WOJCIECH WODO, DAMIAN RYBAK, PRZEMYSŁAW BŁAŚKIEWICZ

Analiza ekosystemu tożsamości cyfrowej w Polsce, stopnia jego wdrożenia i zastosowanie dowodów osobistych z warstwą elektroniczną

Oficyna Wydawnicza Politechniki Wrocławskiej @ Wrocław 2023

WOJCIECH WODO, DAMIAN RYBAK, PRZEMYSŁAW BŁAŚKIEWICZ

Analiza ekosystemu tożsamości cyfrowej w Polsce, stopnia jego wdrożenia i zastosowanie dowodów osobistych z warstwą elektroniczną

Oficyna Wydawnicza Politechniki Wrocławskiej @ Wrocław 2023

Recenzent
dr Miłosz Brakoniecki

Opracowanie redakcyjne i korekta
Katarzyna Sosnowska

Źródło ilustracji na okładce
Olena Ostapienko, iStockphoto

Projekt graficzny oraz skład i łamanie
Janusz M. Szafran

OFICYNA WYDAWNICZA POLITECHNIKI WROCŁAWSKIEJ
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
https://www.oficyna.pwr.edu.pl
https://ksiegarnia.pwr.edu.pl
oficwyd@pwr.edu.pl
zamawianie.ksiazek@pwr.edu.pl

ISBN 978-83-7493-245-5
DOI 10.37190/wodo-rybak-blaskiewicz-2023

Spis treści

Wstęp

Nowy e-dowód to nie tylko środek identyfikacji stosowany w interakcjach z administracją publiczną, ale również doskonałe narzędzie, które można wykorzystywać w sektorze komercyjnym podczas zdalnego i fizycznego potwierdzania tożsamości czy elektronicznego podpisywania dokumentów.

W pracy zostanie omówiona cała gama nowych rozwiązań umożliwiających błyskawiczną i niezawodną weryfikację autentyczności dokumentów z warstwą elektroniczną. Dbanie o ochronę swoich danych osobowych jest w takich sytuacjach niezwykle ważne, z tego względu przedstawiony w publikacji zbiór dobrych praktyk związanych z bezpiecznym użytkowaniem nowych dokumentów jest kluczowy. Większa troska w tym zakresie może uniemożliwić przestępstwo (np. wyłudzenie kredytu na nasze nazwisko czy założenie na nasze nazwisko konta bankowego, które zostanie wykorzystywane do prania brudnych pieniędzy).

Na przestrzeni kilku ostatnich lat ekosystem cyfrowych usług zaufania w Polsce znacząco się rozwinął i uspójnił. Przyczyniły się do tego zmiany legislacyjne na szczeblu Unii Europejskiej i idące w ślad za tym dostrajanie prawodawstwa krajowego. Powstały konkretne usługi zaufania udostępniane publicznie i komercyjnie, które zostały ze sobą zintegrowane i pozwalają w znacznym stopniu uprościć wiele zadań z zakresu weryfikacji tożsamości, zawierania umów, składania wniosków czy przekazywania danych osobowych. W opracowaniu analizujemy poszczególne elementy składowe ekosystemu i pokazujemy, jak korzystać z nich efektywnie.

Odbiorcami pracy są – w założeniu autorów – jednostki sektora administracyjnego, jak i operatorzy usług kluczowych mający styczność z użytkownikami. Zawarte w pracy treści mogłyby być użyteczne również dla całego szeroko rozumianego sektora finansowego – w tym fintechów – oraz dla podmiotów publicznych – w szczególności tych odpowiedzialnych za obrót elektroniczny w sferze publicznej.

Informacje zawarte w opracowaniu będą przydatne także dla osób już posługujących się e-dowodem oraz tych, którzy dołączą do grupy jego posiadaczy. Podane w monografii przykłady użycia pozwolą przedstawić ciągle rosnące

możliwości wykorzystania nowoczesnych dokumentów tożsamości i innych cyfrowych usług zaufania.

Wartością dodaną opracowania jest wskazanie instytucjom, firmom i użytkownikom rozwiązań pozwalających na uproszczenie i podniesienie wiarygodności procesów związanych z weryfikacją tożsamości klientów korzystających z dokumentów tożsamości posiadających warstwę elektroniczną, np.:

- Zdalna weryfikacja tożsamości – szybka i sprawna dzięki rozwiązaniom typu eID[1] firmy Identt czy eDo App[2] dla biznesu firmy PWPW jest szczególnie przydatna w sytuacjach takich jak pandemia.
- Silna weryfikacja tożsamości podczas wizyty np. w banku czy urzędzie – automatyczne mechanizmy weryfikacji autentyczności i integralności oparte na kryptografii w warstwie elektronicznej wraz z porównaniem biometrycznym są niezawodne i eliminują błąd ludzki.
- Nowe możliwości silnego uwierzytelniania (ang. *strong customer authentification* – SCA) w usługach cyfrowych – uwierzytelnienie klienta przez serwis bankowy, które odbywa się z wykorzystaniem dokumentu tożsamości jako składnika sprzętowego.
- Ograniczenie oszustw za pomocą mocnej weryfikacji klienta dostępnej w różnych kanałach.
- Wykorzystanie warstwy elektronicznej zawartej w paszportach do weryfikacji tożsamości obcokrajowców (dzięki zgodności z normą ICAO).
- Biometryczne porównanie twarzy klienta ze zdjęciem dostępnym w warstwie elektronicznej dowodu osobistego w znacznie lepszej jakości niż zdjęcie znajdujące się w warstwie graficznej dokumentu – stanowi to ograniczenie posługiwania się kradzionymi i pożyczonymi dokumentami tożsamości.
- Zawieranie umów, składanie oświadczeń i wniosków dzięki budowie cyfrowego obiegu dokumentów poprzez wykorzystanie podpisów osobistych zawartych w e-dowodach.
- Wykorzystywanie cyfrowych portfeli tożsamości integrujących wiele atrybutów użytkownika z różnych źródeł, dających pełniejszą kontrolę nad zarządzaniem nimi oraz ich udostępnianiem.

1 https://e-id.pl/

2 https://www.edoapp.pl/

1. Wprowadzenie

Obecnie mamy do czynienia z gwałtownym przyspieszeniem procesu elektronizacji obrotu gospodarczego i stosowania usług zaufania opartych na tożsamości cyfrowej. Sytuacja wygląda podobnie również w przypadku dostępu do usług administracji publicznej. Część zmian była zapoczątkowana wewnętrznie, a część została wprowadzona jako odpowiedź na rozporządzenia Unii Europejskiej (UE). Dodatkowo wzajemne przenikanie się na poziomie państw regulacji i aktów publikowanych przez UE doprowadziło w Polsce do zamieszania wynikającego z różnic w nazewnictwie i definicjach.

W Polsce nie jest dostępne kompleksowe opracowanie dotyczące ekosystemu tożsamości cyfrowej, stopnia wdrożenia jego elementów i możliwości ich użycia. Harmonizacja wiedzy i procesów związanych z tożsamością elektroniczną w Polsce i Europie jest wyzwaniem z uwagi nie tylko na ciągłe zmiany legislacyjne i techniczne w tym obszarze, ale również na brak ugruntowanych źródeł wiedzy i kampanii edukacyjnych. Temat cyfrowej tożsamości, chociaż dotyczy każdego obywatela, z rozmaitych powodów nie jest wystarczająco popularny w debatach publicznych.

Temat tożsamości cyfrowej może więc jawić się jako trudny, a przez to mało zachęcający do zgłębiania go. Niniejsza publikacja jest próbą zmiany tego nastawienia przez podjęcie zagadnień z tego obszaru i dokonanie harmonizacji obecnego stanu wiedzy o szeroko pojętej tożsamości cyfrowej w Polsce, ze szczególnym uwzględnieniem nowych dowodów osobistych z warstwą elektroniczną.

Zagadnienia dotyczące cyfrowej tożsamości są złożone, ponieważ wymagają uwzględniania wielu aspektów. Sytuację komplikuje fakt, że informacje z tego zakresu są na ogół rozproszone, a ich scalenie bardzo często powoduje uwidocznienie obszarów, które były wcześniej pomijane – również na stronach rządowych, które w pierwszej kolejności powinny informować o udogodnieniach i usprawnieniach wprowadzanych w ramach wieloletnich projektów finansowanych z pieniędzy podatników. Dlatego zebranie wszystkich danych i ogólnie dostępnych informacji, ich przeanalizowanie i wyciągnięcie wniosków oraz połączenie w logiczną całość jest nie tylko pracochłonne, ale i czasochłonne.

1.1. Cel opracowania, jego zakres i metodyka

Celem opracowania jest dokonanie przeglądu obecnego stanu ekosystemu elektronicznej tożsamości w Polsce w różnych kontekstach, zaczynając od podstaw prawnych, przechodząc przez obecny stan wdrożenia zagadnień związanych z tożsamością cyfrową, a kończąc na konkretnych rozwiązaniach czy narzędziach technologicznych, umożliwiających wykorzystanie danych osobowych zapisanych w formie elektronicznej. W każdym fragmencie opisującym implementację w praktyce poszczególnych rozwiązań jest zawarta krótka opinia o ich użyteczności, zgodności z regulacjami i ocenie zawartych w nich mechanizmów bezpieczeństwa.

Zamiarem autorów było uporządkowanie informacji o istniejących usługach ekosystemu tożsamości cyfrowej i wskazanie przypadków ich użycia przez instytucje i obywateli w codziennych sytuacjach.

Metodyka pracy opiera się na przeglądzie dostępnych źródeł z zakresu literatury przedmiotu, w tym materiałów o charakterze dokumentacji technicznej, projektów aktów prawnych i wzmianek technologicznych. Analizie został poddany stan ekosystemu tożsamości cyfrowej w Polsce (w tym w kontekście europejskim), z uwzględnieniem składających się na niego aktorów i procesów oraz relacji między nimi. Zastosowano podejście opisujące najpierw ogólnie stan rzeczy, a następnie szczegóły wyróżnionych aspektów. W ramach badań poddano analizie różne przypadki użycia cyfrowych usług zaufania i tożsamości elektronicznej w kontekście oceny ich bezpieczeństwa, wygody i wartości dla państwa polskiego i jego obywateli.

Na podstawie zebranych informacji i wiedzy eksperckiej autorów sformułowano dobre praktyki i rekomendacje w zakresie zastosowania poszczególnych elementów ekosystemu tożsamości cyfrowej.

Wdrożone w 2019 r., a następnie uaktualnione w 2021, dowody osobiste z warstwą elektroniczną (e-dowody) rozpoczynają zupełnie nowy rozdział w historii identyfikacji elektronicznej w Polsce. Wprowadzają wiele udogodnień, z którymi warto się zapoznać, aby móc z nich w pełni korzystać. Wraz z nowymi funkcjonalnościami pojawiają się jednak również nowe kategorie zagrożeń, które mogą być wykorzystane przez adwersarzy. Kluczem do zapewnienia bezpieczeństwa jest znajomość rozwiązań i świadomość związanych z nimi zagrożeń.

1.2. Struktura opracowania

Praca została podzielona na rozdziały, które odpowiednio adresują poszczególne elementy ekosystemu tożsamości cyfrowej w Polsce. Kwestie uwarunkowań prawnych i legislacyjnych dotyczących obszarów tożsamości cyfrowej, dokumentów identyfikacyjnych i usług zaufania są przedstawione w rozdz. 2. Wymieniono instytucje i organizacje zarówno na szczeblu międzynarodowym, jak i krajowym, które mają istotny wpływ na rozwój i popularyzację polskiego ekosystem eID.

Rozdział 3 zawiera szczegółowy opis składowych ekosystemu eID: krajowego schematu identyfikacji elektronicznej i krajowej infrastruktury zaufania, a także organizacji i instytucji mających wpływ na jego kształtowanie.

Tematowi dowodów osobistych i ich nowych wersji z elektroniczną warstwą poświęcony jest rozdział 4. Opisane są w nim zarówno właściwości fizyczne, jak i funkcjonalności cyfrowej warstwy dowodu. Wskazane są również dobre praktyki związane z jego użyciem.

Kwestie związane z narzędziami pozwalającymi na korzystanie z elektronicznych usług zaufania wraz z ich funkcjonalnościami zostały przedstawione w rozdziale 5. Zostały w nim uwzględnione aplikacje zarządzające e-dowodami, podpisami elektronicznymi i portfelem tożsamości.

W rozdziale 6 są przedstawione przypadki użycia elektronicznych usług zaufania w sektorze gospodarki oraz wskazane konkretne rozwiązania oferowane zarówno przez publiczny, jak i komercyjny sektor.

Podsumowanie podjętych tematów zawiera rozdział 7. Zostały w nim również wymienione wydarzenia o charakterze politycznym i legislacyjnym, kluczowe dla aktualnego i przyszłego stanu ekosystemu tożsamości cyfrowej w Polsce i Europie.

2. Normy prawne regulujące kwestie dotyczące e-tożsamości

Regulacje prawne są nieodzowne, ponieważ określają fundamenty i zakres działania podmiotów prawnych, określając ich prawa, obowiązki i kary, które można na nie nałożyć. Z punktu widzenia prawa polskiego nie bez znaczenia pozostaje członkostwo w Unii Europejskiej – krajowe regulacje prawne muszą być zintegrowane z prawodawstwem unijnym.

Nie inaczej jest w przypadku norm prawnych odnoszących się do e-tożsamości. Do tych najważniejszych, wpływających na kształtowanie systemu eID należą:

- *Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych*[3].
- *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* (eIDAS)[4].
- Przyszła nowelizacja rozporządzenia nr 910/2014 (eIDAS2)[5].
- *Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej*[6].
- *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1157 z dnia 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się*[7].

Rozporządzenia są najważniejszymi aktami prawnymi wydawanymi przez UE. Są wiążące, co oznacza, że muszą być stosowane w całości na całym obszarze wspólnoty.

Normy prawne zwykle są sformułowane na dużym poziomie ogólności. Z jednej strony pozostają więc dzięki temu, mimo ciągle zmieniającego się ekosystemu, aktualne. Z drugiej jednak wraz ze wzrostem poziomu ogólności zwiększa

3 https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20101671131/U/D20101131Lj.pdf
4 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32014R0910
5 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281
6 https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160001579/U/D20161579Lj.pdf
7 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32019R1157

się liczba obszarów, które nie są jasno sprecyzowane – w niektórych przypadkach może to utrudniać rozstrzygnięcie powstających w ich granicach niejasności.

2.1. Ustawa o dowodach osobistych

Dowód osobisty umożliwia stwierdzenie i potwierdzenie tożsamości i obywatelstwa jego posiadacza na terytorium Rzeczypospolitej Polskiej oraz innych państw członkowskich UE. Dokument ten musi posiadać każdy pełnoletni obywatel. Z tych względów dowód osobisty jest kluczowym elementem, na bazie którego jest budowana e-tożsamość w Polsce.

Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych[8] jest podstawowym aktem prawnym regulującym kwestie związane z dowodem osobistym, wprowadza podział na warstwę graficzną i elektroniczną. Warstwa elektroniczna zawiera:

- dane zamieszczone w warstwie graficznej, z wyjątkiem numeru CAN (ang. *Card Acces Number*)[9] i fizycznie złożonego podpisu posiadacza;
- dane biometryczne w postaci:
  - wizerunku twarzy w znacznie lepszej jakości niż zdjęcie osadzone w warstwie graficznej,
  - odcisków dwóch palców;
- certyfikaty wraz z danymi umożliwiającymi ich użycie:
  - certyfikat identyfikacji i uwierzytelnienia,
  - certyfikat podpisu osobistego, ale tylko w przypadku, gdy wnioskodawca wyraził zgodę na jego umieszczenie,
  - certyfikat potwierdzenia obecności;
- przestrzeń umożliwiającą zamieszczenie kwalifikowanego certyfikatu podpisu elektronicznego.

Nowy e-dowód spełnia wymogi kwalifikowanego urządzenia do składania podpisu elektronicznego, który został określony w rozporządzeniu eIDAS (ang. *electronic IDentification, Authentication and trust Services*). Korzystanie z podpisu kwalifikowanego wymaga wcześniejszego zakupienia odpowiedniego certyfikatu i umieszczenia go w warstwie elektronicznej dowodu osobistego za pomocą odpowiedniej procedury. Operacja wymaga osobistej wizyty w jednym

8 *Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych*. Dz.U. z 2010 Nr 167 poz. 1131. Dostępny w: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20101671131/U/D20101131Lj.pdf

9 Numer podawany podczas nawiązywania połączenia z warstwą elektroniczną dowodu tożsamości.

z punktów partnerskich danego wystawcy certyfikatu. Coraz częściej możliwe jest też skorzystanie z weryfikacji zdalnej w formie wideoweryfikacji lub za pośrednictwem bankowości elektronicznej. Certyfikaty kwalifikowane zwykle są wydawane na okres krótszy niż ważność samego e-dowodu. Obecnie na rynku polskim można zakupić certyfikaty ważne nie dłużej niż 5 lat[10].

Bardzo interesującym rozwiązaniem jest podpis osobisty (dostępny w nowym e-dowodzie). Dane opatrzone takim podpisem traktowane są przez podmioty publiczne równoważnie z podpisem własnoręcznym. W przypadku innych podmiotów konieczne jest wyrażenie zgody przez obie strony. W przyszłości takie rozwiązanie może być powszechnie wykorzystywane jako podpis elektroniczny podczas zdalnego zawierania umów.

Data ważności poszczególnych certyfikatów jest taka sama jak ważność samego dowodu osobistego. Podczas odbioru e-dowodu ustalane są kody umożliwiające korzystanie z certyfikatu identyfikacji i uwierzytelnienia (4-cyfrowy kod PIN1) oraz certyfikatu podpisu osobistego (6-cyfrowy kod PIN2). Przy odbiorze dowodu osobistego otrzymuje się również (w kopercie) kod PUK służący do odblokowania wyżej wymienionych certyfikatów po wpisaniu 3-krotnie nieprawidłowego kodu PIN.

Nowy e-dowód można również szybko unieważnić lub czasowo zawiesić. Ta ostatnia funkcja pozwala na zawieszenie do 14 dni wszystkich certyfikatów w dowodzie, jak i samego dowodu.

Do najważniejszych nowych możliwości uzyskiwanych przez posiadacza dowodu z warstwą elektroniczną można zaliczyć:

- uwierzytelnienie w usługach online za pomocą profilu osobistego;
- składanie podpisu osobistego, ale pod warunkiem jego obecności w warstwie elektronicznej;
- potwierdzanie obecności w określonym miejscu i czasie.

2.2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 (eIDAS)

Już w 2010 r. w ramach Europejskiej Agendy Cyfrowej dostrzeżono problemy utrudniające dalszy rozwój gospodarki cyfrowej na terenie UE. Główną prze-

10 https://www.oirpwarszawa.pl/wp-content/uploads/2022/01/kirp-zestawienie-ofert-podpisu-kwalifikowanego.pdf

szkodą było duże rozdrobnienie rynku cyfrowego połączone z brakiem interoperacyjności między poszczególnymi krajami członkowskimi. Taka sytuacja wymusiła rozpoczęcie prac nad rozporządzeniem, które miało ujednolicić rynek cyfrowy. Celem ustawodawcy było:

- opracowanie wspólnych podstaw bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi;
- utworzenie infrastruktury klucza publicznego na poziomie ogólnoeuropejskim;
- umożliwienie powstania wzajemnie uznawanych środków identyfikacji elektronicznej;
- wzmocnienie współpracy krajów członkowskich w zakresie bezpieczeństwa i interoperacyjności poszczególnych systemów identyfikacji elektronicznej.

Jednym z podstawowych elementów ułatwiających dalszy rozwój wspólnego rynku było wprowadzenie ujednoliconej nomenklatury w szeroko pojętych usługach elektronicznych. Poszczególne definicje zawarte w rozporządzeniu zostały przedstawione i dokładnie opisane w raporcie *Identyfikacja i uwierzytelnienie w usługach elektronicznych*[11] opracowanym przez ekspertów z Obserwatorium.biz. Do tych najważniejszych można zaliczyć:

- identyfikację elektroniczną;
- środek identyfikacji elektronicznej;
- usługę zaufania;
- podpis elektroniczny;
- walidację;
- zaawansowany podpis elektroniczny;
- kwalifikowany podpis elektroniczny.

Wszystkie postanowienia zawarte w eIDAS zakładają neutralność pod względem rozwiązań technologicznych. Rozwiązania te nie będą posiadały żadnych barier formalnych w postaci praw autorskich czy patentów, których obecność mogłaby spowolnić lub nawet utrudnić dalszy rozwój rynku cyfrowego.

Z perspektywy poprawy interoperacyjności bardzo ważna jest budowa Węzła Transgranicznego, który będzie umożliwiał korzystanie z notyfikowanych systemów identyfikacji elektronicznej rozwijanych przez inne kraje UE. Wza-

11 *Identyfikacja i uwierzytelnienie w usługach elektronicznych*. Dostępny w: https://zbp.pl/Aktualnosci/Wydarzenia/Przewodnik-Identyfikacja-i-uwierzytelnienie-w-uslugach-elektronicznych%E2%80%9D

jemne honorowanie środków identyfikacji elektronicznej jest oparte na zasadzie wzajemności, która dopuszcza wykorzystanie notyfikowanych środków identyfikacji elektronicznej we wszystkich krajach członkowskich.

Ostatnim ważnym elementem wprowadzonym w eIDAS są poziomy bezpieczeństwa (ang. *Levels of Assurance* – LoA)[12] odnoszące się do poszczególnych środków identyfikacji elektronicznej. Każdy poziom oznacza inny stopień zaufania względem zbioru danych pozwalających na identyfikację tożsamości, wykorzystywanych środków technicznych, standardów i procedur. W rozporządzeniu wyróżniono następujące poziomy bezpieczeństwa[13]:

- Niski poziom bezpieczeństwa (ang. *low level*) – nie wymaga przeprowadzenia weryfikacji tożsamości. Przykładem może być rejestracja konta na portalu społecznościowym. Podczas procesu uwierzytelnienia wymagane jest podanie przynajmniej jednego czynnika uwierzytelnienia (np. hasła).
- Średni poziom bezpieczeństwa (ang. *substantial level*) – odnosi się do środków identyfikacji elektronicznej, których zgodność została potwierdzona na podstawie danych przedstawionych przez wnioskodawcę. Do procesu uwierzytelnienia są wykorzystywane co najmniej dwa czynniki uwierzytelniania (np. hasło i kod SMS). W przypadku polskiego ekosystemu eID średni poziom bezpieczeństwa zapewnia profil zaufany i system mojeID. Stosowanie tego poziomu ma znacznie obniżyć ryzyko podszycia się lub modyfikacji tożsamości.
- Wysoki poziom bezpieczeństwa (ang. *high level*) – rejestracja wymaga osobistego stawiennictwa posiadacza dokumentu lub skorzystania z metod zdalnej weryfikacji na podstawie danych biometrycznych (ang. *supervised remote*). W przypadku identyfikacji elektronicznej konieczne jest uwierzytelnienie z wykorzystaniem co najmniej dwóch różnych elementów tego procesu (np. skorzystania z karty kryptograficznej i hasła). W polskim ekosystemie eID wysoki poziom bezpieczeństwa zapewnia profil osobisty, w którym identyfikacja odbywa się na podstawie e-dowodu. W kontekście art. 8 eIDAS stosowanie tego poziomu bezpieczeństwa ma zapobiec próbie podszycia się lub modyfikacji tożsamości, zaś podmiot zapewniający taki poziom spełnia określone standardy i bierze odpowiedzialność za prawidłowo przeprowadzoną weryfikację, a także jest jej gwarantem.

12 https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+Levels+of+Assurance

13 https://id4d.worldbank.org/guide/levels-assurance-loas

2.3. eIDAS 2

W 2021 roku Komisja Europejska (KE) opublikowała propozycję nowelizacji eIDAS, tj. rozporządzenia ustanawiającego ramy tożsamości cyfrowej w UE. Propozycja ta jest ogromnym krokiem regulacyjnym w kierunku harmonizacji europejskiego rynku tożsamości elektronicznej oraz stworzenia wspólnych ram i standardów wdrażania nowoczesnych rozwiązań w obszarze usług zaufanych. Stwierdzono, że wdrożenie eIDAS (rozporządzenia pierwotnego) ujawniło jego niekompletność w kontekście nowych potrzeb rynkowych, głównie w odniesieniu do sektora publicznego ze względu na ograniczone możliwości podłączenia się do systemu przez prywatnych dostawców usług, niewystarczającą dostępność zgłoszonych rozwiązań z zakresu identyfikacji elektronicznej we wszystkich państwach członkowskich i brak elastyczności w zakresie wspierania różnych przypadków użycia.

Obecne ramy eIDAS nie obejmują dostarczania atrybutów elektronicznych, takich jak zaświadczenia lekarskie lub kwalifikacje zawodowe, co utrudnia zapewnienie europejskiego prawnego uznania takich referencji w formie elektronicznej. Ponadto eIDAS nie pozwala użytkownikom na ograniczenie udostępniania danych dotyczących ich tożsamości do tego, co jest ściśle niezbędne do świadczenia usługi.

W odpowiedzi na diagnozę z 2021 r. nowe rozporządzenie zaoferuje europejskie ramy tożsamości cyfrowej, dzięki którym do 2030 r. co najmniej 80% obywateli powinno mieć możliwość korzystania z cyfrowego rozwiązania identyfikacyjnego w celu uzyskania dostępu do kluczowych usług publicznych.

