TOŻSAMOŚĆ CYFROWA
REGULACJE EUROPEJSKIE

SYGN. PAB WIB 9/2024

ISBN 978-83-965973-9-7

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

Warszawa, kwiecień 2024

PROGRAM
ANALITYCZNO
BADAWCZY

O Raporcie

Raport **Tożsamość cyfrowa. Regulacje europejskie** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Autorzy:

Raport przygotowany przez zespół w składzie:

Dr hab. prof. UŚ Dariusz Szostek – kierownik projektu
– Profesor Wydziału Prawa i Administracji Uniwersytetu Śląskiego, Dyrektor Międzyuczelnianego Centrum Inżynierii Prawa i Kompetencji Cyfrowych Cyber Science (wspólna jednostka Uniwersytetu Śląskiego, Politechniki Śląskiej, Uniwersytetu Ekonomicznego w Katowicach i NASK), Założyciel i CEO Szostek_Digital i Wspólnicy, Ekspert w Obserwatorium Parlamentu Europejskiego ds. Sztucznej Inteligencji, Polskiego Towarzystwa Informatycznego oraz ZiPSE Polska Cyfrowa, radca prawny. Autor szeregu publikacji z zakresu prawa nowych technologii, publikowanych zarówno w kraju jak i zagranicą m.in. LegalTech (Nomos Germany), czy Blockchain and Law (Nomos, Beck), Komentarze do prawa cywilnego, procedury cywilnej itd. Wdrożenia w ramach Horizon 2020 MAS4AI, czy SHOP4CF, a także wdrożenia w polskich bankach i instytucjach leasingowych narzędzi paperless, w tym biometrycznego podpisu elektronicznego. Certyfikaty m.in. ISO 42001 (dotyczący AI), specjalista w zakresie tożsamości cyfrowej, kwalifikowanych usług zaufanych (także wynikających z eIDAS2), smart contract czy tokenizacji procesów. Wykładowca na Uniwersytecie Śląskim, Akademii Koźmińskiego, Politechnice Śląskiej a także w uczelniach zagranicznych.

Dr Miłosz Brakoniecki
– Współzałożyciel i członek zarządu Obserwatorium.biz. Doktor nauk humanistycznych UAM w Poznaniu (specjalność socjologia), skończył studia podyplomowe ze strategii i planowania biznesu na Akademii Ekonomicznej w Poznaniu. W latach 2006–2014 dyrektor bankowości elektronicznej w Banku Zachodnim WBK, gdzie odpowiadał za rozwój biznesowy bankowości elektronicznej, sprzedaż przez kanały elektroniczne oraz płatności elektroniczne. W latach 2012–2014 członek Prezydium Rady Bankowości Elektronicznej Związku Banków Polskich. Współtwórca największego w Polsce serwisu crowdfoundingowego Siepomaga.pl, Fundacji Siepomaga.pl oraz FinTechów Rachuneo i Compay. W latach 2016–2018 Co-lider Zespołu Cyfrowej Tożsamości Programu Paperless/Cashless przy Ministerstwie Cyfryzacji, w latach 2016–2020 Członek Rady Nadzorczej Diners Club Polska Sp. z o.o. Prelegent w kilkudziesięciu konferencji branżowych w kraju i za granicą, autor licznych publikacji dot. gospodarki cyfrowej i bankowości.

Dominika Rzęsa

– Absolwentka Wydziału Nauk Społecznych Uniwersytetu im. Adama Mickiewicza w Poznaniu. W Obserwatorium.biz zajmuje się przygotowaniem procesów badawczych, analizą i budowaniem procesów biznesowych, analizą usług zaufania, analizą zgromadzonych danych oraz przeprowadzaniem wywiadów i badań.
Posiada doświadczenie w testowaniu serwisów internetowych i aplikacji na urządzenia mobilne (m.in. badania użyteczności serwisów transakcyjnych banków (Złoty Bankier) oraz aplikacji mInstytucja), prowadzeniu wywiadów FGI oraz IDI. Uczestniczyła w licznych opracowaniach analitycznych bazujących na danych jakościowych i ilościowych związanych m.in. z usługami zaufania, identyfikacją elektroniczną.

Piotr Sterczała

– Współzałożyciel i członek zarządu Obserwatorium.biz. Absolwent Wydziału Informatyki i Gospodarki Elektronicznej na Uniwersytecie Ekonomicznym w Poznaniu. W latach 2010–2014 pracował w Banku Zachodnim WBK S.A., gdzie odpowiedzialny był za realizację projektów biznesowych w zakresie bankowości mobilnej i internetowej. W Obserwatorium.biz odpowiada za nadzór i realizację projektów badawczych i analitycznych.

Michał Tabor

– Od 2002 roku zajmuje się bezpieczeństwem informacji, wdrażaniem mechanizmów podpisu elektronicznego, systemów elektronicznej administracji oraz budowaniem systemów zarządzania bezpieczeństwem informacji. Autor wielu rozwiązań z zakresu uwierzytelnienia, podpisu elektronicznego i dokumentu elektronicznego funkcjonujących w Polsce, w szczególności autor szeroko stosowanego mechanizmu składania deklaracji podatkowych i Profilu Zaufanego ePUAP.
Ekspert normalizacyjny ETSI. Posiadacz certyfikatu CISSP. Rzeczoznawca Polskiego Towarzystwa Informatycznego, Ekspert Polskiej Izby Informatyki i Telekomunikacji w zakresie identyfikacji, uwierzytelnienia i podpisu elektronicznego. Absolwent wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Członek zarządu Obserwatorium.biz

Marcin Wolski

– Od 2014 roku pracuje jako Specjalista ds. Bezpieczeństwa Informacji. Posiada kompetencje w zakresie następujących obszarów: system zarządzania bezpieczeństwem informacji, zarządzanie ryzykiem, identyfikacja elektroniczna, usługi zaufania, infrastruktura PKI oraz RODO. Uczestniczył w licznych projektach związanych z usługami zaufania, identyfikacją elektroniczną oraz bezpieczeństwem informacji. Opracowywał dokumentację związaną z infrastrukturą klucza publicznego.
Absolwent Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej w Warszawie. CCSP, Audytor wiodący ISO 27001, audytor systemów identyfikacji elektronicznej w ramach krajowego węzła identyfikacji elektronicznej.

PROGRAM ANALITYCZNO BADAWCZY

O Programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie analizy zjawisk, tworzenia opracowań i porządkowania wiedzy w obszarach cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania ich wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz kreowania wartości dla klientów bankowości. PAB WIB kładzie duży nacisk na rozwój współpracy ze środowiskami akademickimi i eksperckimi, poszukując synergii w zakresie zainteresowań badawczych autorów oraz potrzeb rozwojowych sektora bankowego.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- Nowe technologie w sektorze bankowym, cyberbezpieczeństwo banków i systemy płatnicze
- Ekonomiczna analiza rozwoju sektora bankowego, stabilności banków, otoczenia makroekonomicznego
- Prawno-regulacyjne i legislacyjne uwarunkowania działalności sektora bankowego oraz wyzwania wynikające z orzecznictwa sądów krajowych i europejskich
- ESG i sustainable finance
- Prace analityczno-badawcze w zakresie poszczególnych obszarów funkcjonowania banków oraz w zakresie funkcjonowania wskaźników referencyjnych

Więcej na temat działalności programu na stronie www.pabwib.pl

Kontakt:

dr Tomasz Pawlonka
Dyrektor Programu
m: 505 917 778
e: tpawlonka@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Agnieszka Wicha
m: 661 646 474
e: agnieszka.wicha@zbp.pl

Bartosz Przyborowski
m: 795 933 104
e: bartosz.przyborowski@zbp.pl

Spis treści

Wstęp

Od wielu lat mankamentem podnoszonym w europejskiej dyskusji, zarówno w środowisku bankowym, czy szerzej biznesowym, był brak jednolitej metody identyfikacji elektronicznej tożsamości osób, ale także i innych podmiotów, a ostatnimi czasy także przedmiotów. Wielość narzędzi pozwalających na identyfikację podmiotów, ich różnorodność, czasami lokalność, stanowi poważne wyzwanie dla współczesnego biznesu, ale także europejskiej administracji. Nie licząc rozwiązań zagranicznych, tylko w Polsce mamy szereg narzędzi, w szerszym bądź węższym zakresie pozwalających na identyfikację osób fizycznych. Ich wielość, a także często niekompatybilność stanowi wyzwanie dla obrotu w pełni elektronicznego.

Unia Europejska dostrzegła ten problem, nie tylko podczas okresowego audytu rozporządzenia eIDAS, ale także w strategii cyfryzacji Europy na najbliższy okres. Jak wskazano w preambule do Rezolucji Ustawodawczej Parlamentu Europejskiego i Rady (COM(2021)0281 z 29 lutego 2024 w sprawie wniosku dotyczącego Rozporządzenia Parlamentu Europejskiego I Rady, zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej wskazano, iż już w programie polityki „Droga ku cyfrowej dekadzie" do 2030 r. Decyzją Parlamentu Europejskiego i Rady (UE) 2022/2481 określono założenia i cyfrowe cele unijnych ram, które do 2030 r. mają zapewnić wprowadzenie na szeroką skalę zaufanej, dobrowolnej i kontrolowanej przez użytkownika tożsamości cyfrowej, uznawanej w całej Unii oraz umożliwiającej każdemu użytkownikowi kontrolowanie swoich danych w interakcjach online. Także w europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie wskazano na konieczność zapewnienia bezpiecznej i zaufanej tożsamości cyfrowej, zapewniając ochronę przed ryzykiem w cyberprzestrzeni i przed cyberprzestępczością, w tym kradzieżą tożsamości lub manipulowanie tożsamością. Rezydenci i obywatele UE mają mieć prawo do tożsamości cyfrowej, a zharmonizowane ramy tożsamości cyfrowej powinny przyczyniać się do tworzenia bardziej zintegrowanej Unii poprzez zmniejszenie barier cyfrowych między państwami członkowskimi oraz umożliwienie obywatelom i rezydentom UE czerpania korzyści z cyfryzacji przy jednoczesnym zwiększaniu przejrzystości i ochrony ich praw.

Przyjęte w lutym 2024 r. przez Parlament Europejski zmiany do rozporządzenia eIDAS, wychodzą naprzeciw potrzebom rynku, ale są także odpowiedzią na szereg wymogów określonych w regulacjach takich jak DORA, NIS2 itd. W szczególności europejskie portfele tożsamości cyfrowej powinny mieć wbudowaną funkcję wspólnego panelu zarządzania, aby zapewnić wyższy stopień przejrzystości, prywatności i kontroli użytkownika nad swoimi danymi. Co ciekawe Unia proponuje aby użycie kwalifikowanego podpisu elektronicznego było nieodpłatne dla wszystkich osób, w czynnościach innych niż profesjonalnie, a państwa członkowskie mają podjąć i ustanowić środki zapobiegające nieodpłatnemu użyciu kwalifikowanych podpisów elektronicznych przez osoby fizyczne do celów biznesowych. Europejskie portfele tożsamości cyfrowej powinny mieć możliwość generowania pseudonimów wybranych i używanych przez użytkownika, służących do uwierzytelnienia podczas dostępu do usług online oraz podlegać regularnym ocenom podatności na zagrożenia w cyberprzestrzeni. Powinny też uniemożliwiać kradzież tożsamości, a ich dostawcy uwzględniać przejrzystość oraz rozliczalność. Zmieni to w sposób zasadniczy także i polski rynek tożsamości cyfrowej, gdzie kwalifikowany podpis elektroniczny jest w chwili obecnej narzędziem tożsamości cyfrowej głównie profesjonalistów, a inne „darmowe" narzędzia jak profil zaufany, czy tożsamość potwierdzona przez banki, w sytuacji rozpowszechnienia darmowych kwalifikowanych podpisów elektronicznych (będących równocześnie narzędziem umożliwiającym uwierzytelnienie tożsamości cyfrowej) wraz z rozpowszechnianiem darmowego kwalifikowanego podpisu elektronicznego, będą w odwrocie.

Także w interesie banków i innych instytucji płatności będzie oparcie transakcji o kwalifikowane usługi zaufania i uwierzytelnianie klientów poprzez portfel cyfrowej tożsamości. Zapewnienie wysokiego poziomu bezpieczeństwa bankowości elektronicznej poprzez narzędzia identyfikacji cyfrowej wydawane według wspólnych europejskich ram, a co nie bez znaczenia – z przeniesieniem przynajmniej częściowej odpowiedzialności na dostawców kwalifikowanych usług zaufania, wręcz idealnie wpasowują się w wymagania stawiane bankom w DORA czy NIS 2. Chociaż

wymagają odpowiednich audytów i wprowadzenia w procesy biznesowe.

Mając powyższe na uwadze, przedstawiamy raport dotyczący tożsamości cyfrowej na rynku europejskim i rozwiązań obecnie funkcjonujących z równoczesnym wskazaniem europejskiego portfela tożsamości cyfrowej i ram przygotowanych przez UE do wdrożenia między innymi przez banki w najbliższych dwóch latach. To niewiele czasu, tym bardziej iż wiele narzędzi już należy uwzględnić przy zmianie procesów wymuszonych przez DORA i NIS2

Dr hab. Prof. UŚ Dariusz Szostek

Wprowadzenie

Zakres i cele raportu

W obliczu rosnącego znaczenia cyfrowej tożsamości w świecie cyfrowym, Unia Europejska aktywnie kształtuje politykę dotyczącą jej regulacji i standardów. Rozporządzenie eIDAS oraz jego nowelizacja tzw. eIDAS 2.0[1], są kluczowymi elementami w dążeniu do stworzenia europejskich ram cyfrowej tożsamości, które będą stanowiły bezpieczną i użyteczną podstawę funkcjonowania w publicznych i prywatnych usługach elektronicznych. Europejski portfel tożsamości cyfrowej, jako jedno z proponowanych rozwiązań, ma na celu ułatwienie dostępu do usług cyfrowych przy zachowaniu prywatności i bezpieczeństwa danych.

Raport ma na celu zbadanie obecnych ram regulacyjnych oraz technologicznych aspektów cyfrowej tożsamości, ze szczególnym uwzględnieniem inicjatyw Unii Europejskiej. Zakres raportu obejmuje zarówno przegląd kluczowych zagadnień związanych ściśle ze zdalną identyfikacją oraz uwierzytelnieniem, jak i analizę środków wspierających cyfrową tożsamość, takich jak elektroniczne poświadczenia atrybutów, certyfikaty, podpisy cyfrowe oraz nowoczesne podejścia oparte na technologii blockchain. Dodatkowo, raport adresuje wyzwania związane z ochroną danych, dostępnością oraz bezpieczeństwem cyfrowej tożsamości, proponując jednocześnie możliwe rozwiązania i najlepsze praktyki.

Celem niniejszego opracowania jest dostarczenie wszechstronnej analizy aktualnego stanu i perspektyw rozwoju cyfrowej tożsamości, mając na uwadze dynamicznie zmieniające się środowisko cyfrowe oraz potrzebę zapewnienia wysokiego poziomu bezpieczeństwa i ochrony prywatności użytkowników.

Metodologia przygotowania raportu

Główną techniką wykorzystaną do zgromadzenia i analizy danych był desk-research, co pozwoliło na szeroki przegląd dostępnych źródeł informacji. Celem tej metodologii jest zapewnienie kompleksowego zrozumienia obecnego stanu i potencjalnych przyszłych kierunków rozwoju tożsamości cyfrowej, biorąc pod uwagę zarówno aspekty prawne, technologiczne, jak i społeczne.

W ramach metodologii desk-research przeprowadzono analizę różnorodnych dokumentów. Skupiono się na przepisach prawa, które wpływają na kształtowanie się tożsamości cyfrowej, a także na projektach aktów prawnych, które mogą przynieść zmiany w tym obszarze. Zbadano również dokumenty wydane przez agencje Unii Europejskiej, aby zrozumieć wpływ inicjatyw i rekomendacji UE na rozwój tożsamości cyfrowej. Ważnym elementem analizy były także dane dotyczące pracy grupy eIDAS oraz informacje o pilotażowych projektach tożsamości cyfrowej realizowanych w różnych jurysdykcjach. Nie zapomniano również o opracowaniach krajowych, które mogą dostarczyć cennych wskazówek dotyczących lokalnych podejść do tematu.

W raporcie zastosowano szereg metod, w tym przegląd literatury oraz analizę treści zgromadzonych materiałów. Dokonano także syntezy informacji z różnych źródeł, aby stworzyć spójny obraz badanego zjawiska. W procesie analizy korzystano również z wiedzy ekspertów z zakresu tożsamości cyfrowej, co pozwoliło na weryfikację i uzupełnienie zebranych danych.

[1] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_PL.html z dnia 2 kwietnia 2024

Podejście regulatorów UE w zakresie budowy wspólnej tożsamości cyfrowej dla państw UE

1.1. Koncepcja budowy tożsamości cyfrowej

Współczesny świat cyfrowy stawia przed nami nieustanne wyzwania związane z bezpieczeństwem, prywatnością i zaufaniem w środowisku internetowym. Tożsamość cyfrowa, będąca cyfrowym odpowiednikiem fizycznych atrybutów tożsamości, staje się fundamentem elektronicznej interakcji, umożliwiając uwierzytelnianie osób i instytucji w sieci. Wprowadzenie do raportu o tożsamości cyfrowej opiera się na rozległej analizie praktyki prawnej i technicznej w zakresie tożsamości cyfrowej.

Zgodnie z raportem ENISA[2], dynamiczny rozwój technologii cyfrowych wymaga ciągłego dostosowywania i rozwoju, który nie tylko odpowiada na bieżące potrzeby, ale także przewiduje przyszłe kierunki ewolucji technologii.

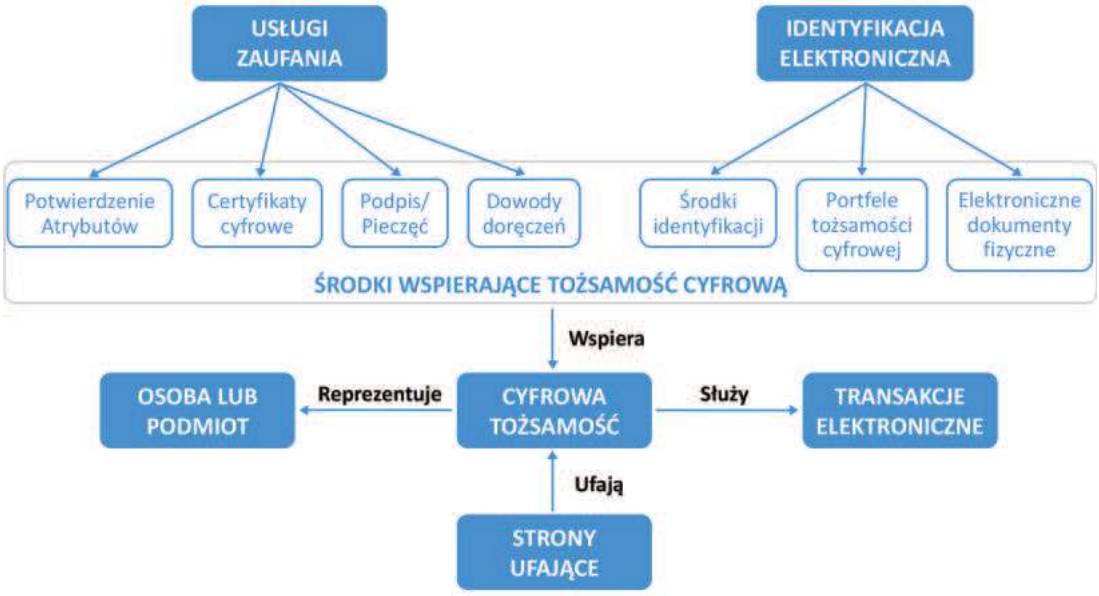
Cyfrowa tożsamość rozwija się na całym świecie i stanowi obecnie jeden z kluczowych obszarów transformacji cyfrowej poszczególnych obszarów gospodarki, administracji publicznej i generalnie funkcjonowania społeczeństwa. Rozwój różni się w zależności od kraju czy regionu. Wiele krajów podejmuje inicjatywy mające na celu ułatwienie korzystania z usług cyfrowych, poprawę efektywności administracyjnej i ochronę prywatności danych osobowych, jednak związane z tym regulacje i technologie nadal ewoluują.

