osobowe (w tym fotografia twarzy) i inne uwidocznione w warstwie graficznej dowodu osobistego	Stacjonarny, on-line, mobilny	Integracja z bazą dokumentów zastrzeżonych	Wysokie	Komercyjny	Około 29 mln posiadaczy dowodów osobistych	Tak, konieczny audyt
Automatyczna i wspomagana operatorem wideoweryfikacja na podstawie warstwy elektronicznej dowodu osobistego	Dane osobowe (w tym fotografia twarzy) i inne uwidocznione w warstwie graficznej dowodu osobistego	Stacjonarny, on-line, mobilny	Integracja z bazą dokumentów zastrzeżonych; weryfikacja autentyczności dokumentu	Niskie	Komercyjny	Około 6 mln posiadaczy elektronicznych dowodów osobistych	Tak, konieczny audyt
Rozwiązanie bazujące na tożsamości bankowej	Dane osobowe: dane ujęte w dowodzie osobistym (bez fotografii twarzy), potwierdzony nr telefonu, nr rachunku bankowego, adres e-mail, adres zameldowania i korespondencyjny	On-line	Login do systemu bankowego, możliwość stworzenia profilu zaufanego	Wysokie	Komercyjny i publiczny	Około 16 mln użytkowników (łącznie potencjał: ok. 22 mln)	Tak, wymagany audyt
AIS	Dane osobowe: imię i nazwisko, adres. Dane finansowe: nr rachunku, historia transakcji	On-line, mobilny	Możliwość oceny wiarygodności klientów (<i>scoring</i>)	Niskie	Komercyjny	Teoretycznie ok. 22 mln użytkowników bankowości, w praktyce aktualny potencjał istotnie mniejszy	Nie

Rozwiązanie – funkcjonalności	Zakres danych	Zakres zastosowań	Dodatkowe funkcjonalności	Wymagania dla dostawców usług	Kanały rynkowe	Potencjał użytkowników	Gotowość na eIDAS2
Przelew weryfikacyjny	Imię i nazwisko oraz adres	On-line, mobilny	–	Niskie	Komercyjny	Około 22 mln użytkowników bankowości	Nie
Kwalifikowany podpis elektroniczny	Dane uwidocznione w dowodzie osobistym; w przypadku podpisu mobilnego – nr telefonu	On-line, mobilny	–	Wysokie	Komercyjny i publiczny	Poniżej 1 mln użytkowników	Tak, wymagany audyt
Profil osobisty	Dane uwidocznione w dowodzie osobistym (bez fotografii twarzy)	Stacjonarny, on-line, mobilny	Możliwość zakładania profilu zaufanego	Średnie	Komercyjny i publiczny	Około 3 mln posiadaczy elektronicznego dowodu osobistego z aktywowaną funkcjonalnością	Tak
Profil zaufany	Dane uwidocznione w dowodzie osobistym (bez fotografii twarzy); potencjalnie możliwość rozszerzenia zakresu danych o inne dane z rejestrów publicznych	On-line, mobilny	–	Niskie	Publiczny	Około 11 mln aktywnych użytkowników i ok. 22 mln użytkowników rozwiązywania bazującego na tożsamości bankowej	Tak
mObywatel	Dane uwidocznione w dowodzie osobistym (bez fotografii twarzy); potencjalnie możliwość rozszerzenia zakresu danych o inne dane z rejestrów publicznych	Stacjonarny, on-line, mobilny	Integracja z bazą dokumentów zastrzeżonych	Niskie	Komercyjny i publiczny	Potencjał użytkowników profilu zaufanego (ok. 11 mln)	Tak

Źródło: opracowanie własne.