Europejska tożsamość cyfrowa jest instrumentem prawnym, który ma na celu zapewnienie w użytku transgranicznym:

- dostępu do wysoce bezpiecznych i godnych zaufania rozwiązań w zakresie tożsamości elektronicznej;
- usług publicznych i prywatnych mogących polegać na zaufanych i bezpiecznych rozwiązaniach tożsamości cyfrowej;
- dostępności osobom fizycznym i prawnym rozwiązań w zakresie tożsamości cyfrowej;
- powiązanie tego rozwiązania z różnymi atrybutami i pozwolenie na ukierunkowane udostępnianie danych dotyczących tożsamości, ograniczone do potrzeb konkretnej żądanej usługi;
- akceptacji kwalifikowanych usług zaufania w UE i równości warunków ich świadczenia.

Bezpieczeństwo i kontrola oferowane przez europejskie ramy tożsamości cyfrowej powinny dawać obywatelom poczucie zaufania, oferując każdemu rozwiązania pozwalające kontrolować, kto ma dostęp do jego cyfrowej tożsamości i do których danych.

W ramach nowelizacji rozporządzenia ma zostać wprowadzony Europejski Cyfrowy Portfel Tożsamości (ang. *EUDI Wallet*), agregujący różnego rodzaju atrybuty i poświadczenia pochodzące od wielu dostawców tożsamości, tj. integracji informacji z wielu źródeł tożsamości. Rozwiązanie to bazuje silnie na koncepcji tożsamości suwerennej (ang. *self-sovereign identity* – SSI), w której to posiadacz danej tożsamości ma pełną kontrolę nad danymi i atrybutami opisującymi jego tożsamość.

Istotną funkcjonalnością ma być możliwość selektywnego ujawnianie atrybutów tożsamości, co ma zapewnić minimalizację przepływu danych, a w konsekwencji wpłynąć na poprawę poziomu prywatności użytkowników i zwiększyć ich kontrolę nad danymi.

2.4. Ustawa o usługach zaufania oraz identyfikacji elektronicznej

Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej[14] wprowadza do prawa polskiego postanowienia eIDAS. Oznacza to, że określa zasady funkcjonowania krajowej infrastruktury zaufania i powołuje krajowy schemat identyfikacji elektronicznej.

Krajowa infrastruktura zaufania jest rozwiązaniem pozwalającym z jednej strony na bezpieczny rozwój usług zaufania na rodzimym rynku, a z drugiej na rozpoznawanie usług zaufania przez inne kraje UE. Jej elementami są:

- rejestr dostawców usług zaufania;
- zaufana lista;
- Narodowe Centrum Certyfikacji.

Krajowy schemat identyfikacji elektronicznej jest architekturą umożliwiającą wykorzystanie środków identyfikacji elektronicznej podczas uwierzytelniania i korzystania z publicznych i prywatnych usług online. Składa się z:

- Krajowego Węzła Identyfikacji Elektronicznej (w skrócie Węzła Krajowego);

14 *Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.* Dz.U. z 2016 poz. 1579. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160001579/U/D20161579Lj.pdf

- przyłączonych do Węzła Krajowego:
  - systemów identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej,
  - systemów teleinformatycznych, w których udostępniane są usługi online;
- Węzła Transgranicznego.

Do Węzła Transgranicznego przyłączane są notyfikowane systemy identyfikacji elektronicznej, tj. systemy spełniające dodatkowe warunki określone w art. 7 eIDAS. Przyłączenie środka identyfikacji do węzła umożliwia wykorzystanie środka identyfikacji elektronicznej w ramach systemów obecnych w innych krajach członkowskich.

Rozporządzenie podkreśla, że wykorzystanie podpisu elektronicznego lub innych usług zaufania wywołuje skutki prawne jedynie wtedy, gdy zostały złożone w okresie ważności poszczególnych certyfikatów. Z tego względu bardzo istotne jest, aby korzystać z ważnych certyfikatów, a w przypadku utraty lub kradzieży jak najszybciej unieważnić dany certyfikat lub środek identyfikacji elektronicznej.

2.5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1157

Wprowadzenie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1157 z dnia 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się[15] miało na celu ujednolicenie i zniwelowanie różnic w poziomie zabezpieczeń krajowych dowodów osobistych wydawanych przez państwa członkowskie. Różnice występujące w tych zabezpieczeniach utrudniały weryfikowanie autentyczności dokumentów, co mogło sprzyjać ich fałszowaniu i skutkować wzrostem liczby przestępstw z tym związanych. Poprawa zabezpieczeń stosowanych w dowodach tożsamości powinna również pozytywnie wpłynąć na sam proces identyfikacji w usługach online. Wykorzystanie dokumentów z warstwą cyfrową bez wątpienia poprawia dostępność i użyteczność usług cyfrowych, co

15 Wprowadzenie *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1157 z dnia 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych* obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się. Dz.U.UE.L.2019.188.67. Dostępny w: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32019R1157

w konsekwencji przekłada się na wzrost popularności całego ekosystemu tożsamości elektronicznej.

Kluczowe postanowienia wspomnianego rozporządzenia dotyczą obowiązku umieszczenia w warstwie elektronicznej dowodu danych biometrycznych w postaci wizerunku twarzy i odcisków dwóch palców. Rozporządzenie to wymusiło na Polsce wydawanie nowej wersji e-dowodu, ponieważ wcześniejszy posiadał tylko jedną cechę biometryczną w postaci zdjęcia wizerunku twarzy, a także pełną zgodność dowodu osobistego ze specyfikacją ICAO Doc 9303[16] stosowaną na całym świecie w paszportach. ICAO Doc 9303 definiuje standardy, których respektowanie przez organ wydający dokument umożliwia usprawnienie wielu procesów, m.in. korzystania z automatycznych kontroli granicznych na lotniskach. W szczególności dokument ICAO określa specyfikację pola przeznaczonego do odczytu maszynowego, tzw. pole MRZ i warstwę elektroniczną dokumentu, tzw. eMRTD, która umożliwia automatyczny odczyt danych zawartych w warstwie graficznej dokumentu, jak również dostęp do danych biometrycznych. Dzięki warstwie elektronicznej możliwa jest także weryfikacja samego dokumentu i danych w nim zawartych pod kątem autentyczności czy integralności.

2.6. Organizacje kształtujące strukturę eID w UE

Normy prawne określają reguły postępowania, z tego względu bardzo ważne jest, aby tworzyć je z uwzględnieniem kodeksu dobrych praktyk, norm i specyfikacji technicznych. Dzięki takiemu podejściu możliwa jest budowa systemu, który zapewnia określony poziom bezpieczeństwa i może być kompatybilny z rozwiązaniami stosowanymi w innych krajach członkowskich UE. W przypadku systemów związanych z tożsamością cyfrową można znaleźć wiele organizacji, których zalecenia są uwzględniane podczas tworzenia nowych aktów prawnych.

W Unii Europejskiej jednym z najważniejszych ośrodków doradczych w kwestiach dotyczących eID jest Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ang. European Union Agency for Cybersecurity – ENISA). Ten specjalistyczny ośrodek oprócz funkcji doradczej pełni również funkcję opiniotwórczą. Obecnie na stronie ENISA dostępnych jest ponad 400 publikacji dotyczących cyberzagrożeń i sposobów ochrony przed nimi. Wśród publikacji związanych z ekosystemem eID znajdują się m.in.:

16 https://www.icao.int/publications/pages/publication.aspx?docnum=9303

- eIDAS compliant eID Solutions[17];
- Remote ID Proofing[18];
- Remote Identity Proofing – Attacks & Countermeasures[19];
- Digital Identity: Leveraging the SSI Concept to Build Trust[20].

Kolejnym ważnym ośrodkiem jest ETSI (ang. European Telecommunications Standards Institute). Instytut ten od wielu lat publikuje normy niezbędne do rozwoju europejskiego rynku telekomunikacyjnego, a przede wszystkim normy dotyczące kwestii technicznych, m.in. cyfrowej tożsamości, np.:

- ETSI TS 119 461 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects*[21];
- ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*[22].

Z perspektywy rozporządzenia w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się istotna jest norma ICAO (ang. *International Civil Aviation Organization*), która wprowadza konieczność dostosowania nowych dowodów osobistych do zaleceń zawartych w dokumencie ICAO 9303[23]. Sama organizacja współpracuje z ponad 190 państwami na całym świecie w ramach rozwoju norm i zaleceń stosowanych w sektorze lotnictwa cywilnego. Zalecenia zawarte w normie ICAO 9303 określają zarówno warstwę graficzną, jak i elektroniczną dokumentów przeznaczonych do odczytu maszynowego. Spełnienie tych wymagań znacząco ułatwia przebieg odprawy granicznej i bagażowej na lotniskach.

17 https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions

18 https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing

19 https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures

20 https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust

21 ETSI TS 119 461 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects*. Dostępny w: https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf

22 ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*. Dostępny w: https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v020301p.pdf

23 https://www.icao.int/publications/pages/publication.aspx?docnum=9303

Również w Polsce istnieje wiele organizacji, które popularyzują rozwój tożsamości cyfrowej. Jedną z najbardziej znanych, związanych ze świadczeniem usług szkoleniowych i doradczych w zakresie eID jest Obserwatorium.biz, którego pracownicy bardzo często uczestniczą w tworzeniu raportów i norm dotyczących dalszego rozwoju ekosystemu eID. Firma współorganizuje konferencje dotyczące tożsamości cyfrowej, m.in:

- CommonSign[24];
- Trusted Economy Forum[25], dawniej EFPE[26] (Europejskie Forum Podpisu Elektronicznego i Usług Zaufania).

Instytucje bankowe w wielu państwach są uznawane za instytucje zaufania publicznego. W przypadku polskiego ekosystemu tożsamości elektronicznej instytucje bankowe odgrywają kluczową rolę, bowiem są jednymi z głównych elementów tworzących system mojeID, w ramach którego wydają jednorazowe środki identyfikacji elektronicznej. Z tego względu instytucje związane z bankowością elektroniczną i organizacje promujące wykorzystanie nowych technologii w sektorze finansowym są aktywnie zaangażowane w promowanie wiedzy i rozwiązań związanych z tożsamością elektroniczną. Na tym polu szczególnie wyróżniają się wymienione poniżej podmioty:

1) Związek Banków Polskich (ZBP[27]) – funkcjonuje od 1991 r. na podstawie *Ustawy z dnia 30 maja 1989 r. o izbach gospodarczych*[28]. Do organizacji tej należy większość banków działających na terenie RP. Zadaniem ZBP jest utworzenie płaszczyzny usprawniającej dyskusję i wymianę informacji między bankami. Podejmowane decyzje umożliwiają integrację środowiska bankowego, poprawę bezpieczeństwa i opracowywanie wspólnych decyzji dotyczących przyszłości całego sektora. Eksperci z ZBP często uczestniczą w pracach legislacyjnych komisji Sejmu i Senatu. Dodatkowo ZBP wydaje publikacje, raporty cykliczne i organizuje konferencje dotyczące stanu i perspektyw rozwoju sektora bankowego. Do najbardziej znanych przedsięwzięć można zaliczyć:

24 https://commonsign.eu/

25 https://trustedeconomyforum.com/pl/

26 https://www.certum.pl/pl/aktualnosci/od-efpe-do-trusted-economy-forum-nowy-wymiar-globalnej-gospodarki/

27 https://zbp.pl/o-zbp/misja

28 *Ustawy z dnia 30 maja 1989 r. o izbach gospodarczych*. Dz.U. z 1989 Nr 35 poz. 195. Dostępny w: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19890350195

- Dokumenty Zastrzeżone[29] będące systemem, do którego każdy może zgłosić utratę dowodu osobistego. Przekazana informacja jest następnie rozsyłana do banków, operatorów komórkowych oraz innych firm i instytucji korzystających z tego systemu.
- Zespół Bezpieczeństwa Banków[30] w ramach, którego funkcjonuje FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP (FinCERT.pl – BCC ZBP). Jego zadaniem jest gromadzenie, analiza i przekazywanie w sektorze bankowym informacji dotyczących możliwych zagrożeń. Centrum to jest uznawane za ISAC (ang. Information Sharing and Analysis Center) polskiego sektora bankowego.
- Opracowanie standardu kwalifikacyjnego *Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych*[31].
- Opracowanie przewodnika *Identyfikacja i uwierzytelnienie w usługach elektronicznych*[32].

2) Warszawski Instytut Bankowości (WIB)[33] – został utworzony z inicjatywy ZBP i banków-fundatorów w celu podejmowania działań na rzecz rozwoju i wypracowywania rozwiązań służących klientom, pracownikom i instytucjom finansowym. Wspólnie z bankami, ZBP, KIR i BIK inicjuje i realizuje projekty ukierunkowane na podnoszenie kompetencji bankowców i jakości praktyk rynkowych instytucji finansowych. Jednym z takich projektów jest Program Analityczno-Badawczy (PAB WIB)[34], który powstał w 2019 r. jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego. Do najbardziej znanych przedsięwzięć można zaliczyć:

- program *Bankowcy dla edukacji*[35];

29 https://dokumentyzastrzezone.pl/system-dz/

30 https://zbp.pl/Dla-Bankow/Cyberbezpieczenstwo/Cyberbezpieczenstwo-bankow-i-ich-klientow

31 https://www.zbp.pl/getmedia/076a1ce8-2850-4415-8a45-0f13389e8f97/Standard-Kwalifikacyjny-Stosowanie-zasad-cyberbezpieczenstwa.pdf

32 https://zbp.pl/Aktualnosci/Wydarzenia/Przewodnik-Identyfikacja-i-uwierzytelnienie-w-uslugach-elektronicznych%E2%80%9D

33 https://www.wib.org.pl/o-nas/

34 https://pab.wib.edu.pl/cele-programu/

35 https://bde.wib.org.pl/

- cykliczny raport *Cyberbezpieczny Portfel*[36];
- raport *Problemy elektronicznego potwierdzania tożsamości* opracowany przez zespół pod kierownictwem prof. Mirosława Kutyłowskiego z Politechniki Wrocławskiej;
- raport *Bezpieczeństwo usług opartych o otwarte interfejsy programistyczne (API) w kontekście implementacji dyrektywy PSD2* opracowany przez zespół pod kierownictwem dr. Miłosza Brakonieckiego z Obserwatorum.biz;
- raport *Biometria w bankowości elektronicznej* opracowany przez zespół z Obserwatorium.biz.

Kontrolę nad rynkiem finansowym sprawuje Komisja Nadzoru Finansowego (KNF), podlegająca pod prezesa rady ministrów. Celem komisji jest zapewnienie prawidłowego funkcjonowania, bezpieczeństwa, stabilności i przejrzystości działania rynku finansowego. W odniesieniu do sektora bankowego KNF wydaje i wycofuje zezwolenia na prowadzenie działalności bankowej, przeprowadza regularne kontrole w nadzorowanych podmiotach, a w przypadku naruszenia przepisów prawa może nakładać kary finansowe na daną instytucję. Komisja Nadzoru Finansowego wydaje również cały szereg wytycznych i zaleceń, które oddziałują na cały sektor. Przykładem rekomendacji dotyczącej cyberbezpieczeństwa jest Rekomendacja D[37].

W kontekście polskiego systemu eID kluczową rolę odgrywa Krajowa Izba Rozliczeniowa (KIR), dostarczająca rozwiązania cyfrowe dla sektora komercyjnego i publicznego. Do tych najbardziej znanych można zaliczyć system mojeID (komercyjny system identyfikacji elektronicznej) oraz elektroniczny podpis kwalifikowany mSzafir.

36 *Cyberbezpieczny Portfel 2022. Edycja IV, lipiec2022*. ZBP, Warszawa 2022. Dostępny w: https://zbp.pl/aktualnosci/wydarzenia/Raport-Cyberbezpieczny-Portfel-2022

37 https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf

3. Ekosystem związany z tożsamością cyfrową w Polsce

W ciągu ostatnich kilkunastu lat rynek e-usług na całym świecie rozwijał się intensywnie. W związku z tym pojawiła się naturalna potrzeba opracowania sprawnego i bezpiecznego mechanizmu uwierzytelnienia na potrzeby podmiotów publicznych i prywatnych.

W początkowych etapach rozwoju eTożsamości brakowało stosownych regulacji prawnych, zaleceń i dobrych praktyk. Z czasem wykształciły się trzy główne modele rynku w zakresie identyfikacji elektronicznej[38]:

- Schemat scentralizowany, w którym kontrolę nad centralnym punktem zarządzania tożsamością cyfrową przeważnie sprawuje państwo. Z tego modelu korzystają: Indie, Zjednoczone Emiraty Arabskie, Pakistan, Włochy i Belgia.
- Schemat federacyjny, który zakłada współpracę sektora prywatnego i publicznego. Skutkiem tej współpracy jest jednoczesne istnienie kilku różnych systemów identyfikacji elektronicznej, wspólnie wpisujących się w ustaloną architekturę (schemat identyfikacji elektronicznej). Współpraca między sektorami zwykle owocuje większą częstością korzystania z e-usług. Jest to najbardziej popularny model rynku w Europie, stosowany zarówno przez państwa uznawane za dojrzałe w zakresie tożsamości cyfrowej (Finlandię i Estonię), jak i kraje dopiero wdrażające eID (Polskę i Wielką Brytanię).
- Schemat otwartego rynku nie jest rozwijany na podstawie zdefiniowanej wcześniej architektury (jak ma to miejsce w schemacie federacyjnym). Oparty jest na standardach i konkretnych wymaganiach, które powinien spełniać podmiot ubiegający się o włączenie do rynku tożsamości elektronicznej. W schemacie tym nie występuje główny podmiot, który pełniłby rolę regulatora. Dobrym przykładem są USA, gdzie za definiowanie standardów i wymagań odpowiada NSTIC (ang. *National Strategy for Trusted Identities in Cyberspace*).

38 https://obserwatorium.biz/the-eid-2017-electronic-identification-in-poland-report.html

Rozwój tożsamości cyfrowej jest również mocno uzależniony od podejścia państwa do kwestii związanych z tradycyjnym dokumentem tożsamości oraz stosownych aktów prawnych.

W czasie tworzenia regulacji w niektórych państwach Europy tradycyjne dowody tożsamości:

- nie istniały (w Danii i Wielkiej Brytanii);
- istniały, ale ich posiadanie było dobrowolne (w Austria, Francji, Finlandii Szwecji i na Węgrzech);
- były obowiązkowe (w Polsce, Słowacji, Estonii, Portugalii, Hiszpanii i Grecji),

Dodatkowo – w zależności od kraju i obowiązujących w nim przepisów – do potwierdzania tożsamości można było wykorzystać również inny dokument (np. paszport w Niemczech czy prawo jazdy w Szwecji). W niektórych krajach same dowody tożsamości były mocno przestarzałe (np. we Francji i w Rumunii).

Obecnie na popularności zyskuje nowy model, stworzony z wykorzystaniem tzw. zdecentralizowanej tożsamości. Koncepcja tożsamości suwerennej (ang. *self-souvereign identity* – SSI) umożliwia zarządzanie własną tożsamością niezależnie od zewnętrznych dostawców. W takim podejściu to obywatel kolekcjonuje różnego rodzaju atrybuty i poświadczenia, które następnie może wykorzystywać według własnego uznania. Z koncepcją tą jest związany Europejski Cyfrowy Portfel Tożsamości, który pojawi się wraz z wejściem w życie eIDAS 2.

3.1. Rozwój tożsamości cyfrowej w Unii Europejskiej

Kierunki, cele i sposoby rozwoju eID przyjęte przez poszczególne kraje członkowskie UE również mogą się od siebie znacznie różnić. Regulacje na poziomie unijnym są dosyć ogólne, w największym stopniu dotyczą wspólnej integracji systemów opracowanych na poziomie krajowym. Różnice w rozwoju eID na terenie UE stają się dostrzegalne dzięki pracy *Overview of Member States' eID strategies* opublikowanej w styczniu 2021 r. przez Deloitte dla Komisji Europejskiej[39]. Mimo że zawarte w niej informacje były aktualne w 2020 r., wciąż jest dobrym punktem odniesienia, pozwalającym zrozumieć podstawy ekosystemu

39 https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/National+Strategies

i cele rozwoju eID na przestrzeni kolejnych lat. Różnice w rozwoju eID istnieją w następujących kategoriach:

- przyjęte cele strategiczne;
- podejście do obowiązku posiadania środka identyfikacji elektronicznej;
- dostępność e-portali pozwalających na korzystanie z usług publicznych.

Bardzo dobry pogląd na różnice w rozwiązaniach eID rozwijanych na terenie UE oddaje ostatni rozdział wspomnianej publikacji, w którym pokrótce został przedstawiony stan poszczególnych ekosystemów w 2020 r.

W tym miejscu warto wspomnieć o Estonii, która jest uznawana za jednego z prekursorów rozwoju cyfrowej tożsamości. Strategię rozwoju eID przedstawiono w tym kraju już w 2000 r., a pierwsze dokumenty tożsamości z warstwą elektroniczną pojawiły się w 2002. Obecnie większość (99%) usług publicznych jest dostępna online. Jedną z nich jest możliwość głosowania w wyborach, które nie są obowiązkowe[40]. Dostępność takiego udogodnienia może wpływać na wyższą frekwencję w wyborach (frekwencja w wyborach parlamentarnych w 2019 r. wyniosła 63,7%[41]), jednak nie jest znacząco wyższa w porównaniu do frekwencji w wyborach parlamentarnych w innych krajach Europy Wschodniej, takich jak:

- Polska – 61,7% (2019);
- Litwa – 47,8% (2020);
- Czechy – 65,4% (2021);
- Łotwa – 59,4% (2022).

Dowód tożsamości z warstwą cyfrową w Estonii posiada prawie 1,3 mln obywateli (ok. 98% populacji). Dodatkowo dostępne są jeszcze inne środki identyfikacji elektronicznej przeznaczone dla obcokrajowców pochodzących z krajów UE (e-Resident Digital ID), obcokrajowców pochodzących spoza UE (Resident Permit Card) oraz pracowników placówek dyplomatycznych (Diplomatic ID). Dzięki dwóm rozwiązaniom (Mobile ID i Smart ID) możliwe jest również wykorzystanie smartfona jako środka identyfikacji elektronicznej. Warto podkreślić, że Estonia wspiera integrację i wykorzystanie oprogramowania *open source* do tego stopnia, że w Internecie można znaleźć dokumentację opisującą komunikację z warstwą elektroniczną dowodu tożsamości. W sierpniu 2021 r. do warstwy elektronicznej dodano dane biometryczne.

40 https://www.coe.int/en/web/electoral-assistance/elecdata

41 https://www.idea.int/data-tools/data/voter-turnout

3.2. Krajowy schemat identyfikacji elektronicznej

Przed wprowadzeniem eIDAS rozwój eID w Polsce następował głównie w sektorze publicznym, a zasady współpracy między sektorem publicznym i prywatnym nie były jednoznacznie określone. Dodatkowo sam schemat nie posiadał centralnego punktu umożliwiającego połączenie dostawców usług (DU) z dostawcami środków identyfikacji elektronicznej (DŚI), co oznacza, że każda integracja przebiegała osobno.

Dopiero wprowadzenie w życie postanowień *Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej* wymusiło utworzenie krajowego schematu identyfikacji elektronicznej, który zakładał istnienie następujących elementów:

- Krajowego Węzła Identyfikacji Elektronicznej (w skrócie Węzła Krajowego) – systemu login.gov.pl będącego pośrednikiem między dostawcami tożsamości, a dostawcami usług.
- Węzła Transgranicznego – wykorzystywanego na potrzeby integracji z usługami cyfrowymi rozwijanymi przez kraje UE. W ramach integracji każde państwo członkowskie z jednej strony powinno uznawać notyfikowane środki identyfikacji elektronicznej innych państw, a z drugiej po spełnieniu odpowiednich warunków może notyfikować własny środek identyfikacji elektronicznej. W przypadku Polski w dalszym ciągu węzeł krajowy nie uznaje notyfikowanych środków identyfikacji elektronicznej innych państw członkowskich UE (stan na 24 marca 2023 r.).
- Dostawców środka identyfikacji elektronicznej – podmiotów potwierdzających i weryfikujących tożsamość osoby, a następnie wydających środek identyfikacji elektronicznej, wykorzystywany następnie do uwierzytelnienia w usługach cyfrowych.
- Dostawców usług – systemów umożliwiających faktyczną realizację usług online.
- Dostawców atrybutów – w praktyce oznacza to integrację z Systemem Rejestrów Państwowych (SRP), którego zadaniem jest dostarczenie dodatkowych atrybutów tożsamości.

Z perspektywy obywatela kluczowe jest zrozumienie istoty działania systemów dostawców środka identyfikacji elektronicznej i dostawców usług zaufania. Są to bowiem elementy, z których bezpośrednio korzysta każdy obywatel. Pierwszy kontakt z tymi systemami może wydawać się nieco skomplikowany,

a świadczone usługi niezrozumiałe, stąd należy edukować obywateli w tym zakresie i upraszczać komunikację.

Środki identyfikacji elektronicznej

Środkiem identyfikacji elektronicznej jest taki zestaw danych, który umożliwia ustalenie tożsamości konkretnej osoby. Na podstawie tych danych możliwa jest identyfikacja i uwierzytelnienie w usługach online. W Polsce do dostawców środka identyfikacji elektronicznej (nazywanych dostawcami tożsamości) zaliczyć można zarówno podmioty publiczne, jak i prywatne (głównie banki).