1.1.1. Definicja cyfrowej tożsamości

Cyfrowa tożsamość została zdefiniowana w normach technicznych NIST[3], termin odnosi się do unikalnej reprezentacji podmiotu (osoby fizycznej, prawnej, urządzenia lub obiektu) zaangażowanego w transakcję online. Jest to zbiór atrybutów związanych z daną jednostką, które są używane w elektronicznych usługach, aby identyfikować użytkowników oraz zarządzać ich dostępem do zasobów i usług. Tożsamość cyfrowa ułatwia procesy uwierzytelniania i autoryzacji w środowiskach cyfrowych, zapewniając bezpieczeństwo i prywatność transakcji. Termin ten obejmuje różnorodne metody i technologie, takie jak certyfikaty cyfrowe, elektroniczne podpisy oraz inne środki kryptograficzne, które umożliwiają bezpieczną wymianę informacji i weryfikację tożsamości w sieci.

Cyfrowa tożsamość oznacza zarówno metody pozwalające na zidentyfikowanie osoby, jak i podmiotu prowadzącego interakcję z usługami jak i możliwość zabezpieczenia wartości dowodowej z transakcji elektronicznych w sposób pozwalający na jednoznaczne wskazanie osoby lub podmiotu uczestniczącego w tych transakcjach. Co do zasady mówimy o tożsamości cyfrowej osób fizycznych i osób prawnych, która umożliwia na jednoznaczne powiązanie transakcji elektronicznych z konkretnym podmiotem. Jednakże coraz częściej termin tożsamość cyfrowa jest używany w kontekście różnego rodzaju obiektów, w szczególności takich, które funkcjonują w transakcjach tj. systemy komputerowe, pojazdy automatyczne lub przedmioty uczestniczące w procesach składających się na tzw. Internet rzeczy (IoT).

W raporcie ENISA Digital Identity Standards przyjęto pokazaną poniżej systematykę w zakresie funkcjonowania środków tożsamości cyfrowej.



Rysunek 1. Środki cyfrowej tożsamości
Źródło: ENISA

[2] Raport ENISA – Digital Identity Standards (3.07.2023) – https://www.enisa.europa.eu/publications/digital-identity-standards
[3] NIST SP 800-63-3 "Digital Identity Guidelines"
[4] Raport ENISA – Digital Identity Standards (3.07.2023)

Środki cyfrowej tożsamości można podzielić na dwie główne kategorie: środki tworzone i zarządzane przez usługi zaufania oraz środki tworzone i wydawane przez schematy identyfikacji.

Środki Tworzone i Zarządzane przez Usługi Zaufania to w szczególności:

- Elektroniczne poświadczenie atrybutów – są to poświadczenia elektroniczne pozwalające na uwierzytelnienie cechy, charakterystyki lub uprawnień osoby fizycznej, prawnej lub obiektu. (por. art. 3 pkt. 43 i 44 eIDAS 2). Poświadczenia te są tworzone przez usługi zaufania, które są w stanie poświadczyć konkretne atrybuty tożsamości.

- Certyfikaty pozwalają na identyfikację właściciela pary kluczy (publicznego i prywatnego). Certyfikaty są wydawane przez usługi zaufania – centra certyfikacji, które weryfikują tożsamość reprezentowaną w certyfikacie, łączą tę tożsamość z kluczem oraz dostarczają informacje stronom polegającym na certyfikacie.

- Podpis elektroniczny może służyć do identyfikacji osoby podpisującej dokument. Pieczęć elektroniczna może być wykorzystana do potwierdzenia integralności i pochodzenia dokumentu od konkretnej osoby prawnej.

- Dowody usługi rejestrowanego doręczenia elektronicznego mają na celu udowodnienie, że określone zdarzenie nadania lub odebrania danych miało miejsce w określonym czasie. Dowody te identyfikują uczestników procesu doręczenia, takich jak nadawca lub odbiorca wiadomości.

Środki Tworzone i Zarządzane przez Systemy Identyfikacji Elektronicznej to:

- Środki Elektronicznej Identyfikacji umożliwiające identyfikację osoby fizycznej lub prawnej w usługach online i offline.

- Portfel cyfrowej tożsamości, który został zdefiniowany w eIDAS 2.0. Portfel umożliwia uwierzytelnienie użytkownika, identyfikację elektroniczną oraz dostarczanie jego określonych atrybutów do stron ufających. Portfel ten stanowi przenośne narzędzie umożliwiające użytkownikom zarządzanie swoją tożsamością cyfrową. Funkcjonowanie portfela cyfrowej tożsamości zostanie szczegółowo omówione w dalszej części niniejszego raportu.

- Elektroniczne dokumenty fizyczne, to w szczególności paszporty biometryczne oraz dokumenty identyfikacyjne zawierające warstwę elektroniczną, która umożliwia udostępnienie danych identyfikujących posiadacza dokumentu.

Każdy z powyżej wymienionych środków wspiera tożsamość cyfrową, umożliwiając stronom ufającym na efektywne przeprowadzenie procesu identyfikacji i uwierzytelniania. Rozwój technologii cyfrowej tożsamości, w tym środków jej wsparcia, odgrywa kluczową rolę w zapewnieniu bezpieczeństwa, prywatności i efektywności elektronicznych transakcji w cyfrowym ekosystemie.

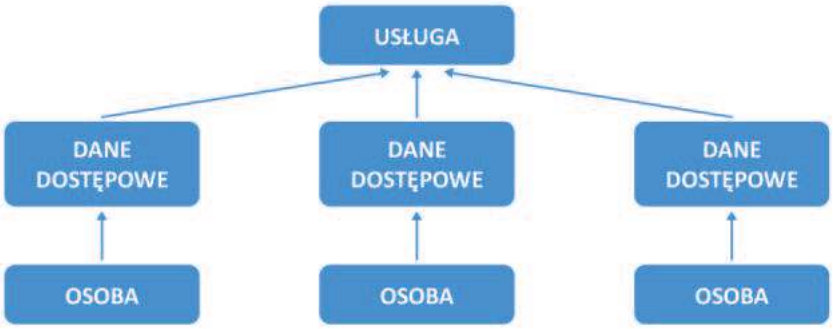
1.1.2. Opis założeń koncepcji

Modele cyfrowej tożsamości na świecie

Możliwość identyfikacji użytkowników w usługach cyfrowych i systemach komputerowych rozwijana jest od samego początku ich powstawania. Istnieje wiele rozwiązań pozwalających na zarządzanie tożsamością użytkowników systemów komputerowych opartych na modelach, które rozwijały się wraz z rozwojem systemów łączności i dostępności Internetu. Poniżej zostają opisane kluczowe przykłady modeli oraz ich implementacji.

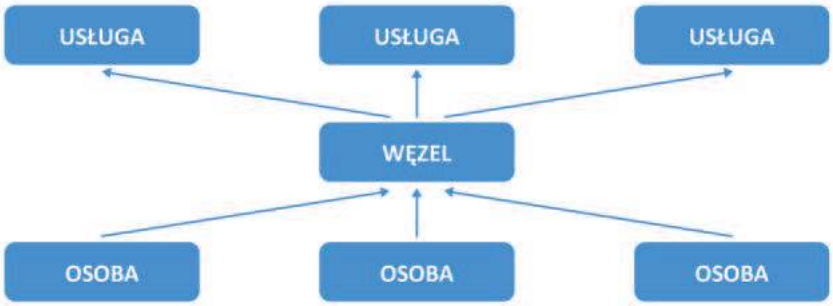
Jednym z modeli cyfrowej tożsamości jest model **scentralizowany** który opiera się na podejściu, w którym kontrola nad danymi dotyczącymi tożsamości użytkowników jest skupiona wokół pojedynczej usługi, która kontroluje dane o tożsamości swoich użytkowników i każdemu z nich przydziela indywidualne dane dostępowe. Przykłady scentralizowanych modeli tożsamości obejmują tradycyjne bazy danych tożsamości w instytucjach rządowych, takich jak system PESEL, systemy identyfikacji klientów w bankach oraz wewnętrzne systemy zarządzania tożsamością w dużych firmach. Modele scentralizowane są budowane przy każdej nowej inicjatywie i nie łączą się między sobą, wobec czego uruchomienie nowego systemu lub przedsięwzięcia wymaga przeprowadzenia procesu rejestracji użytkowników i zbudowania osobnej bazy informacji o ich tożsamościach.

Innym modelem jest model oparty na tzw. **federacji.** W tym podejściu różne podmioty, często o podobnych celach biznesowych lub branżach, łączą się w federację, aby wspólnie zarządzać i udostępniać zasoby cyfrowe. Każda organizacja zachowuje kontrolę nad swoimi zasobami, ale współpracuje z innymi członkami federacji w celu ułatwienia dostępu do zasobów. Przykładem modelu federacyjnego jest system finansowy, gdzie tożsamość pochodząca z jednej instytucji finansowej umożliwia użytkownikowi korzystanie z usług w innej instytucji o podobnym charakterze, typowym modelem federacyjnym jest krajowy system identyfikacji elektronicznej



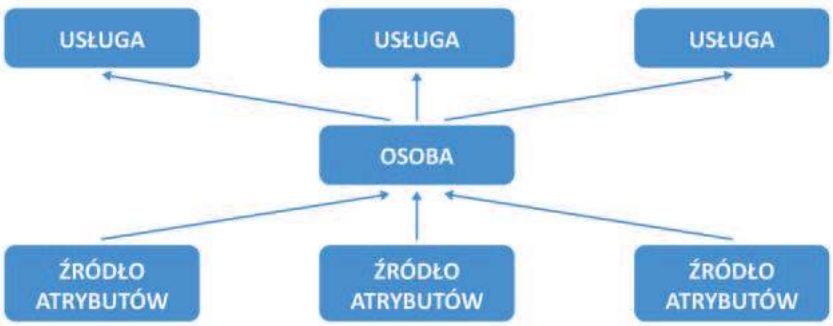
Rysunek 2. Scentralizowany model cyfrowej tożsamości

umożliwiający korzystanie z bankowych środków identyfikacji lub profilu zaufanego w wielu usługach. Model federacyjny pozwala na współdzielenie informacji o tożsamości przez wiele podmiotów i usług. Nie wymaga każdorazowej rejestracji użytkownika w systemie, natomiast wymaga, aby podmioty uczestniczące w systemie federacyjnym miały zaufanie do usług i systemów zarządzających tożsamością użytkowników.



Rysunek 3. Federacyjny model cyfrowej tożsamości

Model **zdecentralizowany** to model tożsamości cyfrowej (ang. Decentralized identity model), który w ostatnich latach zyskuje popularność Jest to podejście, w którym kontrola nad danymi dotyczących tożsamości użytkownika nie jest skupiona u dostawcy tożsamości – np. w jednym centralnym punkcie, ale jest kontrolowana przez samego użytkownika, często za pomocą takich technologii jak blockchain. W modelu zdecentralizowanym w oparciu o różne źródła atrybutów użytkownik zbiera i utrzymuje informacje pozwalające na uwierzytelnianie się w różnych usługach. Podstawą systemu zdecentralizowanego jest utrzymywanie informacji o tożsamości przez sam podmiot, którego dane dotyczą.



Rysunek 4. Zdecentralizowany model cyfrowej tożsamości

Stosowanie różnych modeli cyfrowej tożsamości wymaga zastosowania technologii umożliwiających bezpieczne wykorzystanie w usługach i transakcjach. W szczególności stosowane technologie muszą zapewnić, że tożsamością cyfrową będzie się posługiwała osoba do nich przypisana przy zachowaniu ochrony jej prywatności. Stosowanie różnych technologii zależne jest od środowiska ich wykorzystania, łatwości użycia, możliwości korzystania z komunikacji elektronicznej. Poniżej przedstawiamy podstawowe technologie wspierające wykorzystanie cyfrowej tożsamości.

- Technologie biometryczne: wykorzystują unikalne cechy fizyczne lub behawioralne osoby, takie jak odciski palców, wzór siatkówki oka czy schematy użycia danych systemów. Technologie te znajdują zastosowanie w systemach kontroli dostępu, płatnościach bezdotykowych, bankowości elektronicznej itp. Nośnikiem danych w tych technologiach są bezpośrednio użytkownicy, centralna baza danych przechowująca dane biometryczne lub biometryczne dokumenty tożsamości. Przykładami technologii biometrycznych są paszporty i dokumenty tożsamości biometryczne zawierające dane o wizerunku twarzy oraz odciskach palców, a także system scentralizowany banku wykorzystujące biometrię np. odcisku palca do uwierzytelnienia transakcji w bankomatach.

- Technologie kart chipowych: wykorzystują karty i inne dokumenty plastików z wbudowanym układem mikroprocesora do przechowywania danych tożsamości. Karty chipowe zabezpieczają klucze kryptograficzne, które są powiązane z tożsamością osoby przypisanej do karty, dostęp do kluczy karty zazwyczaj jest zabezpieczony numerem PIN, który jest udostępniony jedynie właścicielowi karty. Takie karty mogą być wykorzystywane do autoryzacji w bankomatach, systemach płatności bezgotówkowych czy kontroli dostępu, karty są także wykorzystywane w rozwiązaniach podpisu elektronicznego.

- Technologie o rozproszonym rejestrze – wykorzystują technologię blockchain do przechowywania i weryfikacji danych tożsamości w rozproszonych blokach danych. Zazwyczaj w zakresie tożsamości technologie blockchain są wykorzystywane razem z innymi technologiami – w szczególności pozwalają na powiązanie urządzań uwierzytelniających będących w posiadaniu użytkownika z atrybutami tożsamości ich właściciela.

- Technologie tokenów pozwalają na zawarcie zaszyfrowanych i uwierzytelnionych danych tożsamości użytkownika i ich przekazanie od dostawcy tożsamości do jego użytkownika. Technologie tokenów są wykorzystywane do przekazania danych o tożsamości na potrzeby transakcji w aplikacjach internetowych (tokeny SAML lub JWT).

- Technologia cyfrowego portfela tożsamości – narzędzie cyfrowe, które umożliwia użytkownikom przechowywanie, zarządzanie i udostępnianie swoich danych tożsamościowych w formie elektronicznej. Co do zasady portfel cyfrowej tożsamości pozwala użytkownikowi samodzielnie przechowywać tokeny dotyczące jego tożsamości oraz w sposób uwierzytelniony udostępniać dane na potrzeby transakcji.

Poniższa tabela prezentuje zestawienie wybranych rozwiązań cyfrowej tożsamości, wraz ze wskazaniem modelu oraz stosowanych technologii.

Tabela 1. Zestawienie systemów cyfrowej tożsamości w ujęciu modelu oraz zastosowanej technologii przekazywania danych

Nazwa systemu identyfikacji	Kraj	Rodzaj modelu	Technologia
Profil zaufany	Polska	Model scentralizowany – udostępniony w ramach krajowego schematu identyfikacji	Token
Polski dowód osobisty (e-ID)	Polska	Model scentralizowany – udostępniony w ramach krajowego schematu identyfikacji	Karta chip
Krajowy schemat identyfikacji	Polska	Model federacji	Token
System mojeID	Polska	Model federacji – oparty na scentralizowanych systemach bankowych	Token

Tabela 1. cd.

Nazwa systemu identyfikacji	Kraj	Rodzaj modelu	Technologia
mObywatel	Polska	Model zdecentralizowany	Portfel cyfrowej tożsamości
Aadhaar	Indie	Model scentralizowany	Identyfikacja biometryczna
Smart-ID	Estonia	Model scentralizowany	Aplikacja mobilna
Verified.Me	Kanada	Model federacji	Token
GOV.UK Verify	Wielka Brytania	Model scentralizowany	Token
SingPass	Singapur	Model scentralizowany	Token
Bank-ID	Szwecja	Model federacji	Token
ID.me	USA	Model scentralizowany	Token
SPID	Włochy	Model federacji	Token
itsme	Belgia	Model scentralizowany/federacja	Portfel cyfrowej tożsamości
Franceconnect	Francja	Model federacji	Token

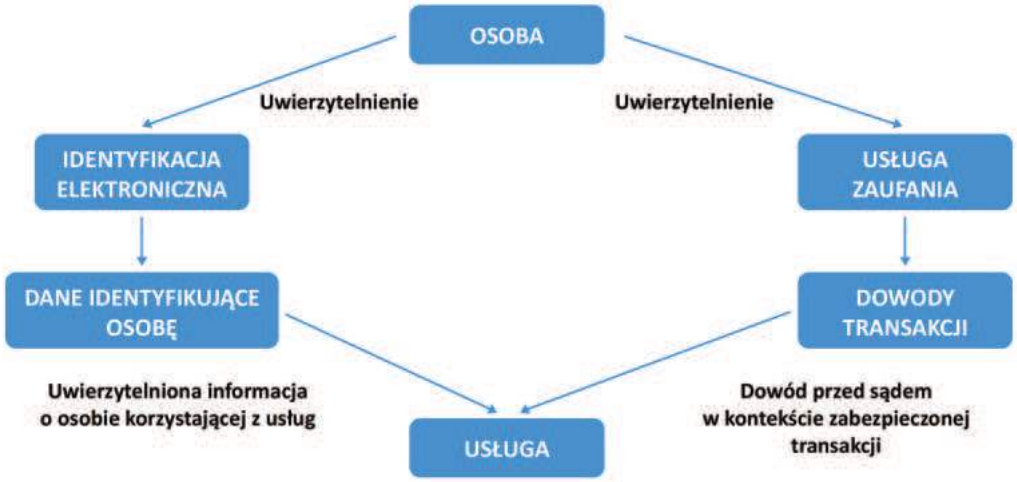
Cyfrowa tożsamość w Unii Europejskiej

Identyfikacja elektroniczna w Unii Europejskiej opiera się na systemie notyfikowanej tożsamości, pozwalając użytkownikom z jednego państwa członkowskiego na bezpieczne korzystanie z usług elektronicznych w innym państwie członkowskim. Transgraniczne węzły identyfikacji elektronicznej umożliwiają wymianę informacji o tożsamości między krajami UE, co ułatwia dostęp do transgranicznych usług publicznych i prywatnych, zapewniając jednocześnie wysoki poziom bezpieczeństwa i ochrony danych osobowych.

Rozporządzenie eIDAS ustanowiło podstawy dla tożsamości cyfrowej w UE, opierając się na identyfikacji elektronicznej dla usług online. Identyfikacja elektroniczna umożliwia unikalną reprezentację osób fizycznych lub prawnych w środowisku cyfrowym. Środek identyfikacji elektronicznej, będący materialną lub niematerialną jednostką, zawiera dane umożliwiające uwierzytelnienie online. Systemy identyfikacji elektronicznej wydają te środki, co ułatwia dostęp do różnorodnych usług cyfrowych. eIDAS pozwala państwom członkowskim na notyfikację swoich środków identyfikacji na różnych poziomach wiarygodności, co z kolei wymaga od wszystkich państw UE akceptacji notyfikowanych środków w usługach publicznych.

Zgodnie z definicją, identyfikacja elektroniczna to proces wykorzystujący dane elektroniczne do unikalnej identyfikacji osób fizycznych lub prawnych. Dane te, po uwierzytelnieniu, są przekazywane od dostawcy tożsamości do usług wykorzystujących tę tożsamość. Informacja ta jest związana z czasem jej przekazania, ale nie dostarcza bezpośrednio danych o transakcji. Bezpieczeństwo systemu odbierającego zależy od implementacji i zabezpieczeń. W kontekście bankowym, wymogi dotyczące bezpieczeństwa są szczególnie wysokie, co ma zapewnić ochronę transakcji finansowych. W systemach wielu innych usług pozabankowych nie ma takich wymagań, wobec czego należy zastosować dodatkowe zabezpieczenia. W celu powiązania tożsamości cyfrowej z transakcją i zapewnienia materiału dowodowego, stosuje się usługi zaufania.

W kontekście cyfrowej tożsamości, usługi zaufania odgrywają kluczową rolę w zapewnianiu bezpieczeństwa transakcji online. Definiowane są jako usługi elektroniczne, które obejmują między innymi tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych oraz elektronicznych znaczników czasu. Cyfrowe certyfikaty, podpisy elektroniczne i pieczęcie stanowią podstawowe narzędzia w usługach zaufania, ułatwiając identyfikację uczestników cyfrowych transakcji. Te narzędzia zapewniają nie tylko autentyczność danych, ale również pełnią funkcję dowodową w przypadku sporów.