6. Weryfikacja wideo na podstawie dowodu osobistego

Wideoweryfikacja na podstawie warstwy graficznej dowodu osobistego to proces polegający na porównaniu – poprzez transmisję wideo w czasie rzeczywistym – danych identyfikujących osobę fizyczną z jej dokumentu tożsamości z wizerunkiem wynikającym z transmisji wideo. W przypadku automatycznej weryfikacji zgodność wizerunku na dokumencie z aktualnym wizerunkiem osoby poddawanej identyfikacji badana jest za pomocą algorytmów sztucznej inteligencji. Analizowana jest również tzw. funkcja żywotności człowieka (poprzez wymóg wykonywania określonych czynności fizycznych, np. poruszania głową), aby wyeliminować przypadki *spoofingu*. Dane stanowiące tożsamość osoby pobierane są z warstwy graficznej poprzez odczytanie ich z kamery podczas transmisji wideo. Autentyczność dokumentu jest sprawdzana przez wymóg przedstawienia do kamery określonych zabezpieczeń optycznych dowodu osobistego. W praktyce numer dokumentu jest automatycznie sprawdzany w bazach dokumentów zastrzeżonych. Wideoweryfikacja może być w pełni automatyczna lub wspomagana przez operatora, który instruuje osobę o poszczególnych czynnościach.

Wideoweryfikacja na podstawie warstwy elektronicznej dowodu osobistego jest procesem podobnym do przedstawionego powyżej. Główną różnicą jest źródło danych stanowiących atrybuty tożsamości. Są one (w tym zdjęcie twarzy) pobierane bezpośrednio z aplikacji ICAO zapisanej w mikroprocesorze dowodu osobistego. Są to dane, które jednocześnie pojawiają się na jego warstwie graficznej. Jednak zgodnie z wymogami ICAO dane przechowywane w warstwie elektronicznej nie zawierają narodowych znaków diakrytycznych. Oznacza to, że dane w warstwie graficznej mogą różnić się od danych w warstwie elektronicznej. Odczyt danych odbywa się za pomocą transmisji NFC, np. za pomocą smartfona. Warunkiem odczytania danych z aplikacji ICAO jest podanie lub zeskanowanie strefy odczytu maszynowego (MRZ), czyli ciągu alfanumerycznego wydrukowanego na dowodzie osobistym. Autentyczność dokumentu weryfikowana jest na podstawie elektronicznego certyfikatu wystawcy dowodu osobistego odczytanego z chipa karty (Country Signing Certification Authority i Country Verifying Certification Authority). Sprawdzenie optycznych zabezpieczeń dokumentu nie jest wymagane.

7. Rozwiązania oparte na tożsamości bankowej

Rozwiązanie to polega na wykorzystaniu już zrealizowanego w bankach procesu identyfikacji (niekoniecznie elektronicznego) – przy pierwotnym nawiązywaniu relacji biznesowych pomiędzy daną osobą a bankiem. Przepisy polskiego prawa bankowego wymagają bardzo rzetelnego i precyzyjnego procesu identyfikacji osoby, która chce zostać klientem banku. Jedynie właściwie zidentyfikowana osoba może uzyskać w banku

elektroniczny środek identyfikacji umożliwiający korzystanie z bankowości elektronicznej. Ideą posługiwania się tożsamością bankową jest to, że za pomocą nadanego przez bank środka identyfikacji elektronicznej (np. indywidualnego loginu z hasłem) klient banku (a równocześnie posiadacz ww. środka identyfikacji elektronicznej) może potwierdzić swoją tożsamość w innej usłudze świadczonej przez inny podmiot. To rozwiązanie popularne w Polsce i oferowane przez firmę należącą do polskiego sektora bankowego (pod nazwą handlową mojeID). Nie wymaga od użytkownika wykonywania dodatkowych czynności identyfikacyjnych poza wprowadzeniem loginu i hasła do systemu transakcyjnego banku. Jego dane (atrybuty tożsamości) zostały już wcześniej zarejestrowane i skontrolowane, a tożsamość została zweryfikowana przez bank. Tak więc tożsamość bankowa otwiera drzwi do innych usług on-line, zapewniając dostawcy usług niezbędne atrybuty identyfikacyjne (np. imię i nazwisko, data urodzenia itp.) klienta. Dlatego jedyną czynnością sprawdzającą w procesie bazującym na tożsamości bankowej jest weryfikacja zgodności loginu i hasła przez bank, który wydał środek identyfikacji elektronicznej. Jednocześnie przypuszcza się, że na etapie nawiązywania pierwotnej relacji klienta z bankiem i wydania klientowi środka identyfikacji elektronicznej proces identyfikacji klienta został przeprowadzony prawidłowo i wydany przez bank środek identyfikacji elektronicznej może także stanowić podstawę dla innego podmiotu do wydania innego środka.