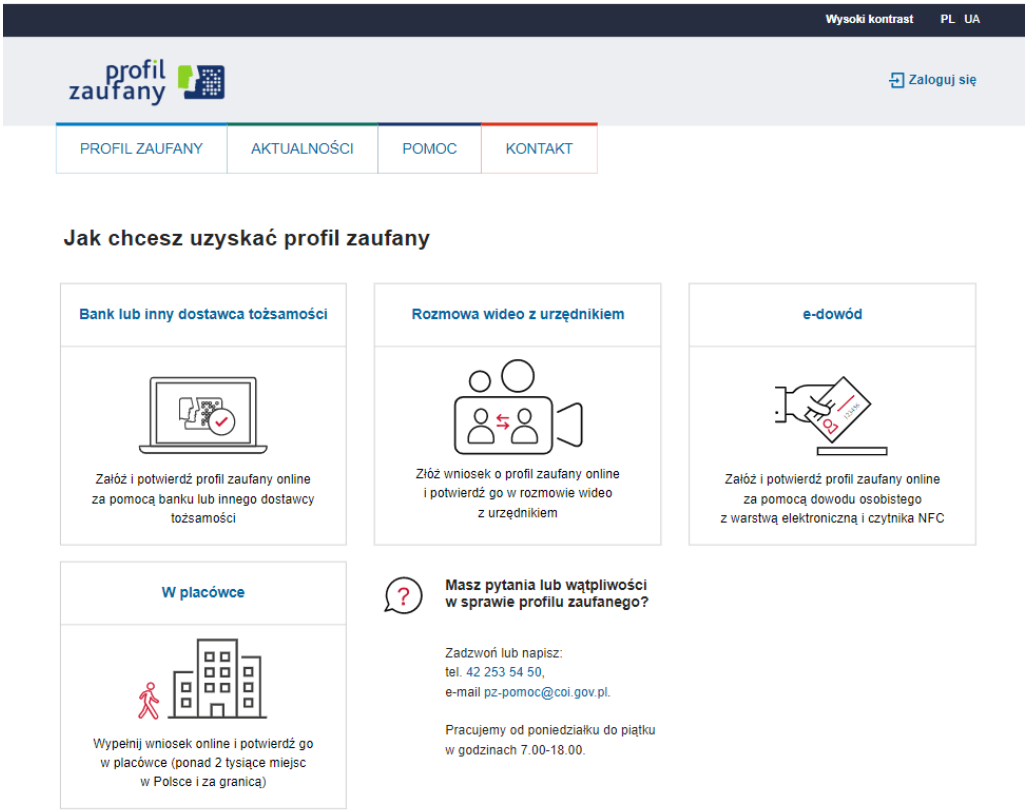
Zgodnie z ustawą o usługach zaufania oraz identyfikacji elektronicznej wszyscy dostawcy środków identyfikacji elektronicznej, którzy zostali zintegrowani z węzłem krajowym, znajdują się w rejestrze systemów identyfikacji elektronicznej przyłączonych do Węzła Krajowego[42]. Obecnie składają się na niego:

- Systemy zaliczane do publicznego systemu identyfikacji elektronicznej:
  - profil zaufany (PZ, eGo),
  - profil osobisty.
- System eID (mojeID) – komercyjny system identyfikacji elektronicznej rozwijany przez KIR. Bywa nazywany węzłem prywatnym lub komercyjnym. Obecnie skupia przede wszystkim podmioty należące do sektora bankowego.

Profil zaufany jest jednym z pierwszych środków identyfikacji elektronicznej. Pierwotnie był powiązany z platformą ePUAP, jednak obecnie umożliwia również uwierzytelnienie w innych serwisach administracji rządowej. Profil zaufany jest wydawany na 3 lata z możliwością przedłużenia jego ważności o następne 3 lata. W celu uzyskania profilu zaufanego należy złożyć wniosek online, a następnie dokonać weryfikacji konta (rys. 3.1):

- online:
  - za pośrednictwem banku lub innego dostawcy tożsamości,
  - w trakcie wideorozmowy z urzędnikiem,
  - korzystając z warstwy elektronicznej dowodu osobistego podczas weryfikacji;

42 https://mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-srodka-identyfikacji/rejestr-dostawcow-srodka-identyfikacji-elektronicznej-przylaczonych-do-wezla-krajowego.html



Rys. 3.1. Metody umożliwiające uzyskanie profilu zaufanego. Źródło: https://pz.gov.pl/pz/registerMainPage

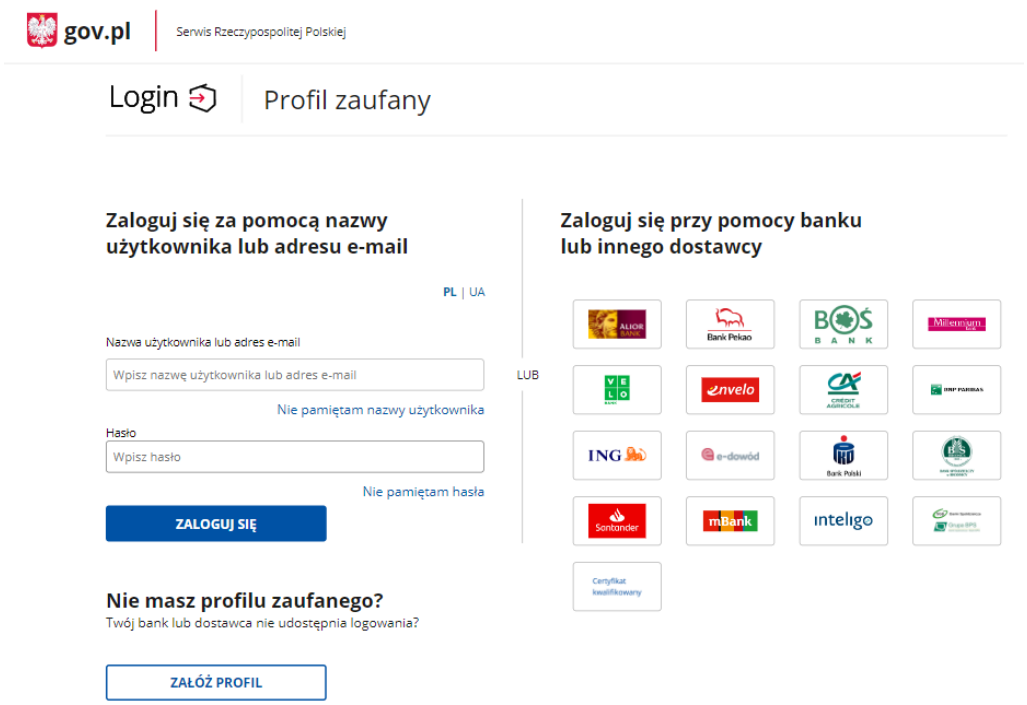
- tradycyjnie (offline) – w jednej z ponad 2 tys. placówek w Polsce i za granicą (głównie w jednostkach administracji publicznej)[43].

W celu uzyskania dostępu do profilu zaufanego obywatel może skorzystać z kilku metod uwierzytelnienia (rys. 3.2):

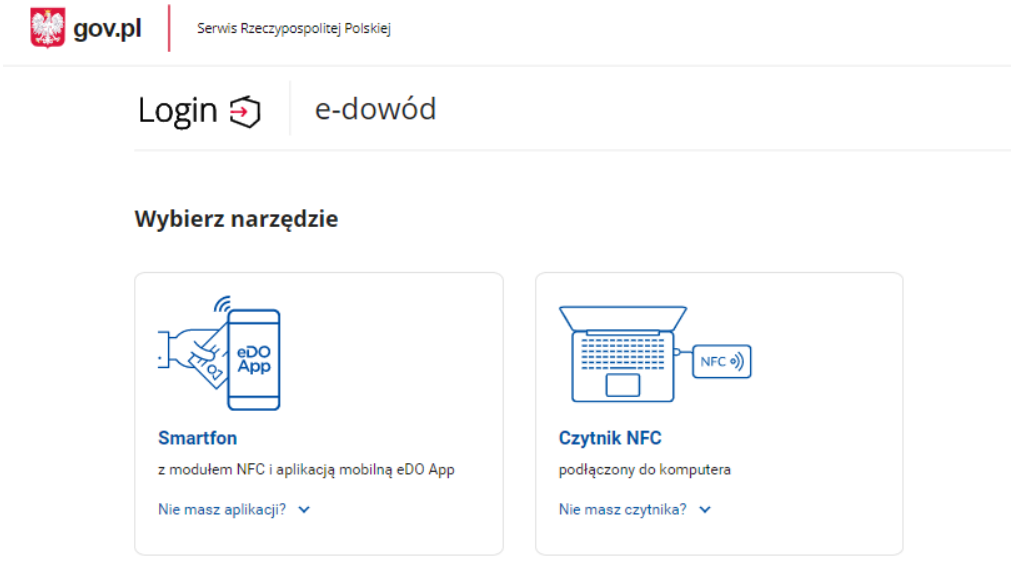
- hasła ustawionego w profilu zaufanym oraz kodu otrzymanego w SMS-ie jako drugiego składnika uwierzytelnienia (2FA);
- systemu bankowego lub innego dostawcy zintegrowanego z profilem zaufanym;
- e-dowodu, a dokładnie profilu osobistego;
- certyfikatu kwalifikowanego za pośrednictwem aplikacji Podpis GOV.

Profil osobisty jest środkiem identyfikacji elektronicznej bezpośrednio związanym z e-dowodem. Podczas procesu uwierzytelniania swojej tożsamości

43 https://pz.gov.pl/pz/confirmationPointAddressesList



Rys. 3.2. Sposoby konfigurowania uwierzytelnienia w profilu zaufanym



Rys. 3.3. Logowanie do usług online za pomocą dowodu z warstwą elektroniczną. Źródło: https://login.e-dowod.gov.pl/sie-frontend/#/

w ramach usług online potrzebny jest certyfikat identyfikacji i uwierzytelnienia, z którego można skorzystać po podaniu najpierw numeru CAN widocznego w warstwie graficznej dowodu, a następnie 4-cyfrowego kodu PIN. Samo nawiązanie połączenia z warstwą elektroniczną odbywa się za pośrednictwem:

- smartfonu z modułem NFC za pomocą aplikacji eDO App (metoda najczęściej wykorzystywana ze względu na jej wygodę i brak dodatkowych kosztów po stronie obywatela);
- czytnika NFC podłączonego do komputera i aplikacji e-dowód Menedżer.

Proces uwierzytelnienia za pomocą e-dowodu jest intuicyjny dzięki instrukcjom wyświetlającym się w kolejnych krokach (rys. 3.3).

Obecnie profil osobisty jest dostępny jako metoda uwierzytelnienia w przypadku większości publicznych usług online, może go założyć każdy obywatel w momencie otrzymania e-dowodu. Z tych względów jest to obecnie najbardziej dostępny, przystępny i praktyczny środek identyfikacji elektronicznej, którego popularność ze względu na nowy dowód rośnie z miesiąca na miesiąc. W 2022 roku wydano ponad 3,5 mln e-dowodów[44], zaś w 2023 ponad 2 mln starych dowodów straci ważność i będzie musiało zostać wymienionych na nowe[45].

Dostawcy usług

Środek identyfikacji elektronicznej służy do uzyskania dostępu do usług online oferowanych przez podmioty publiczne (zintegrowane z węzłem krajowym) i prywatne (dostępne za pośrednictwem komercyjnego systemu mojeID). Warto podkreślić, że w znacznej mierze to właśnie dostawcy usług odgrywają główną rolę w popularyzacji wykorzystania eID w społeczeństwie. Zarówno liczba, jak i jakość usług dostępnych online ma bezpośredni wpływ na powszechność korzystania z cyfrowej tożsamości.

Pierwszą publiczną usługą online była Elektroniczna Platforma Usług i Administracji Publicznej (ePUAP), która miała usprawnić komunikację (przesyłanie pism i wniosków) obywateli z instytucjami publicznym. Do publicznych usług online można zaliczyć również:

- PUE ZUS;

44 https://www.cpd.gov.pl/o-nas/statystyki/

45 https://businessinsider.com.pl/wiadomosci/miliony-polakow-musza-wymienic-dowody-osobiste-inaczej-5-tys-zl-kary/8d8nkbr

- Internetowe Konto Pacjenta (IKP);
- portal emp@tia – umożliwiający składanie wniosków dotyczących świadczeń socjalnych oferowanych przez państwo;
- aplikację mObywatel – umożliwiającą okazywanie i potwierdzanie tożsamości w rzeczywistości, w aplikacjach mobilnych i usługach online;
- serwisy udostępniane przez poszczególne samorządy terytorialne (np. eUrząd, Gminne Systemy Komunikacji Online, Elektroniczne Biuro Obsługi Interesanta).

Pełna lista dostawców usług jest dostępna na stronie BIP Ministra Cyfryzacji[46].

Warto jeszcze wspomnieć o współpracy sektora publicznego i komercyjnego w ramach krajowego schematu identyfikacji elektronicznej, której podstawę stanowi przede wszystkim mojeID. To bezpieczne narzędzie rozwijane przez KIR jest powszechnie wykorzystywane do potwierdzania tożsamości w komercyjnych i publicznych usługach online, czyli wygodne i natychmiastowe potwierdzenie tożsamości bez konieczności stosowania tradycyjnych metod w postaci wizyty w placówce czy spotkania z kurierem[47]. Z mojeID korzysta kilkadziesiąt przedsiębiorstw należących do[48, 49]:

- branży telekomunikacyjnej;
- branży medycznej;
- branży ubezpieczeniowej;
- branży usług użyteczności publicznej – dostawcy wody, prądu, gazu, podmioty zajmujące się gospodarką odpadami;
- administracji publicznej.

Obecnie liczba integracji z mojeID stale rośnie[50].

W znacznej większości przypadków mojeID umożliwia potwierdzanie tożsamości za pośrednictwem instytucji bankowych, w których ze względu na świadczone usługi i wymogi regulacyjne mechanizmy starannej identyfikacji zostały wdrożone już przed wielu laty.

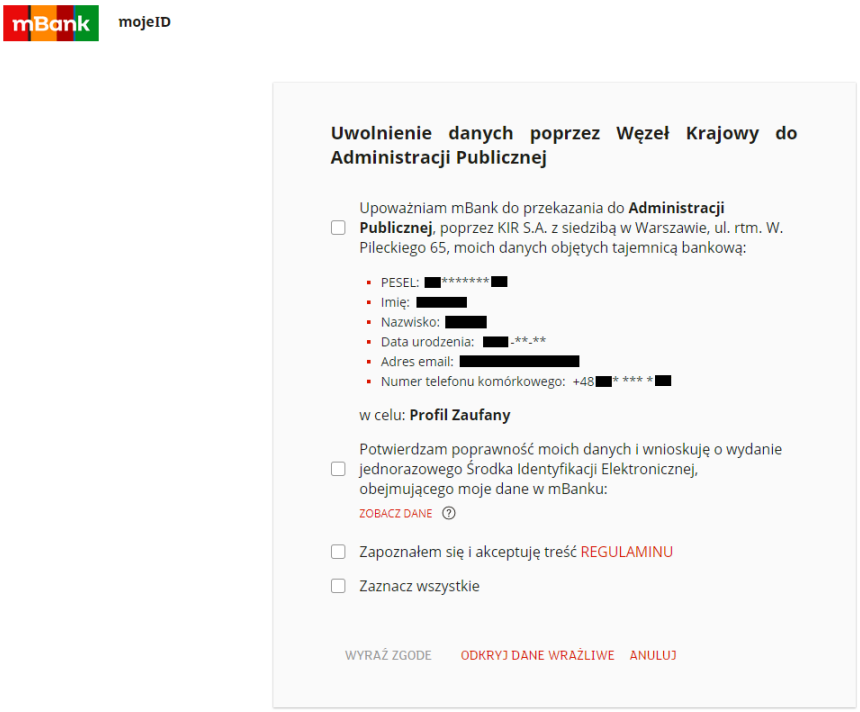
46 https://mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-uslug/wezel-krajowy-zintegrowani-dostawcy-uslug.html

47 https://www.mojeid.pl/#co-to-jest-moje-id

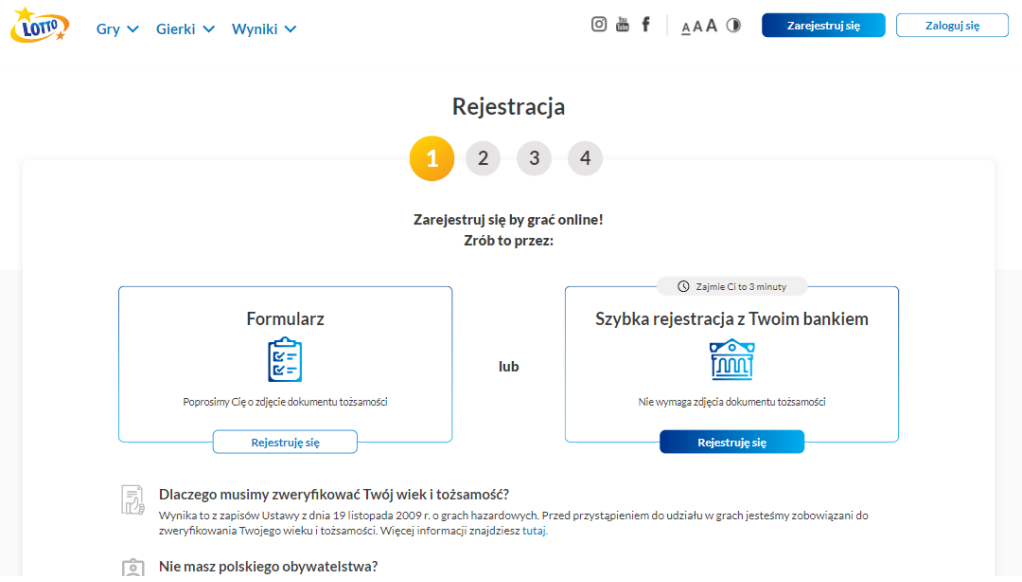
48 https://www.mojeid.pl/#zastosowanie

49 https://www.mojeid.pl/#dostawcy-uslug

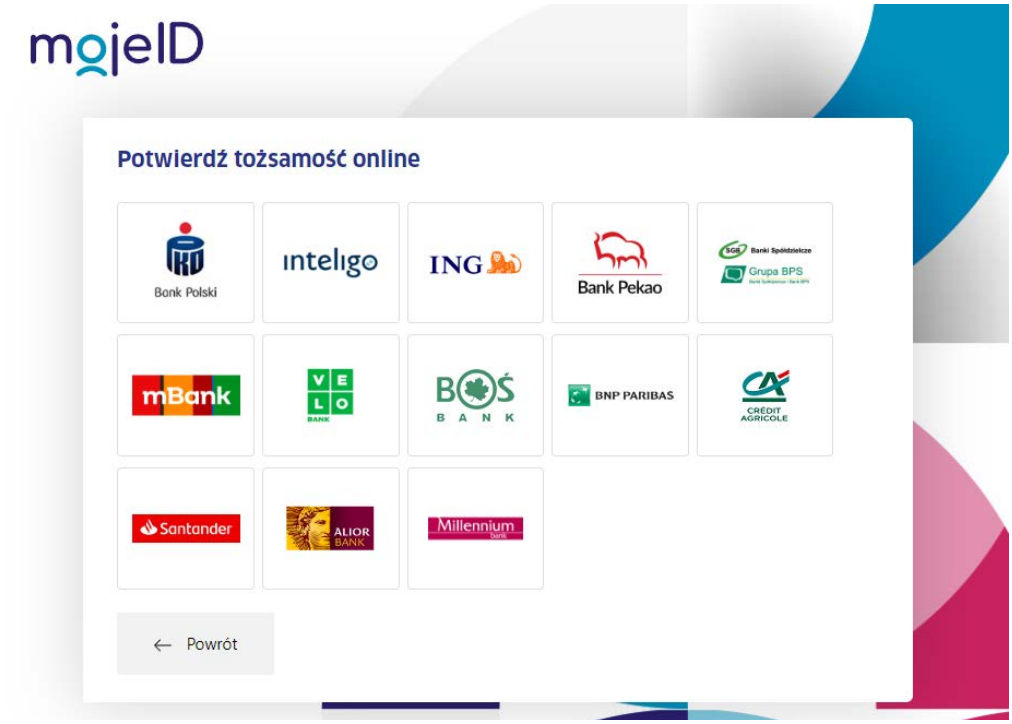
50 https://www.mojeid.pl/archiwum-aktualnosci/



Rys. 3.4. Zestaw danych przekazywany podczas uwierzytelnienia za pomocą mojeID w profilu zaufanym



Rys. 3.5. Potwierdzenie tożsamości z wykorzystaniem systemu mojeID podczas rejestracji na stronie lotto.pl



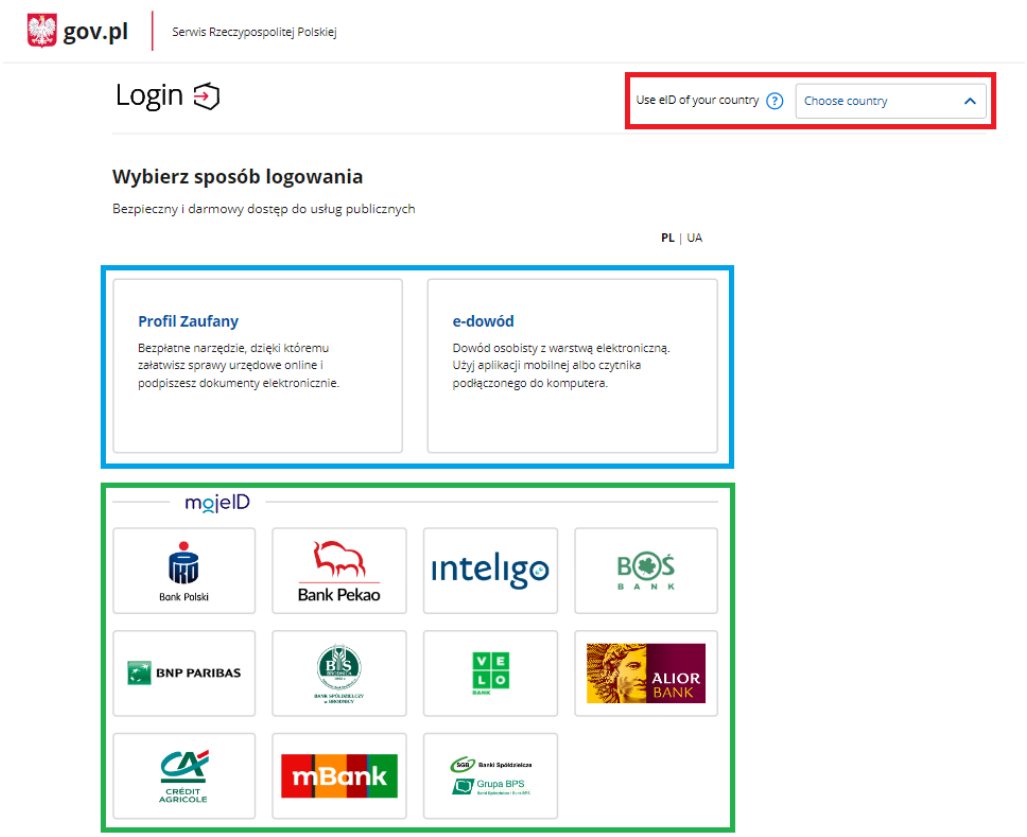
Rys. 3.6. Instytucje bankowe, w których można potwierdzić tożsamość podczas rejestracji/zakładania konta na stronie lotto.pl

W praktyce tego typu operacje polegają na wydaniu przez bank jednorazowego środka identyfikacji elektronicznej, który potwierdza pewien zestaw atrybutów tożsamości (rys. 3.4). W przypadku niektórych usług publicznych i komercyjnych (np. rejestracji na stronie lotto.pl (rys. 3.5)) w celu uwierzytelnienia można wykorzystać system mojeID.

Korzystanie z systemu mojeID jest intuicyjne: po wybraniu odpowiedniego banku (rys. 3.6) powinniśmy zalogować się w sposób tradycyjny do bankowości elektronicznej, następnie po wyrażeniu odpowiednich zgód otrzymamy do wglądu dane, które zostaną udostępnione dostawcy usług. Podczas całej operacji korzysta się z zabezpieczeń oferowanych przez system bankowy podczas zwykłego użytkowania (np. powiadomienia push w mobilnej aplikacji).

Zestawienie większości środków identyfikacji elektronicznej można zaobserwować podczas logowania do ePUAP-u (rys. 3.7).

Na rysunku 3.7 kolorem czerwonym zaznaczono integrację z Węzłem Transgranicznym, która miałaby umożliwić korzystanie z notyfikowanych środków

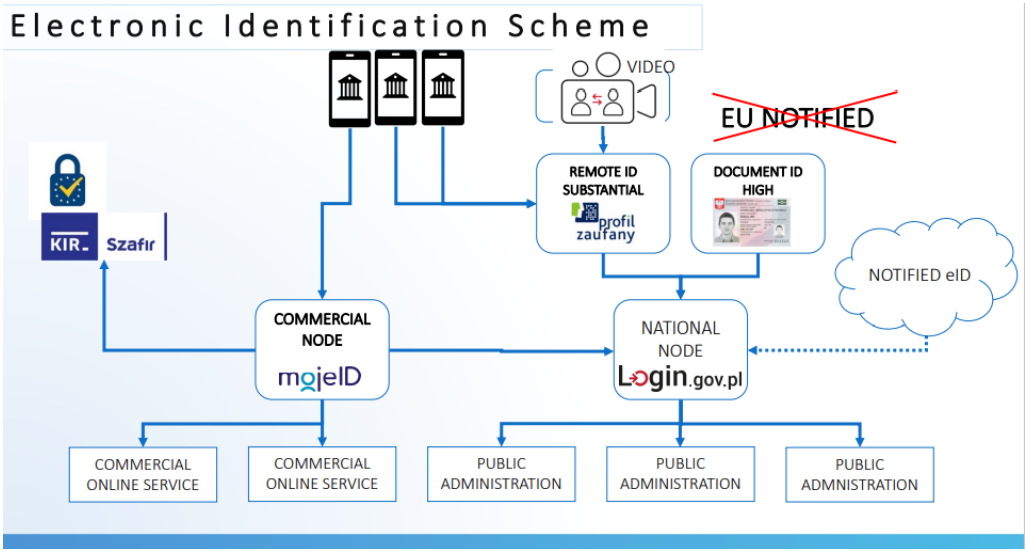


Rys. 3.7. Zestawienie większości obecnie dostępnych środków identyfikacji elektronicznej na podstawie dostępnych metod uwierzytelnienia na ePUAP

identyfikacji elektronicznej wydanych w innych państwach członkowskich UE. Ponieważ Polska w dalszym ciągu ich nie uznaje, funkcja ta nie jest dostępna (stan na 24 marca 2023 r.). Kolor niebieski oznacza środki identyfikacji elektronicznej dostępne w ramach publicznego systemu identyfikacji elektronicznej, a zielony – integrację z komercyjnym systemem identyfikacji elektronicznej (mojeID).