Rysunek 5. Identyfikacja elektroniczna i usługi zaufania

Podpis elektroniczny ma szczególne zastosowanie w składaniu oświadczeń woli online, łącząc w sposób jednoznaczny treść oświadczenia z identyfikacją jego autora. Zaawansowany podpis elektroniczny zapewnia jednoznaczne wskazanie tożsamości podpisującego, wiarygodność – że tylko osoba wskazana w podpisie mogła go złożyć, oraz integralność – potwierdzającą, że żadna zmiana nie została wykonana. Kwalifikowany podpis elektroniczny dostarcza bezpieczeństwa stronie ufającej, dając jego niezaprzeczalność, domniemania prawne oraz równoważność podpisowi własnoręcznemu. Stosowanie kwalifikowanego podpisu elektronicznego zapewnia to nie tylko wiarygodność transakcji, ale również chroni prawa stron.

Kwalifikowane usługi zaufania oferują wysoki poziom bezpieczeństwa, Zabezpieczają one strony transakcji, oferując domniemania prawne m.in odnoszące się do autentyczności i integralności podpisów i treści podpisywanych dokumentów.

Rysunek 6. Podpisy elektroniczne

Rozporządzenie eIDAS wprowadziło rozwiązania, które znacząco przyczyniły się do rozwoju usług cyfrowych w UE. Jednakże dynamiczny rozwój potrzeb biznesowych, nowe wyzwania w zakresie bezpieczeństwa oraz postęp technologiczny wskazują na konieczność dokonania zmian i aktualizacji przepisów, aby nadal wspierać innowacje i zapewniać wysoki poziom bezpieczeństwa w cyfrowym ekosystemie.

Unia Europejska przyjmuje proaktywne podejście do cyfrowej tożsamości przygotowując wdrożenie europejskiego portfela cyfrowej tożsamości (ang. *European*

Digital Identity Walet – EDIW), wymagając od wszystkich państw członkowskich wydania swoim obywatelom portfela, który jest certyfikowany zgodnie ze wspólnymi ramami odniesienia w celu osiągnięcia interoperacyjności dostępu do usług sektora rządowego i prywatnego. Podstawową regulacją w tym zakresie jest rozporządzenie eIDAS 2.0. Europejski portfel tożsamości cyfrowej w projektowanych założeniach to aplikacja mobilna lub usługa w chmurze obliczeniowej z dostępem przez inne urządzenia elektroniczne użytkowników, która umożliwia obywatelom i przedsiębiorstwom UE przechowywanie oraz udostępnianie swoich dokumentów tożsamości i poświadczeń w usługach publicznych i prywatnych.

Jednym z podstawowych założeń wynikających z implementacji EDIW[5] jest stworzenie bardziej zintegrowanej unii cyfrowej poprzez redukcję cyfrowych barier między państwami członkowskimi oraz umożliwienie obywatelom i mieszkańcom Unii korzystania z korzyści płynących z digitalizacji, jednocześnie zwiększając przejrzystość i ochronę ich praw. Bardziej zharmonizowane podejście do identyfikacji cyfrowej powinno zmniejszyć ryzyka i koszty wynikające z obecnego rozdrobnienia spowodowanego stosowaniem zróżnicowanych krajowych rozwiązań lub, w niektórych państwach członkowskich, brakiem takich elektronicznych rozwiązań identyfikacji.

Potrzeby w zakresie tożsamości w usługach administracji i komercyjnych

Unia Europejska wskazuje na podstawowe problemy w zakresie tożsamości w dostępnych obecnie systemach identyfikacji cyfrowej oferowanych przez rządy w UE[6]:

- systemy nie są dostępne dla całej populacji, często ograniczają się do usług publicznych online i nie umożliwiają płynnego dostępu transgranicznego;
- tylko 14% kluczowych dostawców usług publicznych we wszystkich państwach członkowskich pozwala na transgraniczne uwierzytelnianie za pomocą systemu e-ID;
- wzrost wolumenu zdarzeń identyfikacji pomiędzy krajami członkowskimi jest powolny.

Odpowiedzią na powyższe problemy ma być implementacja europejskiego portfela cyfrowej tożsamości, który ma wzmocnić jednolity rynek europejski, umożliwiając obywatelom, rezydentom oraz przedsiębiorstwom na identyfikację i uwierzytelnianie online i offline w sposób:

- bezpieczny -> dane dot. tożsamości muszą być przechowywane i udostępniane za pomocą bezpiecznych protokołów komunikacji;
- godny zaufania -> dane dot. tożsamości muszą pochodzić z wiarygodnych źródeł;
- przyjazny użytkownikowi, wygodny i dostępny -> prosty interfejs umożliwiający każdemu użytkownikowi skorzystanie z tożsamości cyfrowej;
- zharmonizowany w całej Unii -> rozpoznawanie tożsamości w ramach EDIW przez wszystkie kraje członkowskie, bez żadnych barier.

Z całą pewnością w dobie cyberzagrożeń, w tym oszustw związanych z atakami na tożsamość, podstawową potrzebą jest dostarczenie użytkownikom takich narzędzi, które zapewnią najwyższą ochronę przed oszustwami mającymi na celu wyłudzanie danych, podszywanie się pod tożsamość, oszustwa finansowe. Cyfrowy portfel jest narzędziem wspierającym zastosowanie regulacji DORA i NIS2.

Problemy i wyzwania – ochrona danych, linkowalność, zewnętrzne wpływy, dostępność, niezależność

W kontekście rozwoju koncepcji cyfrowej tożsamości, warto zwrócić uwagę na problemy i wyzwania

Problem nr 1

Utrata prywatności danych osobowych użytkowników

Wyzwania:

- implementacja skutecznych mechanizmów ochrony przed atakami hackerskimi lub innymi, w tym wyciekami danych,
- zapewnienie bezpieczeństwa danych w całym cyklu ich życia (od utworzenia, przez przechowywanie, udostępnianie, aż po usunięcie),
- propagowanie edukacji dotyczącej bezpieczeństwa informacji wśród użytkowników.

[5] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

[6] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (dostęp 29.02.2024 r.)

Problem nr 2

Możliwość powiązania danych nt. osób na podstawie metadanych oraz informacji pozostawianych w różnych serwisach internetowych

Wyzwanie:

Ograniczenie możliwości powiązania różnych informacji na temat użytkownika ze sobą, aby zapobiec utracie prywatności oraz manipulacji danymi.

Problem nr 3

Nadmiarowe udostępnianie danych przez Administratorów do podmiotów trzecich

Wyzwanie:

Ograniczenie ryzyka związanego z wykorzystywaniem danych o tożsamości przez zewnętrzne podmioty, takie jak rządy, administracja, przedsiębiorcy itd., w celach nadzoru, profilowania czy marketingu.

Problem nr 4

Brak powszechności dostępności usług cyfrowych

Wyzwanie:

Zapewnienie dostępności cyfrowej tożsamości dla wszystkich użytkowników, zwłaszcza dla osób starszych, niepełnosprawnych czy o niskim statusie społeczno-ekonomicznym.

Problem nr 5

Zapewnienie niezależności użytkownikom w związku z problemem zbyt dużej zależności od cyfrowych usług, w tym cyfrowej tożsamości

Wyzwanie:

Przygotowanie rozwiązań awaryjnych czy też alternatywnych na wypadek przerw w działaniu technologii, awarii technicznych, błędów systemowych lub innych problemów technicznych, które mogą utrudnić lub uniemożliwić dostęp do usług cyfrowych.

Problem nr 6

Kradzież, wyłudzenie, podszycie się pod cyfrową tożsamość

Wyzwanie:

Weryfikacja tożsamości w cyfrowym środowisku stanowi wyzwanie w obliczu coraz to nowszych zagrożeń, takich jak ataki biometryczne, tzw deep-fakes czy posługiwanie się sztucznie wygenerowanymi dokumentami tożsamości, a także wykorzystywaniem narzędzi AI.

1.1.3. Portfele cyfrowej tożsamości

Tożsamość użytkowników oraz ochrona prywatności mają kluczowe znaczenie dla bezpieczeństwa transakcji w Internecie, a obawy dotyczące prywatności i bezpieczeństwa danych w środowisku cyfrowym skutkują rozwojem innowacyjnych rozwiązań mających na celu ochronę indywidualnych praw użytkowników. Jednym z takich rozwiązań jest koncepcja Self-Sovereign Identity (SSI), która stanowi nowoczesne podejście do zarządzania tożsamością cyfrową. To podejście umożliwia użytkownikom pełną kontrolę nad swoimi danymi tożsamości bez konieczności polegania na centralnych organach zarządzających lub pośrednikach.

SSI jest odpowiedzią na potrzebę ewolucji w zakresie modeli zarządzania tożsamością cyfrową. Dzięki SSI, użytkownicy mogą bezpośrednio przekazywać swoje dane do dostawców usług, zwiększając tym samym poziom prywatności i bezpieczeństwa. Ten model suwerennej tożsamości skupia się na indywidualnej autonomii, umożliwiając użytkownikom samodzielne zarządzanie i kontrolowanie swoich danych tożsamościowych[7]

Kluczowym aspektem architektury SSI są cztery składniki: model rejestru identyfikatorów, model rejestru roszczeń, rozwiązania uwierzytelniające i roszczenia weryfikowalne. Wszystkie te elementy opierają się na technologii blockchain, która zapewnia zdecentralizowaną bazę danych zastępującą tradycyjne procesy rejestracji. Dzięki temu, SSI oferuje nowe możliwości w zarządzaniu tożsamością cyfrową, zachowując jednocześnie wysoki poziom bezpieczeństwa i prywatności[8]

[7] Giannopoulou, A., & Wang, F. (2021). Self-sovereign identity. *Internet Policy Rev.*, 10. https://doi.org/10.14763/2021.2.1550.

[8] Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A Survey on Essential Components of a Self-Sovereign Identity. *Comput. Sci. Rev.*, 30, 80-86. https://doi.org/10.1016/j.cosrev.2018.10.002.

Niezależna tożsamość (SSI) rewolucjonizuje sposób, w jaki użytkownicy mogą identyfikować się w usługach online, umożliwiając im pełną kontrolę nad danymi identyfikacyjnymi bez konieczności łączenia się z centralnymi węzłami tożsamości. SSI, porównywane do portfela z dokumentami, daje użytkownikowi możliwość wyboru, które dane chce udostępnić, zwiększając tym samym prywatność i bezpieczeństwo w cyfrowym świecie.

Portfel niezależnej tożsamości bazuje na weryfikowalnych poświadczeniach, które użytkownicy mogą otrzymywać od różnych instytucji, takich jak administracja publiczna czy banki. Te poświadczenia są globalnie weryfikowalne i mogą być bezpiecznie używane w różnych usługach online. Umożliwiają one użytkownikowi potwierdzenie określonych informacji, takich jak pełnoletność, bez konieczności ujawniania innych danych osobistych.

W najbliższej przyszłości stosowanie SSI stanie się standardem w Unii Europejskiej, co wymusi na każdej usłudze online akceptowanie tego typu identyfikacji. Państwa członkowskie będą mogły wydawać weryfikowalne poświadczenia, a kwalifikowani dostawcy usług zaufania będą mogli wydawać potwierdzenia określonych atrybutów, co zrewolucjonizuje obecne systemy identyfikacji.

Korzystanie z niezależnej tożsamości zwiększa bezpieczeństwo danych użytkownika, odpowiadając na rosnące potrzeby rynku w zakresie prywatności. Mechanizmy SSI są rozwijane przy wsparciu projektów finansowanych przez Unię Europejską, co podkreśla znaczenie tej technologii w kontekście europejskim.

Niezależna tożsamość stanowi przełom w zarządzaniu tożsamością cyfrową[9], umożliwiając użytkownikom większą kontrolę nad swoimi danymi i ułatwiając korzystanie z usług online. Jest to krok w kierunku bardziej zdecentralizowanego i bezpiecznego środowiska cyfrowego, które stawia na pierwszym miejscu prywatność i autonomię użytkowników.

Główne elementy Self-Sovereign Identity opierają się na weryfikowalnych poświadczeniach, czyli cyfrowych odpowiednikach tradycyjnych dokumentów tożsamości, takich jak dowody osobiste czy prawa jazdy. Użytkownik może otrzymywać te poświadczenia od różnych instytucji, takich jak administracja publiczna, banki czy dostawcy usług zaufania. Weryfikowalne poświadczenia umożliwiają użytkownikom udowodnienie określonych informacji bez konieczności ujawniania dodatkowych danych osobistych.

Portfel tożsamości, to cyfrowe narzędzie, które umożliwia użytkownikom przechowywanie, zarządzanie i używanie ich weryfikowalnych poświadczeń. Działanie portfela jest podobne do fizycznego zawierającego karty i dokumenty tożsamości, w którym to właściciel potwierdza sposób identyfikacji i użycia odpowiednich do potrzeby kart.

Założeniami funkcjonowania SSI jest pełna kontrola użytkownika nad danymi, to on lub ona decyduje, jakie dane udostępnia i w jakim zakresie. Decentralizacja – eliminuje potrzebę centralnych węzłów tożsamości i usług identyfikacji. Dzięki temu użytkownicy mogą zarządzać swoją tożsamością niezależnie, bez pośredników.

Te elementy razem tworzą podstawy systemu Self-Sovereign Identity, który ma na celu zapewnienie większej kontroli użytkowników nad ich danymi osobowymi w cyfrowym świecie, zwiększając jednocześnie prywatność i bezpieczeństwo.

Podstawą dla stosowania technologii Self-Sovereign Identity jest mechanizm Verifable Credentials szczegółowo opisany w standardzie Verifiable Credentials Data Model v2.0[10]. Weryfikowalne poświadczenie to cyfrowy odpowiednik tradycyjnych dokumentów, takich jak dyplomy, prawa jazdy czy certyfikaty. Jest to dokument cyfrowy, który może być zabezpieczony i weryfikowany za pomocą technologii kryptograficznych, co umożliwia potwierdzenie autentyczności poświadczenia oraz tożsamości jego wystawcy. Takie podejście zapewnia wysoki poziom bezpieczeństwa i zaufania w cyfrowym świecie, umożliwiając bezpieczne udostępnianie i weryfikowanie informacji.

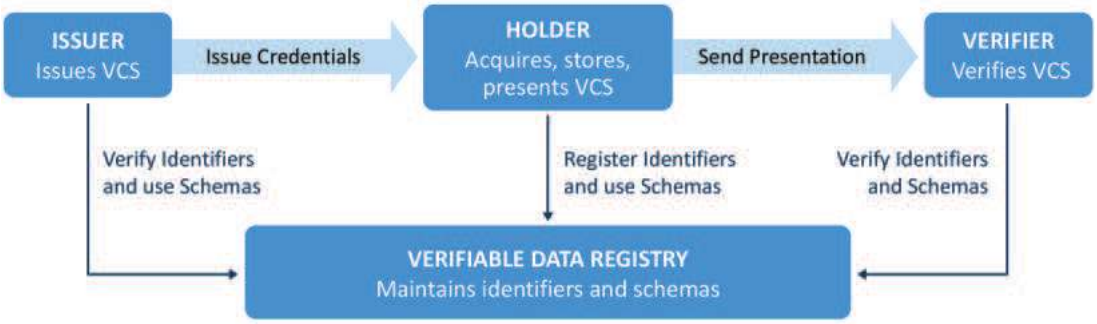
Poniższy graf przedstawia ekosystem funkcjonowania weryfikowalnych poświadczeń.

Ekosystem weryfikowalnych poświadczeń obejmuje kilka kluczowych ról: Wydawcę (Issuer), Właściciela (Holder), Weryfikującego (Verifier) oraz Weryfikowalny Rejestr Danych (Verifiable Data Registry). Oto szczegółowy opis każdej z tych ról:

1. **Wydawca** (Issuer) to podmiot, który twierdzi pewne informacje o jednym lub większej liczbie podmiotów, tworzy z tych twierdzeń weryfikowalne poświadczenie i przekazuje je właścicielowi. Przykładami wydawców mogą być korporacje, organizacje non-profit, rządy i osoby fizyczne.

[9] Szostek D (red) 2021, Legal tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym – Rozdział 2. Komunikacja elektroniczna – niezależna tożsamość i rozproszone potwierdzenia (aut. Michał Tabor)

[10] https://www.w3.org/TR/vc-data-model-2.0/



Rysunek 7. Ekosystem weryfikowalnych poświadczeń
Źródło: W3C

2. **Właściciel** (Holder) to podmiot posiadający jedno lub więcej weryfikowalnych poświadczeń i który jest zdolny do generowania z nich weryfikowalnych prezentacji. Właścicielami mogą być studenci, pracownicy, klienci lub jakiekolwiek inne osoby lub podmioty, które potrzebują udowodnić pewne informacje na swój temat.

3. **Weryfikujący** (Verifier) otrzymuje jedno lub więcej weryfikowalnych poświadczeń, w ramach weryfikowalnej prezentacji, w celu przetworzenia i akceptacji. Weryfikujący są odpowiedzialni za weryfikację autentyczności i ważności weryfikowalnych prezentacji i zawartych w nich poświadczeń. Przykładami mogą być pracodawcy, personel ochrony i strony internetowe wymagające uwierzytelnienia użytkowników.

4. **Weryfikowalny Rejestr Danych** (Verifiable Data Registry) to system, który pośredniczy w tworzeniu i weryfikacji identyfikatorów, kluczy i innych istotnych danych, takich jak schematy weryfikowalnych poświadczeń, rejestry unieważnień i publiczne klucze wydawców, niezbędne do korzystania z weryfikowalnych poświadczeń. Rejestr ten zapewnia, że dane są odporne na manipulacje i dokładnie rejestruje, które podmioty kontrolują określone dane. Przykłady weryfikowalnych rejestrów danych obejmują zaufane bazy danych, zdecentralizowane bazy danych, rządowe bazy danych identyfikatorów, rozproszone rejestry oraz usługi statusu poświadczeń.

Wzajemne relacje między tymi rolami opierają się na wydawaniu weryfikowalnych poświadczeń przez wydawców właścicielom, przedstawianiu tych poświadczeń przez właścicieli weryfikującym oraz weryfikacji tych poświadczeń przez weryfikujących, z potencjalnym wsparciem informacji przechowywanych w weryfikowalnych rejestrach danych.

Kluczową cechą weryfikowalnych poświadczeń jest ich weryfikowalność. Oznacza to, że każdy, kto otrzymuje weryfikowalne poświadczenie, może zweryfikować jego autentyczność oraz upewnić się, że zostało ono wydane przez zaufanego wystawcę i nie zostało zmienione po wydaniu. Dzięki temu weryfikowalne poświadczenia stanowią niezawodny sposób na potwierdzanie tożsamości i uprawnień w środowisku cyfrowym.

Weryfikowalne poświadczenia zapewniają wysoki poziom ochrony prywatności i kontroli nad udostępnianymi informacjami. Posiadacz poświadczenia może decydować, które informacje są udostępniane weryfikatorom, a technologie takie jak dążenie do zerowej wiedzy (zero-knowledge proofs) pozwalają na udowodnienie posiadania poświadczenia bez konieczności ujawniania jego zawartości. Taka selektywna dyskrecja sprzyja ochronie danych osobowych i minimalizacji ryzyka naruszenia prywatności.

Kolejną ważną cechą weryfikowalnych poświadczeń jest ich odporność na fałszerstwa. Wykorzystanie zaawansowanych technik kryptograficznych, takich jak podpisy cyfrowe, sprawia, że bardzo trudno jest sfałszować takie poświadczenie. Dzięki temu weryfikowalne poświadczenia stanowią solidną i wiarygodną formę potwierdzania różnego rodzaju twierdzeń w Internecie.

Norma opisuje przypadki użycia weryfikowalnych poświadczeń wykorzystywanych na potrzeby udostępniania informacji o uprawnieniach i danych w systemach akademickich, które nie mają bezpośredniego zastosowania w sektorze finansowym. Jednakże należy wskazać, że na bazie ww. norm można wykorzystywać poświadczenia potwierdzające dane dostępowe do systemów bankowych, informacje o posiadanym koncie bankowym lub wykonanym przelewie.

Rodzaje portfeli

Do utrzymywania weryfikowalnych poświadczeń wykorzystywane są różnego rodzaju portfele pozwalające zbieranie i udostępnianie poświadczeń.