8. AIS

Dyrektywa PSD2¹⁴ otworzyła nowe możliwości wykorzystania danych klientów będących w posiadaniu banków. Dyrektywa wykreowała podwaliny nowego rynku, tzw. otwartego rynku bankowego (*open banking*), tworzonego przez różnego rodzaju usługi, które mogą być świadczone na podstawie trzech filarów:

- 1) dostępu do informacji o koncie klienta (AIS, Account Information Service),
- 2) inicjacji płatności (PIS, Payment Initiation Service),
- 3) potwierdzenia dostępności środków na rachunku (CAF, Confirmation of the Availability of Funds).

Zgodnie z PSD2 realizacja powyższych usług jest możliwa nie tylko bezpośrednio przez klienta danego banku, lecz także – w imieniu klienta – przez upoważnioną osobę trzecią (TPP, Third Party Provider). W przypadku identyfikacji szczególne znaczenie ma usługa AIS. Polega ona na dostarczaniu przez podmiot uprawniony do świadczenia tej usługi, na polecenie i za zgodą użytkownika, skonsolidowanych informacji dotyczących rachunku lub rachunków płatniczych użytkownika dostępnych on-line prowadzonych przez jednego lub wielu innych dostawców usług płatniczych. Usługa umożliwia zatem

¹⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, Dz. Urz. UE L 337 z 23.12.2015 r.

dostęp do określonych danych identyfikujących osobę (imię i nazwisko oraz adres). Dzięki udostępnieniu przez banki swojego API możliwe jest pobranie przez TPP (i klienta – po zalogowaniu się do systemu bankowego) danych klienta i na tej podstawie ustalenie ich zgodności z zadeklarowanymi danymi.

Zakres udostępnianych danych jest znacznie mniejszy niż w przypadku omówionych wcześniej rozwiązań. W praktyce korzystanie z usługi AIS jest dość utrudnione, ponieważ pomimo nałożonego na banki obowiązku oferowania interfejsu dostępowego do komunikacji z TPP nie ma w tym zakresie jednolitego standardu i jednoznacznego katalogu danych, jakie banki mają udostępniać w ramach AIS.

9. Przelew weryfikacyjny

Przelew weryfikacyjny to dość popularna forma zdalnej weryfikacji tożsamości. Rozwiązanie to wykorzystuje fakt, że dane wymagane do realizacji przelewu bankowego to m.in. imię i nazwisko lub nazwa nadawcy przelewu, czyli osoby posiadającej rachunek bankowy obciążany w związku z przelewem. Przelew weryfikacyjny jest więc zwykłym przelewem bankowym, zazwyczaj na niewielką kwotę (np. 1 zł lub 0,01 zł), zlecanym przez osobę identyfikowaną podmiotowi weryfikującemu tożsamość. Koncepcja przelewu weryfikacyjnego opiera się zatem na porównaniu danych personalnych wskazanych w procesie identyfikacji z danymi widniejącymi na zleceniu przelewu (nazwa nadawcy przelewu). Przelewy weryfikacyjne są dość popularne zwłaszcza w przypadku pożyczek krótkoterminowych, a zwłaszcza usług Buy Now Pay Later (BNPL). Ta forma weryfikacji tożsamości opiera się przede wszystkim na zaufaniu, jakie towarzyszy bankom oraz procedurach otwierania rachunków bankowych. Jednocześnie korzysta z domniemania, że osoba posiadająca rachunek bankowy została prawidłowo zweryfikowana w momencie otwarcia rachunku i nie przekazywała osobom trzecim danych uwierzytelniających do swojego rachunku. Słabością przelewu weryfikacyjnego jest ograniczony zakres danych osoby podlegającej identyfikacji. Na tę słabość zwróciła uwagę również Komisja Nadzoru Finansowego, wskazując, że „dane te posłużą jedynie do weryfikacji tożsamości klienta”¹⁵.

10. Kwalifikowany podpis elektroniczny

Podpis elektroniczny oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które są używane

¹⁵ https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_meto-de_wideoweryfikacji_66066.pdf (dostęp: 13.09.2022).

przez podpisującego jako podpis. Kwalifikowany podpis elektroniczny oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego. Siłą podpisu kwalifikowanego jest gwarancja prawna, która traktuje go tak samo jak podpis własnoręczny.