O popularności i użyteczności polskiego ekosystemu eID świadczy nie tylko duża liczba integracji i innowacyjnych usług cyfrowych, ale przede wszystkim świadomość obywateli, z jakich usług mogą skorzystać. W Polsce nie ma pełnej listy dostępnych dla obywateli publicznych i prywatnych dostawców usług. Szczątkowe informacje o systemie mojeID można znaleźć na oficjalnej stronie produktu[51].

51 https://www.mojeid.pl/archiwum-aktualnosci/



Rys. 3.8. Schemat identyfikacji elektronicznej uwzględniający obecność węzła komercyjnego.
Źródło: M. Tabor (2020), Trust services and eID in Poland in relation to the EU. Prezentacja z konferencji EFPE 2020

Rozwiązania stosowane w sektorze publicznym są wprawdzie wymienione w Rejestrze Dostawców Usług[52], ale jedynie z nazwy, bez przedstawienia możliwości każdego z nich.

Schematycznym podsumowaniwem informacji na temat elektronicznych mechanizmów identyfikacji w Polsce jest rys. 3.8[53].

3.3. Krajowa infrastruktura zaufania

Z rozwojem usług elektronicznych nierozerwalnie związane jest zawieranie umów i podpisywanie dokumentów na odległość – w tym celu wykorzystywany jest mechanizm podpisu cyfrowego, który umożliwia powiązanie podpisującego z podpisanym dokumentem. W takich sytuacjach przy zachowaniu odpowiednich procedur podpis cyfrowy jest odpowiednikiem podpisu tradycyjnego.

Wprowadzenie postanowień ustawy o usługach zaufania oraz identyfikacji elektronicznej wymaga powołania krajowej infrastruktury zaufania, która

52 https://mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-uslug/wezel-krajowy-zintegrowani-dostawcy-uslug.html

53 https://www.youtube.com/watch?v=jqckYtslXLg

w praktyce jest wdrożeniem mechanizmów pozwalających na weryfikację autentyczności podpisu wraz z zapewnieniem dowodów jego niezaprzeczalności.

Krajowa infrastruktura zaufania składa się z:

- Rejestru dostawców usług zaufania – będącego spisem konkretnych dostawców i świadczonych przez nich usług zaufania. Rejestr jest prowadzony elektronicznie i jawnie publikowany na stronie (Narodowego Centrum Certyfikacji – NCCert).
- Zaufanej listy – zawierającej listę kwalifikowanych dostawców i świadczonych przez nich usług zaufania. Lista jest publikowana na stronie internetowej nccert.pl i pozwala na rozpoznanie kwalifikowanych usług zaufania w UE.
- Narodowego Centrum Certyfikacji – będącego częścią Narodowego Banku Polskiego (NBP). Pełni rolę głównego urzędu certyfikacji w polskiej infrastrukturze zaufania, a odpowiada za wytwarzanie, wydawanie i unieważnianie certyfikatów dostawców usług zaufania.

Na stronie internetowej nccert.pl można znaleźć rejestr kwalifikowanych i niekwalifikowanych usług zaufania, do których należą m.in. znacznik czasu (zapewniający istnienie dokumentu w określonym momencie czasu), pieczęć elektroniczna (przeznaczona dla podmiotów prawnych, potwierdzająca integralność danych w dokumencie i tożsamość prawną jego wystawcy) czy podpis cyfrowy (przeznaczony dla osób fizycznych). Takie kwalifikowane usługi zaufania pełnią istotną rolę w ekosystemie eID, ponieważ ich wykorzystanie wywołuje wiążący skutek prawny.

Dokładny opis dostępnych usług zaufania wraz z przykładami i nazwami firm/podmiotów świadczących wybrane usługi można znaleźć w raporcie *Biznes bez papieru – Komercjalizacja eID i usług zaufania w Polsce i Europie*[54] przygotowanym przez Obserwatorium.biz.

Do zadań NCCert należy również utrzymanie zaufanej listy (ang. *trusted services list* – TSL)[55]. Lista ta umożliwia rozpoznawanie krajowych kwalifikowanych usług zaufania na terenie Europy. Jest publikowana na stronie Komisji Europejskiej i zawiera spis kwalifikowanych dostawców usług wraz z świadczonymi przez nich usługami.

54 *Biznes bez papieru – Komercjalizacja eID i usług zaufania w Polsce i Europie*. Dostępny na: https://obserwatorium.biz/biznes-bez-papieru-komercjalizacja-eid-i-uslug-zaufania-w-polsce-i-europie.html

55 https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

Z technicznego punktu widzenia krajowa infrastruktura zaufania przypomina typową infrastrukturę klucza publicznego (ang. *public key infrastructure* – PKI), która umożliwia sprawne zarządzanie certyfikatami cyfrowymi. Najbardziej istotnym elementem PKI jest centralna instytucja (w omawianym przypadku NCCert), nazywana też urzędem certyfikacji (ang. *certification authority* – CA). Instytucja ta wydaje certyfikaty poszczególnym podmiotom (w omawianym przypadku dostawcom usług zaufania), które z kolei wydają certyfikaty swoim klientom (użytkownikom, obywatelom). Dzięki takiej architekturze wystarczy zaufać NCCert, ponieważ każdy certyfikat wydany klientowi końcowemu jest wydawany przez podmiot, któremu zaufał wcześniej NCCert. Taka hierarchia weryfikacji certyfikatów jest nazywana łańcuchem zaufania (*ang. chain of trust*) lub ścieżką certyfikacji.

Do najpopularniejszych usług zaufania można zaliczyć podpis elektroniczny. Wyróżniane są następujące rodzaje podpisów elektronicznych[56]:

- Zwykły podpis elektroniczny – jego uzyskanie nie wymaga weryfikacji tożsamości; certyfikat zawiera podstawowe informacje jak imię, nazwisko i adres e-mail właściciela.
- Zaawansowany podpis elektroniczny – jego złożenie umożliwia jednoznaczną identyfikację podpisującego; certyfikat zawiera imię, nazwisko i numer identyfikacyjny (PESEL, numer dowodu). Sam podpis jest składany na podstawie danych znanych posiadaczowi podpisu (np. po podaniu hasła i/lub kodu SMS).
- Kwalifikowany podpis elektroniczny – w odróżnieniu od innych typów podpisów elektronicznych powoduje skutek prawny jak podpis własnoręczny. Podobnie jak zaawansowany podpis cyfrowy pozwala na jednoznaczną identyfikację osoby. Cały cykl życia podpisu kwalifikowanego wymaga spełnienia dodatkowych wymagań, począwszy od przeprowadzenia starannego procesu weryfikacji tożsamości osoby ubiegającej się o podpis elektroniczny, a skończywszy na bezpiecznym przechowywaniu certyfikatu (na karcie kryptograficznej lub w module HSM (ang. *hardware security module*)). Obecnie kwalifikowane podpisy elektroniczne można złożyć za pomocą:
  - Czytnika i karty – polega na wykorzystaniu karty kryptograficznej, która po podaniu kodu PIN umożliwia podpisanie wybranego dokumentu

56 https://podpisujzdalnie.pl/baza-wiedzy/roznica-miedzy-kwalifikowanym-zaawansowanym-a-niekwalifikowanym-podpisem-elektronicznym

za pośrednictwem dedykowanej aplikacji. Przykładem tego rozwiązania jest podpis kwalifikowany, który po zakupie może być umieszczony w e-dowodzie.

– Aplikacji mobilnej lub rozwiązań chmurowych – wszystkie wymagane elementy do złożenia podpisu są przechowywane na zewnętrznym serwerze w module HSM, który spełnia odpowiednie wymagania i jest przeznaczony do przechowywania i zarządzania kluczami kryptograficznymi. Z tego rozwiązania korzysta mSzafir, SimplySign i rSign.

4. Dowody osobiste

Dowód osobisty jest powszechnie stosowanym dokumentem potwierdzającym tożsamość jego posiadacza. W Polsce obowiązek jego posiadania ma każdy obywatel, który ukończył 18 r.ż., ale możliwe jest również wyrobienie tymczasowego dowodu osobistego osobom młodszym. Podstawowe akty prawne dotyczące dowodu osobistego to:

- *Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych*[57].
- *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 5 października 2021 r. w sprawie wzoru dowodu osobistego, jego wydawania i odbioru oraz utraty, uszkodzenia, unieważnienia i zwrotu*[58].

Dodatkowymi aktami prawnymi stosownymi do omawianych w niniejszym opracowaniu funkcjonalności dowodu osobistego są:

- *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*[59].
- *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 lutego 2019 r. w sprawie warstwy elektronicznej dowodu osobistego*[60].

Należy też wspomnieć o sformułowanym przez Międzynarodową Organizację Lotnictwa Cywilnego (ang. *International Civil Aviation Organization* – ICAO) standardzie *Doc 9303. Machine Readable Travel Documents*, w którym zdefiniowane są wymogi dotyczące elektronicznych dokumentów podróżnych[61].

4.1. E-dowód 2.0

W Polsce dowód osobisty przed 2001 rokiem miał formę tzw. zielonej książeczki – wyłącznie papierowego dokumentu ze zdjęciem. W 2001 roku rozpoczęto

57 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101671131

58 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210001865

59 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20050640565

60 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000400

61 ICAO, *Doc 9303. Machine Readable Travel Documents*. Dostępny w: https://www.icao.int/publications/Documents/Forms/AllItems.aspx

proces dostosowania formatu dokumentu do standardu ICAO Doc 9303, zgodnie z którym dokument podróży powinien być możliwy do odczytania maszynowego. Usprawnia to bowiem np. odprawę graniczną na lotniskach. Zmiany uwzględniały przejście do obecnej formy karty plastikowej: format ID-1, standard ISO 7810[62]. Sukcesywnie (w 2013, 2015 i 2019 roku) wprowadzano kolejne zmiany, z których każda była implementacją nowych form zabezpieczeń przed kopiowaniem oraz dodatkowych danych w warstwie graficznej, a ostatnia również pierwszej wersji warstwy elektronicznej. Ostatecznie w 2021 roku wprowadzono obecnie wydawaną wersję dowodu osobistego (tzw. e-dowód 2.0), która oprócz tego, że umożliwia realizację działań w polskich urzędach, odpowiada też normom UE (rozporządzenie KE 2019/1157[63]) dotyczącym jakości i ilości danych przechowywanych w dokumencie identyfikacyjnym.

Dane przechowywane w dowodzie osobistym

Dane przechowywane w dowodzie są wprowadzane etapowo. Blankiet dokumentu, dostarczony przez Polską Wytwórnię Papierów Wartościowych (PWPW), podlega personalizacji w Centrum Personalizacji Dokumentów MSWiA. Na tym etapie w strefie inspekcji wizualnej dokumentu pojawiają się dane identyfikacyjne posiadacza:

- imię (imiona) i nazwisko oraz nazwisko rodowe;
- imiona rodziców;
- datę i miejsce urodzenia, obywatelstwo;
- płeć;
- zdjęcie i wizerunek podpisu odręcznego;
- numer PESEL.

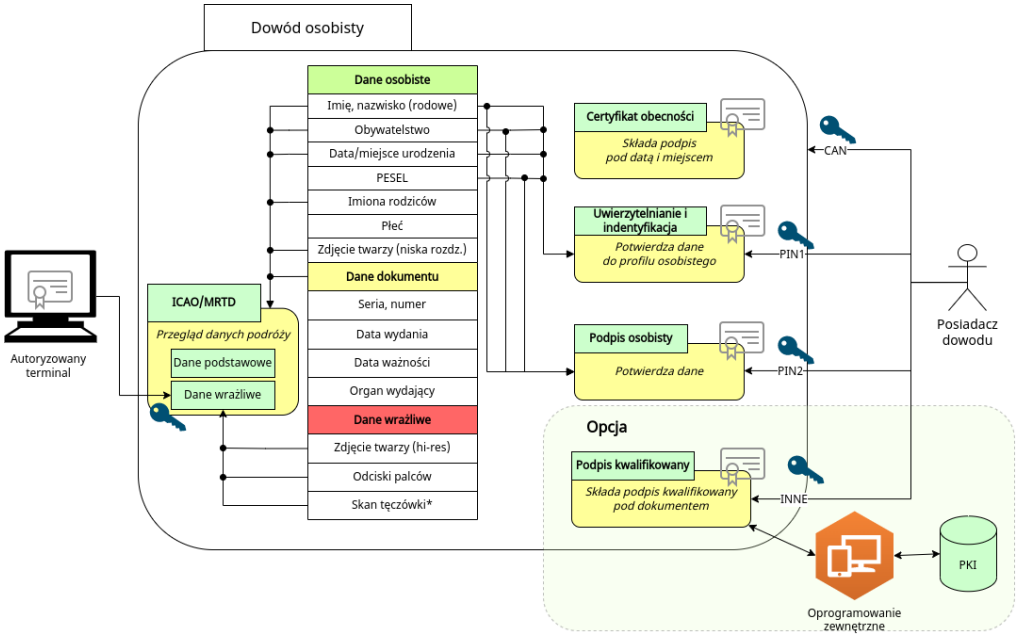
Dodatkowo nanoszone są informacje dotyczące samego dokumentu:

- seria i numer;
- data wydania i data ważności;
- organ wydający;
- numer CAN (ang. *card access number*).

Na rewersie dokumentu umieszczana jest też strefa MRZ (ang. *machine readable zone*) – zapis alfanumeryczny przeznaczony do odczytu maszynowego

62 https://www.iso.org/standard/31432.html

63 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32019R1157



Rys. 4.1. Architektura warstwy elektronicznej polskiego e-dowodu

za pomocą technik rozpoznawania pisma. Dane zapisane w MRZ to kraj wydania dokumentu, numer dowodu, data urodzenia, obywatelstwo, płeć, nazwisko i imiona posiadacza oraz cyfry kontrolne.

Dane warstwy graficznej są też zapisywane w warstwie elektronicznej. Dodatkowo umieszczane są w niej:

- dane biometryczne: odciski palców oraz zdjęcie twarzy;
- certyfikaty: obecności, identyfikacji i uwierzytelniania oraz – na życzenie posiadacza dowodu – certyfikat podpisu osobistego;
- rozwiązania komercyjne do składania kwalifikowanego podpisu cyfrowego, których uruchomienie może nastąpić dopiero po wydaniu dokumentu przez urząd państwowy i na drodze porozumienia posiadacza dowodu osobistego z zewnętrznym dostarczycielem tego typu usługi[64].

W momencie odbioru dokumentu następuje nadanie i zapisanie w nim poufnych i znanych tylko posiadaczowi numerów PIN1 i PIN2. W odrębnym, opcjonalnym procesie przeprowadzanym z dostawcą kwalifikowanych podpisów

64 Lista akredytowanych dostawców tego typu usługi jest publikowana przez Narodowe Centrum Certyfikacji pod adresem https://www.nccert.pl/uslugi.htm

cyfrowych dane w dowodzie osobistym mogą zostać rozszerzone o informacje niezbędne do składania kwalifikowanych podpisów cyfrowych.

Oprócz danych w warstwie elektronicznej przechowywane są również biblioteki programowe dostarczające jednolitych mechanizmów wykonywania operacji kryptograficznych i komunikacyjnych, programy (aplety), które realizują poszczególne funkcjonalności dokumentu, a także system operacyjny odpowiedzialny za komunikację z urządzeniami zewnętrznymi (czytnikami) oraz uruchamianie apletów.

Polskie dowody osobiste spełniają zawarte w ICAO Doc 9303 wymogi dotyczące elektronicznych dokumentów podróży. Jako takie w warstwie elektronicznej muszą zawierać:

- powtórzenie danych ze strefy MRZ;
- biometrię twarzy;
- odciski palców;
- biometrię tęczówki (jeśli pobrano);
- podpisy cyfrowe pod w/w danymi złożone przez wystawcę dokumentu;
- inne elementy techniczne wykorzystywane przez aplikację ICAO podczas działania.

Na rysunku 4.1 podano dane przechowywane w elektronicznej warstwie dowodu oraz zaznaczono sposób propagowania tych danych do różnych funkcjonalności realizowanych przez e-dowód. Przedstawiono też najbliższe środowisko dowodu osobistego i punkty zabezpieczania dostępu do przechowywanych danych. Dokładniejsze omówienie tych zagadnień znajduje się w dalszej części tego rozdziału.

4.2. Zabezpieczenia w dokumencie z 2021 roku

Zabezpieczenia w dowodzie osobistym można rozpatrywać ze względu na obszar ich działania. Bezpieczeństwo warstwy graficznej zależy od techniki produkcji i personalizacji dokumentu, a ma na celu uniemożliwienie lub znaczne utrudnienie wytworzenia dokumentu poza legalnym obiegiem. W przypadku warstwy elektronicznej bezpieczeństwo zależy od sposobów konstrukcji komponentów elektronicznych i wykonywanych przez nie protokołów. W tym wypadku wymogiem jest nie tylko uniemożliwienie nielegalnego stworzenia urządzenia elektronicznego mogącego udawać dowód osobisty, ale też zapobieganie nieuprawnionemu dostępowi do danych przechowywanych w formie elektronicznej. Normy

Rys. 4.2. Awers i rewers polskiego e-dowodu wydawanego po 7 listopada 2021 roku

i atesty to z kolei sformalizowanie tych technicznych elementów w oderwaniu od konkretnych rozwiązań technicznych.

Warstwa graficzna

Zabezpieczenia przed kopiowaniem w warstwie graficznej występują już na poziomie czystego blankietu dokumentu, ale w procesie personalizacji wykorzystuje się dodatkowe techniki zabezpieczające. Rysunek 4.2 przedstawia awers i rewers dowodu osobistego wydawanego po 7 listopada 2021 roku ze wskazanymi obszarami zabezpieczeń[65]:

1) Zmienny obraz laserowy naniesiony w technice MLI (ang. *multiple laser image* – MLI) – przedstawia dwie różne wersje zdjęcia w zależności od kąta patrzenia.
2) Grawerowanie na wyskok – druk wypukły, wyczuwalny w dotyku, dostrzegalny przy świetle padającym pod kątem. W tej technice wykonany jest też napis nazwiska i imion.

65 https://www.gov.pl/app/rdp/web/rdp/dowod-osobisty-wzor-2021

3) Nadruk farbą o zmiennym kolorze, zależnym od kąta patrzenia.
4) Mikrotekst – we wskazanym miejscu przy użyciu szkła powiększającego można dostrzec tekst RZECZPOSPOLITA POLSKA.
5) Druk giloszowy (siatka ciągłych linii) z płynną zmianą koloru (efekt irysowy).
6) Efekt dyfrakcyjny – kontur mapy Polski z wpisanymi literami RP zamieniają się kolorami przy obrocie o 90 stopni.
7) Wytłoczenia – wyczuwalna w dotyku zmiana gładkości dokumentu, widoczna też pod światło.
8) Druk giloszowy.
9) Przezroczysty grawerunek laserowy (ang. *transparent laser engraving* – TLE) – wypukły napis widoczny pod ostrym kątem.

Należy dodać, że powyższe zabezpieczenia uwidaczniają się w świetle widzialnym. Dodatkowe detale wykonane w technice druku giloszowego w kolorach zielonym, niebieskim i czerwonym oraz litery RP na awersie i napis POLSKA na rewersie są widoczne w świetle ultrafioletowym (356 nm).

Mechanizm bezpieczeństwa w przypadku warstwy graficznej polega przede wszystkim na technologicznej trudności wykonania kopii lub modyfikacji gotowego dokumentu. Naniesione informacje powodują nieodwracalne zmiany w podłożu poliwęglanowym blankietu, co praktycznie uniemożliwia wykorzystanie wydanego dokumentu do jego przerobienia. Z drugiej strony wytworzenie czystych blankietów i poprawne naniesienie informacji o posiadaczu dokumentu wymaga różnych procesów, w związku z czym jednoczesne przełamanie wszystkich zastosowanych zabezpieczeń jest niemal niemożliwe.

Warstwa elektroniczna

Część elektroniczna dowodu osobistego jest odczytywana przez czytniki za pomocą bezprzewodowej technologii NFC (*ang. near field communication*). Tworzy to dwie możliwości ataku: nieautoryzowany dostęp do dowodu, czyli aktywne angażowanie dowodu w komunikację bez wiedzy posiadacza dokumentu (ang. *skimming*), oraz podsłuchiwanie komunikacji (ang. *eavesdropping*), czyli pasywne zdobywanie informacji z sesji świadomie zainicjowanej przez posiadacza dowodu.

Każde rozpoczęcie sesji z warstwą elektroniczną jest poprzedzane podaniem numeru CAN – jest to sześciocyfrowy kod wydrukowany na awersie dokumentu, pod zdjęciem, oraz na jego rewersie w postaci kodu kreskowego. Poprawny numer

CAN umożliwia kontynuację sesji komunikacyjnej i realizację konkretnych funkcjonalności dowodu osobistego. Na tym etapie dostęp do certyfikatu potwierdzenia obecności jest możliwy bez dodatkowych informacji. Pozostałe funkcjonalności są realizowane dopiero po podaniu odpowiednich kodów zabezpieczających PIN1 i PIN2. Pierwszy kod, 4-cyfrowy, umożliwia dostęp do certyfikatu identyfikacji i uwierzytelniania, drugi, 6-cyfrowy, daje dostęp do certyfikatu podpisu osobistego. Trzykrotne błędne podanie któregokolwiek z tych kodów powoduje zablokowanie dostępu do tych funkcji dowodu. Posiadacz dowodu może je odblokować, podając 8-cyfrowy kod PUK. Trzykrotne błędne wpisanie kodu PUK powoduje permanentną blokadę dostępu do zablokowanych certyfikatów, a jedyną możliwością przywrócenia funkcjonalności jest wymiana dowodu na nowy.

Kody PIN1 i PIN2 posiadacz dowodu ustala w momencie odbioru dowodu w urzędzie i może je zmieniać dowolnie za pomocą aplikacji eDO App. Kod PUK otrzymuje się wraz z dowodem osobistym w zamkniętej kopercie i podobnie jak PIN1 i PIN2 należy go utrzymywać w tajemnicy. Jest to zatem zabezpieczenie typu „coś, co wiem", natomiast kod CAN można traktować jako zabezpieczenie „coś, co mam". Należy jednak pamiętać, że dostępność kodu CAN dla osób trzecich jest wysoka w zasadzie przy każdym przedstawieniu dokumentu, dlatego odporność na ataki aktywne w warstwie elektronicznej zależy przede wszystkim od tajności kodów PIN.

W komunikacji bezprzewodowej zawsze istnieje możliwość przechwycenia transmisji danych przez trzecią stronę. Protokół NFC wykorzystywany do komunikacji dowodu z czytnikami jest zaprojektowany tak, by zasięgiem obejmował jedynie urządzenia w bezpośredniej odległości (kilku centymetrów). Niemniej jednak istnieją prace potwierdzające możliwość skutecznego podsłuchania transmisji NFC za pomocą odpowiednich urządzeń na odległość większą niż kilkadziesiąt centymetrów.

Warto w tym miejscu podkreślić wagę pierwszego zabezpieczenia – numeru CAN. W momencie ustanowienia połączenia bezprzewodowego z czytnikiem numer ten jest przekazywany do niego odrębnym (tj. nie radiowym) kanałem – najczęściej w wyniku wpisania go na klawiaturze czytnika. W ten sposób powstaje sytuacja, w której dowód osobisty oraz czytnik dysponują pewną, teoretycznie nieznaną podsłuchującej osobie wartością, którą mogą wykorzystać do wstępnego wzajemnego uwierzytelnienia oraz do ustanowienia kryptograficznego klucza symetrycznego, który posłuży do szyfrowania dalszej komunikacji radiowej. W przypadku realizacji funkcjonalności elektronicznego dokumen-

tu podróży funkcję numeru CAN pełnią informacje zamieszczone w warstwie MRZ dokumentu. Ważne w tym wszystkim jest to, że przekazanie informacji o CAN/MRZ powinno wiązać się (w zamyśle) ze świadomym działaniem posiadacza dowodu osobistego: wyjęciem go z portfela, wpisaniem kodu na klawiaturze lub zeskanowaniem go w czytniku.

Gradacja zabezpieczeń informacji w warstwie elektronicznej (CAN, PIN1, PIN2) zabezpiecza dalszą komunikację radiową i dostęp do danych przechowywanych w warstwie elektronicznej na wyższych poziomach protokołu. Przesyłane dane, wyniające np. z użycia certyfikatu identyfikacji i uwierzytelniania (chronionego przez PIN1) lub certyfikatu podpisu osobistego (PIN2) są chronione protokołem kryptograficznym, działającym w dwójnasób:

- Po pierwsze: czytnik i dowód osobisty przechodzą proces wzajemnego uwierzytelniania, sprawdzający uprawnienia czytnika do możliwości dostępu do żądanych danych. Podstawą protokołu jest kryptografia asymetryczna. Uprawnione czytniki to takie, które dysponują certyfikatem wydanym przez odpowiednie organy państwa.
- Po drugie: po skutecznym uwierzytelnieniu komunikacja między czytnikiem a dowodem jest szyfrowana kluczem, którego nie sposób odgadnąć, bazując wyłącznie na przesyłanych komunikatach.