Portfel krawędziowy („edge wallet") i portfel w chmurze („cloud wallet") to dwa różne podejścia do przechowywania i zarządzania cyfrowymi tożsamościami oraz poświadczeniami w kontekście Self-Sovereign Identity (SSI). Każde z nich ma swoje specyficzne zalety i ograniczenia, które sprawiają, że są one lepiej dopasowane do różnych scenariuszy użytkowania.

Portfel krawędziowy jest aplikacją zainstalowaną bezpośrednio na urządzeniu użytkownika, takim jak smartfon, tablet czy komputer. Wszystkie dane, w tym klucze kryptograficzne i poświadczenia, są przechowywane lokalnie na urządzeniu użytkownika. Dzięki temu rozwiązaniu użytkownik ma pełną kontrolę nad swoimi danymi i nie musi polegać na zewnętrznych dostawcach usług. Portfele krawędziowe są uważane za bardziej „czyste" rozwiązania SSI, ponieważ zasadniczo eliminują potrzebę zaufania do strony trzeciej. Jednak wymagają one od użytkownika odpowiedzialności za bezpieczeństwo i backup swoich danych[11].

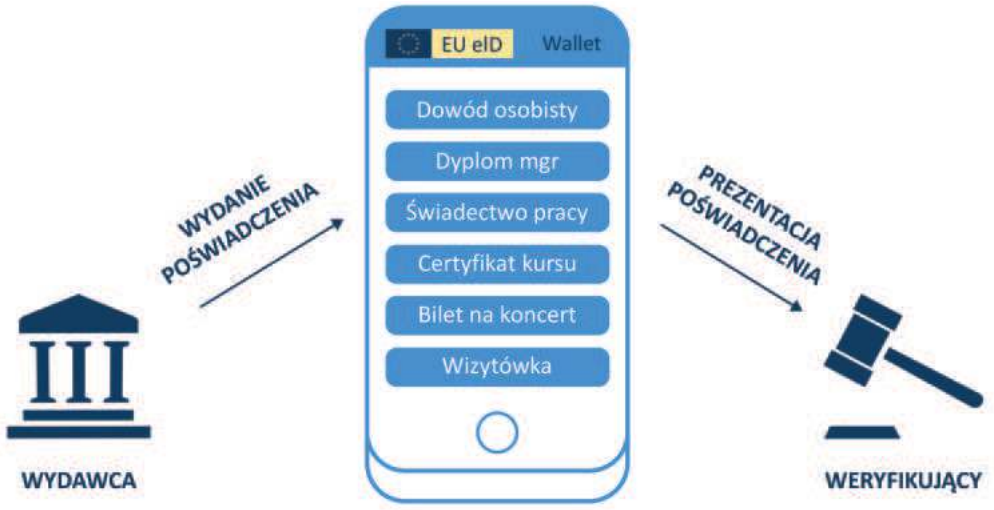
Portfel w chmurze, w przeciwieństwie do portfela krawędziowego, przechowuje dane użytkownika na zdalnych serwerach prowadzonych przez dostawcę usług. Dzięki temu użytkownicy mogą uzyskać dostęp do swoich poświadczeń i tożsamości z dowolnego urządzenia posiadającego połączenie z internetem. Jest to szczególnie przydatne w przypadku utraty lub uszkodzenia urządzenia fizycznego. Portfele w chmurze oferują większą elastyczność i wygodę, ale zwiększają zależność od dostawcy usług i mogą stwarzać dodatkowe ryzyko dla prywatności i bezpieczeństwa danych użytkownika.

Wybór między portfelem krawędziowym a portfelem w chmurze zależy od wielu czynników, w tym od priorytetów użytkownika dotyczących bezpieczeństwa, prywatności, wygody oraz dostępności. Oba rozwiązania mają swoje miejsce w ekosystemie SSI, a decyzja powinna być podyktowana konkretnym przypadkiem użycia i preferencjami użytkownika.

1.1.4. Europejski portfel cyfrowej tożsamości

Unia Europejska bazując na opisanym powyżej modelu tożsamości niezależnej (Self Severeign Identity) realizuje projekt wdrożenia Europejskich Ram Tożsamości Cyfrowej, której głównym elementem będzie wdrożenie Europejskiego Portfela Cyfrowej Tożsamości. Całość rozwiązania będzie oparta o wdrożoną nowelizację rozporządzenia eIDAS, wprowadzającą prawne podstawy funkcjonowania rozporządzenia portfela cyfrowej tożsamości.

Europejski portfel cyfrowej tożsamości to produkt, ale również i usługa, która umożliwi użytkownikowi przechowywanie danych dotyczących tożsamości, danych uwierzytelniających i atrybutów związanych z jego tożsamością, udostępnianie ich stronom ufającym na żądanie i wykorzystywanie ich do uwierzytelniania w trybie online i offline, a także składanie kwalifikowanych podpisów i pieczęci elektronicznych. Inaczej to środek identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz

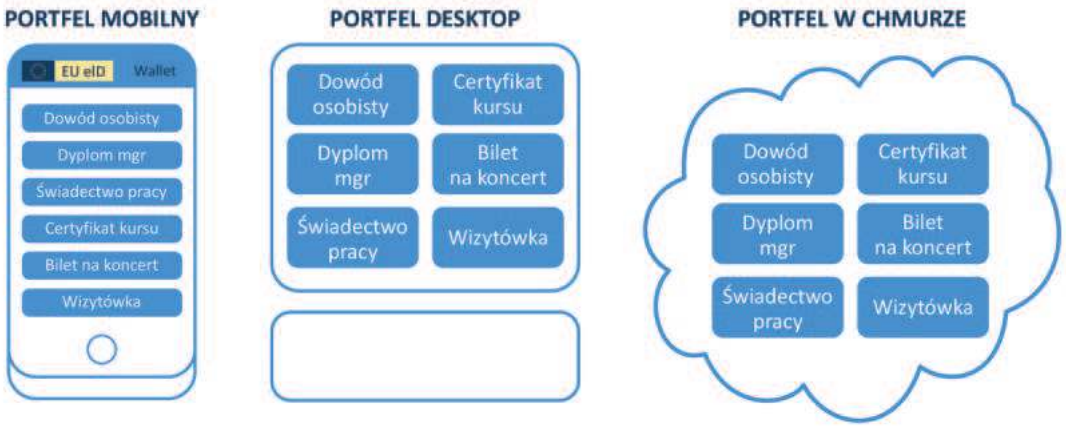


Rysunek 8. Europejski portfel tożsamości cyfrowej

[11] https://decentralized-id.com/development/wallets/

innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych.

Portfel będzie mógł być dostarczony jako rozwiązanie mobilne instalowane na urządzeniach osobistych w tym telefonach komórkowych, rozwiązanie desktop lub rozwiązanie dostępne w chmurze.



Rysunek 9. Rodzaje portfeli

Portfel umożliwia pobieranie, przechowywanie i udostępnianie elektronicznych poświadczeń atrybutów, których wydawcami będą kraje członkowskie Unii Europejskiej oraz dostawcy usług zaufania.

Użytkownikami portfeli cyfrowej tożsamości będą osoby fizyczne, osoby prawne oraz osoby fizyczne reprezentujące osoby fizyczne lub osoby prawne. Taka konstrukcja pozwoli na zbudowanie jednolitego sposobu identyfikacji zarówno firm jak i obywateli Unii Europejskiej. Portfel osoby fizycznej będzie pozostawał pod jej wyłączną kontrolą, dzięki temu użytkownik portfela za jego pomocą będzie mógł się zidentyfikować oraz przekazać atrybuty swojej tożsamości. Portfele osób prawnych będą bezpośrednio lub pośrednio nadzorowane przez osoby reprezentujące osoby prawne, modele funkcjonowania portfeli dla przedsiębiorstw są jeszcze we wczesnej fazie opracowania technicznego i organizacyjnego.

W portfelu cyfrowej tożsamości utrzymywane będą różnorodne rodzaje poświadczeń, które mają na celu ułatwienie identyfikacji i uwierzytelniania użytkowników w cyfrowym ekosystemie. Analiza dostępnych dokumentów pozwala na wyróżnienie kilku kluczowych rodzajów poświadczeń:

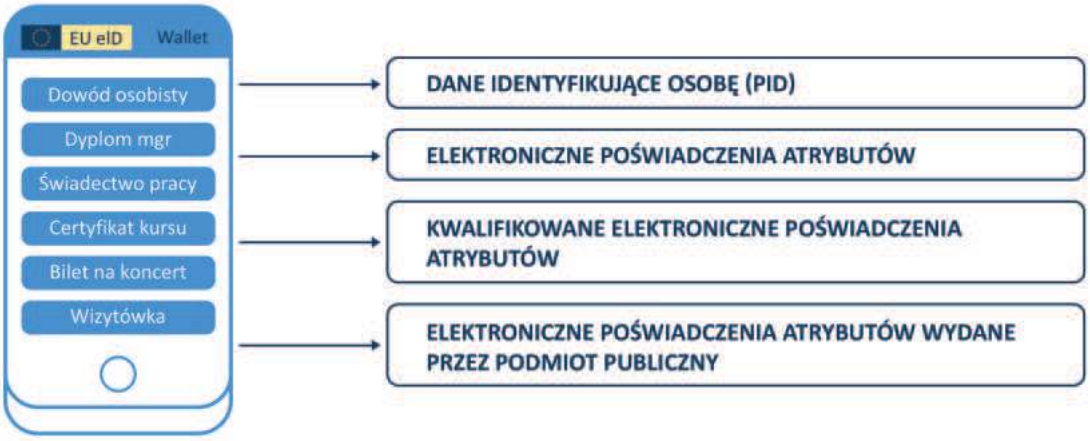
- **Dane identyfikacyjne osoby** (Person Identification Data, PID): PID są niezbędne do weryfikacji tożsamości użytkownika portfela cyfrowego na wysokim poziomie wiarygodności (Level of Assurance, LoA). Obejmują one informacje pozwalające na jednoznaczną identyfikację osoby w cyfrowym ekosystemie.

- **Elektroniczne Poświadczenia Atrybutów** (Electronic Attestation of Attributes, EAA): Są to poświadczenia w postaci elektronicznej, które pozwalają na uwierzytelnienie określonych atrybutów. Atrybuty te mogą opisywać cechy, charakterystyki lub właściwości osoby fizycznej, prawnej, lub przedmiotu. EAA mogą być wydawane przez dowolnego dostawcę usług zaufania, a ich regulacje i zasady wykorzystania często określone są w ramach specyficznych dla sektora ram prawnych lub umownych. EAA mogą być wykorzystywane w różnych kontekstach, takich jak potwierdzanie kwalifikacji zawodowych, uprawnień do prowadzenia pojazdów, czy też atrybutów związanych z identyfikacją cyfrową.

- **Kwalifikowane Elektroniczne Poświadczenia Atrybutów** (Qualified Electronic Attestation of Attributes, QEAA): QEAA to specjalny rodzaj EAA, które są wydawane przez Kwalifikowanych Dostawców Usług Zaufania (Qualified Trust Service Providers, QTSP) i spełniają szczególne wymogi określone w rozporządzeniu eIDAS. QEAA zapewniają najwyższy poziom bezpieczeństwa i są uznawane w całej Unii Europejskiej. Mogą być wykorzystywane w szczególnie wrażliwych kontekstach cyfrowych, gdzie wymagana jest wysoka pewność co do autentyczności poświadczanych atrybutów.

- **Elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny**

za źródło autentyczne lub w jego imieniu, pełnią te same zadania do kwalifikowane elektroniczne poświadczenia atrybutów, ale mogą być wydawane przez podmiot sektora publicznego, taki jak urząd państwowy, agencja rządowa lub inna instytucja publiczna, jest uznany za odpowiedzialny za zarządzanie i utrzymanie źródła autentycznych danych, takiego jak rejestr ludności, rejestr przedsiębiorstw, rejestr pojazdów itp. Wydając takie poświadczenie, instytucja publiczna potwierdza, że dane zawarte w poświadczeniu są zgodne z informacjami przechowywanymi w oficjalnym, uznawanym za wiarygodne źródle danych. Na przykład, urząd stanu cywilnego może wydać elektroniczne poświadczenie atrybutów potwierdzające datę i miejsce urodzenia osoby, opierając się na danych z rejestru ludności.



Rysunek 10. Poświadczenia przetwarzane przez portfel

Takie poświadczenia są istotnym elementem infrastruktury cyfrowej państwa i transgranicznego funkcjonowania usług w Unii Europejskiej, umożliwiającym uproszczenie i usprawnienie wielu procesów administracyjnych i biznesowych poprzez cyfryzację tradycyjnych form potwierdzania informacji, co przyczynia się do wzrostu efektywności i oszczędności czasu zarówno dla obywateli, jak i administracji.

Portfel powstaje jako inicjatywa Komisji Europejskiej, mająca na celu stworzenie standardowego, interpretacyjnego i bezpiecznego rozwiązania cyfrowej tożsamości dla obywateli Unii Europejskiej.

Poniżej wymieniono cechy europejskiego portfela cyfrowej tożsamości związane z jego planowaną implementacją i użyciem:

1. **Wspólny standard, wspólna architektura techniczna**

   Europejski portfel będzie wydawany przez każdy kraj członkowski Unii Europejskiej w oparciu o zbudowane przez siebie rozwiązanie, ale oparty jest na wspólnym standardzie cyfrowej tożsamości, który jest akceptowany we wszystkich krajach członkowskich UE. Dzięki temu użytkownicy mają możliwość korzystania z jednego, wspólnego rozwiązania cyfrowej tożsamości na terenie całej Unii Europejskiej.

2. **Bezpieczeństwo – wysoki poziom zaufania i bezpieczeństwa**

   Europejskie portfele tożsamości muszę spełniać wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa, w szczególności w zakresie wymogów dotyczących potwierdzania i weryfikacji tożsamości, zarządzania środkami identyfikacji elektronicznej oraz uwierzytelniania – zastosowanie zaawansowanych technologii kryptograficznych i certyfikacji. Ponadto portfel jest zgodny z ogólnym rozporządzeniem o ochronie danych (RODO), a państwa członkowskie zobowiązane są do określenia środków technicznych i organizacyjnych w celu zapewnienia wysokiego poziomu ochrony danych osobowych.

3. **Interoperacyjność**

   Europejskie portfele elektroniczne wspierają interoperacyjność rozwiązania. Oznacza to, że użytkownicy mogą korzystać z tego samego portfela cyfrowej tożsamości do dostępu do różnych

usług oferowanych przez różne instytucje, usług publicznych, administracyjnych, finansowych, zdrowia czy edukacji. Zharmonizowane podejście i ramy interoperacyjności pozwolą na łatwe i jednolite korzystanie z różnych usług online na terenie Unii Europejskiej.

4. **Kontrola użytkownika**

   Użytkownik portfela sam zarządza swoimi danymi oraz atrybutami, które chce przechowywać czy udostępniać. EDIW daje użytkownikom pełną kontrolę i zwiększa ich prywatność.

5. **Wygoda i mobilność – aplikacja mobilna**

   Podczas tworzenia europejskiego portfela niezbędne jest uwzględnienie potrzeb i zrozumienie przeciętnego użytkownika. Dla ich wygody portfel jest dostępny w formie aplikacji mobilnej, co pozwala użytkownikom na łatwe korzystanie z cyfrowej tożsamości na swoich smartfonach. Ponadto, umożliwia on użytkownikom przenoszenie swojej cyfrowej tożsamości pomiędzy różnymi urządzeniami, co zapewnia wygodę i mobilność w korzystaniu z usług online.

6. **Dostępność dla obywateli UE**

   Szeroka dostępność i użyteczność europejskich portfeli tożsamości cyfrowej powinna prowadzić do większej ich akceptacji oraz zaufania do nich zarówno wśród osób prywatnych, jak i prywatnych dostawców usług. Każdy obywatel Unii Europejskiej ma prawo do korzystania z Europejskiego portfela cyfrowej tożsamości, co sprawia, że jest on dostępny i akceptowalny dla szerokiego spektrum użytkowników w całej Unii Europejskiej.

7. **Różne rodzaje identyfikacji**

   Obsługa różnych rodzajów dokumentów identyfikacji, np. paszporty, dowody osobiste, karty pobytu. Europejskie portfele cyfrowej tożsamości będą obsługiwać różne rodzaje dokumentów identyfikacyjnych, co umożliwi użytkownikom korzystanie z różnych form identyfikacji w jednym, spójnym rozwiązaniu cyfrowej tożsamości.

8. **Potencjał**

   EDIW ma potencjał do rozwijania się i integrowania z różnymi usługami cyfrowymi, zarówno tymi na poziomie krajowym, jak i europejskim. Taka cecha może przyczynić się do ułatwienia korzystania z różnych usług online i zwiększenia efektywności procesów administracyjnych w całej Unii Europejskiej.

9. **Dostępność – offline i online**

   Wszystkie europejskie portfele tożsamości cyfrowej powinny umożliwiać użytkownikom elektroniczne identyfikowanie się i uwierzytelnianie online oraz offline w kontekście transgranicznym na potrzeby dostępu do szerokiego zakresu usług publicznych i prywatnych.

Architektura referencyjna europejskiego portfela cyfrowej tożsamości

Koncepcja architektury referencyjnej portfela opiera się na różnorodnych elementach, które współtworzą ekosystem cyfrowej tożsamości w Unii Europejskiej. Na podstawie załączonego dokumentu „European Digital Identity Wallet Architecture and Reference Framework[12]".

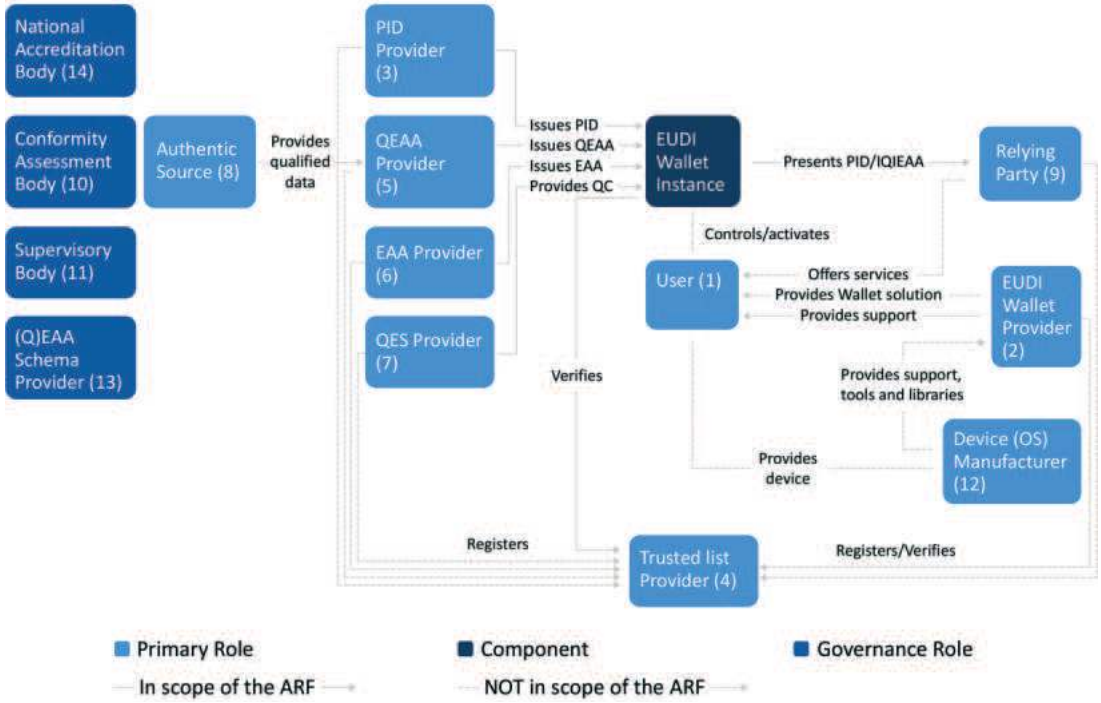
Dokument architektury referencyjnej został opracowany przez grupę ekspertów delegowanych przez państwa członkowskie do pracy nad dokumentem – tzw. eIDAS Expert Group. Prezentowany w niniejszym opracowaniu dokument ARF 1.3 nie jest ostateczną wersją architektury, która w procesie wdrażania portfela będzie ulegała rozszerzeniu i uzupełnieniu.