Zaawansowany mechanizm podpisu elektronicznego bazuje na kryptografii klucza publicznego, która jest zagadnieniem tak obszernym i specjalistycznym, że wymagałaby odrębnego opracowania. Kwalifikowany podpis elektroniczny to narzędzie zapewniające silną weryfikację tożsamości. Nie jest to jednak rozwiązanie powszechne, gdyż obecnie stosowane jest głównie przez przedsiębiorców, a jego zakres stosowania obejmuje przede wszystkim czynności wynikające z przepisów prawa (np. podpisywanie sprawozdań finansowych). Stąd jego przydatność społeczna jest ograniczona. Równocześnie należy podkreślić, że co do zasady podpis kwalifikowany jest usługą zaufania przeznaczoną do podpisywania dokumentów, a jej przydatność w dziedzinie identyfikacji elektronicznej ma charakter poboczny.

11. Profil osobisty

Zgodnie z art. 2 ust. 1 pkt 10 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych¹⁶ profil osobisty jest środkiem identyfikacji elektronicznej zawierającym dane potwierdzone certyfikatem identyfikacji i uwierzytelniania. Obecnie wydawane w Polsce dowody osobiste zawierają warstwę elektroniczną. Warstwa elektroniczna obejmuje m.in. certyfikat identyfikacji i uwierzytelnienia z danymi umożliwiającymi elektroniczną identyfikację i uwierzytelnienie. Identyfikatory spełniają wymagania stawiane kwalifikowanemu urządzeniu do składania podpisu elektronicznego i umożliwiają jego posiadaczowi:

- 1) uwierzytelnianie w serwisach internetowych za pomocą profilu osobistego,
- 2) używanie podpisu osobistego;
- 3) potwierdzanie obecności w określonym czasie i miejscu.

Posługiwanie się dowodem osobistym z profilem osobistym dla wyżej wskazanych celów wymaga posiadania przez użytkownika czytnika kart i odpowiedniego oprogramowania. Mikroprocesor RFID dowodu osobistego, w którym umieszczona jest warstwa elektroniczna, umożliwia bezstykową komunikację pomiędzy dowodem a czytnikiem (np. smartfonem). Z tego powodu, aby odczytać dane z warstwy elektronicznej, wystarczy przyłożyć dokument do czytnika. Użytkownik wprowadza następnie tzw. nr CAN (Card Access Number), który jest wydrukowany w formie kodu kreskowego na rewersie dowodu osobistego. Jest to wymagane w celu nawiązania (poprzez czytnik kart)

¹⁶ Dz. U. z 2010 r. Nr 167, poz. 1131 z późn. zm.

połączenia pomiędzy warstwą elektroniczną dowodu osobistego a urządzeniem lub systemem teleinformatycznym. Po wprowadzeniu numeru CAN sprawdzana jest jego zgodność w celu ustanowienia szyfrowanego połączenia pomiędzy czytnikiem a dowodem osobistym (PACE; Password Authenticated Connection Establishment).

Rozwiązanie bazujące na profilu osobistym jest oferowane przez jedną ze spółek Skarbu Państwa w formie aplikacji instalowanej na smartfony. W Polsce, ze względu na stosunkowo małą liczbę wydanych elektronicznych dowodów osobistych, nie jest to obecnie powszechnie stosowane rozwiązanie.

12. Profil zaufany

Zgodnie z art. 3 pkt 14 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne¹⁷ profil zaufany jest środkiem identyfikacji elektronicznej zawierającym zbiór danych identyfikujących i opisujących osobę fizyczną. Profil zaufany potwierdza tożsamość osoby w kontaktach z administracją publiczną. Wydawany jest na wniosek obywatela po pozytywnej realizacji pierwszych etapów procesu identyfikacji. Dopuszczalne są następujące metody w tym zakresie:

- 1) poprzez fizyczną weryfikację tożsamości na podstawie okazanego dowodu osobistego lub paszportu lub innego dokumentu pozwalającego na jednoznaczne potwierdzenie tożsamości osoby;
- 2) przy użyciu kwalifikowanego podpisu elektronicznego, pod warunkiem, że podpis zawiera co najmniej imię i nazwisko oraz PESEL;
- 3) przy użyciu środka identyfikacji elektronicznej służącego do uwierzytelniania w systemie informatycznym banku krajowego (rozwiązanie bazujące na tzw. tożsamości bankowej), o ile środek ten potwierdza imię i nazwisko oraz PESEL;
- 4) z wykorzystaniem profilu osobistego.