W efekcie tego dane wrażliwe zawarte w warstwie elektronicznej są chronione przed dostępem osób postronnych dysponujących technologią umożliwiającą podsłuchanie.

Innym aspektem bezpieczeństwa jest możliwość stworzenia warstwy elektronicznej dowodu osobistego poza oficjalnym obiegiem, tj. podrobienia e-dowodu przez:

- Stworzenie aplikacji na urządzenie typu smart-card, która będzie zgodna z protokołem ICAO i dostarczy podstawowych informacji o posiadaczu dokumentu.
- Stworzenie aplikacji realizującej funkcjonalności polskiego dowodu osobistego (wykorzystującej certyfikaty obecności, podpisu osobistego i potwierdzenia obecności).

W pierwszym wypadku należy stwierdzić, że zbudowanie takiej aplikacji jest poniekąd możliwe, jeśli byłaby to dokładna kopia już wystawionego dokumentu. Mimo że dane zwracane przez taką aplikację muszą być certyfikowane podpisem kraju-wystawcy dokumentu, dopuszczalna jest weryfikacja bez udziału dokumentu (ang. *passive authentication* – zob. ICAO 9303, cz. 11, rozdz. 5), gdzie nie jest wymagana znajomość tajnych kluczy dokumentu. Pozostałe dane są

znane, gdyż standard protokołu i sposób przekazywania tych danych jest otwarty i publicznie dostępny (zob. podrozdz. 4.6). Nie ma to jednak odniesienia do danych wrażliwych i biometrycznych, których skuteczne podrobienie i cerfyfikacja nie są możliwe, a sklonowane dane nie zostaną przyjęte, gdyż w przypadku dostępu do tych informacji przeprowadzana jest zawsze aktywna autentykacja dokumentu.

W drugim wypadku należy podkreślić, że samodzielne wygenerowanie certyfikatów oraz odpowiednich kluczy kryptograficznych, które tworzyłyby poprawne podpisy w ramach funkcjonalności certyfikowania dostępnych w dowodzie osobistym nie jest możliwe. Można się spodziewać, że istnieje możliwość ekstrakcji już gotowych danych kryptograficznych z istniejącego e-dowodu, ale modyfikacja ich tak, by odpowiadały innej osobie, jest niemożliwa. Dane podpisywane są bowiem certyfikatem, który powinien być w posiadaniu tylko i wyłącznie CPD MSWiA.

Warto podkreślić, że specyfikacja komunikacji, struktury wewnętrznej i protokołów kryptograficznych wykorzystanych w e-dowodzie w tej części jego funkcjonalności pozostaje zamknięta i wiedza o niej jest strzeżona przez PWPW. Taka zamkniętość specyfikacji bardzo utrudnia, jeśli nie uniemożliwia, niezależnym badaczom weryfikację poprawności stworzonych rozwiązań i nie jest typowym podejściem w obszarach zastosowań kryptograficznych. O ile tego rodzaju *security by obscurity*[66] daje początkowo dobre gwarancje bezpieczeństwa, to należy brać pod uwagę dwie kwestie:

- Zamknięte rozwiązania uniemożliwiają weryfikację przez szersze gremia badaczy, przez co porzucany jest dodatkowy element zabezpieczenia w postaci wielotorowej i niezależnej weryfikacji stosowanych praktyk.
- W wypadku, gdy utajnione rozwiązanie zostanie przełamane, np. na drodze inżynierii wstecznej, dzięki postępowi w nauce lub wskutek wycieku informacji producenta, a będzie ono zawierało luki, których producent nie zauważył lub nie wyeliminował, polegając na właśnie przełamanej „tajności", luki takie mogą być wykorzystywane w sposób nielegalny, a fakt ich poznania może pozostawać ukryty.

Autorzy niniejszej publikacji nie zakładają, że wytwórca warstwy elektronicznej dowodu osobistego pozostawił w niej luki lub niedociągnięcia. Należy

66 Dosłownie: bezpieczeństwo przez zaciemnienie – określenie używane w odniesieniu do rozwiązań, których bezpieczeństwo polega częściowo na zachowaniu w tajemnicy sposobu przetwarzania danych.

jedynie mieć na względzie to, że w obecnej sytuacji nie ma możliwości zweryfikowania, czy takie luki istnieją, i pozostaje zaufanie do poprawności proceduralnej części procesu wdrożenia e-dowodu.

Normy i atestacja

Jednym z podstawowych mechanizmów definiowania bezpieczeństwa systemów informatycznych jest określenie ich zgodności z *Common Criteria*[67] zdefiniowanymi w standardzie ISO/IEC 15408[68]. Procesor warstwy elektronicznej dowodu osobistego musi być na przynajmniej piątym (z maksymalnie siedmiu) poziomów EAL (ang. *electronic assurance level*). Przekłada się to na silną zgodność z wymaganiami określonymi przez klienta i stosowaniem rygorystycznych procedur tworzenia komercyjnego produktu informatycznego oraz średni stopień implementacji specjalistycznych zabezpieczeń kryptograficznych. Wymagania stawiane systemowi operacyjnemu to wypełnienie postanowień Java Card Protection Profile[69] w wersji przynajmniej 3.0 (według dokumentu ANSSI-PP-2010/03-M01[70]) oraz osiągnięcie przynajmniej poziomu EAL5 (nieco niższy poziom, tj. EAL4, wymagany jest od poszczególnych apletów realizujących klienckie funkcjonalności).

W ramach prawa obowiązującego w Polsce wymogi techniczne dotyczące warstwy elektronicznej zawarte są w Załączniku 1 do *Rozporządzenia MSWiA z 26 lutego 2019 r. w sprawie warstwy elektronicznej dowodu osobistego*[71].

4.3. Weryfikacja autentyczności dokumentów

Zadanie stwierdzenia, czy prezentowany dowód osobisty jest autentyczny, polega na zweryfikowaniu szeregu elementów zabezpieczających (zob. podrozdz. 4.2). Nie wymaga to specjalistycznej wiedzy, a jedynie w przypadku (weryfika-

67 https://www.commoncriteriaportal.org/.

68 https://www.iso.org/standard/72891.html

69 Są to opracowane przez Oracle zestawy wymogów bezpieczeństwa oprogramowania dla platformy Java Card, ułatwiają ewaluację tworzonego oprogramowania pod kątem zgodności z Common Criteria. Wymogi te są dostępne w: https://www.oracle.com/java/technologies/javacard-protection-profile.html

70 https://sogis.org/uk/pp_pages/others/pp_jcs_open.html

71 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000400

cji) warstwy fizycznej możliwości obejrzenia dokumentu w ostrym świetle lub w świetle ultrafioletowym o długości fali 356 nm w wypadku zabezpieczeń widocznych oraz sprawdzenia dotykowo w wypadku zabezpieczeń wyczuwalnych w ten sposób. W warunkach słabego oświetlenia lub w przypadku wad wzroku osoby weryfikującej dokładne sprawdzenie tych zabezpieczeń może być utrudnione. Niektóre cechy są wyczuwalne dotykowo, co utrudnia ich weryfikację np. w rękawiczkach ochronnych.

W każdym wypadku poprawne przeprowadzenie weryfikacji jest jednak możliwe tylko wtedy, gdy osoba sprawdzająca zna metody, którymi może się posłużyć i ma świadomość mechanizmów bezpieczeństwa wbudowanych w blankiet dowodu osobistego, które dodatkowo różnią się między poszczególnymi edycjami.

Dołączenie do dowodu warstwy elektronicznej znacząco rozszerza i upraszcza możliwości weryfikacji dokumentu, gdyż – jak wspomniano wcześniej – dane cyfrowe stanowią duplikat danych umieszczonych w warstwie elektronicznej. Umożliwia to zatem porównanie informacji uzyskanych z obu źródeł, a przy założeniu, że dane z warstwy elektronicznej są w zasadzie niepodrabialne, identyczność informacji z obu warstw stanowi niepodważalny dowód ich prawdziwości.

Warto dodać, że w przypadku elektronicznego odczytu danych nie jest wymagana żadna specyficzna wiedza czy przeszkolenie z zakresu mechanizmów zabezpieczeń, tak jak to ma miejsce przy weryfikacji zabezpieczeń warstwy graficznej. Całą funkcjonalność realizuje bowiem dedykowane oprogramowanie lub urządzenie, a jego operatorowi pozostaje tylko stwierdzenie identyczności informacji z obu lokalizacji danych.

4.4. Przypadki użycia nowych dokumentów

W dowodzie osobistym dostępne są standardowo dwa, opcjonalnie trzy lub cztery, certyfikaty i aplikacje je wykorzystujące (rys. 4.1). Umożliwiają one interakcję z systemami cyfrowymi realizującymi takie funkcjonalności, jak np. logowanie się do serwisów, potwierdzanie obecności i tożsamości, składanie cyfrowego podpisu osobistego lub kwalifikowanego podpisu cyfrowego.

Potwierdzenie obecności

Dowód generuje cyfrowy podpis pod znacznikiem czasu (ang. *timestamp*) i danymi opisującymi miejsce, dzięki czemu istnieje możliwość potwierdzenia jego

obecności w danym miejscu i czasie. Jest to odpowiednik odręcznego podpisu na liście obecności czy potwierdzeniu odebrania usługi, np. odbycia wizyty u lekarza.

W tej aktywności wymagane jest podanie jedynie numeru CAN.

Uwierzytelnianie i identyfikacja

Warstwa elektroniczna dowodu umożliwia jednej stronie, tj. posiadaczowi dowodu, uwierzytelnienie się w portalach administracji publicznej[72], a drugiej, np. policji czy straży granicznej, zidentyfikowanie posiadacza podobnie jak na podstawie standardowej wersji dowodu. Wykorzystując tę funkcjonalność, posiadacz dowodu może potwierdzić swoje dane: imię, nazwisko, datę i miejsce urodzenia, numer PESEL i obywatelstwo.

Dostęp do procedury uwierzytelniania (logowania na portalu) możliwy jest po skorzystaniu z certyfikatu identyfikacji i uwierzytelnienia po podaniu numeru CAN i PIN1.

Podpis osobisty

Zależnie od decyzji posiadacza w jego dowodzie może zostać uruchomiony certyfikat podpisu osobistego. Umożliwi on składanie pod dokumentami cyfrowych podpisów osobistych, które w komunikacji z organami państwa mają taką samą wagę, jaką ma podpis odręczny. Podpis taki składany jest pod danymi pozwalającymi na identyfikację posiadacza: imieniem, nazwiskiem, informacją o obywatelstwie i numerem PESEL. Dodatkowo podpis osobisty jest wiążący w wypadku dokumentów wymienianych w komunikacji z innymi podmiotami, jeśli te wyrażą zgodę na taki sposób ich przetwarzania.

Złożenie podpisu osobistego wymaga podania kodu CAN, a następnie kodu PIN2.

Dokument podróży

Polskie dowody osobiste z warstwą elektroniczną spełniają normy ICAO dotyczące elektronicznych dokumentów podróży w formacie TD1 MRTD. Zawierają dane identyfikujące posiadacza dokumentu (imię, nazwisko, obywatelstwo, zdjęcie

72 Przykładowymi portalami są: ePUAP, CEIDG, PUE, praca.gov.pl, biznes.gov.pl.

w niskiej rozdzielczości), do których dostęp wymaga podania numeru CAN. Dane biometryczne (odcisk palca, wysokiej rozdzielczości zdjęcie twarzy) są dostępne jedynie dla certyfikowanych, czyli posiadających klucze kryptograficzne i certyfikaty wydawane przez odpowiednie władze, czytników/terminali. W takim wypadku dowód i terminal przeprowadzają kryptograficzny protokół PACE[73], który sprawdza poświadczenia obu elementów: autoryzację terminalu do dostępu do danych biometrycznych oraz poprawność tych danych (sprawdzany jest podpis pod tymi danymi, wystawiany przez organ wydający dowód osobisty).

Kwalifikowany podpis cyfrowy

W warstwie elektronicznej dowodu osobistego jest miejsce na umieszczenie certyfikatu i aplikacji przeznaczonych do składania kwalifikowanego podpisu cyfrowego. Uruchomienie tej funkcjonalności nie jest domeną organów państwowych. Aby otrzymać tę funkcjonalność, posiadacz dowodu może zwrócić się do komercyjnych dostawców. Umożliwi ona składanie za pomocą dowodu osobistego kwalifikowanego podpisu cyfrowego, którego moc wiążąca jest taka jak moc podpisu złożonego z wykorzystaniem komercyjnie dostępnych kart i urządzeń podpisujących. Zastosowania nowego e-dowodu – zarówno te wyżej wspomniane, jak i inne – zostały szczegółowo omówione przez Krzysztofa Bieńkowskiego w webinarze *E-dowód osobisty – Twoja cyfrowa tożsamość w 15 praktycznych przykładach*[74].

4.5. Dobre praktyki związane z użytkowaniem dokumentu

Dowód osobisty jest nośnikiem wrażliwych danych osobowych i z tego względu powinien być przedmiotem szczególnej uwagi posiadacza. Warto jednak przytoczyć postanowienie Naczelnego Sądu Administracyjnego z 9.12.2001 (II SA 2869/00)[75], według którego ustalenie tożsamości osoby na podstawie dowodu osobistego bez utrwalenia danych w nim zawartych nie stanowi przetwarzania danych osobowych.

73 https://www.icao.int/Security/FAL/TRIP/Documents/TR%20%20Supplemental%20Access%20Control%20V1.1.pdf

74 https://www.youtube.com/watch?v=fDhozOQZO7c

75 https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-sa-2869-00-wyrok-naczelnego-sadu-administracyjnego-520144118

Okazywanie dowodu

Dowód osobisty powinien znajdować się pod stałą kontrolą jego posiadacza, z wyłączeniem sytuacji, w których osoba trzecia jest uprawniona do jego przejęcia. Przez okazanie rozumie się przedstawienie dokumentu (zawartych na nim informacji), ale nie wręczenie go osobie kontrolującej.

Jednym z typowych postępowań, w których prawo nakazuje okazanie dowodu na żądanie, jest wypisywanie przez kontrolera wezwania do zapłaty kary za brak ważnego biletu na przejazd (np. w środkach komunikacji publicznej) – regulowane jest to *Ustawą z dnia 15 listopada 1984 r. Prawo przewozowe*[76]. Prawo do wylegitymowania może mieć też licencjonowany ochroniarz, ale wyłącznie na obszarze/w budynku przez niego chronionym. Zgodnie z *Ustawą z dnia 22 sierpnia 1997 r. o ochronie osób i mienia*[77] przed okazaniem dokumentu można prosić o przedstawienie legitymacji służbowej.

Nie należy zostawiać dowodu osobistego w recepcji hotelu czy innych miejsc noclegowych, choćby tylko w celu zameldowania się. W takich wypadkach wystarczające powinno być okazanie dowodu.

Inne osoby mogące prosić o przedstawienie dokumentu to m.in. pracownicy państwowi pełniący swoje obowiązki (np. kontrolerzy skarbowi, pracownicy ZUS-u czy inspekcji handlowej), a także funkcjonariusze BOR-u, ŻW, SW. Na wezwanie należy też przedstawić dokument podczas kupowania alkoholu, jeśli ustalenie wieku kupującego jest utrudnione – podstawę prawną stanowi *Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi*[78].

Warto zwrócić uwagę, że najbardziej rozpowszechnioną do niedawna formą łamania norm bezpieczeństwa dotyczących danych zawartych w dowodzie osobistym było pozostawianie tego dokumentu w zastaw, np. w różnego rodzaju wypożyczalniach. Zgodnie z *Ustawą z dnia 6 sierpnia 2010 r. o dowodach osobistych*[79] taki wymóg ze strony wypożyczającego może być karany grzywną lub pozbawieniem wolności do 1 miesiąca[80].

76 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19840530272

77 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19971140740

78 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19820350230

79 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101671131

80 Przypadki zastosowania takiej praktyki można (i należy) zgłaszać Głównemu Inspektorowi Danych Osobowych.

Przedstawienie do wglądu

Ta czynność zakłada, że dowód jest przekazany osobie trzeciej, a zatem posiadacz dokumentu traci z nim kontakt. Prawo wykonania takich czynności przysługuje jedynie funkcjonariuszom policji, straży granicznej w trakcie pełnienia obowiązków służbowych, np. na przejściu granicznym, po przedstawieniu podstawy wykonywanej czynności, o ile nie jest oczywista. Warto wiedzieć, że w sytuacjach nieoczywistych przed oddaniem dokumentu można prosić o przedstawienie legitymacji służbowej.

Tworzenie kserokopii

W kwestii praktykowanego, np. w bankach, robienia kserokopii dowodu osobistego Generalny Inspektor Ochrony Danych Osobowych w uzasadnieniu[81] powołuje się na wyrok NSA z 19.12.2001 r. (II SA 2869/00)[82], który określa takie działanie jako sposób techniczny mający na celu przechowywanie danych w nim zawartych (na równi z np. przepisaniem tych danych do odpowiedniego formularza). W tym świetle tworzenie kserokopii dowodu można uważać za dopuszczalne, jeśli podmiot wchodzący w posiadanie kserokopii jest uprawniony do przetwarzania wszystkich danych osobowych zawartych na blankiecie oraz spełnione są inne przepisy związane z takim przetwarzaniem danych.

W artykule 2 *Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*[83] są przedstawione podmioty uprawnione do przetwarzania danych osobowych zawartych w dowodzie osobistym, a w art. 34 ust. 4 podane ich uprawnia do tworzenia kserokopii dowodu. Lista zawiera oprócz podmiotów z obszaru usług prawnych i księgowych także m.in. podmioty prowadzące działalność kantorową, pośredników sprzedaży nieruchomości (z ograniczeniami), podmioty prowadzące działalność w zakresie gier losowych, operatorów pocztowych i podmioty udostępniające skrytki sejfowe.

81 https://archiwum.giodo.gov.pl/pl/329/1534

82 https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-sa-2869-00-wyrok-naczelnego-sadu-administracyjnego-520144118

83 https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180000723/U/D20180723Lj.pdf

Ochrona warstwy elektronicznej

Jak wspomniano, pierwszą linią ochrony przed niepowołanym dostępem do danych w warstwie elektronicznej jest numer dostępowy CAN znajdujący się na awersie dokumentu. Przy okazywaniu dokumentu (bez odczytu komputerowego) można zasłonić część z numerem, uniemożliwiając jego odczyt. Jest to działanie zgodne z zasadą minimalizacji ekspozycji danych: jeśli ktoś wykonuje czynności niezwiązane z warstwą elektroniczną dowodu, wiedza o numerze CAN jest mu niepotrzebna.

Kolejnymi elementami zabezpieczającymi dostęp do funkcjonalności dowodu są numery PIN1 i PIN2. Jako że mogą być ustalane przez posiadacza dowodu, zastosowanie mają standardowe uwagi dotyczące kodów PIN:

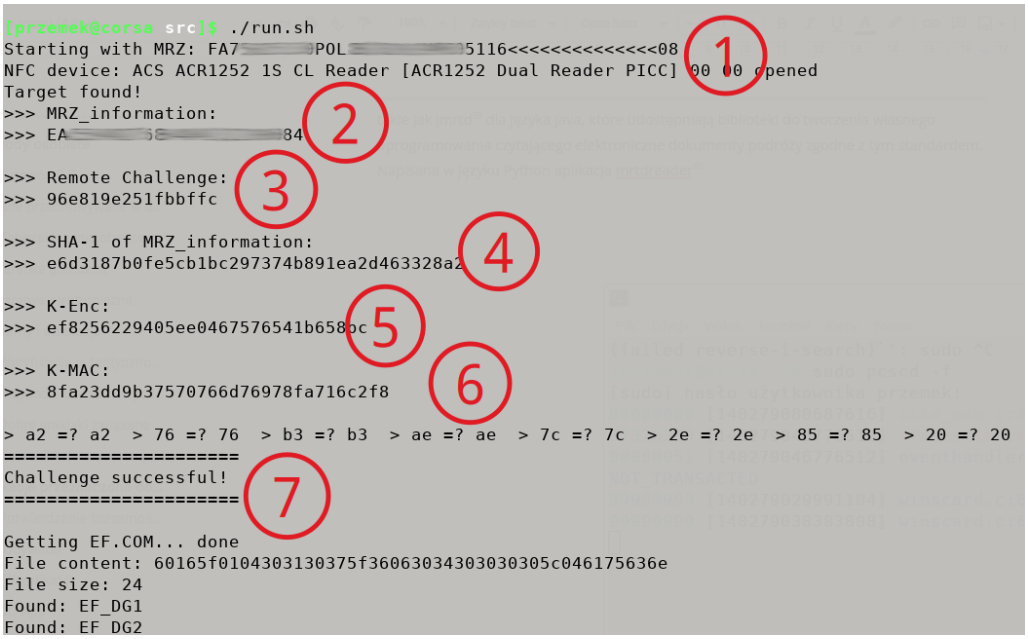
- Należy unikać wiązania kodów z łatwymi do odgadnięcia numerami z życia osobistego (datą urodzenia, numerem mieszkania, numerem telefonu).
- Kody PIN najlepiej zapamiętać lub zapisać w bezpiecznym miejscu, niezwiązanym z miejscem przechowywania dowodu osobistego (np. portfelem).
- Nie należy udostępniać kodów PIN, ponieważ nawet osoba zaufana, by zapamiętać bezbłędnie powierzony jej PIN, najpewniej zapisze go. Pomijając samą zasadność uprawniania osoby trzeciej do posługiwania się naszą tożsamością, spowodujemy powstanie elementu poufnej informacji poza naszą kontrolą.

Kod PUK – służący do odblokowywania i zmiany numerów PIN – również należy przechowywać w bezpiecznym miejscu, niezwiązanym wprost z miejscem przechowywania dowodu osobistego.

Nawiązywanie komunikacji z dowodem przez NFC można skutecznie uniemożliwić, przechowując dokument w specjalnie przygotowanej koszulce nieprzepuszczalnej dla fal radiowych. Podobnie jak w przypadku kart płatniczych, ten prosty zabieg niweczy próby zdalnego odczytania dowodu.

4.6. Komunikacja z warstwą elektroniczną dokumentu

Dostęp do danych i certyfikatów zawartych w elektronicznej części dowodu osobistego jest strzeżony kodami CAN, PIN1 i PIN2, znanymi posiadaczowi dokumentu. Ponadto dane wrażliwe i operacje składania podpisów są chronio-



Rys. 4.3. Interakcja z warstwą elektroniczną polskiego e-dowodu.
1 – Uruchomienie programu z podaną drugą linią pola MRZ, 2 – Przekształcenie danych z MRZ w klucz (odpowiednik CAN), 3 –Przesłanie przez dokument podróżny „wyzwania" (losową liczbę), które czytnik powinien przetworzyć zgodnie z informacjami zawartymi w kluczu odczytanym z MRZ, 4 – Skrót kryptograficzny danych z MRZ, 5 – Wygenerowany klucz szyfrujący komunikację między dokumentem a czytnikiem, 6 – Wygenerowany klucz potwierdzający autentyczność informacji przesyłanych między dokumentem a czytnikiem, 7 – Sekwencja wyzwań i poprawnych odpowiedzi skutkuje udanym odczytem pierwszego pliku (EF.COM) z informacjami zawartymi w dokumencie

ne mechanizmami opartymi na szyfrowaniu asymetrycznym, a dostęp do tych funkcjonalności jest ograniczony do stron posiadających odpowiednie cyfrowe certyfikaty dostępu. Niemniej jednak istnieje możliwość odczytania niektórych danych z dowodu osobistego z wykorzystaniem ogólnie dostępnych urządzeń i oprogramowania.

Jak zaznaczono na rys. 4.1, aplikacja ICAO w wersji podstawowej (tj. nieautoryzowanej) ma dostęp do takich danych jak np. imię i nazwisko, data urodzenia posiadacza dowodu. Protokół komunikacyjny takiej aplikacji i dowolnego czytnika NFC jest otwarty i publicznie dostępny[84]. Istnieją też otwarte implementacje

84 Doc 9303, cz. 11.

tego standardu, np. jmrtd[85] dla języka Java, które udostępniają biblioteki do tworzenia własnego oprogramowania czytającego elektroniczne dokumenty podróży zgodne z tym standardem. Na rysunku 4.3 przedstawiono przykład interakcji aplikacji mrtdreader[86] z dokumentem podróżnym zgodnym z ICAO (program nieznacznie zmodyfikowano w celu poprawienia czytelności, dane wrażliwe zamazano).

Dalsza komunikacja pozwala na odczytanie podstawowych danych posiadacza dokumentu, w tym na pobranie zdjęcia twarzy w niskiej rozdzielczości.

4.7. Postępowanie w przypadku utraty dowodu osobistego

Bez względu na zastosowane mechanizmy zabezpieczeń dokumentów niektóre aspekty bezpieczeństwa w dalszym ciągu spoczywają na obywatelu. Są one szczególnie istotne w sytuacjach kryzysowych (np. w przypadku zgubienia lub kradzieży dokumentu). Od posiadacza dokumentu wymagają podjęcia stanowczych i zdecydowanych działań w celu zminimalizowania ryzyka i konsekwencji wynikających z zaistniałej sytuacji. Stres związany z takim zdarzeniem wywołuje dodatkowo negatywne emocje (w postaci np. niepokoju), które wpływają na racjonalność podejmowanych decyzji. Jednym ze skutków kradzieży dowodu osobistego może być kradzież tożsamości i potencjalne straty finansowe wynikające np. z podpisania na nazwisko posiadacza ukradzionego dokumentu jakiejś umowy lub zaciągnięcia kredytu. Bardzo często następstwem kradzieży dowodu osobistego jest powstanie różnych sytuacji prawnych, które wymagają dodatkowych wyjaśnień na policji lub przed sądem.