Architektura referencyjna portfela tożsamości cyfrowej definiuje wiele różnych ról uczestników ekosystemu, w tym użytkowników portfeli EUDI, dostawców portfeli EUDI, dostawców danych identyfikacyjnych osób (PID), dostawców zaufanych list, dostawców kwalifikowanych i niekwalifikowanych elektronicznych poświadczeń atrybutów, a także zaufane źródła i strony polegające (Relying Parties). Każda z tych ról ma swoje zadania i odpowiedzialności, co zapewnia kompleksową i zintegrowaną strukturę zarządzania tożsamością cyfrową.

Architektura określa cykl życia portfela EUDI, począwszy od instalacji instancji portfela przez użytkownika, poprzez aktywację i zarządzanie instancją portfela, aż po jej ewentualne wycofanie. Każdy etap cyklu życia jest ściśle zdefiniowany, wraz z wymaganiami dotyczącymi zaufania i bezpieczeństwa.

Określono również model danych, który zarządza różnymi rodzajami poświadczeń w ekosystemie EUDI, w tym danymi identyfikacyjnymi osób (PID),

[12] The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework v. 1.3 (02.2024)



Rysunek 11. Role w Europejskim Portfelu Cyfrowej Tożsamości
Źródło: ARF 1.3

kwalifikowanymi i niekwalifikowanymi elektronicznymi poświadczeniami atrybutów (QEAAs i EAAs). Model danych opisuje formaty, wymagania i procesy związane z wydawaniem, zarządzaniem i weryfikacją tych poświadczeń.

ARF ma na celu ułatwienie tworzenia interoperacyjnych i zdecentralizowanych ekosystemów cyfrowej tożsamości, w których użytkownicy mają kontrolę nad swoimi danymi osobowymi, a jednocześnie są spełniane wymogi dotyczące bezpieczeństwa, prywatności i ochrony danych. Jest to jedna z inicjatyw na poziomie Unii Europejskiej mających na celu rozwijanie i promowanie zaawansowanych rozwiązań cyfrowej tożsamości w Europie. W związku z powyższym, architektura referencyjna określiła interfejsy API, które umożliwiają komunikację i wymianę danych między różnymi rozwiązaniami cyfrowej tożsamości, z uwzględnieniem różnych uczestników tej komunikacji.

Architektura zawiera szczegółowy model zaufania, który określa, jakie relacje zaufania muszą istnieć między różnymi stronami w ekosystemie w różnych etapach cyklu życia portfela EUDI oraz poświadczeń. Model zaufania obejmuje zarówno aspekty autentykacji, jak i autoryzacji, co jest kluczowe dla bezpieczeństwa i prywatności w całym ekosystemie.

Dokument zawiera również specyfikacje dla rozwiązań portfeli EUDI, w tym uwagi dotyczące projektowania, komponenty architektury, logikę architektury, rodzaje przepływów danych, uwierzytelnianie i autoryzację stron polegających, a także procesy zatwierdzania przez użytkownika. Te wymagania zapewniają, że wszystkie rozwiązania portfeli EUDI będą interoperacyjne, bezpieczne i zgodne z założeniami Unii Europejskiej dotyczącymi cyfrowej tożsamości.

Zgodnie z założeniami Komisji Europejskiej architektura referencyjna EUDI Wallet stanowi kompleksowy zbiór zasad i wymagań, które mają na celu zapewnienie interoperacyjności, bezpieczeństwa i prywatności w zarządzaniu cyfrową tożsamością w Unii Europejskiej. Dokument szczegółowo opisuje różne aspekty ekosystemu, od ról uczestników, przez cykl życia portfela i model danych, po model zaufania i wymagania techniczne, tworząc solidną podstawę dla implementacji i dalszego rozwoju Europejskiej Tożsamości Cyfrowej.

1.1.5. Koncepcja rozproszenia zasobów informacyjnych dla określania tożsamości cyfrowej

W rozdziale 1.1.2 opisano modele cyfrowej tożsamości: centralny, federacyjny i zdecentralizowany. Każdy z tych modeli powstawał w zakresie potrzeb definiowanych przez użytkowników systemów oraz w granicach rozwoju technologii. Analiza każdego z tych modeli wskazuje cechy stosowania każdego z nich przedstawione w poniższej tabeli:

Cecha	Scentralizowany	Federacyjny	Zdecentralizowany
Rejestracja użytkownika	W każdym systemie osobna	Jednorazowa	Jednorazowa
Łączność	W ramach pojedynczego systemu	Pomiędzy systemami	Do celów weryfikacji
Dostępność offline	Tak	Nie	Tak
Możliwość śledzenia	W ramach pojedynczego systemu	Tak na poziomie węzłów	Ograniczona lub niemożliwa
Zależność od dostawcy usługi	Dostawca systemu definiuje zakres danych	Dostawca tożsamości definiuje zakres danych	Niezależna
Zarządzanie danymi	Dostawca systemu	Dostawca tożsamości	Właściciel danych

Analiza wyżej wymienionych cech modeli wskazuje na bardzo dużą elastyczność, bezpieczeństwo i możliwość zastosowania systemów zdecentralizowanych. Większość budowanych na świecie rozwiązań zdecentralizowanych jest opartych o możliwości wykorzystania rozproszonego rejestru i w niniejszym raporcie wskażemy kilka głównych rozwiązań.

Budowa zdecentralizowanych[13] systemów tożsamości cyfrowej opiera się na kilku kluczowych technologiach i koncepcjach, które umożliwiają bezpieczne zarządzanie i weryfikację tożsamości bez konieczności polegania na scentralizowanych autorytetach.

Technologia blockchain jest fundamentem wielu systemów zdecentralizowanej tożsamości, zapewniających bezpieczny i niezmienny rejestr, w którym przechowywane i weryfikowane są zdecentralizowane identyfikatory (DIDs) oraz rejestrowane weryfikowalne poświadczenia. Same weryfikowalne poświadczenia zazwyczaj nie wymagają przechowywania w sieciach blockchain ze względu na ew. ujawnienie danych w nich się znajdujących. Przechowywanie weryfikowalnych poświadczeń jest realizowane w portfelach cyfrowej tożsamości opisanych w rozdziale Portfele cyfrowej tożsamości.

Kolejną technologię stosowaną na potrzeby rozproszonej tożsamości stanowią zdecentralizowane identyfikatory[14] [15] (DIDs). DID to unikalne, trwałe identyfikatory, które pozwalają osobom fizycznym udowodnić swoją tożsamość w Internecie bez polegania na centralnym autorytecie. DIDs są przechowywane w blockchainie, co zapewnia ich niezmienność i publiczną weryfikację, umożliwiając jednostkom pełną kontrolę nad ich informacjami.

Weryfikowalne poświadczenia są wydawane przez zaufane podmioty (takie jak rządy lub instytucje edukacyjne) i kryptograficznie powiązane z DID danej osoby, potwierdzające pewne atrybuty, takie jak imię, wiek lub kwalifikacje. Opis weryfikowalnych poświadczeń został zawarty w rozdziale 1.1.3.

Równolegle z wykorzystanie technologii blockchain rozproszona tożsamość może być oparta o infrastrukturę klucza publicznego (PKI), która służy do generowania kluczy kryptograficznych i wydawania certyfikatów potwierdzających przywiązanie klucza do podmiotu lub osoby. Klucze zabezpieczają komunikację między podmiotami w sieci blockchain, a także mogą stanowić zabezpieczenie weryfikowalnych identyfikatorów. Ta infrastruktura wspiera tworzenie bezpiecznych cyfrowych tożsamości przez uwierzytelnianie tożsamości użytkowników i zapewnienie integralności transakcji.

[13] https://www.okta.com/identity-101/what-is-decentralized-identity/

[14] https://ethereum.org/en/decentralized-identity

[15] https://www.identity.com/decentralized-identity/

Rozproszona tożsamość może wykorzystywać dowody o zerowej wiedzy[16], czyli metody kryptograficzne pozwalające osobom na udowodnienie posiadania potwierdzeń i informacji bez ujawniania samych informacji, co dodatkowo zwiększa prywatność i bezpieczeństwo w procesie weryfikacji cyfrowej tożsamości.

W oparciu o wyżej wymienione technologie powstały rozwiązania ramowe pozwalające na ich implementację, rozwiązania te są cały czas rozwijane i stanowią podstawę wielu inicjatyw technologicznych:

- Hyperledger Indy[17] to otwarta platforma od Linux Foundation, wspierająca zarządzanie cyfrowymi tożsamościami poprzez funkcje takie jak rejestrowanie, przechowywanie danych, zarządzanie kluczami i weryfikację. Wykorzystuje ona zdecentralizowane identyfikatory (DID) i weryfikowalne poświadczenia (VC), kluczowe dla modelu nSSI.

- Sovrin Network[18], został zbudowany w oparciu o ramy i technologię Hyperledger Indy, to publiczny blockchain służący zarządzaniu tożsamością cyfrową z możliwością tworzenia i zarządzania DIDs oraz VC.

- DIDcomm[19] jest oparty o rozwiązania powstałe w ramach projektu Hyperledger Aries[20], jest to protokół umożliwiający bezpieczną komunikację w ekosystemie SSI, wykorzystujący DIDs do identyfikacji i wymiany VC.

W oparciu o wyżej wymienione technologie utworzono inicjatywę EBSI[21], czyli European Blockchain Services Infrastrukture, to inicjatywa Unii Europejskiej mająca na celu wspieranie integracji transgranicznej cyfrowych usług publicznych. Wykorzystuje technologię blockchain do zapewnienia wysokiego poziomu bezpieczeństwa, przejrzystości oraz odporności na zmiany w procesach cyfrowych. EBSI jest kluczowym elementem strategii cyfryzacji UE i ma za zadanie umożliwić wydajną, bezpieczną i zharmonizowaną wymianę danych między państwami członkowskimi.

Budowa EBSI jest oparta o sieć rozproszonych węzłów blockchain na terenie Europy. Jest to pierwsza infrastruktura blockchain na skalę UE, prowadzona przez sektor publiczny, z pełnym poszanowaniem europejskich wartości i przepisów. Węzły EBSI obsługują wiele protokołów (protokoły wymienne) i pełny zestaw interfejsów API. Głównym obecnie obsługiwanym protokołem jest Hyperledger Besu (z konsensusem IBFT 2.0)[22].

Jednym z głównych obszarów zastosowania EBSI jest budowa cyfrowej tożsamości. Dzięki wykorzystaniu technologii blockchain, EBSI umożliwia tworzenie i zarządzanie cyfrowymi tożsamościami, które są nie tylko bezpieczne, ale również łatwe w użyciu i uniwersalnie akceptowane w całej Unii Europejskiej. Cyfrowa tożsamość w ramach EBSI zapewnia użytkownikom kontrolę nad ich danymi osobowymi, umożliwiając im decydowanie, które informacje są udostępniane i komu.

1.1.6. Porównanie planowanych rozwiązań europejskich w stosunku do wybranych rozwiązań światowych

Dynamicznie rozwijające się technologie i ciągłe zmiany w globalnych usługach nie pozostają bez odpowiedzi technologicznych i prawnych. Różne kraje podejmują inicjatywy na rzecz ułatwienia zarządzania tożsamością cyfrową swoich obywateli, nawet pomimo zróżnicowania lokalnych legislacji można zauważyć wiele podobieństw podejmowanych rozwiązań. Poniżej w ujęciu tabelarycznym przedstawiono opisy zebranych inicjatyw europejskich i światowych.

[16] ETSI TR 119 476 V1.1.1 (2023-08) – Electronic Signatures and Infrastructures (ESI); Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes

[17] https://training.linuxfoundation.org/training/introduction-to-hyperledger-sovereign-identity-blockchain-solutions-indy-aries-and-ursa/

[18] https://sovrin.org

[19] https://didcomm.org

[20] https://www.hyperledger.org/projects/aries

[21] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home

[22] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/QAs?option=659622446 (EBSI FAQ Dostęp 16.03.2024)

Rozwiązanie Kraj	Opis
mObywatel Polska	mObywatel 2.0, dostępny bezpłatnie na smartfony, jest cyfrowym asystentem obywatela ułatwiającym załatwianie spraw urzędowych. Umożliwia przechowywanie dokumentów, szybkie realizowanie formalności urzędowych oraz oszczędność czasu i pieniędzy. mObywatel oferuje również mDowód, który zastępuje tradycyjny dowód osobisty w większości sytuacji codziennych, z wyjątkiem m.in. przekraczania granic kraju i załatwiania spraw w bankach. Aplikacja wprowadza nową jakość usług cyfrowych, zapewniając dostęp do e-skrzynek pocztowych i informacji o pojazdach oraz uprawnieniach kierowcy[23]. https://www.gov.pl/web/mobywatel
Verified.Me Kanada	Opracowany przez SecureKey Technologies Inc., to nowoczesny i bezpieczny sposób na weryfikację cyfrowej tożsamości, ułatwiający szybki dostęp do potrzebnych usług i produktów online, osobiście oraz telefonicznie. Jest to wygodne i bezpieczne rozwiązanie dla Kanadyjczyków, pozwalające na weryfikację ich cyfrowych tożsamości. https://www.interac.ca/
Connect.Me USA	Connect.Me to pierwszy portfel cyfrowy oparty na technologii Sovrin, który umożliwia użytkownikom tworzenie prywatnych, kryptograficznych połączeń, gromadzenie cyfrowych poświadczeń i prezentowanie dowodów cyfrowych w sposób prywatny i bezpieczny. Pozwala również na bezpieczne przechowywanie kopii zapasowych portfela cyfrowego oraz odpowiadanie na bezpieczne wiadomości od dowolnego połączenia. Wczesnymi użytkownikami aplikacji są platformy takie jak Truu i CULedger. Connect.Me obejmuje integrację z firmą weryfikującą tożsamość, Onfido, umożliwiając użytkownikom weryfikację tożsamości za pomocą fizycznych poświadczeń i uzyskanie cyfrowego poświadczenia wykorzystywanego w ekosystemie Sovrin . https://www.evernym.com/
Lissi Niemcy	Portfel Lissi to innowacyjne narzędzie umożliwiające zarządzanie cyfrowymi poświadczeniami i tożsamością w bezpieczny sposób. Stworzony przez startup Lissi GmbH, który wykluł się w ramach jednostki innowacji Commerzbank AG – neosfer, portfel ten bazuje na standardach globalnych, takich jak Verifiable Credentials i OpenID, aby wspierać bezpieczne interakcje między organizacjami a ich klientami na całym cyklu życia klienta. Użytkownicy mogą otrzymywać cyfrowe certyfikaty, karty członkowskie, przepustki pracownicze, licencje itp., przechowywać i zarządzać nimi, a następnie prezentować na żądanie, aby uzyskać dostęp do usług cyfrowych. Portfel Lissi umożliwia również nawiązywanie zaufanych połączeń z organizacjami oraz odbieranie wiadomości z zewnętrznych usług bez użycia haseł. https://www.lissi.id/
Trinsic USA	Portfel Trinsic to cyfrowy portfel tożsamości samodzielnej (SSI), który umożliwia użytkownikom odbieranie, przechowywanie i udostępnianie cyfrowych poświadczeń. Jest to pierwszy portfel SSI, który udowodnił interoperacyjność i stał się jednym z najczęściej używanych portfeli SSI na świecie. Portfel ten jest łatwy w użyciu dla użytkowników końcowych, a jednocześnie oferuje zaawansowane funkcjonalności dla programistów dzięki integracji z API Trinsic i Trinsic Studio. https://trinsic.id
Aadhaar Indie	System identyfikacji biometrycznej z Indii, który zapewnia unikalny 12-cyfrowy numer identyfikacyjny mieszkańcom. Jest to największa na świecie baza danych biometrycznych, umożliwiająca identyfikację osób na podstawie danych biometrycznych i demograficznych. Aadhaar służy jako narzędzie do usprawnienia dostępu do usług rządowych, finansowych i innych, poprawiając efektywność i ograniczając oszustwa. https://www.uidai.gov.in/en/
SingPass Singapur	SingPass to system zarządzania tożsamością w Singapurze, który umożliwia mieszkańcom dostęp do różnych usług rządowych (i nie tylko) online. Użytkownicy mogą za jego pomocą bezpiecznie logować się do ponad 60 usług cyfrowych rządu. SingPass oferuje również możliwość weryfikacji tożsamości za pomocą biometrii, co zwiększa bezpieczeństwo i wygodę użytkowania. https://www.singpass.gov.sg/main/

[23] https://www.gov.pl/web/mobywatel

Rozwiązanie Kraj	Opis
ID.me USA	Platforma zarządzania tożsamością w USA, która umożliwia użytkownikom bezpieczne potwierdzenie swojej tożsamości online, a także dostęp do usług rządowych, zdrowotnych i handlowych. Zapewnia jednolite logowanie i silne uwierzytelnianie dla różnych usług, ułatwiając dostęp do nich bez potrzeby wielokrotnego potwierdzania tożsamości. https://www.id.me
SPID Włochy	SPID, czyli Sistema Pubblico di Identità Digitale, to włoski system zarządzania tożsamością cyfrową, który umożliwia obywatelom i przedsiębiorstwom dostęp do usług online świadczonych przez administrację publiczną za pomocą jednolitego systemu uwierzytelniania. Użytkownicy mogą za jego pośrednictwem bezpiecznie korzystać z różnych usług cyfrowych, korzystając z jednego loginu i hasła. Więcej informacji o SPID znajdziesz na stronie włoskiego rządu. https://www.spid.gov.it/en/
Itsme Belgia	Belgijska aplikacja umożliwiająca bezpieczne logowanie, potwierdzanie transakcji i podpisywanie dokumentów cyfrowych za pomocą telefonu komórkowego. Użytkownicy mogą za jej pomocą korzystać z różnych usług online, oferowanych przez instytucje publiczne, banki oraz inne firmy, ciesząc się jednocześnie wysokim poziomem bezpieczeństwa. Więcej informacji o itsme® znajdziesz na ich oficjalnej stronie internetowej. https://www.itsme-id.com/en-BE
Smart-ID Estonia	Popularne w Estonii rozwiązanie do bezpiecznej autoryzacji i podpisywania cyfrowego, umożliwiające użytkownikom łatwy dostęp do różnych usług elektronicznych. Używa ono zaawansowanych technologii, aby zapewnić wygodę i bezpieczeństwo w cyfrowym świecie. Więcej informacji znajdziesz na oficjalnej stronie Smart-ID. https://www.smart-id.com

1.2. Stopień zaawansowania prac nad koncepcją tożsamości cyfrowej

Rozporządzenie eIDAS[24] (Electronic Identification, Authentication and Trust Services) stanowi kluczowe ramy prawne dla usług identyfikacji elektronicznej i zaufania w Unii Europejskiej. W lutym 2024 Parlament Europejski przyjął rewizję tego rozporządzenia (tzw. eIDAS 2.0), mającą na celu dostosowanie go do szybko zmieniającego się krajobrazu cyfrowego. Nowelizacja ta skupia się na zwiększeniu interoperacyjności, wzmocnieniu zaufania oraz rozszerzeniu zastosowania eIDAS na sektor prywatny. Wprowadzenie obowiązkowych cyfrowych portfeli tożsamości dla obywateli UE stanowi jeden z kluczowych elementów tej rewizji, mający na celu ułatwienie dostępu do różnorodnych usług cyfrowych oraz poprawę ochrony prywatności użytkowników.