Weryfikacja fizyczna przybiera klasyczną formę sprawdzania tożsamości na podstawie określonych dokumentów publicznych. Etap ten może przeprowadzić konsul, naczelnik urzędu skarbowego, wojewoda, Zakład Ubezpieczeń Społecznych i Narodowy Fundusz Zdrowia, banki krajowe lub operatorzy pocztowi (tzw. punkty potwierdzenia). Założenie profilu zaufanego z wykorzystaniem kwalifikowanego podpisu elektronicznego nie wydaje się racjonalne, gdyż w rzeczywistości oznacza stworzenie jednego identyfikatora elektronicznego (o funkcjonalności ograniczonej do kontaktów z administracją publiczną) przy użyciu innego elektronicznego środka identyfikacji (o szerokiej funkcjonalności).

¹⁷ Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.

13. mObywatel

mObywatel to mobilna aplikacja rządowa będąca cyfrowym portfelem, w którym można przechowywać określone dane pochodzące z dokumentów publicznych (takich jak dowód osobisty czy prawo jazdy). Szczególną cechą rozwiązania mObywatel jest możliwość zdalnej weryfikacji tożsamości poprzez przekazanie danych osobowych (zdjęcie, imię i nazwisko) dowolnej osobie/instytucji/firmie w postaci kodu QR. Dane w tym rozwiązaniu pochodzą bezpośrednio z rejestrów publicznych, w szczególności z rejestru dowodów osobistych. mObywatel jest swoistym prekursorem europejskiego portfela tożsamości cyfrowej, o którym mowa we wniosku dotyczącym rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w zakresie ustanowienia ram europejskiej tożsamości cyfrowej (eIDAS2)¹⁸. mObywatel nie zawiera szeregu funkcjonalności przypisanych do projektowanego europejskiego portfela tożsamości cyfrowej, jednak koncepcyjnie jest do niego podobny. Został on stworzony głównie z myślą o kontaktach obywatela z administracją publiczną, ale przepisy nie wykluczają możliwości jego wykorzystania, a zwłaszcza funkcjonalności zdalnej weryfikacji tożsamości, w relacjach obywatel–sektor biznesowy.

14. Hasło jednorazowe SMS

Numery telefonów wydawane przez polskich operatorów GSM są indywidualnie przyporządkowane do poszczególnych osób. Dotyczy to również przedpłaconych kart SIM. W konsekwencji numer telefonu jest specyficznym atrybutem tożsamości, który jest jednoznacznie, choć nie na stałe, związany z daną osobą. Ze względu na powszechność korzystania z telefonów komórkowych oraz wspomnianą wcześniej indywidualną relację z osobą, popularne stało się stosowanie haseł jednorazowych w SMS-ach jako metody uwierzytelniania i autoryzacji. Ryzyko nadużyć związanych z korzystaniem z telefonu komórkowego, m.in. przejęcie przez osobę nieuprawnioną, powoduje, że nie jest to metoda bezpieczna. Dlatego ogranicza się tylko do uwierzytelniania i autoryzacji. Jest powszechnie stosowana w bankowości, również jako jeden z elementów tzw. silnego uwierzytelniania klienta.

15. Hasła do aplikacji

Szeroka dostępność usług on-line, a jednocześnie duża popularność telefonów komórkowych sprawiły, że na znaczeniu zyskały aplikacje mobilne, które z jednej

¹⁸ <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0281&from=EN> (dostęp: 13.09.2022).

strony zapewniają wygodny i bezpłatny dostęp do usług, a z drugiej – dodatkowy instrument autoryzacji i uwierzytelnianie. Tym samym hasła do aplikacji stały się alternatywnym instrumentem autoryzacji i uwierzytelniania dla jednorazowych haseł SMS. Są uważane za bezpieczniejsze niż hasła SMS, ponieważ nie są ujawniane (w przeciwieństwie do haseł SMS wyświetlanych na ekranie smartfona).