Sytuację komplikuje również fakt, że utratę dokumentów należy jak najszybciej zgłosić jednocześnie w kilku różnych instytucjach, których istnienia nie jest świadoma zdecydowana większość społeczeństwa. Utrata dowodu osobistego oznacza konieczność natychmiastowego wykonania następujących czynności, które mogą uchronić przed niepożądanymi konsekwencjami[87]:

- Zastrzec utracony dokument w systemie Dokumenty Zastrzeżone (DZ), tj. rozwiązaniu nadzorowanym przez ZBP, którego celem jest przekazywanie informacji o zastrzeżonych dokumentach do banków, operatorów telefonii

85 http://jmrtd.org

86 https://github.com/rubund/mrtdreader

87 https://dokumentyzastrzezone.pl/zastrzeganie-dokumentow/

komórkowej oraz tysięcy innych firm i instytucji z niego korzystających. Zgłoszenia można dokonać osobiście w niektórych placówkach banku, telefonicznie pod numerem +48 828 828 828 lub za pośrednictwem konta BIK.
- Powiadomić policję, gdy mamy podejrzenie, że dokument został skradziony.
- Zgłosić utratę dokumentu w najbliższym urzędzie gminy, w placówce konsularnej lub unieważnić go za pośrednictwem portalu gov.pl[88].
- Skontaktować się z dostawcą podpisu kwalifikowanego w celu jego unieważnienia, o ile podpis ten był umieszczony w e-dowodzie.

Wraz z wprowadzeniem pierwszego dowodu osobistego z warstwą elektroniczną (tj. po 4 marca 2019 r.) stworzono możliwość jego czasowego zawieszenia. Dotyczy to np. sytuacji, gdy dokument zaginął, ale istnieje duże prawdopodobieństwo, że się odnajdzie. Zawieszenie dowodu nie może trwać dłużej niż 14 dni kalendarzowych. Po upływie tego czasu nieodnaleziony dokument zostanie automatycznie unieważniony, co wiąże się z koniecznością wyrobienia kolejnego dowodu. Na portalu gov.pl można zawiesić zarówno swój e-dowód[89], jak i dziecka lub innej osoby posiadającej prawo do posiadania dowodu osobistego, ale pozostającej pod naszą opieka prawną[90].

Utrata dowodu osobistego to nie jedyne możliwe zagrożenie związane z tym dokumentem. Zawsze należy być świadomym, że codziennie mają miejsce wycieki danych wrażliwych. Dobrą praktyką, która pozwala zabezpieczyć się przed ich ewentualnymi skutkami, może być wykupienie alertów w serwisach typu chronpesel.pl lub w Biurze Informacji Kredytowej (BIK). Tego typu serwisy posiadają płatne usługi umożliwiające ostrzeganie osób w przypadku, gdy inny podmiot sprawdza dane dotyczące naszej zdolności kredytowej.

Więcej o BIKu, oferowanych przez niego alertach, metodach kradzieży danych osobowych i zbiorze dobrych praktyk związanych z użytkowaniem dowodu osobistego można dowiedzieć się, słuchając Damiana Rybaka w podcaście *Alerty BIK, czyli czy warto inwestować w zwiększające bezpieczeństwo finansowe* zrealizowanym w Kole Naukowym White Hats w ramach projektu „Cyberakcja – bezpieczna bankowa aplikacja"[91].

88 https://www.gov.pl/web/gov/zglos-utrate-lub-uszkodzenie-swojego-dowodu-osobistego-uniewaznij-dowod

89 https://www.gov.pl/web/gov/zglos-zawieszenie-lub-cofnij-zawieszenie-swojego-e-dowodu

90 https://www.gov.pl/web/gov/zglos-lub-cofnij-zawieszenie-e-dowodu-osobistego-dziecka-lub-innej-osoby

91 https://whitehats.pwr.edu.pl/cyberakcja/

5. Aplikacje przeznaczone do używania i zarządzania tożsamością cyfrową

W Polsce jednym z najpowszechniejszych środków identyfikacji elektronicznej jest obecnie e-dowód. Posiadanie jego najnowszej wersji (z warstwą elektroniczną) jest źródłem wielu udogodnień wynikających z formy zapisu danych dotyczących tożsamości posiadacza dokumentu i związanych z tym możliwości korzystania z cyfrowej tożsamości. Oparcie środka identyfikacji elektronicznej na obowiązkowym dowodzie osobistym gwarantuje szybką popularyzację i dostępność tego sposobu potwierdzania tożsamości.

Naturalnym posunięciem było opracowanie metod mających na celu uproszczenie korzystania z cyfrowej tożsamości. Wynikiem tego było stworzenie przez MSWiA, COI, NASK i PWPW aplikacji na smartfony i komputery osobiste, które umożliwiają sprawne nawiązywanie komunikacji za pomocą NFC i interakcję z elektroniczną warstwą dowodów osobistych.

W początkowej fazie dostępne były jedynie aplikacje przeznaczone na komputer, które do komunikacji wymagały zakupienia odpowiedniego czytnika do kart bezstykowych. Nieco później pojawiły się wspomniane wyżej aplikacje przeznaczone na smartfony.

5.1. Potwierdzanie tożsamości i danych osobowych

Najpopularniejsze w Polsce aplikacje przeznaczone do zarządzania cyfrową tożsamością oraz składania i weryfikowania podpisów elektronicznych są dostępne na różne platformy. Jedne z nich działają w trybie on-line, inne przeznaczone są na smartfony, a jeszcze inne umożliwiają wykorzystanie komputera stacjonarnego. Oprogramowanie przedstawione w niniejszym rozdziale umożliwia m.in.:

- weryfikowanie autentyczności warstwy elektronicznej e-dowodu;
- odczyt danych zawartych w warstwie elektronicznej e-dowodu;
- podpisywanie i weryfikowanie podpisu dokumentu;
- szyfrowanie i odszyfrowanie dokumentów;
- uwierzytelnianie do usług dostępnych w ramach Krajowego Węzła Tożsamości (zwanego Węzłem Krajowym) za pomocą e-dowodu.

Przypadki użycia oprogramowania w celu zarządzania tożsamością cyfrową oraz składania i weryfikowania podpisów elektronicznych prezentuje Wojciech Wodo w webinarze *Science Mission impossible – Cybersecurity* zrealizowanym we współpracy ze Stacją Naukową PAN w Paryżu[92].

mObywatel

Aplikacja jest nazywana cyfrowym portfelem na dokumenty i usługi e-administracji. Dostępne w niej dane pochodzą z rejestrów państwowych. Ich pobranie wymaga potwierdzenia tożsamości za pośrednictwem np. Profilu Zaufanego lub banku. Informacje o aplikacji przekazane w tym rozdziale pochodzą ze strony gov.pl[93], z regulaminu aplikacji mObywatel[94], a także są pokłosiem własnych doświadczeń i obserwacji autorów.

Wszystkie dane przechowywane w aplikacji w pamięci telefonu są zaszyfrowane. Jednym ze składników wykorzystywanych do utworzenia klucza szyfrującego jest indywidualny numer identyfikacyjny IMEI (ang. *International Mobile Equipment Identity*) [95], z tego względu aplikacja wymaga nadania dostępu do uprawnień w ramach grupy: wykonywanie połączeń telefonicznych i zarządzanie nimi. Aktywacja większości usług wymaga uwierzytelnienia w Węźle Krajowym.

W aplikacji mObywatel dostępne są usługi, m.in.:

- mObywatel (dawniej mTożsamość) – umożliwia pobranie danych osobowych użytkownika z rejestru PESEL i Rejestru Dowodów Osobistych na smartfon oraz wykorzystywanie ich do okazywania w celu potwierdzania tożsamości, przekazania danych osobowych innym użytkownikom lub podmiotom (instytucjom[96]) w celu skorzystania z oferowanych przez nie usług. Wyjątkiem są sytuacje, w których istnieje wymóg prawny okazania dowodu osobistego, np. przy przekraczaniu granicy[97] (rys. 5.1).

92 W. Wodo, *Science Mission impossible – Cybersecurity*. Dostępny w: https://www.youtube.com/watch?v=v-QG_aWWWSc

93 https://www.gov.pl/web/mobywatel

94 https://www.mobywatel.gov.pl/mobywatel.android.regulamin.12.0.0.pdf

95 Numer trwale przypisany do konkretnego telefonu, wykorzystywany w sieciach GSM do rozpoznawania poszczególnych urządzeń.

96 https://www.podatki.gov.pl/wyjasnienia/do-e-urzedu-skarbowego-zalogujesz-sie-aplikacja-mobywatel

97 https://www.gov.pl/web/mobywatel/mobywatel-dokument

Rys. 5.1. Ekrany główne usługi mObywatel i aplikacji mWeryfikator

- mPojazd – odwzorowuje dane zawarte w dowodzie rejestracyjnym, polisie OC i karcie pojazdu na podstawie danych z Centralnej Ewidencji Pojazdów (CEP).
- mPrawo jazdy – odzwierciedla tradycyjne Prawo jazdy, zawiera informacje zawarte w Centralnej Ewidencji Kierowców (CEK).
- Punkty karne – usługa jest dodawana automatycznie podczas aktywowania usługi mPrawo jazdy.
- mLegitymacja szkolna, mLegitymacja studencka – są cyfrowymi odpowiednikami tradycyjnych legitymacji, których posiadanie uprawnia do korzystania z odpowiednich ulg. Aktywowanie mLegitymacji wymaga zeskanowania kodu QR wydawanego przez daną placówkę oświaty.
- eRecepta – umożliwia realizowanie eRecept bez podawania numeru PESEL. Usługa jest częścią Internetowego Konta Pacjenta (IKP).
- Unijny Certyfikat Covid.
- inne (np. serwisy informacyjne, możliwość zakupu biletu kolejowego, Karta Dużej Rodziny[98]).

98 https://mc.bip.gov.pl/publiczna-aplikacja-mobilna/informacje-o-publicznej-aplikacji-mobilnej.html

Dzięki współpracy usługi mObywatel z aplikacją mWeryfikator możliwe jest przekazywanie dokumentów na inny smartfon w celu potwierdzenia ich autentyczności.

Każdy dokument może wzbudzić wątpliwości dotyczące jego autentyczności. Nie inaczej jest w przypadku dokumentów okazywanych w ramach aplikacji mObywatel – ich autentyczność można sprawdzać na podstawie weryfikacji[99]:

- graficznej – obejmuje weryfikację hologramu (koloru godła RP przy zmianie kąta padania światła podczas przechylania telefonu), elementów dynamicznych (falującej biało-czerwonej flagi), aktualnej daty i daty ostatniego pobrania danych;
- funkcjonalnej – polega na wykonaniu określonych czynności na urządzeniu, np. sprawdzenie wydanych certyfikatów i ich ważności;
- kryptograficznej – wymaga przekazania do aplikacji mWeryfikator danych wraz z umieszczonym pod nimi podpisem przez zeskanowanie kodu QR, generowanego przez aplikację w ramach usługi mObywatel i zawierającego klucze szyfrujące transmisję.

Rozpoczęcie korzystania z aplikacji staje się możliwe po ustaleniu hasła dostępu. Jeżeli urządzenie posiada czytnik linii papilarnych, możliwe jest ustawienie dostępu do aplikacji po podaniu odcisku palca i kodu PIN. W przypadku zapomnienia hasła lub kodu PIN konieczne staje się ponowne odinstalowanie i zainstalowanie aplikacji, a w związku z tym pobranie danych zawartych w rejestrach państwowych. Zgubienie lub kradzież telefonu są sytuacjami, w których po zgłoszenia zdarzenia pobrane na urządzenie certyfikaty są unieważniane.

Usługi w ramach aplikacji mObywatel są udostępniane off- i online. Offline otrzymuje się dostęp do dokumentów, o których informacje są pobierane z rejestrów państwowych, a następnie przechowywane w zaszyfrowanej formie w telefonie. Dostęp do internetu jest wymagany tylko na czas pobierania danych oraz w celu odświeżenia pobranych wcześniej danych, które wiąże się z ponownym uwierzytelnieniem użytkownika w ramach Węzła Krajowego.

Usługami offline są m.in.: mObywatel, mPrawo jazdy, mLegitymacja studencka, Unijny Certyfikat Covid. Z kolei usługi online zwykle związane są z dynamicznie zmieniającymi się danymi i do poprawnej pracy wymagają dostępu do internetu. Do usług online zaliczane są m.in.: Punkty karne, eRecepta, Polak za granicą.

99 https://www.gov.pl/web/mobywatel/zabezpieczenia1

Podsumowując: aplikacja mObywatel jest rozwiązaniem nowoczesnym i wygodnym ze względu na faktyczną dostępność i użyteczność zebranych w niej usług. Za pewną niedogodność można uznać fakt, że w systemie Android zablokowana jest możliwość wykonywania zrzutów ekranu, funkcja ta jest jednak dostępna w systemie iOS. Największy problem związany z aplikacją mObywatel stanowi brak szkoleń z zakresu weryfikacji autentyczności dokumentu w wersji elektronicznej. Problem jest na tyle poważny, że w niektórych przypadkach dotyczy on również weryfikacji dokumentów przez komisje wyborcze. Najbardziej skuteczną metodą weryfikowania autentyczności dokumentów obecnych w mObywatel jest skorzystanie z aplikacji mWeryfikator.

mWeryfikator

Aplikacja umożliwia opartą na kryptografii weryfikację online danych osobowych zawartych w dokumentach dostępnych w ramach usług narzędzia mObywatel. Weryfikacja odbywa się w aplikacji mWeryfikator, po przesłaniu danych z aplikacji mObywatel. Dane są jedynie wyświetlane na ekranie smartfona, nie są one w żaden sposób zapisywane. Operację inicjuje użytkownik aplikacji mObywatel, klikając „Przekaż". Następnie należy wskazać, że dane zostaną przekazane osobie weryfikującej tożsamość. Po tym etapie zostanie wygenerowany kod QR, który jest skanowany przez użytkownika aplikacji mWeryfikator. Ostatnim krokiem jest wyrażenie zgody przez użytkownika aplikacji mObywatel na dokonanie jednostronnego przekazania danych. Na urządzenia z systemem Android dane przesyłane są za pomocą łączności Bluetooth, zaś na urządzenia z systemem iOS może to być zarówno Bluetooth, jak i WiFi. Transmisja odbywa się w sposób bezpieczny i uniemożliwiający modyfikację danych osobowych. Po zakończonym przesyłaniu danych w aplikacji mWeryfikator wyświetlane jest zdjęcie, imię i nazwisko osoby, której dane zostały przesłane (rys. 5.1).

Wykorzystanie narzędzia mWeryfikator jest metodą zapewniającą największą skuteczność weryfikacji autentyczności dokumentów, do których ma się dostęp w aplikacji mObywatel. Ze względu na pewne ograniczenia techniczne (głównie różnice w specyfikacji Bluetootha) nie jest możliwa wymiana danych między aplikacjami zainstalowanymi na innych rodzinach systemów operacyjnych (Android i iOS) z wykorzystaniem WiFi czy Bluetootha. Z tego powodu od pewnej wersji aplikacji twórcy przewidzieli mechanizm wymiany między urządzeniami serii kodów QR zawierających odpowiednie dane.

Trudno wskazywać ograniczenia techniczne jako powód problemu w przypadku otwartego standardu, jakim jest Bluetooth. Bardziej prawdopodobne wydają się nieuczciwe praktyki monopolistyczne jednego z producentów. W niektórych przypadkach te ograniczenia mogą utrudnić bądź uniemożliwić posłużenie się aplikacją mWeryfikator w celu, w jakim została stworzona.

Informacje dotyczące aplikacji mWeryfikator pochodzą ze strony www.gov.pl, regulaminu aplikacji mWeryfikator[100], a także są efektem własnych doświadczeń i obserwacji autorów.

eDO App

Aplikacja umożliwia uzyskanie dostępu do warstwy elektronicznej dowodu osobistego za pomocą smartfonu z modułem NFC. W innych przypadkach warunkiem komunikacji jest posiadanie specjalnego czytnika kart bezstykowych. Ta rozwijana przez PWPW aplikacja jest dostępna na platformie Android, iOS i Huawei. Na telefonie nie przechowuje danych osobowych zawartych w e-dowodzie, pozwala jedynie na ich odczyt oraz użycie obecnych w nim certyfikatów.

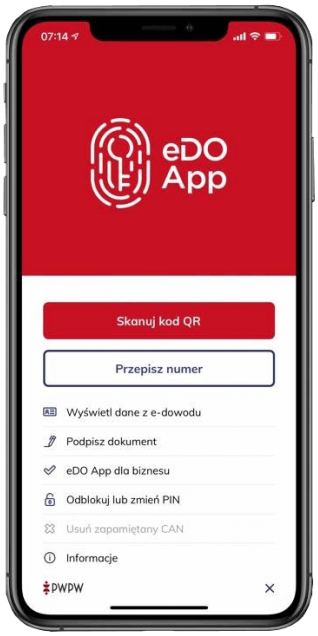
Aplikacja eDO App pozwala na (rys. 5.2):

- bezpieczne potwierdzanie tożsamości;
- złożenie podpisu osobistego lub kwalifikowanego[101];
- dostęp do warstwy elektronicznej dowodu osobistego:
  - wyświetlenie danych z e-dowodu lub paszportu,
  - podpisanie dokumentu,
  - zmianę i odblokowanie kodu PIN e-dowodu;
- kontakt z urzędami administracji publicznej:
  - założenie i potwierdzenie Profilu Zaufanego,
  - uwierzytelnienie w ramach Węzła Krajowego (login.gov.pl);
- automatyczną weryfikację autentyczności i ważności dokumentu, wykorzystującą odpowiedni certyfikat i usługę OCSP wystawcy certyfikatu.

Przygotowana przez PWPW aplikacja jest bardzo przydatna przy logowaniu się do e-usług za pomocą e-dowodu. Ponieważ w znacznym stopniu upraszcza korzystanie z dokumentu tożsamości w najnowszej wersji, zwiększa jego popularność jako środka identyfikacji. Wykorzystanie smartfona z NFC eliminuje

100 https://www.mobywatel.gov.pl/mweryfikator.regulamin.7.0.0.pdf

101 Jeśli został wcześniej zakupiony i załadowany do warstwy elektronicznej.



Rys. 5.2. Ekran główny aplikacji eDO App

konieczność zakupu specjalnego czytnika kart bezstykowych przy korzystaniu z aplikacji przeznaczonych na komputer.

Integrację aplikacji z rozwiązaniami dostarczanymi przez inne firmy umożliwia PWPW. Dla klienta skorzystanie z takiej integracji ogranicza się do zeskanowania kodu QR lub przepisania kodu operacji partnera. Obecnie (stan na marzec 2023 r.) PWPW poinformowała na swojej stronie[102] o integracji z kilkoma instytucjami, m.in. z:

- PKO BP – w celu zakupu obligacji skarbowych z wykorzystaniem potwierdzenia tożsamości za pomocą aplikacji eDO App;
- mBank – w celu zdalnego potwierdzenia tożsamości podczas zakładania konta;
- SIGNIUS – w celu zdalnego podpisania dokumentu;
- Authlogic – firmą rozwijającą API służące do weryfikacji tożsamości za pomocą różnych metod;
- PGNiG – w celu zdalnego podpisania umowy;
- IC Solutions – firmą tworzącą IC Pen, tj. system digitalizacji dokumentów.

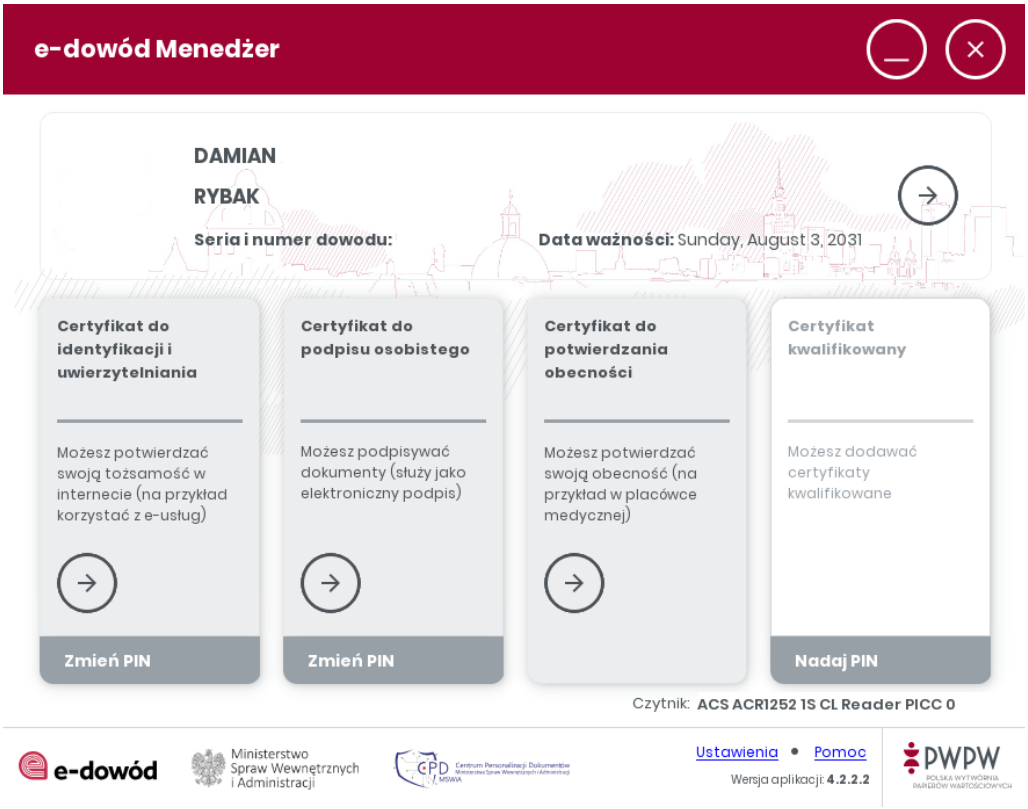
102 https://www.pwpw.pl/aktualnosci,1.html

Korzystanie z eDO App eliminuje potrzebę zakupu specjalnego czytnika zbliżeniowego. Niekiedy może być przydatna funkcja umożliwiająca podpisanie pliku pdf. Aplikacja nie posiada jednak funkcji pozwalającej na weryfikowanie dokumentu opatrzonego podpisem elektronicznym.

Informacje dotyczące aplikacji eDO App pochodzą ze strony pwpw.pl, jej regulaminu [103], a także są efektem doświadczeń i obserwacji autora.

e-dowód Menedżer

Jednym z komponentów oprogramowania e-dowód jest aplikacja e-dowód Menedżer, w skład której wchodzą następujące narzędzia:



Rys. 5.3. Ekran główny aplikacji e-dowód Menedżer

103 https://edoapp.pl/regulamin

- e-dowód Monitor – wykorzystywany do wykrycia, czy e-dowód znajduje się w czytniku, a następnie do utrzymania bezpiecznego połączenia z kartą;
- e-dowód Podaj CAN – umożliwia podanie numer CAN i nawiązanie bezpiecznego połączenia z warstwą elektroniczną e-dowodu.

Aplikacja ta umożliwia odczyt danych zawartych w elektronicznej warstwie e-dowodu i wykonanie podstawowych operacji na tych danych (rys. 5.3), tj. zmianę kodu PIN czy sprawdzenie szczegółów poszczególnych certyfikatów. Dodatkową funkcją jest integracja e-dowodu z przeglądarkami, a w konsekwencji umożliwienie logowania do usług dostępnych w ramach Węzła Krajowego, np. do platformy ePUAP.

ReadID

Aplikacja ReadID (rys. 5.4) jest jednym z bardziej popularnych rozwiązań przeznaczonych do zarządzania cyfrową tożsamością. Pierwotnie była wykorzystywana do nawiązania połączenia z warstwą elektroniczną w nowych paszportach, ponieważ dokumenty podróżne muszą odpowiadać normie ICAO Doc 9303 (eMRTD). Nowe dowody osobiste również muszą spełniać wymogi tej normy, dlatego aplikacja umożliwia odczyt tylko danych zapisanych na określonym poziomie dostępu.

Rys. 5.4. Przykładowe dane odczytane za pomocą aplikacji ReadID

W skład aplikacji ReadID wchodzą:

- ReadID Me – umożliwia odczyt danych zawartych w warstwie regulowanej normą ICAO po odczycie danych zawartych w strefie MRZ. Jeżeli odczyt danych ze strefy MRZ z wykorzystaniem techniki optycznego odczytu znaków (ang. *optical character recognition* – OCR) nie jest możliwy, rozwiązaniem jest nawiązanie połączenia z warstwą elektroniczną po podaniu numeru CAN lub numeru dokumentu i terminu jego ważności oraz daty urodzenia posiadacza.
- ReadID Ready – pozwala na integrację z rozwiązaniami dostarczanymi przez innych dostawców oraz weryfikowanie przez inne podmioty tożsamości na podstawie danych zawartych w warstwie regulowanej normą ICAO.

5.2. Podpis elektroniczny – formaty i weryfikacja

Uwzględniając aktualne statystyki dotyczące wydanych certyfikatów kwalifikowanych podpisów elektronicznych[104] (ponad 550 tys. w 2020 r.[105]), aktywnych profili zaufanych (ponad 15 mln w 2022 r.[106]) oraz spersonalizowanych nowych e-dowodów (ponad 10 mln do 2023 r.[107]) można powiedzieć, że na przestrzeni ostatnich kilku lat rynek podpisów cyfrowych w Polsce rozwinął się – coraz częściej tego rodzaju podpisem są potwierdzane umowy i podpisywane dokumenty.

Przeglądu ekosystemu podpisów elektronicznych w Polsce dokonał w styczniu 2023 r. Margus Pala w artykule *Qualified Electronic Signature Ecosystem in Poland*[108]. Uzupełnieniem niniejszego podrozdziału jest również zaktualizowany w 2021 r. przewodnik *Podpis elektroniczny w procesie inwestycyjno-budowlanym*[109].