1.2.1. Regulacje obowiązujące

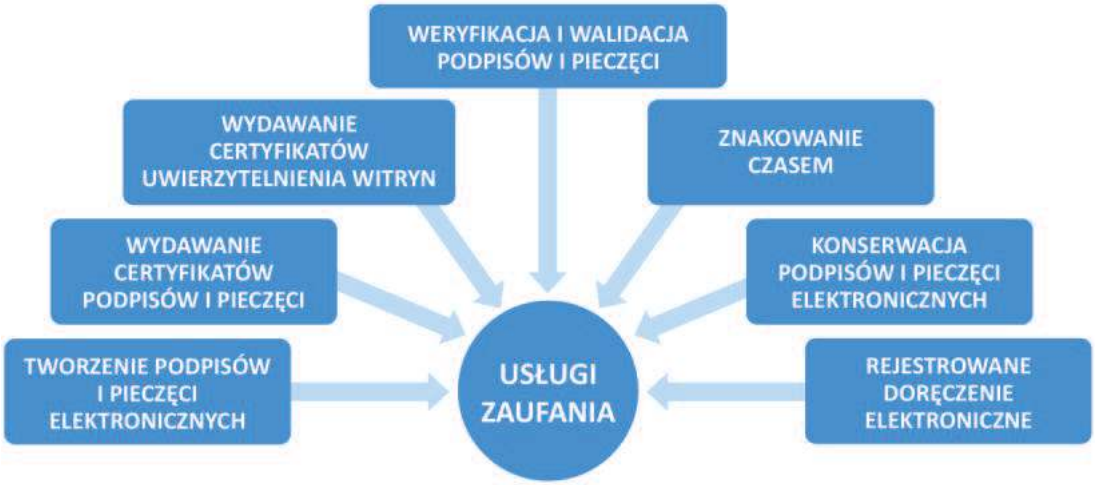
eIDAS to regulacja Unii Europejskiej, która została wprowadzona w 2014 roku w celu stworzenia jednolitego ramienia prawno-technicznego dla elektronicznej identyfikacji i usług związanych z zaufaniem w ramach państw członkowskich UE. Celem eIDAS jest ułatwienie korzystania z usług elektronicznych na terenie Unii Europejskiej, zwiększenie bezpieczeństwa cyfrowego oraz wspieranie rozwoju jednolitego rynku cyfrowego.

Regulacja eIDAS określa standardy i zasady dotyczące elektronicznej identyfikacji, uwierzytelniania i usług związanych z zaufaniem, takich jak elektroniczne podpisy, pieczęcie, certyfikaty cyfrowe, usługi doręczania elektronicznego, oraz usługi znakowania czasem. eIDAS wprowadza również zasady uznawania i interoperacyjności usług cyfrowych między państwami członkowskimi UE, co umożliwia korzystanie z tych usług w ramach wymiany dokumentów transgranicznie. eIDAS ma na celu zapewnienie zaufania i bezpieczeństwa w elektronicznych transakcjach na terenie Unii Europejskiej, promowanie innowacji w obszarze usług cyfrowych oraz ułatwienie korzystania z usług elektronicznych dla obywateli, przedsiębiorstw i instytucji publicznych w Europie. Podstawowym zakresem

[24] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

regulacji eIDAS jest funkcjonowanie systemów identyfikacji elektronicznej i usług zaufania.

Rozporządzenie eIDAS definiuje „usługi zaufania" jako elektroniczne usługi, które obejmują tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów dla tych usług. Obejmuje również tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych oraz konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami. Rozporządzenie eIDAS wprowadza w życie proces elektronizacji, oferując framework dla podpisów i pieczęci elektronicznych, które pełnią funkcje analogiczne do tradycyjnych odpowiedników na papierze. W szczególności, kwalifikowane podpisy elektroniczne mają moc zastępowania podpisów własnoręcznych, a pieczęcie elektroniczne służą do potwierdzania autentyczności i integralności dokumentów elektronicznych.



Rysunek 12. Usługi zaufania zgodnie z rozporządzeniem eIDAS

Rozporządzenie to wprowadza rozróżnienie pomiędzy identyfikacją elektroniczną a usługami zaufania, z których każdy z obszarów podlega odrębnym modelom regulacyjnym w UE. Identyfikacja elektroniczna skupia się na przekazywaniu informacji o tożsamości użytkownika usługom online, gdzie głównym źródłem tożsamości są informacje zbierane i udostępniane przez kraje członkowskie UE. W zakresie identyfikacji elektronicznej, jej kształtowania na rynku wewnętrznym, kraje członkowskie mają dużą autonomię, pod warunkiem przypisania zunifikowanego modelu wiarygodności.

Usługi zaufania są zdefiniowane jako te, które zazwyczaj świadczone są za wynagrodzeniem i obejmują tworzenie, weryfikację, i walidację podpisów elektronicznych, pieczęci elektronicznych, znaczników czasu, dowodów wysyłania i otrzymania przesyłek za pomocą przesyłek doręczenia elektronicznego oraz raportów z walidacji podpisu elektronicznego. Co do zasady, takie zdefiniowanie usług zaufania z założenia ma pozwolić na funkcjonowanie konkurującego między sobą rynku dostawców tych usług, pozwolić na wybór usług najlepiej dostosowanych do potrzeb biznesowych. Jednocześnie dostawcy usług zaufania podlegają nadzorowi krajów członkowskich UE, w których mają siedzibę.

Rozporządzenie eIDAS działa bezpośrednio i nie wymaga dodatkowej implementacji przez ustawę krajową, choć w Polsce funkcję tę realizuje Ustawa o usługach zaufania i identyfikacji elektronicznej, która wprowadziła dodatkowe przepisy, regulujące nadzór nad dostawcami usług zaufania i identyfikacji elektronicznej. Identyfikacja elektroniczna jako proces potwierdzania tożsamości za pomocą środków elektronicznych, umożliwia użytkownikom bezpieczne korzystanie z usług online. W Polsce, systemy takie jak Profil Zaufany czy bankowe środki identyfikacji elektronicznej, zapewniają dostęp do usług publicznych i komercyjnych. Podpis elektroniczny, definiowany jako dane elektroniczne służące jako podpis, umożliwia składanie oświadczeń woli w formie dokumentowej, a jego kwalifikowana postać w formie elektronicznej na podstwie m.in art. 78(2) k.c. Jego bezpieczeństwo gwarantowane jest przez dostawców usług zaufania, którzy podlegają rygorystycznym wymogom bezpieczeństwa i nadzorowi.

Zaawansowane i kwalifikowane podpisy elektroniczne stanowią specjalne kategorie podpisów elektronicznych, które spełniają dodatkowe wymogi, takie jak unikalne przyporządkowanie do podpisującego oraz możliwość jednoznacznej weryfikacji tożsamości podpisującego. Kwalifikowane podpisy elektroniczne, oparte na kwalifikowanym certyfikacie i urządzeniu do składania podpisu, są prawnie równoważne podpisom własnoręcznym. Kwalifikowane urządzenia do składania podpisu elektronicznego, takie jak karty kryptograficzne lub usługi sieciowe, zapewniają bezpieczne i kontrolowane przez podpisującego środowisko do składania podpisów. Karty te nie mogą być współdzielone między pracownikami ani oddawane pracodawcy, co zapewnia ich wyłączną kontrolę przez podpisującego. Kwalifikowane certyfikaty podpisu elektronicznego są wydawane przez dostawców usług zaufania po dokładnej weryfikacji tożsamości podpisującego. Certyfikaty te są jawne i dołączane do każdego podpisanego dokumentu, umożliwiają weryfikację złożonych podpisów elektronicznych.

Rozporządzenie eIDAS wprowadziło także zasady funkcjonowania usługi zaufania rejestrowanego doręczenia elektronicznego. Doręczenie elektroniczne stanowi przekazanie dokumentów lub danych w postaci elektronicznej pomiędzy stronami trzecimi w sposób bezpieczny, zapewniający identyfikację stron oraz dowody nadania oraz doręczenia. Rejestrowane doręczenie elektroniczne zastępuje listy polecone a dowody z doręczenia są odpowiednikami potwierdzenia nadania i doręczenia poleconej korespondencji. Kwalifikowana usługa rejestrowanego doręczenia elektronicznego dostarcza dowody zapewniające domniemania prawne nadania i doręczenia. W Polsce dodatkowo ustawą z 18 listopada o doręczeniach elektronicznych[25] wprowadzono krajowy system doręczeń elektronicznych, w ramach którego do końca 2024 roku wszystkie podmioty publiczne oraz spółki prawa handlowego będą obowiązkowo przyjmowały korespondencje za pomocą doręczeń elektronicznych.

Rozporządzenie ustanowiło ramy prawne do stosowania także usługi znakowania czasem zapewniającej integralność dokumentu lub danych w postaci elektronicznej od momentu ich oznaczenia datą i godziną. Znakowanie czasem stanowi dowód, że w momencie oznakowania treść istniała i nie zmieniła się po oznakowaniu. Poza znakowaniem czasem zdefiniowano szereg usług wspierających tj. usługi walidacji i konserwacji podpisów i pieczęci elektronicznej, które zapewniają właściwe rozpoznanie podpisów i pieczęci elektronicznej oraz zabezpieczenie ich wiarygodności dowodowej w długim czasie.

[25] Dz.U. 2020 poz. 2320

1.2.2. Nowe regulacje

Zrealizowany w latach 2012-2021 przegląd rozporządzenia eIDAS miał na celu poprawę jego skuteczności, rozszerzenie korzyści na sektor prywatny oraz promowanie zaufanych tożsamości cyfrowych dla wszystkich Europejczyków. Komisja Europejska zauważyła brak pełnej harmonizacji w ramach eIDAS, co utrudniło współpracę między systemami eID różnych krajów oraz usługami zaufania. To ograniczyło możliwość pełnej interoperacyjności, a eIDAS nie doprowadził do oczekiwanego poziomu rozpowszechnienia elektronicznych tożsamości i usług zaufania na jednolitym rynku UE, szczególnie w sektorach prywatnym i publicznym, co ograniczyło jego efektywność. Dodatkowo, sektor prywatny nie został w pełni zaangażowany w rozwijanie i korzystanie z usług zaufania, co wpłynęło na integrację cyfrową gospodarki. Wreszcie, procedury certyfikacji usług zaufania nie zostały wystarczająco uproszczone i ujednolicone, co mogło zniechęcać do ich wdrażania i używania.

Komisja Europejska przedstawiła projekt nowelizacji rozporządzenia eIDAS w oparciu o wyniki oceny funkcjonowania obecnego rozporządzenia, identyfikując kluczowe obszary do ulepszenia, takie jak harmonizacja, interoperacyjność, zaangażowanie sektora prywatnego i procedury certyfikacji. Te wyzwania skłoniły do zaproponowania eIDAS 2.0, mającego na celu wzmocnienie systemu cyfrowej tożsamości i usług zaufania w UE. Na podstawie preambuły sprawie wniosku[26] dotyczącego rozporządzenia zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej, podjęto szereg inicjatyw mających na celu zmianę zasad funkcjonowania cyfrowej tożsamości w UE poprzez następujące inicjatywy.

Opracowanie Ogólnounijnych Ram Bezpiecznej Publicznej Identyfikacji Elektronicznej, które mają na celu stworzenie systemu interpretacyjnych podpisów cyfrowych, aby zapewnić obywatelom kontrolę nad ich tożsamością i danymi w Internecie oraz umożliwić dostęp do publicznych, prywatnych i transgranicznych usług cyfrowych. Zapewnienie do 2030 wprowadzenia na szeroką skalę zaufanej tożsamości cyfrowej opartej o Europejski Portfel Tożsamości Cyfrowej, który byłby uznawany w całej Unii i umożliwiał kontrolowanie swoich danych w interakcjach online.

[26] Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 29 lutego 2024 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Zmniejszenie barier cyfrowych i ułatwienie dostępu poprzez zharmonizowane ramy tożsamości cyfrowej mają na celu zmniejszenie barier cyfrowych między państwami członkowskimi, umożliwiając obywatelom i rezydentom Unii korzystanie z cyfryzacji przy jednoczesnym zwiększeniu przejrzystości i ochrony ich praw. Wzmocnienie Rynku Wewnętrznego dzięki zharmonizowanemu podejściu do identyfikacji elektronicznej ma na celu wzmocnienie rynku wewnętrznego poprzez ułatwienie identyfikacji i uwierzytelniania tożsamości online i offline w bezpieczny, godny zaufania i wygodny sposób. Promowanie zaufanych, bezpiecznych i innowacyjnych rozwiązań dzięki jednolitemu systemowi notyfikacji systemów identyfikacji elektronicznej ma zostać uproszczone i przyspieszone, aby promować dostęp do wygodnych, zaufanych, bezpiecznych i innowacyjnych rozwiązań w zakresie uwierzytelniania i identyfikacji.

Te inicjatywy są częścią szerszego wysiłku na rzecz modernizacji i unifikacji cyfrowej tożsamości w Unii Europejskiej, mającego na celu zwiększenie bezpieczeństwa, zaufania i wygody dla obywateli i przedsiębiorstw w całej UE. Komisja Europejska wytyczyła cele na cyfrową dekadę do roku 2030, stawiając na rozwój umiejętności cyfrowych obywateli, transformację cyfrową przedsiębiorstw, a także budowę bezpiecznej i zrównoważonej infrastruktury cyfrowej. Wizja ta zakłada, że co najmniej 80% Europejczyków będzie posiadać podstawowe umiejętności cyfrowe, a 75% przedsiębiorstw będzie korzystać z chmury, AI lub dużych zbiorów danych, podnosząc tym samym konkurencyjność europejskiej gospodarki. Ponadto, dążenie do podwojenia udziału UE w światowej produkcji najlepszej jakości półprzewodników oraz zapewnienie gigabitowej łączności dla każdego to tylko niektóre z wyznaczonych celów mających na celu stworzenie solidnej podstawy dla europejskiej przyszłości cyfrowej.

Program „Droga ku cyfrowej dekadzie”[27] wprowadza systematyczny roczny cykl współpracy między państwami członkowskimi a Komisją Europejską, by wspólnie realizować postanowienia strategii. Dzięki ustrukturyzowanemu systemowi monitorowania, bazującemu na indeksie gospodarki cyfrowej i społeczeństwa cyfrowego (DESI), oraz corocznym sprawozdaniom oceniającym postępy, Unia Europejska dąży do utrzymania dynamiki zmian i identyfikacji ewentualnych wyzwań na drodze do realizacji cyfrowych aspiracji.

Projekty z udziałem różnych krajów, stanowiące część inicjatywy, mają na celu przyspieszenie realizacji transgranicznych inwestycji, zwiększenie interoperacyjności i bezpieczeństwa cyfrowego jednolitego rynku. Wspieranie innowacji poprzez projekty takie jak rozwój procesorów o niskim poborze mocy, rozwój łączności 5G czy bezpieczna komunikacja kwantowa, ma kluczowe znaczenie dla osiągnięcia wizji zrównoważonej i inkluzywnej przyszłości cyfrowej, której podstawą są solidne fundamenty technologiczne i zaangażowanie wszystkich państw członkowskich.

Rozporządzenie eIDAS 2.0 stanowi kluczowy element strategii Unii Europejskiej mającej na celu zapewnienie pełnej harmonizacji zasad i warunków stosowania usług zaufania w państwach członkowskich, co umożliwi pełną interoperacyjność pomiędzy krajowymi systemami identyfikacji elektronicznej (eID) oraz usługami zaufania. Ma to na celu ułatwienie realizacji transgranicznych transakcji cyfrowych zarówno w sektorze publicznym, jak i prywatnym, poprzez zwiększenie interoperacyjności. Dąży również do zaangażowania sektora prywatnego w większym stopniu w rozwój i wykorzystanie usług zaufania, co przyczyni się do przyspieszenia adopcji cyfrowych tożsamości i usług zaufania.

Dodatkowo, nowelizacja rozporządzenia koncentruje się na usprawnieniu procesów certyfikacji usług zaufania poprzez wprowadzenie jednolitych procedur certyfikacji, co ma na celu ułatwienie ich wdrożenia oraz zagwarantowanie wysokiego poziomu bezpieczeństwa i zaufania. Celem inicjatywy jest także zapewnienie odpowiedniego poziomu ochrony prywatności i bezpieczeństwa danych osobowych, zgodnie z obowiązującymi przepisami, takimi jak RODO.

W wyniku wprowadzenia rozporządzenia funkcjonować będą następujące usługi zaufania obejmujące katalog usług dotychczas objętych przepisami unijnymi oraz nowych usług:

- Tworzenie podpisów elektronicznych lub pieczęci elektronicznych: Usługa umożliwiająca użytkownikom tworzenie cyfrowych wersji ich własnoręcznych podpisów lub oficjalnych pieczęci organizacji, które są legalnie wiążące w środowisku cyfrowym.

- Walidacja podpisów elektronicznych lub pieczęci elektronicznych: Proces weryfikacji i potwierdzania ważności podpisów elektronicznych lub pieczęci elektronicznych, zapewniający, że podpis lub pieczęć nie zostały zmienione od momentu ich utworzenia.

- Konserwacja podpisów elektronicznych, pieczęci elektronicznych, certyfikatów podpisów elektronicznych lub certyfikatów pieczęci elektronicznych: Usługa polegająca na utrzymaniu ważności i integralności

[27] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pl#droga-ku-cyfrowej-dekadzie

powyższych elementów przez określony czas, nawet jeśli technologie lub standardy ulegną zmianie

- Zarządzanie urządzeniami do składania podpisu elektronicznego na odległość lub urządzeniami do składania pieczęci elektronicznej na odległość: Usługa umożliwiająca zdalne generowanie i zarządzanie podpisami lub pieczęciami elektronicznymi, bez konieczności fizycznej obecności podpisującego

- Wydawanie elektronicznych poświadczeń atrybutów: Proces wydawania cyfrowych dokumentów potwierdzających określone atrybuty lub uprawnienia osoby lub organizacji, takie jak tożsamość, kwalifikacje zawodowe czy uprawnienia do dostępu.

- Walidacja elektronicznych poświadczeń atrybutów: Proces sprawdzania i potwierdzania ważności elektronicznych poświadczeń atrybutów, zapewniający, że informacje są aktualne i niezmienione.

- Tworzenie elektronicznych znaczników czasu: Usługa polegająca na generowaniu dowodów cyfrowych potwierdzających dokładny czas wykonania określonych czynności cyfrowych lub stworzenia dokumentu cyfrowego.

- Walidacja elektronicznych znaczników czasu: Proces weryfikacji elektronicznych znaczników czasu, mający na celu potwierdzenie ich dokładności i ważności.

- Świadczenie usług rejestrowanego doręczenia elektronicznego: Usługi pozwalające na bezpieczne i potwierdzane doręczanie elektronicznych dokumentów lub wiadomości pomiędzy stronami, zapewniające dowód wysłania i odbioru.

- Walidacja danych przekazywanych za pośrednictwem usług rejestrowanego doręczenia elektronicznego i związanych z nimi dowodów: Proces sprawdzania ważności i integralności danych przesyłanych za pomocą rejestrowanego doręczenia elektronicznego oraz związanych z tym dowodów wysyłki i odbioru.

- Archiwizacja elektroniczna danych elektronicznych i dokumentów elektronicznych: Usługi związane z długoterminowym przechowywaniem danych elektronicznych i dokumentów elektronicznych w sposób zapewniający ich integralność, dostępność i odtwarzalność w przyszłości.

- Rejestrowanie danych elektronicznych w rejestrze elektronicznym: Usługi umożliwiające rejestrowanie i przechowywanie danych elektronicznych w dedykowanych rejestrach cyfrowych, zapewniających ich bezpieczeństwo, wiarygodność i łatwy dostęp.

Rysunek 13. Dotychczasowe i nowe usługi zaufania

Szczególne znaczenie dla rozwoju transakcji elektronicznych będą miały nowe usługi zaufania wydawania elektronicznych potwierdzeń atrybutów, które wraz z europejskim elektronicznym potwierdzeniem atrybutów umożliwią pobieranie i dostęp do różnego rodzaju poświadczeń dotyczących osób fizycznych, osób prawnych oraz obiektów. Jednocześnie wprowadzenie usługi archiwizacji danych i dokumentów

oraz usługi zapisu do elektronicznego rejestru będą miały bardzo duży wpływ na zmianę sposobu dostępu i zarządzania danymi w internecie.

1.2.3. Harmonogram wdrożenia

W dniu 29 lutego 2024 roku parlament Europejski przyjął w głosowaniu plenarnym nowelizację rozporządzenia eIDAS, natomiast ww. zmianę przejęła Rada Unii Europejskiej w dniu 26 marca 2024. Rozporządzenie wejdzie w życie 20 dni po jego publikacji.

W momencie wejścia w życie rozporządzenia eIDAS dostawcy usług zaufania będą mogli zacząć świadczyć usługi zgodnie z nowymi wymaganiami, jednakże pełne funkcjonowanie znowelizowanych przepisów będzie wymagało wprowadzenia aktów implementujących.

Poniższa tabela przedstawia rozporządzenia implementujące dotyczące usług zaufania, które będą wdrażane w kolejnych miesiącach po wejściu w życie rozporządzenia.