16. Karta TAN

Karty z numerami kodów (Transaction Authentication Number, TAN) były jednym z pierwszych instrumentów uwierzytelniania i autoryzacji, popularne zwłaszcza w bankowości. W czasach gdy telefony komórkowe stanowiły dobra luksusowe, a ceny SMS-ów były wysokie, karty TAN intensywnie się rozwijały. Karty TAN mogą stanowić wydruk kodów na zwykłej kartce papieru lub na karcie z tworzywa sztucznego, podobnej do karty kredytowej. Często kolejne numery (kody) pokrywane są nadrukiem lub folią, którą usuwa się przed użyciem, ujawniając ukryte hasło – ułatwia to ustalenie liczby niewykorzystanych kodów, a jednocześnie zabezpiecza kody przed nieautoryzowanym odczytem.

17. Token

Token to urządzenie peryferyjne służące do uzyskiwania dostępu do chronionych zasobów elektronicznych. Idea tokena opiera się zwykle na wygenerowanym przez niego kodzie, czyli jednorazowym hasle. Jest to więc bardziej wyrafinowana, zdigitalizowana forma karty TAN. Token jest używany dodatkowo lub zamiast hasła. Niektóre tokeny mogą przechowywać klucze kryptograficzne lub hasła. Tokeny są nadal obecne jako instrumenty wykorzystywane w procesie identyfikacji (uwierzytelniania i autoryzacji), zwłaszcza w obszarze bankowości, ale zakres ich wykorzystania jest znacznie większy niż wcześniej.

18. Wideoweryfikacja na podstawie wzorca zapisanego w nośniku danych użytkownika lub w rejestrach usługodawcy

Wideoweryfikacja może bazować na wizerunku twarzy odczytywanego na żywo w procesie identyfikacji, ale porównywanego ze wzorem zarejestrowanym w innym zasobie niż dokument identyfikacyjny (i np. jego mikroprocesor). W takim przypadku dane biometryczne rzadko są przechowywane centralnie w bazie danych biometrycznych usługodawcy, ale raczej lokalnie, tj. na urządzeniu należącym do użytkownika (np. w smartfonie). Ta metoda ogranicza się tylko do uwierzytelniania i autoryzacji, a pozostałe (wcześniejsze) etapy procesu identyfikacji muszą być wykonane innymi metodami.

19. Weryfikacja odcisków palców na podstawie wzorca zapisanego w nośniku danych użytkownika lub w rejestrach usługodawcy

Ta metoda jest analogiczna do wideoweryfikacji opartej na wzorcu przechowywanym w lokalnym nośniku danych lub w rejestrach usługodawcy. Ze względu na wrażliwość danych biometrycznych, jakimi są odciski palców, weryfikacja ogranicza się w praktyce do sytuacji, w której wzór odcisku palca jest przechowywany lokalnie (np. na posiadanym przez użytkownika smartfonie). Podobnie jak w poprzednim przypadku, ta metoda jest ograniczona do etapów uwierzytelniania i autoryzacji.

Wnioski

Polska ma bardzo rozwinięte i szeroko stosowane rozwiązania w zakresie zdalnej identyfikacji. Analizując ich zakres działania, można wyodrębnić dwie zasadnicze grupy:

- 1) rozwiązania pozwalające na weryfikację tożsamości i wydanie środka identyfikacji elektronicznej oraz
- 2) rozwiązania służące uwierzytelnianiu i autoryzacji.

Istotna część analizowanych rozwiązań znajduje swoje zastosowanie zarówno w publicznych, jak i komercyjnych kanałach.

Spośród wszystkich analizowanych rozwiązań na szczególną uwagę zasługują dwa, tj. rozwiązanie bazujące na tożsamości bankowej oraz wideoweryfikacja na podstawie warstwy elektronicznej dowodu osobistego. Tożsamość bankowa to rozwiązanie masowe oparte na procesach realizowanych przez banki podczas otwierania rachunków bankowych. Rozwiązanie to jest niezwykle wygodne dla użytkownika, ponieważ nie wymaga żadnych czynności poza standardowym logowaniem do systemu bankowego. Jednocześnie jest to rozwiązanie bezpieczne, ponieważ banki, na podstawie obowiązującego prawa i własnego interesu, przy nawiązywaniu pierwszej relacji z klientem przywiązują dużą wagę do weryfikacji tożsamości. Ze względu na te cechy tożsamość bankowa jest wykorzystywana jako metoda potwierdzania tożsamości w celu uzyskania innego środka identyfikacji elektronicznej, jakim jest profil zaufany.