104 https://esign.pl/aktualnosci/e-podpis-w-2022-roku-ktore-firmy-beda-musialy-w-niego-zainwestowac/

105 https://www.money.pl/gospodarka/podpis-elektroniczny-ma-juz-20-lat-a-ty-masz-juz-swoj-6359279182264449a.html

106 https://www.gov.pl/web/cyfryzacja/15-milionow-profili-zaufanych

107 https://www.gov.pl/web/cyfryzacja/10-milionow-dowodow-osobistych-z-warstwa-elektroniczna

108 M. Pala, *Qualified Electronic Signature Ecosystem in Poland*. Dostępny w: https://eideasy.com/qualified-electronic-signature-ecosystem-in-poland/

109 *Podpis elektroniczny w procesie inwestycyjno-budowlanym. Przewodnik dla organów administracji architektoniczno-budowlanej*. Dostępny w: https://www.gunb.gov.pl/sites/default/files/attachment/podpis_elektroniczny_-_przewodnik_dla_organow_aab_0.pdf

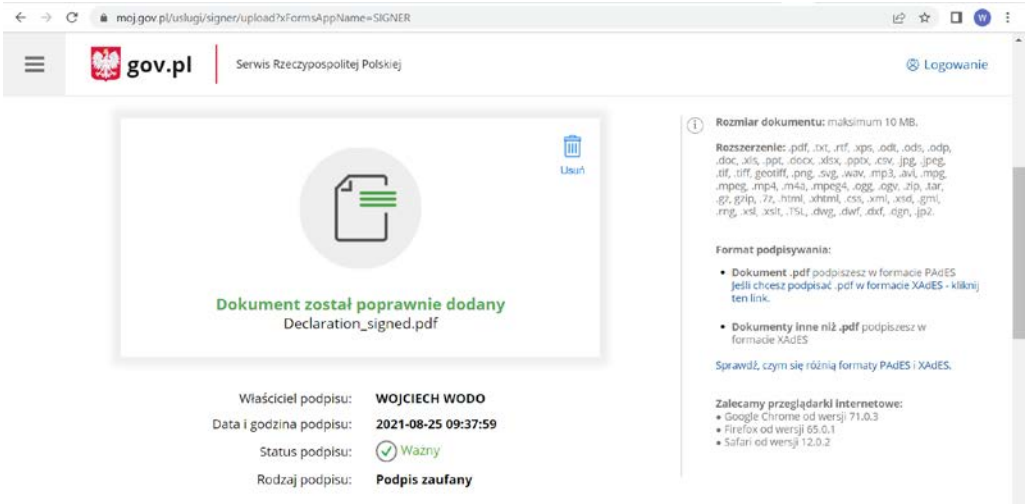
e-PUAP oraz podpis zaufany i jego weryfikacja

Ta bezpłatna platforma online służy do kontaktu z różnymi urzędami: za jej pośrednictwem można wysyłać wnioski lub pisma oraz odbierać pisma z urzędów.

Profil zaufany jest bezpośrednio powiązany z Elektroniczną Platformą Usług Administracji Publicznej (ePUAP) i z jednej strony umożliwia do niej dostęp (usługa uwierzytelniania), z drugiej można go wykorzystać do podpisywania dowolnego dokumentu elektronicznego podpisem zaufanym, będącym integralną częścią profilu zaufanego.

Podpis zaufany jest podpisem elektronicznym, którego autentyczność i integralność zapewnia pieczęć elektroniczna ministra do spraw cyfryzacji. Zawiera m.in. dane identyfikujące osobę, w której imieniu wystawiany jest podpis, tj. numer PESEL, identyfikator środka identyfikacji elektronicznej, który posłużył do jego złożenia, oraz czas jego złożenia. Dlatego w ciele podpisu w polu Powód znajduje się informacja: „Opatrzono pieczęcią ministra właściwego do spraw informatyzacji w imieniu: FIRSTNAME LASTNAME, PESEL: 1234567890, PZ ID: USERNAME". Usługa podpisu zaufanego wykorzystuje zaawansowaną pieczęć elektroniczną, używając kwalifikowanego certyfikatu wydanego przez Eurocert.

Każda osoba posiadająca profil zaufany może składać zaufany podpis elektroniczny, równoważny w skutkach podpisowi własnoręcznemu tylko w kontak-



Rys. 5.5. Weryfikacja online podpisu elektronicznego w formacie PAdES w serwisie rządowym

tach z administracją publiczną w Polsce lub jeśli obie strony umowy wyrażają zgodę na taką formę. Aby podpisać dokument profilem zaufanym lub zweryfikować już złożony podpis, należy skorzystać z serwisu rządowego[110].

Podpis zaufany ma format XAdES lub PAdES, typ otoczony, co oznacza podpis zawarty w kontenerze dokumentu głównego XML lub osadzony w dokumencie PDF. Wynik weryfikacji dokumentu PDF z podpisem w formacie PAdES przedstawia rys. 5.5.

e-dowód Podpis elektroniczny

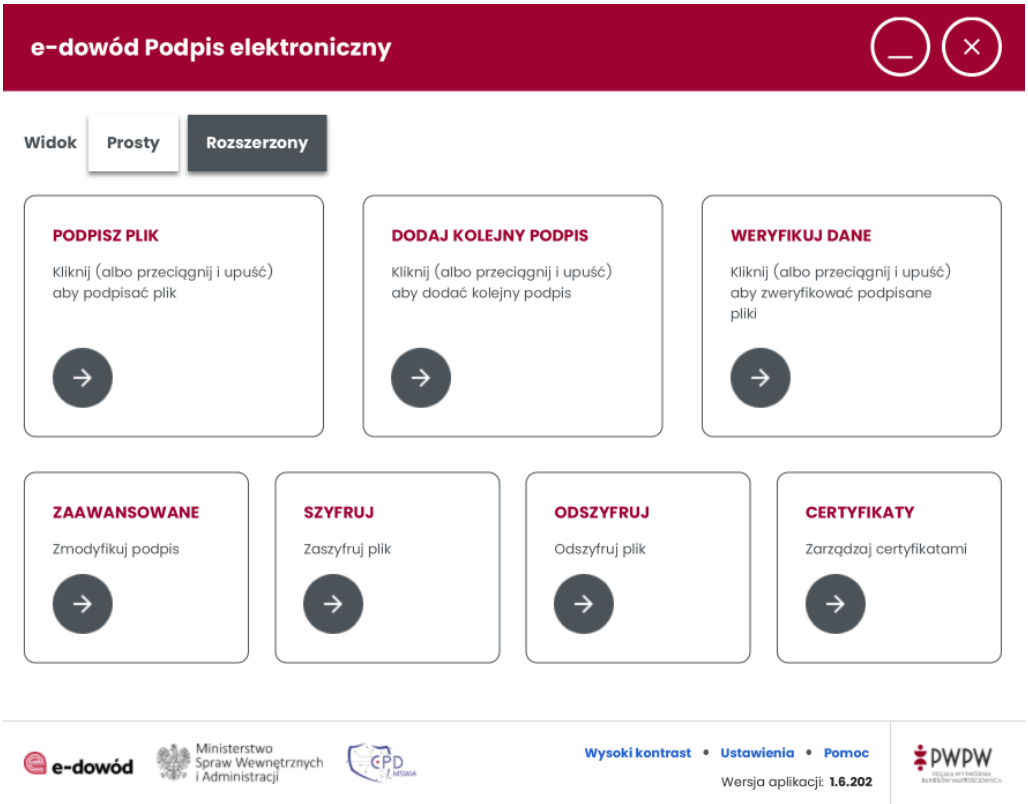
Aplikacja komputerowa służy do składania podpisu elektronicznego na dowolnym pliku (tekstowym, binarnym, multimedialnym, XML) i jego weryfikacji (rys. 5.6). Narzędzie obsługuje certyfikaty kwalifikowane i niekwalifikowane, wydawane przez: PWPW, Certum by Asseco, Enigma, Eurocert i Krajową Izbę Rozliczeniową. Dodatkowo do skorzystania z niej wymagane jest posiadanie czytnika do kart bezstykowych.

Podczas wykonywania podpisu elektronicznego możliwe jest wybranie predefiniowanych profili (e-Puap, e-Deklaracje, Gov.pl). Istnieje również możliwość wybrania własnych ustawień dotyczących formatu, wariantu, funkcji skrótu i typu zobowiązania podpisu. Aplikacja posiada rozbudowane opcje pozwalające ustawić znacznik PDF (symbol graficzny naniesiony na podpisany dokument), serwer czasu i domyślne ustawienia dotyczące składania podpisów. Narzędzie wykorzystuje domyślnie najsłabszą dostępną funkcję skrótu (SHA-256) do składania podpisu, podczas gdy dostępne są znacznie bezpieczniejsze rozwiązania (SHA-512). Dobrą praktyką jest domyślne ustawianie najbardziej bezpiecznych opcji, ponieważ przeciętny użytkownik najprawdopodobniej nigdy nie będzie ich modyfikował. Na domyślnym źródle czasu powinien zostać ustawiony nie czas lokalny, ale czas pobierany z serwera NTP, np. z domyślnie wskazanego w aplikacji adresu serwera NTP[111] utrzymywanego przez Główny Urząd Miar.

Z aplikacją e-dowód Podpis elektroniczny udostępniane jest oprogramowanie eDOSignCli.exe. Narzędzie pracuje w trybie wiersza poleceń (ang. *command line interface* – CLI), oferując możliwości podobne do tych, jakie ma jego graficzny odpowiednik.

110 https://moj.gov.pl/uslugi/signer/upload?xFormsAppName=SIGNER

111 https://www.gum.gov.pl/pl/uslugi/zegar/524,Zegar.html



Rys. 5.3. Ekran główny aplikacji e-dowód Menedżer

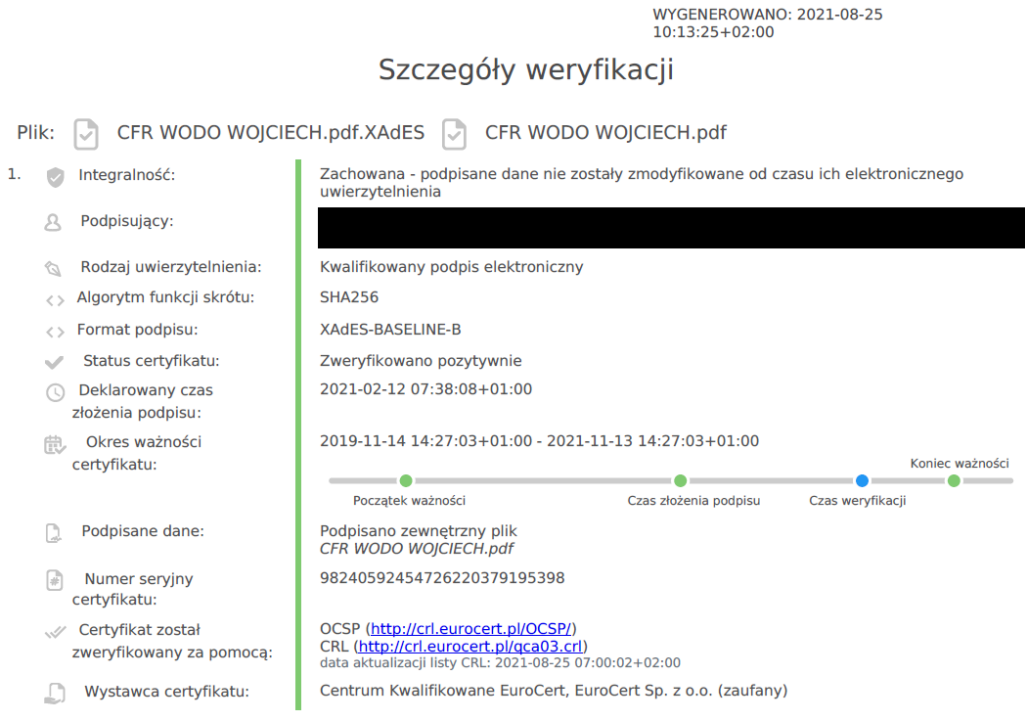
Madkom SA

Firma jest dostawcą niekwalifikowanych usług zaufania, wpisanym do Rejestru Dostawców Usług Zaufania prowadzonego przez Narodowy Bank Polski[112]. Zasady świadczenia usługi są regulowane przez *Politykę świadczenia usługi* Madkom S.A.[113]

System Automatycznej Weryfikacji Podpisu Elektronicznego (SAWPE) dostępny jest pod adresami https://weryfikacjapodpisu.pl i https://verifysignature.eu/. Można go wykorzystać do weryfikacji podpisów złożonych w formacie XAdES, PAdES oraz dokumentów podpisanych za pomocą podpisu zaufanego i podpisu osobistego. System umożliwia wygenerowanie i zapisanie Elektro-

112 https://www.nccert.pl/uslugiNK.htm

113 *Polityka świadczenia usługi* Madkom S.A. Dostępne w: https://weryfikacjapodpisu.pl/policy



Rys. 5.7. Szczegóły weryfikacji online podpisu elektronicznego w formacie XAdES na platformie firmy Madkom

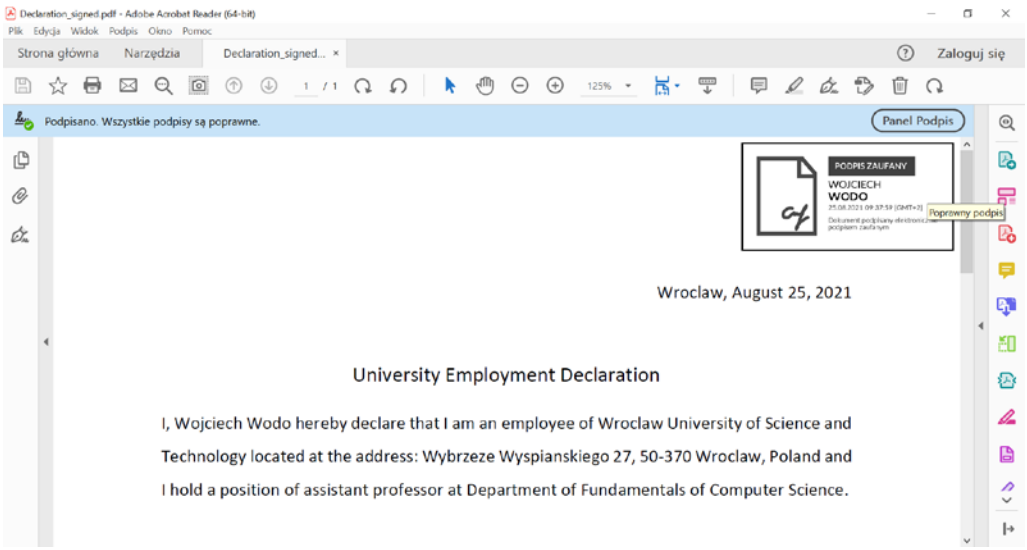
nicznego Poświadczenia Weryfikacji (EPW). System do weryfikacji podpisu elektronicznego jest zgodny z rozporządzeniem eIDAS. Aplikacja wykorzystuje m.in. unijny system list zaufania (TSL) i dlatego pozwala na skuteczną weryfikację podpisów z całej Unii Europejskiej.

Wynik weryfikacji dokumentu PDF z zewnętrznym podpisem w formacie XAdES przedstawia rys. 5.7.

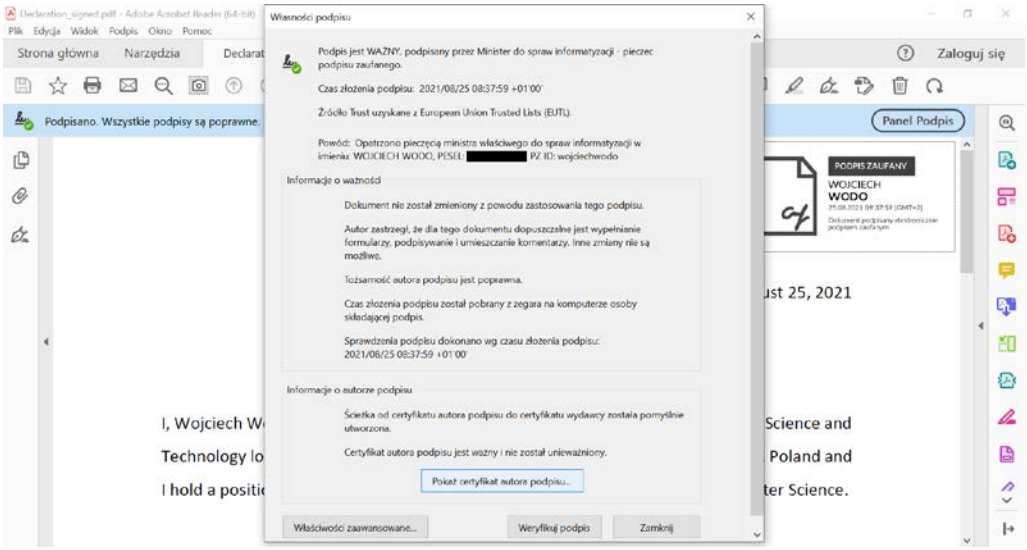
Adobe Acrobat Reader

Bezpłatna przeglądarka plików PDF jest wyposażona w moduł związany z podpisami i pieczęciami elektronicznymi. Dzięki zaimplementowanym mechanizmom automatycznej weryfikacji podpisów i obsługi certyfikatów podpisów elektronicznych możliwe jest zarówno podpisywanie dokumentów, jak i weryfikacja oraz przeglądanie właściwości podpisów już złożonych.

Na dokumencie z osadzonym podpisem w formacie PadES, wykonanym za pomocą podpisu zaufanego (rys. 5.8) widoczny jest wynik automatycznej we-

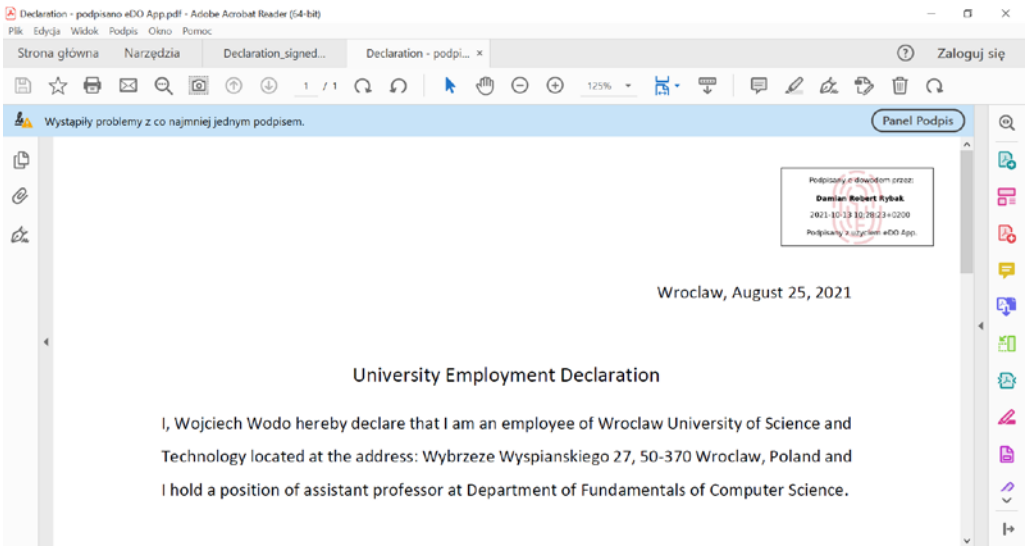


Rys. 5.8. Dokument PDF wraz z osadzonym podpisem zaufanym – widok w programie Acrobat Reader

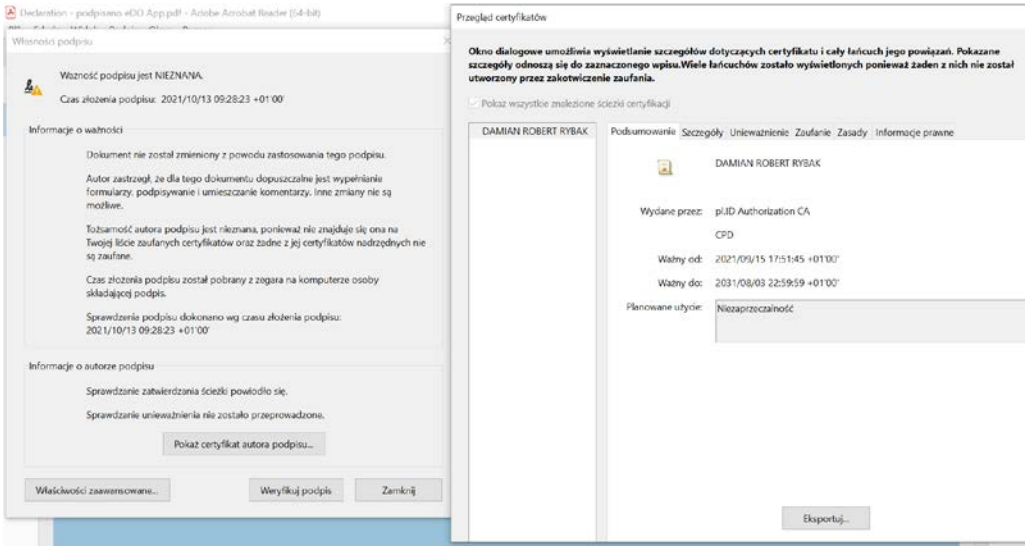


Rys. 5.9. Właściwości podpisu zaufanego osadzonego w dokumencie PDF – widok w programie Acrobat Reader

ryfikacji podpisu wraz z informacją i możliwością przejścia do panelu podpisu. Po wejściu w detale podpisu widać dodatkowe informacje odczytane z samego podpisu – o jego wystawcy i czasie wystawienia – wraz z możliwością odczytu danych z certyfikatu (rys. 5.9).



Rys. 5.10. Dokument PDF wraz z osadzonym podpisem osobistym – widok w programie Acrobat Reader



Rys. 5.11. Właściwości osadzonego w dokumencie PDF podpisu osobistego i jego certyfikatu – widok w programie Acrobat Reader

Podpis zaufany, ponieważ jest realizowany w formie kwalifikowanej pieczęci elektronicznej, a certyfikat użyty do jej wytworzenia pochodzi od kwalifikowanego dostawcy usług zaufania (Eurocert), znajduje się na europejskiej liście zaufania (EUTL).

Na rysunku 5.10 przedstawiono podgląd dokumentu podpisanego również z wykorzystaniem formatu podpisu PadES, ale pochodzącego z e-dowodu. Automatyczna weryfikacja wykazuje jednak (rys. 5.11), że certyfikat wystawcy podpisu (pl.ID) nie znajduje się na zaufanej liście podmiotów. Weryfikacja ścieżki certyfikatu wydanego przez takiego wystawcę na podstawie bazy danych certyfikatów kwalifikowanych jest zatem niemożliwa. Aby móc przeprowadzić weryfikację tego wystawcy, należy poszerzyć bazę danych wystawców zaufanych certyfikatów w systemie operacyjnym (certyfikat pl.ID Root CA) lub dodać ten konkretny certyfikat (pl.ID Authorization CA) do bazy zaufanych certyfikatów. Politykę certyfikacji tego wystawcy określa dokument znajdujący się na stronie rządowej[114] i w tym wypadku może on stanowić źródło zaufania. Należy jednak zaznaczyć, że nie jest to standardowa procedura operacji weryfikacji certyfikowanego podpisu elektronicznego.

114 https://www.gov.pl/web/mswia/polityka-certyfikacji

6. Wykorzystanie cyfrowej tożsamości w gospodarce

Szacuje się, że pod koniec 2022 r. nowe dowody tożsamości będzie miało już około 10 mln obywateli, przy czym PIN aktywowało ok. 30–40 proc. Z bieżących statystyk dostępnych na stronie Centrum Personalizacji Dokumentów[115] wynika, że proces przechodzenia na nowe dowody z warstwą elektroniczną przebiega sprawnie i wkrótce większość uprawnionych do tego Polaków będzie dysponować tym źródłem tożsamości.

Za sprawą zwiększonej powszechności rozwiązań z zakresu tożsamości cyfrowej sektor finansowy zaczął wprowadzać w obszarze swoich działań zmiany pozwalające na zastosowanie takich środków identyfikacji. Skutkiem jest uproszczenie i przyspieszenie wielu procedur, a więc oszczędność czasu przy jednoczesnym zachowaniu bezpieczeństwa.

Zdalne potwierdzanie tożsamości jest w sektorze finansowym jednym z kluczowych procesów. Tak zwany *remote ID proofing*[116] jest możliwy do przeprowadzenia w zautomatyzowany sposób za pomocą nowego e-dowodu dzięki rozwiązaniu oferowanemu przez firmę Identt [117] czy dzięki aplikacji eDO App dla biznesu[118] stworzonej przez PWPW. Rozwiązanie to – zgodnie z politykami bezpieczeństwa regulacji AML (ang. *Anti Money Laundering*) – spełnia wymagania związane z procedurą eKYC (ang. *Electronic Know Your Customer*) nałożoną na podmioty finansowe w związku z przeciwdziałaniem praniu brudnych pieniędzy i finansowania terroryzmu.

W Polsce możliwość zdalnego otwierania konta właśnie z wykorzystaniem e-dowodu[119] (na podstawie eID firmy Identt) uruchomił jako pierwszy w Polsce Bank Pekao. Otrzymał za to nawet nagrodę Cashless Fintech 2021 w kategorii Projekt Fintech.