Artykuł rozporządzenia	Termin wdrożenia (miesiące)	Zakres aktu implementującego
art. 45c ust. 4	6	normy referencyjne, specyfikacje i procedury kwalifikowanego elektronicznego poświadczania atrybutów
art. 45d(2)	6	normy odniesienia, specyfikacje i procedury dotyczące katalogu atrybutów i schematów poświadczania atrybutów oraz procedur weryfikacji kwalifikowanych elektronicznych poświadczeń atrybutów
45da(6)	6	normy referencyjne, specyfikacje i procedury elektronicznego poświadczania atrybutów wydawane przez organ sektora publicznego odpowiedzialny za autentyczne źródło lub w jego imieniu
45da(7)	6	normy referencyjne, specyfikacje i procedury powiadamiania organów sektora publicznego odpowiedzialnych za autentyczne źródło
art. 19a ust. 2	12	normy referencyjne, specyfikacje i procedury dotyczące środków, o których mowa w art. 19a ust. 1 lit. a)
20(4)	12	normy referencyjne, specyfikacje i procedury akredytacji jednostek oceniających jednostkę, wymogi w zakresie audytu dla jednostek oceniających zgodność oraz systemy oceny zgodności
21(4)	12	formaty i procedury inicjowania kwalifikowanej usługi zaufania
art. 24 ust. 1a	12	normy referencyjne, specyfikacje techniczne i procedury weryfikacji tożsamości i atrybutów przy wydawaniu kwalifikowanego certyfikatu
24(5)	12	normy odniesienia, specyfikacje i procedury dotyczące wymogów, o których mowa w art. 24 ust. 2 lit. b)–h)
28(6)	12	normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanych certyfikatów podpisu elektronicznego
art. 29a ust. 2, 39a	12	normy referencyjne, specyfikacje techniczne i operacyjne dla zdalnych QSCD (kwalifikowanych urządzeń do składania podpisu i pieczęci)
31(3), 39(3)	12	formaty i procedury dotyczące wykazu certyfikowanych QSCD (kwalifikowanych urządzeń do składania podpisu i pieczęci)
32(3)	12	Normy referencyjne, specyfikacje i procedury walidacji kwalifikowanych podpisów elektronicznych
art. 32a ust. 3	12	Standardy referencyjne, specyfikacje i procedury walidacji zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach
33(2)	12	normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanej usługi walidacji

Artykuł rozporządzenia	Termin wdrożenia (miesiące)	Zakres aktu implementującego
34(3)	12	normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanej usługi przechowywania kwalifikowanych podpisów elektronicznych
38(6)	12	normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanych certyfikatów pieczęci elektronicznych
42(2)	12	normy referencyjne, specyfikacje i procedury dotyczące powiązania daty i czasu z danymi oraz dokładności źródeł czasu
44(2)	12	normy referencyjne, specyfikacje i procedury dotyczące procesów wysyłania i odbierania danych
45(3)	12	normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanych certyfikatów uwierzytelniania witryn internetowych
45ga(2)	12	normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanych usług archiwizacji elektronicznej
art. 45i(3)	12	normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanych rejestrów elektronicznych
art. 46a ust. 8	12	formaty i procedury sporządzania sprawozdania rocznego organu nadzorczego w ramach europejskiego instrumentu wymiany walut
art. 46b ust. 8	12	formaty i procedury sporządzania sprawozdania rocznego organu nadzorczego w zakresie usług zaufania
art. 46e ust. 7	12	ustalenia proceduralne dotyczące Europejskiej Grupy Współpracy ds. Tożsamości Cyfrowej
26(2)	24	referencyjne standardy, specyfikacje i procedury dotyczące zaawansowanych podpisów elektronicznych
36(2)	24	normy referencyjne, specyfikacje i procedury dotyczące zaawansowanych pieczęci elektronicznych

Największy wpływ na funkcjonowanie rynku finansowego będzie miało funkcjonowanie portfela cyfrowej tożsamości. Każde państwo członkowskie musi zapewnić co najmniej jeden europejski portfel tożsamości cyfrowej w terminie 24 miesięcy od dnia wejścia w życie aktów wykonawczych. Z kolei te akty wykonawcze powinny zostać opublikowane nie później niż 6 miesięcy od wejścia w życie rozporządzenia. W efekcie należy się spodziewać, że stosowne akty wykonawcze zostaną opublikowane do końca 2024 roku, natomiast państwa członkowskie będą zobligowane do wdrożenia portfeli zgodnych z tymi aktami implementującymi nie później niż do końca 2026 roku.

Na rynek finansowy największy wpływ ma zobowiązanie akceptacji portfela cyfrowej tożsamości przez wszystkie podmioty zobowiązane na podstawie prawa Unii lub prawa krajowego do stosowania silnego uwierzytelnienia użytkownika do celów identyfikacji elektronicznej lub w przypadku gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie zobowiązania umownego w ciągu 36 miesięcy od momentu wejścia w życie wyżej wymienionych aktów implementujących, tj. do końca 2027 roku.

Zalety rozwiązania europejskiego

2.1. Zalety logiczno-techniczne proponowanego rozwiązania

Przedstawienie przypadków użycia

W preambule w punkcie 11 znowelizowanej wersji eIDAS wskazano, że „europejskie portfele tożsamości cyfrowej powinny ułatwiać stosowanie zasady jednorazowości i tym samym zmniejszać obciążenie administracyjne oraz wspierać transgraniczną mobilność obywateli i rezydentów Unii oraz przedsiębiorstw w całej Unii, a także sprzyjać rozwojowi interoperacyjnych usług administracji elektronicznej w całej Unii", a z kolei w punkcie 7 jest mowa o bardziej zharmonizowanym podejściu do identyfikacji elektronicznej, które powinno zmniejszyć ryzyko i koszty wynikające z obecnej fragmentacji spowodowanej stosowaniem rozbieżnych rozwiązań krajowych lub – w niektórych państwach członkowskich – brakiem takich rozwiązań w zakresie identyfikacji elektronicznej. Takie podejście powinno wzmocnić rynek wewnętrzny, umożliwiając obywatelom i rezydentom Unii, określonym w prawie krajowym, oraz przedsiębiorstwom identyfikowanie się i uwierzytelnianie swojej tożsamości online i offline w sposób bezpieczny, godny zaufania, przyjazny dla użytkownika, wygodny, dostępny i zharmonizowany w całej Unii[28]. Przytoczenie zapisów z preambuły ma na celu zobrazowanie generalnych zalet proponowanego rozwiązania, a w dalszej części niniejszego rozdziału zostaną przedstawione przypadki użycia, które nie tylko są w fazie koncepcyjnej, ale także podlegają walidacji.

W ramach czterech wielkoskalowych pilotaży portfela cyfrowej tożsamości prowadzone są testy specyfikacji technicznej wspólnego zestawu narzędzi dla unijnego portfela tożsamości cyfrowej oraz prototypu oprogramowania[29]. Przed jego wprowadzeniem w państwach członkowskich unijny portfel tożsamości cyfrowej jest pilotowany w ramach czterech dużych projektów, które rozpoczęto w dniu 1 kwietnia 2023 r. Celem tych projektów jest przetestowanie cyfrowych portfeli tożsamości w rzeczywistych scenariuszach obejmujących różne sektory. Bierze w tym udział ponad 250 prywatnych przedsiębiorstw i organów publicznych z 25 państw członkowskich oraz Norwegii, Islandii i Ukrainy.

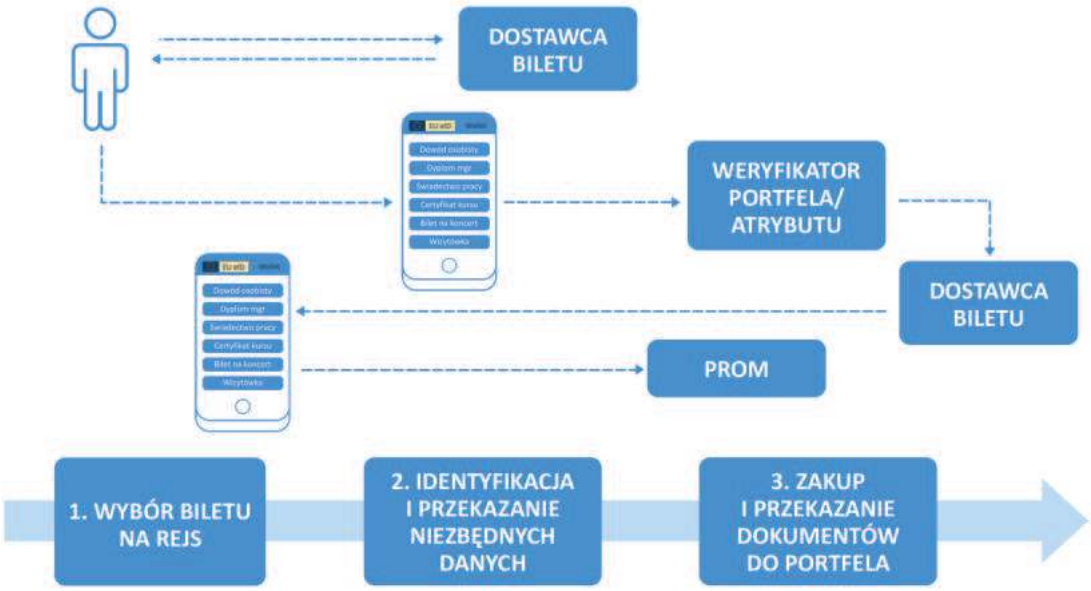
W szczególności testom podlega jedenaście następujących przypadków użycia:

1. **Dostęp do usług rządowych**: Bezpieczny dostęp do cyfrowych usług publicznych, takich jak ubieganie się o paszport lub prawo jazdy, składanie zeznań podatkowych lub dostęp do informacji o ubezpieczeniu społecznym.
2. **Otwarcie konta bankowego:** Weryfikacja tożsamości użytkownika podczas otwierania internetowego konta bankowego, eliminująca potrzebę wielokrotnego podawania przez użytkownika swoich danych osobowych
3. **Rejestracja karty SIM:** Potwierdzenie tożsamości do celów umów przedpłaconych i post-paid kart SIM (rejestracja i aktywacja), ograniczenie oszustw i kosztów ponoszonych przez operatorów sieci komórkowych.
4. **Mobilne prawo jazdy:** przechowywanie i okazywanie mobilnego prawa jazdy zarówno w interakcjach online, jak i fizycznych, np. w przypadku przekazywania prawa jazdy przez kierowcę na poboczu drogi.
5. **Podpisywanie umów:** Tworzenie bezpiecznych podpisów cyfrowych do podpisywania umów online, eliminujące potrzebę stosowania dokumentów papierowych i podpisów fizycznych.
6. **Obsługa recept:** Dostarczanie szczegółowych informacji o receptach do aptek i inicjowanie wydawania produktów leczniczych.
7. **Podróżowanie:** Przedstawianie informacji z dokumentów podróży (np. paszportu, wizy i innych dokumentów), co pozwala na szybki i łatwy dostęp podczas przechodzenia przez kontrolę bezpieczeństwa i odprawę celną na lotnisku.
8. **Tożsamość cyfrowa organizacji:** Udowodnienie, że podmiot jest prawowitym przedstawicielem organizacji.
9. **Płatności:** weryfikacja tożsamości użytkownika podczas inicjowania płatności online.
10. **Certyfikat wykształcenia:** Dowód posiadania poświadczeń edukacyjnych, takich jak dyplomy, stopnie naukowe i certyfikaty, ułatwiający ubieganie się o pracę lub dalszą edukację.
11. **Dostęp do świadczeń z zabezpieczenia społecznego:** Unijny portfel tożsamości cyfrowej ma służyć do bezpiecznego uzyskiwania dostępu do informacji i świadczeń z zabezpieczenia społecznego użytkownika, takich jak świadczenia emerytalne lub rentowe. Można go również wykorzystać do ułatwienia swobodnego przemieszczania się poprzez przechowywanie dokumentów, takich jak Europejska Karta Ubezpieczenia Zdrowotnego.

[28] https://www.europarl.europa.eu/doceo/document/A-9-2023-0038-AM-006-006_PL.pdf (dostęp 13.03.2024 r.)
[29] https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation (dostęp 14.03.2024 r.)

Jednym z wybranych przypadków użycia jest podróżowanie, które w celu przybliżenia może wyglądać w następujący sposób:

- Właściciel portfela wybiera bilet i wskazuje uwierzytelnianie portfelem by dostarczyć jednocześnie wszystkie wymagane informacje (zamiast ręcznego wypełniania formularza).
- Użytkownik jest przekierowany do serwisu (instytucji), który weryfikuje portfel/atrybuty i to ta instytucja przesyła wymagane informacje bezpośrednio do serwisu promowego.
- Użytkownik kontynuuje zakup biletu oraz wybiera opcję, aby karta pokładowa została przesłana bezpośrednio do portfela.
- Podczas przeprawy promowej użytkownik prezentuje kartę pokładową za pomocą portfela.



Rysunek 14. Wybrany przypadek użycia – podróż promem

Poza powyższym ogólnym przypadkiem biznesowego wykorzystania portfela tożsamości cyfrowej, należy zwrócić szczególną uwagę na następujące przypadki użycia w usługach finansowych, które są aktualnie przedmiotem prac wielkoskalowych pilotaży.

Portfel pozwoli na autoryzację transakcji bankowych za pośrednictwem konta, w tym celu wykorzystana zostanie funkcjonalność portfela umożliwiająca autoryzację transakcji bankowych online. Kluczowym aspektem jest tu zapewnienie bezpieczeństwa zgodnie z dyrektywą PSD2/RTS oraz przyszłymi regulacjami PSD3/PSR1/RTS. Portfel zapewni równowagę między bezpieczeństwem a wygodą użytkowania, oferując płatności z konta bankowego wykorzystując numery IBAN oraz poprzez usługę inicjowania płatności (PISP), jak również opcję płatności przez portfel płatniczy.

Wymaganiem certyfikacyjnym portfela jest wsparcie silnego i dwuskładnikowego uwierzytelnienia, w której jeden ze składników to posiadanie (np. urządzenie mobilne z zainstalowanym portfelem EUDIW), a drugi to wiedza (np. PIN) lub inherencja (np. cechy biometryczne). Użytkownik będzie w stanie zrealizować płatność bez konieczności wprowadzania dodatkowych danych, takich jak hasła czy inne ciągi znaków.

Inicjacja możliwości płatniczych portfela wymagać będzie przeprowadzenia procesu rejestracji portfela u dostawcy usług płatniczych (ASPSP). Proces rejestracji jest niezbędny do umożliwienia wykorzystania portfela do autoryzacji płatności. Ta rejestracja pozwala użytkownikowi i jego bankowi określić, które instrumenty płatnicze mogą być autoryzowane przy użyciu portfela. W efekcie portfel otrzymuje poświadczenie, które pozwala mu działać jako mechanizm autoryzacji transakcji płatniczych.

Użycie portfela w płatnościach online, pozwala użytkownikowi na wybranie opcji płatności bezpośrednio

z konta na stronie internetowej sprzedawcy (lub w aplikacji), gdzie użytkownicy będą mogli korzystać z portfela do autoryzacji tych transakcji. Scenariusz ten zakłada, że użytkownik zarejestrował portfel jako metodę silnego uwierzytelnienia klienta (SCA) w swoim profilu klienta banku, a obciążenie jego rachunku płatniczego jest dostępne dla sprzedawcy. Portfel pozwoli na szybkie i bezproblemowe autoryzowanie płatności, zwiększając tym samym szanse na pomyślne zakończenie transakcji bez potrzeby wielokrotnego uwierzytelniania czy wprowadzania dodatkowych danych.

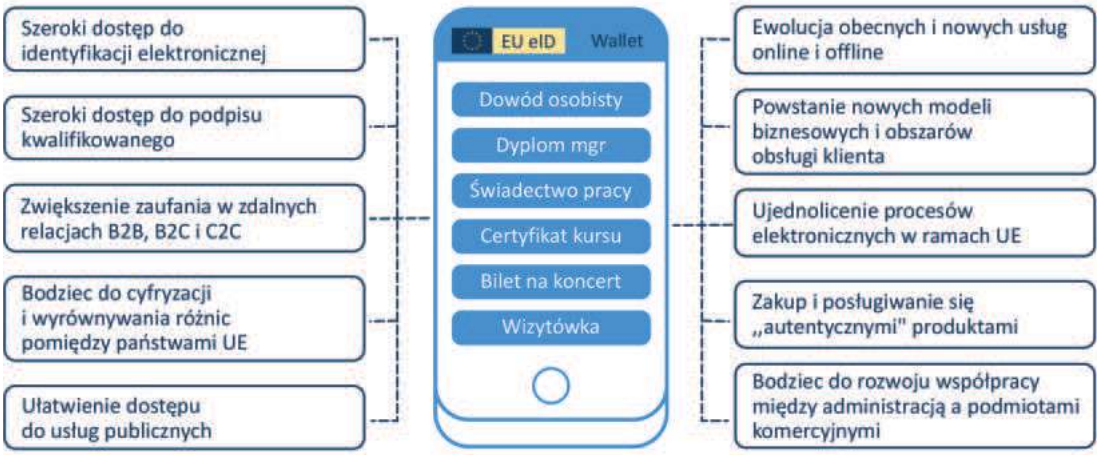
Każdy projekt pilotażowy będzie wykorzystywał elementy wdrożenia wzorcowego (Referencyjne Ramy Architektoniczne) opracowanego przez Komisję Europejską i ma się przyczynić do dalszego zwiększenia jego bezpieczeństwa, łatwości obsługi i interoperacyjności.

Analiza zaadresowanych potrzeb

Koncepcja europejskiego portfela cyfrowej tożsamości w swoich założeniach ma przynieść obywatelom Unii Europejskiej szereg korzyści w zakresie identyfikacji elektronicznej, jak i klasycznej identyfikacji w świecie offline. W rozdziale 1.1.1 wskazano generalne problemy dla tożsamości cyfrowej, które de facto są także ryzykami dla obywateli czy systemów korzystających z tożsamości cyfrowej. O czym wspomniano już wyżej, są to następujące ryzyka:

- utrata prywatności danych osobowych użytkowników,
- możliwość powiązania danych nt. osób na podstawie metadanych oraz informacji pozostawianych w różnych serwisach internetowych,
- nadmiarowe udostępnianie danych przez administratorów danych do podmiotów trzecich,
- brak powszechności dostępności usług cyfrowych,
- zapewnienie niezależności użytkownikom w związku z problemem zbyt dużej zależności od cyfrowych usług, w tym cyfrowej tożsamości,
- kradzież, wyłudzenie, podszycie się pod cyfrową tożsamość.

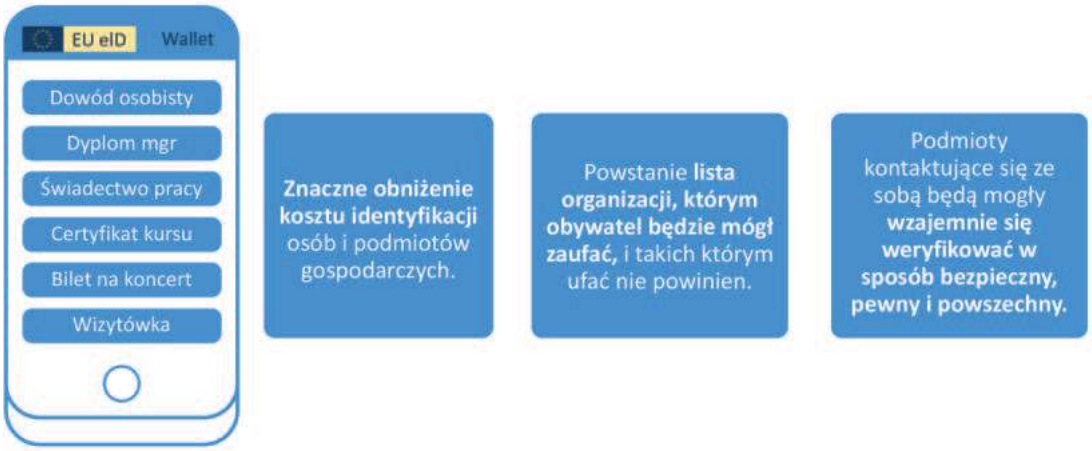
Rysunek 2 prezentuje korzyści oraz społeczne i operacyjne implikacje wdrożenia portfela. Są to korzyści z perspektywy zarówno użytkownika portfela, jak i podmiotów korzystających w sposób pośredni jak strony ufające.