Wideoweryfikacja oparta na warstwie elektronicznej dowodu osobistego jest również rozwiązaniem bardzo bezpiecznym, gdyż eliminuje subiektywną weryfikację tożsamości na podstawie wizerunku twarzy oraz subiektywną weryfikację autentyczności dokumentów tożsamości. Czynności te wykonywane są automatycznie. Porównania twarzy dokonują systemy informatyczne oparte na sztucznej inteligencji i zapewniające bardzo niski poziom błędów. Autentyczność dokumentu jest weryfikowana na podstawie

elektronicznych certyfikatów, które nie zostały jak dotąd sfałszowane przez przestępców. Jedynym problemem, jaki pozostaje, jest obecnie stosunkowo niewielka liczba dowodów osobistych z warstwą elektroniczną. Jednak wzrasta ona systematycznie w miarę wygasania terminu ważności dowodów osobistych bez mikroprocesora.

Tożsamość bankowa i wideoweryfikacja na podstawie warstwy elektronicznej dowodu osobistego zapewniają zatem największą użyteczność społeczną pod względem bezpieczeństwa i potencjalnej dostępności dla użytkowników.

Bibliografia

Akty prawne

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, Dz. Urz. UE L 337 z 23.12.2015 r.
- 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, Dz. Urz. UE L 257 z 28.08.2014 r.
- 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), Dz. U. UE L 119 z 4.05.2016 r.
- Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych, Dz. U. z 2010 r. Nr 167, poz. 1131 z późn. zm.
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.
- Wniosek Komisji Europejskiej z dnia 3 czerwca 2021 r.: Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej; COM(2021) 281 final.

Literatura

- Allen C., *The path to self-sovereign identity*, 2016, <https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/> (dostęp: 13.09.2022).
- Girdwoyń P., *Zarys kryminalistycznej taktyki obrony*, Zakamycze, Kraków 2004.
- Goode A., *Digital identity: solving the problem of trust*, „Biometric Technology Today” 2019, vol. 2019, issue 10.
- Sakson-Obada O., *Rozwój ja cielesnego w kontekście wczesnej relacji z opiekunem*, „Roczniki Psychologiczne” 2008, 11(2).

- Technical Report TR 119 460 V1.1.1 (2021-02): Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects*, European Telecommunications Standards Institute ETSI 2021, https://www.etsi.org/deliver/etsi_tr/119400_119499/119460/01.01.01_60/tr_119460v010101p.pdf (dostęp: 13.09.2022).
- Technology Landscape for Digital Identification*, World Bank 2018, <https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf> (dostęp: 13.09.2022).
- Toth K., Anderson-Priddy A., *Self-sovereign digital identity: a paradigm shift for identity*, „IEEE Security & Privacy Magazine” 2019, 17(3).
- Wagner K. *et al.*, *Self-sovereign identity. a position paper on blockchain enabled identity and the road ahead*, Blockchain Bundesverband: Berlin, Germany 2018, https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity_-_Blockchain-Bundesverband-2018.pdf (dostęp: 13.09.2022).

Analysis of electronic identification methods used in Poland

Summary: The article is based on the analysis of technological solutions used in Poland in the field of electronic (remote) identification. These solutions were analyzed in terms of various criteria, including: adequacy to individual stages of the identification process as well as various types of functionalities and features, such as scope of used data, scope of applications, requirements for service providers, as well as expected compliance with eIDAS2. The article leads to the conclusion that Poland has very developed and widely used solutions in the field of electronic identification. In principle, they may be grouped into tools used to issue means of electronic identification and tools used in authentication as well as authorisation stages. Moreover, a significant part of the analyzed tools are applicable both in the public and commercial channels. Among all the solutions constituting the subject of this research, the greatest social utility from the point of view of security and public accessibility is ensured by: bank identity solutions and video verification based on the electronic layer of the ID card.

Keywords: eIDAS2, identity, identification, means of electronic identification.