115 https://www.cpd.gov.pl/o-nas/statystyki/

116 https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing

117 https://e-id.pl/

118 https://www.edoapp.pl/biznes

119 https://www.cashless.pl/9814-pekao-konto-na-selfie-edowod

Potwierdzanie danych osobowych za pomocą jednorazowego środka identyfikacji jest kolejnym przykładem zastosowania ekosystemu tożsamości cyfrowej. Rozwiązanie takie oferuje usługa mojeID[120] Krajowej Izby Rozliczeniowej zrzeszającej dostawców tożsamości (głównie z sektora finansowego) oraz dostawców usług, którzy akceptują ten sposób potwierdzania danych swoich klientów za ich zgodą. To rozwiązanie znacząco przyspiesza proces zakładania konta klienta i zawieranie umowy świadczenia usług, np. dostawy gazu (np. PGNiG) czy rejestracji w placówce prywatnej opieki medycznej (np. Medicover).

Korzystając z cyfrowej tożsamości (Profilu Zaufanego) można – za pośrednictwem portalu Platforma Usług Elektronicznych (PUE) ZUS – wysłać dokumenty i wnioski do ZUS-u. Microsoft Teams umożliwia potwierdzenie tożsamości i podpisanie dokumentu e-dowodem[121] lub na platformie firmy Autenti[122], na której można w zaawansowany sposób zarządzać obiegiem dokumentów w biznesie. Autenti[123] udostępnia m.in. funkcjonalność podpisywania i weryfikowania dokumentów z wykorzystaniem różnego rodzaju podpisów elektronicznych. Dodatkowo usługa Broker ID i zintegrowane w niej rozwiązania umożliwiają dokonywanie zdalnej weryfikacji tożsamości swoich klientów.

Dzięki złagodzeniu rygorów KNF dotyczących weryfikacji tożsamości klientów zawierających umowy ubezpieczeń na życie[124] firmy ubezpieczeniowe mogą skorzystać ze zdalnej weryfikacji tożsamości, np. z mojeID mogą korzystać klienci Nationale-Nederlanden, Open Life i PZU, a także majątkowej spółki PKO Ubezpieczenia, zaś duża sieć multiagencyjna OVB wyposażyła swoich agentów w narzędzie dające im możliwość bezpiecznej weryfikacji klienta, przygotowane przez wrocławski fintech Identt[125].

Przedstawione w tym rozdziale zastosowania cyfrowej tożsamości, nowych dowodów i innych usług zaufania są tylko fragmentem większej całości – wierz-

120 https://www.mojeid.pl/

121 https://www.pwpw.pl/Aktualnosci/2021/12/w-microsoft-teams-potwierdzisz-tozsamosc-i-podpiszesz-dokument-e-dowodem.html

122 https://www.money.pl/gospodarka/autenti-laczy-sily-z-microsoft-teams-6781831030094752a.html

123 https://autenti.com/pl/

124 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_metode_wideoweryfikacji_66066.pdf

125 https://www.cashless.pl/8800-weryfikacja-tozsamosci-zyciowka

chołkiem góry lodowej. Nie było intencją autorów dokonywanie pełnego jej przeglądu. Przytoczone przykłady maja uświadomić, jak szerokie jest spektrum możliwości stosowania elektronicznej tożsamości, z którego mogą czerpać na równi obie strony: i biznes, i jego klienci. W tym kontekście nie powinna dziwić więc decyzja wielu przedsiębiorstw o integracji rozwiązań opartych na cyfrowej tożsamości ze swoimi produktami i usługami. Jest to zdecydowanie potwierdzenie kierunku rozwoju tego obszaru gospodarki i uwiarygodnienie samych rozwiązań jako takich.

7. Zakończenie

Tożsamość cyfrowa jest problemem złożonym, a wpływ na nią ma wiele różnych czynników. Z tego względu w pracy przedstawiono ją jako dziedzinę wymagającą podejścia interdyscyplinarnego, ponieważ jako jedyne pozwala na harmonizację wiedzy i zrozumienie mechanizmów jej działania.

Obowiązujące akty prawne mające największy wpływ na funkcjonowanie i kształt tożsamości cyfrowej w Polsce były czynnikiem, który zdecydował o podstawowym zakresie tematycznym niniejszego opracowania. Przywołane regulacje w dużej mierze mają na celu zwiększenie dostępu do usług online, zainicjowanie współpracy między sektorem publicznym i prywatnym, jak i współpracy między poszczególnymi krajami członkowskimi Unii Europejskiej. Określają ramy świadczonych usług i relacje między uczestnikami obrotu, uzupełniają i harmonizują przepisy, wypełniając luki w obszarach, które mocno rozwinęły się w ostatnim czasie. Niektóre regulacje poprawiają również kwestie związane z zapewnieniem odpowiedniej wiarygodności i bezpieczeństwa środków umożliwiających identyfikację elektroniczną. Zaletą większości aktów prawnych jest fakt, że zostały one opracowane w oparciu o wieloletnie doświadczenia i sprawdzone standardy z wielu różnych dziedzin.

Rozwój ekosystemu tożsamości cyfrowej jest uzależniony od danego kraju. Różnice są związane z wieloma czynnikami, a jednym z podstawowych jest przyjęty schemat rynku w zakresie identyfikacji elektronicznej. W Polsce rozwój tożsamości cyfrowej jest oparty na schemacie federacyjnym, który umożliwia wzajemną współpracę podmiotów publicznych i prywatnych. Model federacyjny jest najbardziej popularny w Europie – schemat ten w większości krajów ułatwia popularyzację systemu wśród obywateli. Kolejnym czynnikiem, od którego jest uzależniony rozwój eID, są obowiązujące akty prawne regulujące tradycyjną tożsamość. W przypadku Polski za naturalne należałoby uznać wykorzystanie obowiązkowego dowodu osobistego i opracowanie na jego podstawie jednego z najbardziej popularnych środków identyfikacji elektronicznej w kraju.

Duże znaczenie w kontekście całego ekosystemu eID w Polsce ma ustawa o usługach zaufania oraz identyfikacji elektronicznej. Na mocy tego aktu praw-

nego określono krajowy schemat identyfikacji elektronicznej i krajową infrastrukturę zaufania.

Krajowy schemat identyfikacji elektronicznej wprowadził znaczne uproszczenie w postaci Węzła Krajowego. Rozwiązanie to wprawdzie znacząco ułatwia integrację z innymi systemami, nie jest jednak jeszcze w pełni gotowe – nie wspiera integracji z węzłem transgranicznym. Polska do końca 2022 r. nie posiadała żadnego środka identyfikacji elektronicznej notyfikowanego przez UE. Bardzo interesującą inicjatywą jest system mojeID, określany niekiedy jako węzeł komercyjny. Jego podstawą są jednorazowe środki identyfikacji elektronicznej wydawane przez niektóre banki. Rozwiązanie jest zintegrowane z Węzłem Krajowym, ale nie posiada dużej liczby integracji z prywatnymi serwisami.

Krajowa infrastruktura zaufania jest strukturą zapewniającą funkcjonowanie PKI na potrzeby podpisu kwalifikowanego. Rolę centrum certyfikacji pełni Narodowe Centrum Certyfikacji. Poza pełnieniem standardowych czynności, do których zobligowane jest CA, NCCert prowadzi listę TSL, którą publikuje na stronie Komisji Europejskiej. Listy TSL są bardzo istotnym elementem, który pozwala na rozpoznawanie kwalifikowanych usług zaufania w Unii Europejskiej.

Dalszy rozwój ekosystemu tożsamości cyfrowej jest tylko kwestią czasu. W bliskiej perspektywie duże znaczenie będzie miało wprowadzenie regulacji eIDAS2, w ramach której znajdzie się Europejski Portfel Cyfrowej Tożsamości[126]. Rozwiązania[127], które pojawią się w przyszłości, z pewnością będą wspierały podejście globalne, interoperacyjne i oparte na zdalnym potwierdzaniu tożsamości. Coraz więcej jest informacji o potencjalnym wykorzystaniu technologii *blockchain*, na popularności zyskuje również tożsamość niezależna/suwerenna (ang. *self sovereign identity* – SSI), tj. podejście zakładające, że to właśnie użytkownik będzie dysponował własnymi atrybutami tożsamości.

Ograniczenia opracowania

Kształtowanie ekosystemu tożsamości cyfrowej w Polsce nie jest zagadnieniem w pełni otwartym, dostęp do szczegółowych informacji jest utrudniony. Specyfikacje dotyczące poszczególnych rozwiązań nie są dostępne i nie można ich po-

126 https://obserwatorium.biz/nowelizacja-eidas-wprowadza-europejski-portfel-cyfrowej-tozsamosci.html

127 https://obserwatorium.biz/top-5-trendow-w-eid-i-uslugach-zaufania-ktore-zmienia-rynek.html

zyskać w całości. Dodatkowo ekosystem eID cały czas jest w fazie rozwoju, dlatego informacje prezentowane w tej pracy mogą być niepełne lub nieaktualne, a po pewnym okresie czasu nie odzwierciedlać stanu faktycznego. Te czynniki wpływają również na ograniczoną liczbę publikacji dotyczących eID w Polsce.

Istotne elementy mające znaczący wpływ na kształtowanie się ekosystemu elektronicznych usług zaufania zaistniałe w i po 2022 r.

W obszarze tożsamości elektronicznej dokonują się zmiany o charakterze prawnym, obyczajowym, jak i technologicznym. Celem autorów było zwrócenie uwagi na kilka istotnych faktów czy koncepcji, które będą kształtowały ten obszar naszego życia w najbliższej przyszłości:

- 29 grudnia 2022 r. Prezydent Ukrainy podpisał ustawę numer 2801-IX o wzajemnym uznawaniu kwalifikowanych elektronicznych usług zaufania i implementacji przepisów UE w zakresie identyfikacji elektronicznej. Jest ona efektem porozumienia między Ukrainą a UE o wzajemnej akceptowalności kwalifikowanych elektronicznych usług zaufania[128].
- Polska w czerwcu 2022 r. zgłosiła do notyfikacji środki identyfikacji elektronicznej[129]. Profil zaufany oraz profil osobisty zostały notyfikowane w grudniu 2022 r. jako środki identyfikacji elektronicznej w UE i mogą być używane do identyfikacji ich posiadacza w usługach elektronicznych administracji publicznej w innych krajach unijnych. Co więcej, notyfikacja potwierdza, że te środki spełniają warunki bezpieczeństwa odpowiednio na poziomie znaczącym (ang. *substantial*) w przypadku profilu zaufanego i wysokim (ang. *high*) w przypadku profilu osobistego. Lista pozostałych notyfikowanych w UE środków dostępna jest na stronie KE [130].
- Koncepcja tożsamości suwerennej (ang. SSI – *Self Sovereign Identity*)[131] nabiera coraz większego znaczenia – kilka dużych organizacji (np. Decen-

128 https://www.lsw.com.pl/alerty/kwalifikowane-podpisy-elektroniczne-uzyskane-w-unii-europejskiej-beda-wazne-takze-w-ukrainie/

129 https://obserwatorium.biz/polska-notyfikowala-srodki-identyfikacji-elektronicznej.html

130 https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

131 A. Preukschat, D. Reed, *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*, Manning, 2021.

tralized Identity Foundation) i konsorcjów (np. W3C) o międzynarodowym zasięgu stara się wypracować standardy w tym zakresie.

- Propozycja nowelizacji dyrektywy UE eIDAS 2[132] wprowadza wiele zmian w obszarze tożsamości cyfrowej, środków identyfikacji i podpisów elektronicznych. Jej główne założenia dotyczą wprowadzenia Europejskiego Portfela Tożsamości jako środka identyfikacji na wysokim poziomie bezpieczeństwa wraz z możliwością selektywnego prezentowania atrybutów elektronicznej tożsamości, bazującego w dużej mierze na założeniach tożsamości suwerennej.
- Pilotażowe wdrożenie Europejskiego Portfela Tożsamości Cyfrowej[133] przez konsorcjum EWC[134] będzie kluczowym benchmarkiem dla wszystkich podmiotów, które będą angażowały się w opracowywanie elektronicznych portfeli tożsamości. Podczas prac nad prototypowym rozwiązaniem powstaną prawdopodobnie rekomendacje co do stosowanych środków technicznych, jak i pewnych aspektów logiki biznesowej rozwiązań. Być może w toku prac zostaną ujednolicone wymagania i stosowane standardy wobec podmiotów integrujących się z takimi portfelami. W działaniach konsorcjum nie zabraknie polskiego akcentu – jego członkiem została firma SIGNIUS SA, zaś partnerem firma Obserwatorium.biz.
- Uchwalenie przez Radę Ministrów projektu ustawy zrównujące dokumenty zawarte w aplikacji mObywatel z dokumentami w rozumieniu tradycyjnym[135] 28 lutego 2023 r., a następnie przyjęcie jej przez Sejm 9 marca 2023 r.[136] jest znaczącym sygnałem od rządu o kierunku, w którym będzie zmierzał, jeśli chodzi o wykorzystania cyfrowych dokumentów oraz portfela tożsamości. Nie ulega wątpliwości, że projekt mObywatel 2.0 nabrał znaczenia i staje się priorytetowym działaniem w ramach cyfryzacji tożsamości w Polsce. W ramach projektu ustawy zostały znacząco rozszerzone scenariusze i przypadki użycia, w których obywatel będzie mógł

132 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

133 https://signius.pl/2023/01/27/signius-bierze-udzial-w-pilotazu-europejskiego-portfela-tozsamosci-cyfrowej/

134 https://eudiwalletconsortium.org/

135 https://www.gov.pl/web/premier/projekt-ustawy-o-aplikacji-mobywatel

136 https://inwestycje.pl/gospodarka/sejm-przyjal-ustawe-o-aplikacji-mobywatel-zrownujaca-e-dokumenty-z-tradycyjnymi/

zamiennie posługiwać się portfelem tożsamości mObywatel i dowodem osobistym. Dowód osobisty pozostanie w pewnych wypadkach jedynym uznawanym środkiem identyfikacji, np. przy przekraczaniu granicy kraju. Przegłosowano również kluczową poprawkę dotyczącą udostępniania przez ministra właściwego do spraw informatyzacji aktualnego kodu źródłowego aplikacji mObywatel w Biuletynie Informacji Publicznej.

Podziękowania

Chcielibyśmy serdecznie podziękować tym, którzy przyczynili się do powstania niniejszej publikacji za sprawą ożywionych dyskusji na temat cyfrowej tożsamości, oraz tym, którzy dzięki swoim cennym spostrzeżeniom pomogli podnieść jej wartość merytoryczną. Ukłony składamy: Janowi Szajdzie, Piotrowi Giedziunowi oraz Arkadiuszowi Lewandowskiemu z Identt sp. z o.o., Michałowi Taborowi z Obserwatorium.biz, Jerzemu Judyckiemu z PWPW SA., Lucjanowi Hanzlikowi z CISPA, a szczególnie kłaniamy się Pawłowi Narolskiemu za komentarze do manuskryptu.

Bibliografia

Biznes bez papieru – Komercjalizacja eID i usług zaufania w Polsce i Europie. Dostępny w: https://obserwatorium.biz/biznes-bez-papieru-komercjalizacja-eid-i-uslug-zaufania-w-polsce-i-europie.html

Cyberbezpieczny Portfel 2022. Edycja IV, lipiec2022. ZBP, Warszawa 2022. Dostępny w: https://zbp.pl/aktualnosci/wydarzenia/Raport-Cyberbezpieczny-Portfel-2022

ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*. Dostępny w: https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v020301p.pdf

ETSI TS 119 461 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects*. Dostępny w: https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf

http://jmrtd.org

https://archiwum.giodo.gov.pl/pl/329/1534

https://autenti.com/pl/

https://bde.wib.org.pl/

https://businessinsider.com.pl/wiadomosci/miliony-polakow-musza-wymienic-dowody-osobiste-inaczej-5-tys-zl-kary/8d8nkbr

https://commonsign.eu/

https://dokumentyzastrzezone.pl/system-dz/

https://dokumentyzastrzezone.pl/zastrzeganie-dokumentow/

https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+Levels+of+Assurance

https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/National+Strategies

https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

https://edoapp.pl/regulamin

https://e-id.pl/

https://esign.pl/aktualnosci/e-podpis-w-2022-roku-ktore-firmy-beda-musialy-w-niego-zainwestowac/

https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home
https://eudiwalletconsortium.org/
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32014R0910
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32019R1157
https://github.com/rubund/mrtdreader
https://id4d.worldbank.org/guide/levels-assurance-loas
https://inwestycje.pl/gospodarka/sejm-przyjal-ustawe-o-aplikacji-mobywatel-zrownujaca-e-dokumenty-z-tradycyjnymi/
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19820350230
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19840530272
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19971140740
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20050640565
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101671131
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000400
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210001865
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20101671131/U/D20101131Lj.pdf
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160001579/U/D20161579Lj.pdf
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180000723/U/D20180723Lj.pdf
https://mc.bip.gov.pl/publiczna-aplikacja-mobilna/informacje-o-publicznej-aplikacji-mobilnej.html
https://mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-srodka-identyfikacji/rejestr-dostawcow-srodka-identyfikacji-elektronicznej-przylaczonych-do-wezla-krajowego.html
https://mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-uslug/wezel-krajowy-zintegrowani-dostawcy-uslug.html
https://moj.gov.pl/uslugi/signer/upload?xFormsAppName=SIGNER
https://obserwatorium.biz/nowelizacja-eidas-wprowadza-europejski-portfel-cyfrowej-tozsamosci.html
https://obserwatorium.biz/polska-notyfikowala-srodki-identyfikacji-elektronicznej.html
https://obserwatorium.biz/the-eid-2017-electronic-identification-in-poland-report.html
https://obserwatorium.biz/top-5-trendow-w-eid-i-uslugach-zaufania-ktore-zmienia-rynek.html

https://pab.wib.edu.pl/cele-programu/
https://podpisujzdalnie.pl/baza-wiedzy/roznica-miedzy-kwalifikowanym-zaawansowanym-a-niekwalifikowanym-podpisem-elektronicznym
https://pz.gov.pl/pz/confirmationPointAddressesList
https://signius.pl/2023/01/27/signius-bierze-udzial-w-pilotazu-europejskiego-portfela-tozsamosci-cyfrowej/
https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-sa-2869-00-wyrok-naczelnego-sadu-administracyjnego-520144118
https://sogis.org/uk/pp_pages/others/pp_jcs_open.html
https://whitehats.pwr.edu.pl/cyberakcja/
https://trustedeconomyforum.com/pl/
https://www.cashless.pl/8800-weryfikacja-tozsamosci-zyciowka
https://www.cashless.pl/9814-pekao-konto-na-selfie-edowod
https://www.certum.pl/pl/aktualnosci/od-efpe-do-trusted-economy-forum-nowy-wymiar-globalnej-gospodarki/
https://www.coe.int/en/web/electoral-assistance/elecdata
https://www.commoncriteriaportal.org/.
https://www.cpd.gov.pl/o-nas/statystyki/
https://www.edoapp.pl/biznes
https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust
https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions
https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing
https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures
https://www.gov.pl/app/rdp/web/rdp/dowod-osobisty-wzor-2021
https://www.gov.pl/web/cyfryzacja/10-milionow-dowodow-osobistych-z-warstwa-elektroniczna
https://www.gov.pl/web/cyfryzacja/15-milionow-profili-zaufanych
https://www.gov.pl/web/gov/zglos-lub-cofnij-zawieszenie-e-dowodu-osobistego-dziecka-lub-innej-osoby
https://www.gov.pl/web/gov/zglos-utrate-lub-uszkodzenie-swojego-dowodu-osobistego-uniewaznij-dowod
https://www.gov.pl/web/gov/zglos-zawieszenie-lub-cofnij-zawieszenie-swojego-e-dowodu
https://www.gov.pl/web/mobywatel

https://www.gov.pl/web/mobywatel/mobywatel-dokument
https://www.gov.pl/web/mobywatel/zabezpieczenia1
https://www.gov.pl/web/mswia/polityka-certyfikacji
https://www.gov.pl/web/premier/projekt-ustawy-o-aplikacji-mobywatel
https://www.gum.gov.pl/pl/uslugi/zegar/524,Zegar.html
https://www.icao.int/publications/pages/publication.aspx?docnum=9303
https://www.icao.int/Security/FAL/TRIP/Documents/TR%20%20Supplemental%20Access%20Control%20V1.1.pdf
https://www.idea.int/data-tools/data/voter-turnout
https://www.iso.org/standard/31432.html
https://www.iso.org/standard/72891.html
https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf
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_metode_wideoweryfikacji_66066.pdf
https://www.lsw.com.pl/alerty/kwalifikowane-podpisy-elektroniczne-uzyskane-w-unii-europejskiej-beda-wazne-takze-w-ukrainie/
https://www.mobywatel.gov.pl/mobywatel.android.regulamin.12.0.0.pdf
https://www.mobywatel.gov.pl/mweryfikator.regulamin.7.0.0.pdf
https://www.mojeid.pl/
https://www.mojeid.pl/#co-to-jest-moje-id
https://www.mojeid.pl/#dostawcy-uslug
https://www.mojeid.pl/#zastosowanie
https://www.mojeid.pl/archiwum-aktualnosci/
https://www.money.pl/gospodarka/autenti-laczy-sily-z-microsoft-teams-6781831030094752a.html
https://www.money.pl/gospodarka/podpis-elektroniczny-ma-juz-20-lat-a-ty-masz-juz-swoj-6359279182264449a.html
https://www.nccert.pl/uslugi.htm
https://www.nccert.pl/uslugiNK.htm
https://www.oirpwarszawa.pl/wp-content/uploads/2022/01/kirp-zestawienie-ofert-podpisu-kwalifikowanego.pdf
https://www.oracle.com/java/technologies/javacard-protection-profile.html
https://www.podatki.gov.pl/wyjasnienia/do-e-urzedu-skarbowego-zalogujesz-sie-aplikacja-mobywatel

https://www.pwpw.pl/aktualnosci,1.html
https://www.pwpw.pl/Aktualnosci/2021/12/w-microsoft-teams-potwierdzisz-tozsamosc-i-podpiszesz-dokument-e-dowodem.html
https://www.wib.org.pl/o-nas/
https://www.youtube.com/watch?v=fDhoz0QZ07c
https://www.youtube.com/watch?v=jqckYtslXLg
https://www.zbp.pl/getmedia/076a1ce8-2850-4415-8a45-0f13389e8f97/Standard-Kwalifikacyjny-Stosowanie-zasad-cyberbezpieczenstwa.pdf
https://zbp.pl/Aktualnosci/Wydarzenia/Przewodnik-Identyfikacja-i-uwierzytelnienie-w-uslugach-elektronicznych%E2%80%9D
https://zbp.pl/Dla-Bankow/Cyberbezpieczenstwo/Cyberbezpieczenstwo-bankow-i-ich-klientow
https://zbp.pl/o-zbp/misja
ICAO, *Doc 9303. Machine Readable Travel Documents*. Dostępny w: https://www.icao.int/publications/Documents/Forms/AllItems.aspx
Identyfikacja i uwierzytelnienie w usługach elektronicznych. Dostępny w: https://zbp.pl/Aktualnosci/Wydarzenia/Przewodnik-Identyfikacja-i-uwierzytelnienie-w-uslugach-elektronicznych%E2%80%9D
Pala M., *Qualified Electronic Signature Ecosystem in Poland*. Dostępny w: https://eideasy.com/qualified-electronic-signature-ecosystem-in-poland/
Podpis elektroniczny w procesie inwestycyjno-budowlanym. Przewodnik dla organów administracji architektoniczno-budowlanej. Dostępny w: https://www.gunb.gov.pl/sites/default/files/attachment/podpis_elektroniczny_-_przewodnik_dla_organow_aab_0.pdf
Polityka świadczenia usługi Madkom S.A. Dostępny w: https://weryfikacjapodpisu.pl/policy
Preukschat A., Reed D., *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*, Manning, 2021.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1157 z dnia 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych. Dz.U.UE.L.2019.188.67. Dostępny w: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32019R1157
Ustawa z dnia 30 maja 1989 r. o izbach gospodarczych. Dz.U. z 1989 Nr 35 poz. 195. Dostępny w: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19890350195

Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Dz.U. z 2016 poz. 1579. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160001579/U/D20161579Lj.pdf

Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych. Dz.U. z 2010 Nr 167 poz. 1131. Dostępny w: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20101671131/U/D20101131Lj.pdf

Wodo W., *Science Mission impossible – Cybersecurity*. Dostępny w: https://www.youtube.com/watch?v=v-QG_aWWWSc

Harmonizacja wiedzy i procesów związanych z tożsamością elektroniczną w Polsce i Europie jest wyzwaniem z uwagi na ciągłe zmiany legislacyjne i techniczne w tym obszarze, jak również brak ugruntowanych źródeł wiedzy i kampanii edukacyjnych. Temat cyfrowej tożsamości, chociaż dotyczy każdego obywatela, nie jest wystarczająco obecny w debatach publicznych – dlatego zdecydowaliśmy się na zgłębienie tego zagadnienia i zaprezentowanie go jak najszerszemu gronu odbiorców.

Na przestrzeni ostatnich lat powstały różne usługi zaufania, udostępniane publicznie i komercyjnie. Zostały one ze sobą zintegrowane i pozwalają uprościć wiele zadań z zakresu weryfikacji tożsamości, zawierania umów, składania wniosków czy przekazywania danych osobowych.

W książce analizujemy poszczególne elementy składowe ekosystemu usług cyfrowych w Polsce i pokazujemy, jak korzystać z nich efektywnie. Prezentujemy, jak działa i co oferuje nowy dowód osobisty z warstwą elektroniczną (e-dowód), w jaki sposób wykorzystywać podpisy elektroniczne i je łatwo weryfikować, czym jest portfel tożsamości mObywatel i co oferuje oraz jak będzie wyglądać koncepcja europejskiego portfela tożsamości EUDI Wallet.

Wydawnictwa Politechniki Wrocławskiej
są do nabycia w sprzedaży wysyłkowej:
zamawianie.ksiazek@pwr.edu.pl

ISBN 978-83-7493-245-5
DOI 10.37190/wodo-rybak-blaskiewicz-2023