Rysunek 15. Społeczne i operacyjne implikacje z wdrożenia portfela

Powszechny dostęp do identyfikacji elektronicznej umożliwi realizację wielu transakcji online takich jak: zakładanie kont bankowych, dostęp do usług rządowych, pobieranie zaświadczeń, poświadczeń czy certyfikatów. Posiadanie portfela ułatwi także funkcjonowanie w świecie fizycznym np. podróżując po świecie wyłącznie w oparciu o tożsamość przechowywaną w portfelu. Z jednolitą tożsamością wiążą się także korzyści i potrzeby różnych interesariuszy zaprezentowane na rysunku 16.

- portfel jako jednolite narzędzie do identyfikacji to korzyść w postaci znacznego obniżenia kosztu identyfikacji dla podmiotów gospodarczych



Rysunek 16. Dostępność identyfikacji a bezpieczeństwo konsumentów i akceptantów

- portfel ma zapewnić bezpieczne środowisko komunikacji tylko z podmiotami uprawnionymi do odczytywania danych w nim zawartych

Wskazania dotyczące GDPR

Nowelizowane rozporządzenie eIDAS kładzie bardzo duży nacisk na ochronę danych osobowych. Pojęcia takie jak: kontrola nad danymi użytkownika, uniemożliwienie profilowania, respektowanie zasady minimalizacji danych, domyślna ochrona danych to pojęcia występujące w rozporządzenie kilkukrotnie.

- W preambule w punkcie 12 nowelizacji eIDAS wskazano, że jednym z celów rozporządzenia jest „ustanowienie szczególnych zabezpieczeń uniemożliwiających dostawcom środków identyfikacji elektronicznej i elektronicznych poświadczeń atrybutów **łączenie** danych osobowych uzyskanych w ramach świadczenia innych usług z danymi osobowymi przetwarzanymi w celu świadczenia usług objętych zakresem stosowania niniejszego rozporządzenia. Dane osobowe związane z dostarczaniem europejskich portfeli tożsamości cyfrowej powinny być logicznie oddzielone od wszelkich innych danych będących w posiadaniu dostawcy europejskiego portfela tożsamości cyfrowej".

- W preambule punkt 13, wskazano, że „Europejskie portfele tożsamości cyfrowej powinny mieć wbudowaną funkcję wspólnego panelu zarządzania, aby zapewnić wyższy stopień przejrzystości, prywatności i kontroli użytkowników nad ich danymi osobowymi. Funkcja ta powinna zapewniać łatwy i przyjazny dla użytkownika interfejs wraz z przeglądem wszystkich stron ufających, którym użytkownik udostępnia dane, w tym atrybuty, oraz rodzaju danych udostępnionych każdej ze stron ufających. Powinna ona umożliwiać użytkownikom śledzenie wszystkich transakcji przeprowadzonych za pośrednictwem europejskiego portfela tożsamości cyfrowej (...)".

- W preambule punkt 14, wskazano, że „Państwa członkowskie powinny włączyć do europejskiego portfela tożsamości cyfrowej różne technologie chroniące prywatność, takie jak dowód z wiedzą zerową (zero knowledge proof). Te metody kryptograficzne powinny umożliwiać stronie ufającej zweryfikowanie, czy dane stwierdzenie oparte na danych identyfikujących osobę i poświadczeniu atrybutów jest prawdziwe, bez ujawniania jakichkolwiek danych, na których opiera się to stwierdzenie, chroniąc tym samym prywatność użytkownika".

- W preambule punkt 15 wskazano, że „Wszyscy obywatele i rezydenci Unii określeni w prawie krajowym powinni być uprawnieni do bezpiecznego żądania, wybierania, łączenia, przechowywania, usuwania, udostępniania i prezentacji danych dotyczących swojej tożsamości oraz żądania usunięcia swoich danych osobowych w przyjazny dla użytkownika i wygodny sposób, pod wyłączną kontrolą użytkownika, przy jednoczesnej możliwości selektywnego ujawniania danych osobowych".

Z całą pewnością wprowadzenie EDIW jest silnym przykładem respektowania prawa wynikającego z rozporządzenia ogólnego o ochronie danych (GDPR) oraz rzeczywistego umożliwienia obywatelom UE zapewnienia prywatności oraz kontroli nad danymi.

2.2. Ryzyka związane z koncepcją europejską tożsamości cyfrowej

Skrócona analiza ryzyk potwierdzania tożsamości

Potwierdzanie tożsamości pełni kluczową rolę w licznych procesach i obszarach życia, zarówno prywatnego, jak i biznesowego. Przykładowe sytuacje, w których się z nim spotykamy, obejmują:

1. W transakcjach finansowych, w kontaktach z bankiem, podczas zakupów online oraz przy innych operacjach finansowych, potwierdzanie tożsamości odgrywa kluczową rolę. Dzięki temu instytucje finansowe mogą upewnić się, że osoba dokonująca transakcji jest prawowitym właścicielem konta lub uczestnikiem transakcji.

2. W sprawach urzędowych, podczas załatwiania formalności w urzędach, odbierania przesyłek czy korzystania z usług publicznych, konieczne jest potwierdzenie tożsamości.

3. Opieka zdrowotna wymaga potwierdzenia tożsamości w placówkach medycznych, podczas wizyt u lekarza czy odbierania recept. Jest to niezbędne dla zapewnienia bezpieczeństwa pacjentów oraz prawidłowego prowadzenia dokumentacji medycznej.

4. W przypadku ubezpieczeń, potwierdzenie tożsamości jest konieczne do obsługi polisy.

W okresie pandemii COVID-19 znacząco przyspieszył rozwój narzędzi wspomagających proces potwierdzania tożsamości. Poza klasycznymi metodami, takimi jak fizyczna weryfikacja przez człowieka, dostępne są obecnie rozwiązania w pełni lub częściowo zautomatyzowane, wykorzystujące systemy biometryczne oraz sztuczną inteligencję. Niemniej jednak, mimo różnorodności metod potwierdzenia tożsamości, wciąż pozostaje podstawowe ryzyko **niepoprawnej weryfikacji tożsamości,** zarówno w środowisku fizycznym, jak i wirtualnym, z uwagi na takie zagrożenia jak:

- podstawienie fałszywego lub skradzionego dokumentu tożsamości przez atakującego,
- ataki prezentacyjn**e** tzw. deep-fakes[30], maski 2D i 3D,
- błędy oprogramowania,
- wstrzyknięcia danych do systemu potwierdzenia tożsamości w celu oszukania systemu weryfikującego,
- błędy człowieka wynikające z braku kompetencji lub zmęczenia.

Kolejnym ryzykiem związanym z procesem potwierdzania tożsamości jest brak jednolitego podejścia na rynku w zakresie akceptacji różnych metod potwierdzania tożsamości oraz związanej z tym interoperacyjności. Niektóre państwa członkowskie stosują bardziej restrykcyjne kryteria, jeśli chodzi o akceptację różnorodnych metod, na przykład tych zdalnych (np. automatyczne potwierdzanie tożsamości za pomocą mechanizmów biometrycznych). Związane z tym ryzyko wiąże się również z funkcjonowaniem na rynku metod o zróżnicowanym poziomie wiarygodności, które w różnych krajach członkowskich są wykorzystywane np. do wydawania certyfikatów kwalifikowanych.

Koncepcja europejska polegająca na zapewnieniu możliwości posiadania przez każdego obywatela portfela cyfrowej tożsamości (zgodnie z definicją eIDAS jest to środek identyfikacji elektronicznej[31]), ma w szczególności na celu zmniejszenie poziomu wskazanych ryzyk poprzez dostarczenie obywatelom Unii Europejskiej jednolitego oraz transgranicznego środka identyfikacji elektronicznej. Portfel ma umożliwić wiarygodne potwierdzenie tożsamości przez strony ufające, jednocześnie ograniczając używanie metod potwierdzania tożsamości o wątpliwej wiarygodności.

Wskazanie ryzyk przy zastosowaniu modelu

Koncepcja europejskiego portfela cyfrowej tożsamości niesie ze sobą co najmniej kilka ryzyk, które muszą zostać zaadresowane przez wydawców (dostawcy) portfela, jak i podmioty utrzymujące technologię związaną z tym modelem tożsamości. Podstawowym ryzykiem dotyczącym bezpieczeństwa ekosystemu tego rozwiązania, zauważanym przez autorów niniejszego opracowania, jest ryzyko niewłaściwego zarządzania kluczami kryptograficznymi przez poszczególnych aktorów. Kryptografia stanowi fundamentalny mechanizm bezpieczeństwa, zapewniający zarówno poufność komunikacji, jak i integralność przekazywanych danych dotyczących tożsamości. Klucze kryptograficzne będą wykorzystywane w szczególności:

- po stronie wydawcy portfela, aby ustanowić bezpieczną sesję z użytkownikiem,

[30] Technika obróbki obrazu, polegająca na łączeniu obrazów twarzy ludzkich przy użyciu technik sztucznej inteligencji. Wykorzystuje algorytmy uczenia maszynowego, aby tworzyć łudząco realistyczne ruchome obrazy – źródło: https://cyberprofilaktyka.pl/blog/deepfake-jak-sztuczna-inteligencja-moze-nas-oszukiwac_i40.html (dostęp 08.03.2024 r.)

[31] https://www.europarl.europa.eu/doceo/document/A-9-2023-0038-AM-006-006_PL.pdf (dostęp 13.03.2024 r.)

- przez użytkownika portfela, który będzie posiadał klucze prywatne do uwierzytelnienia się w usłudze online,

- przez stronę ufającą (np. sklep internetowy), która będzie musiała posłużyć się kluczami do ustanowienia bezpiecznej sesji komunikacyjnej z użytkownikiem portfela.

Niewłaściwe zarządzanie tymi kluczami może prowadzić do poważnych zagrożeń dla bezpieczeństwa, takich jak nieautoryzowany dostęp do danych lub informacji o transakcji, fałszerstwa czy naruszenia prywatności. Dlatego też należy zadbać o odpowiednie procedury zarządzania kluczami kryptograficznymi (na poziomie architektonicznym, jak i organizacyjnym) w celu minimalizacji tego ryzyka.

Ryzyko podstawienia fałszywej aplikacji, która udaje oryginalny portfel cyfrowej tożsamości, jest kolejnym ryzykiem w kontekście różnych transakcji elektronicznych. Ryzyko polegać może na zastąpieniu oryginalnej aplikacji przez niebezpieczną lub złośliwą wersję, która może prowadzić do przechwycenia danych, kradzieży tożsamości czy wykonania nieautoryzowanej transakcji finansowej. Mechanizm zaproponowany przez regulację eIDAS 2.0, polegający na utrzymywaniu przez każdy kraj członkowski listy uprawnionych stron ufających, ma na celu zmniejszenie tego ryzyka poprzez umożliwienie użytkownikowi portfela cyfrowej tożsamości nawiązywania relacji tylko z zaufanymi podmiotami. Wdrożenie takiego mechanizmu pozwoli użytkownikowi na potwierdzenie autentyczności podmiotu np. sklepu internetowego lub aplikacji, na której wykonuje płatność, co zwiększy zaufanie i bezpieczeństwo procesu transakcyjnego. Jednakże, mimo że mechanizm ten może pomóc w ograniczeniu ryzyka podstawienia fałszywej aplikacji, nadal istnieje potrzeba zachowania ostrożności i świadomości ze strony użytkowników. Konieczne jest również regularne monitorowanie i aktualizowanie listy uprawnionych stron ufających, aby zapewnić, że tylko wiarygodne i bezpieczne podmioty mają dostęp do procesu uwierzytelniania i nawiązywania komunikacji z użytkownikiem. Dodatkowo, edukacja użytkowników w zakresie rozpoznawania potencjalnych zagrożeń jest niezmiernie kluczowa dla skutecznej ochrony przed tego typu atakami.

W dniu 3 czerwca 2021 roku Komisja Europejska przyjęła Rekomendację wzywającą Państwa Członkowskie do pracy nad opracowaniem Narzędzi, obejmujących architekturę techniczną i ramy referencyjne (ARF), zbiór wspólnych standardów i specyfikacji technicznych oraz zestaw wspólnych wytycznych i najlepszych praktyk. Rekomendacja określa, że te wyniki posłużą jako podstawa do wdrożenia propozycji Ramowego Systemu Europejskiej Tożsamości Cyfrowej, przy czym proces opracowywania Narzędzi nie będzie ingerował ani nie będzie z góry ustalał procesu legislacyjnego[32]. Proces tworzenia architektury ma charakter ekspercki, natomiast każda zainteresowana strona, która zechce uczestniczyć w procesie opiniowania architektury może dodać swoją kontrybucję (istnieje możliwość pobrania kodu źródłowego portfela). Niemniej, na tak wczesnym etapie koncepcji EDIW należy wskazać ryzyko jego złej konstrukcji. Ryzyko może prowadzić do różnych problemów związanych z bezpieczeństwem, wydajnością i użytecznością. Niektóre z potencjalnych zagrożeń związanych z nieprawidłową konstrukcją portfela cyfrowej tożsamości obejmują:

- Bezpieczeństwo danych: słaba konstrukcja portfela cyfrowej tożsamości może prowadzić do luk w zabezpieczeniach, co może doprowadzić do nieautoryzowanego dostępu do poufnych danych użytkownika, takich jak dane osobowe.

- Brak interoperacyjności: nieprawidłowo skonstruowany portfel może mieć trudności z integracją z innymi systemami czy platformami, co może utrudnić użytkownikom korzystanie z różnych usług i aplikacji online.

- Użyteczność: zła konstrukcja interfejsu użytkownika (UI) lub doświadczenia użytkownika (UX) może prowadzić do frustracji użytkowników i zmniejszenia przyjęcia rozwiązania przez nich.

Potencjalnym remedium na powyższe ryzyko są prowadzone na dużą skalę pilotaże europejskiego portfela cyfrowej tożsamości, które w warunkach testowych przy udziale dużych podmiotów takich jak np. linie lotnicze, biura podróży, podmioty finansowe mają potwierdzić zarówno bezpieczeństwo rozwiązania, jak i jego użyteczność[33].

Zgodnie z definicją nowelizowanego eIDAS, EDIW to „środek identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej[34]". Analizując przytoczoną definicję, należy zwrócić

[32] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework?tab=readme-ov-file (dostęp 13.03.2024 r.)
[33] https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation (dostęp 13.03.2024 r.)
[34] https://www.europarl.europa.eu/doceo/document/A-9-2023-0038-AM-006-006_PL.pdf, art. 3 pkt 43.

uwagę na potencjalne ryzyko związane z procesem zasilania danych do portfela, jako że portfel ma umożliwiać przechowywanie danych identyfikujących osobę oraz różnych poświadczeń atrybutów. Portfel z definicji ma być swoistym kontenerem danych oraz atrybutów, a dane zasilane powinny być z wiarygodnych źródeł. Zgodnie z art. 5a pkt 5 lit. f, portfele „muszą zapewniać, aby dane identyfikujące osobę, które są dostępne w systemie identyfikacji elektronicznej, w ramach którego zapewniany jest europejski portfel tożsamości cyfrowej, niepowtarzalnie reprezentowały osobę fizyczną, osobę prawną, lub osobę fizyczną reprezentującą osobę fizyczną lub prawną, oraz były powiązane z tym europejskim portfelem tożsamości cyfrowej". Zanim to nastąpi, każdy kraj członkowski, oferując swoim obywatelom portfel, musi dokonać wewnętrznie potwierdzenia tożsamości każdego użytkownika przed zasileniem danych.

Odniesienie do ryzyka pozostającego i sposobów zabezpieczeń

Niniejszy rozdział przybliżył zarówno korzyści, jak i nowe wyzwania wynikające z koncepcji europejskiej, która stawia sobie za cel zmniejszenie ryzyka poprzez promowanie interoperacyjności oraz wprowadzenie jednolitego mechanizmu potwierdzania tożsamości we wszystkich krajach Unii Europejskiej. Niemniej, należy również wziąć pod uwagę potencjalne zagrożenia związane z błędną implementacją przepisów prawnych, takimi jak technologiczne niedoskonałości w projektowaniu i wdrożeniu portfela cyfrowej tożsamości. W tym kontekście istotne jest rozważenie pozostającego ryzyka rezydualnego, które może pozostać nawet po uwzględnieniu środków bezpieczeństwa na każdym etapie życia produktu.

Jednym z kluczowych zagrożeń jest ryzyko phishingu i kradzieży tożsamości. Pomimo że koncepcja europejska narzuca określone wymagania dotyczące komunikacji między stronami oraz identyfikacji, istotną rolę odgrywa także duży poziom odpowiedzialności użytkownika portfela w zakresie udostępnienia danych osobowych. Jednym z zabezpieczeń jest ciągła edukacja użytkowników oraz stworzenie rozwiązań, które uniemożliwią komunikację portfela z nieautoryzowanymi podmiotami.

Innym ważnym ryzykiem, które może wystąpić pomimo ustanowienia standardów i regulacji, jest zróżnicowany poziom onboardingu do portfela na poziomie krajowym. Każdy kraj może opierać się na własnych metodach i procedurach, co może prowadzić do nabycia portfela przez przestępców. Aby zapewnić większe bezpieczeństwo, niezbędne jest dążenie do dopuszczenia na rynek jedynie certyfikowanych dostawców i produktów w zakresie potwierdzania tożsamości.

Ostatnim zidentyfikowanym ryzykiem jest możliwość tworzenia tzw. „łańcucha tożsamości" poprzez portfel jako narzędzia elektronicznej identyfikacji o najwyższym poziomie wiarygodności. Szczególnie w kontekście transakcji online, strony ufające muszą przeprowadzać analizę ryzyka, decydując każdorazowo, czy są gotowe zaakceptować tożsamość pochodzącą z portfela bez dodatkowej weryfikacji, na przykład żywotności w procesach KYC/AML.

2.3. Dlaczego rozwiązanie można uznać za perspektywiczne

O cechach Europejskiego Portfela Tożsamości Cyfrowej wspomnieliśmy już w poprzednich rozdziałach nie raz, jednak co czyni lub raczej co uczyni go perspektywicznym rozwiązaniem? Sam fakt, iż jest on w fazie testowej czyni go narzędziem z ogromnym potencjałem dalszego rozwoju. Przede wszystkim cyfrowy portfel nie został gwałtownie obligatoryjnie wprowadzony na rynek, a jako dobrowolne narzędzie, do którego użytkownicy przekonują się w swoim tempie. „Grupa testowa" to obywatele państw członkowskich, którzy sprawdzają możliwości portfela na własnej skórze, a to daje spore możliwości rozwoju i dopasowania się do potrzeb użytkowników, co najpewniej zaowocuje w perspektywie kolejnych lat. Zebrane razem doświadczenie pomoże w ulepszeniu usługi oraz dostosowaniu jej i integracji na poziomie krajowym oraz europejskim. Ponadto, Komisja Europejska podjęła szereg działań, które skupiają się na dopracowaniu i przygotowaniu rozwiązania na najwyższym poziomie pod względem bezpieczeństwa, użyteczności wspierające transgraniczne działania i procesy.

Możliwość, konieczność oraz efektywność używania cyfrowego portfela wymaga odpowiedniego przygotowania prawnego. EDIW może funkcjonować w ramach UE, dzięki przepisom niejako wymuszającym jego stosowanie. Mowa o rozporządzeniach wystosowanych przez Komisję europejską oraz ustawach na poziomie krajowym. Poniżej lista przepisów prawa związanych z Europejskim Portfelem Tożsamości Cyfrowej:

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80)

2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/6797 oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady8 mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie rozporządzenia (UE) nr 910/2014.

3. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

Ponadto, korzystanie z portfela jest zgodne z GDPR (General Data Protection Regulation) (w Polsce znanym jako RODO) oraz europejską regulacją Cyber Security Act.

Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) jest agencją Unii Europejskiej, której zadaniem jest wspieranie państw członkowskich UE oraz instytucji UE w zapewnieniu wysokiego poziomu cyberbezpieczeństwa w Europie. Jej prace obejmują również opracowywanie zaleceń, wytycznych i raportów dotyczących różnych aspektów cyberbezpieczeństwa, w tym także kwestii związanych z cyfrową tożsamością. ENISA powołała – ENISA European Competent Authorities for Trust Services (ECATS) Expert Group (Article 19 Expert Group) – grupę ekspertów, którzy czuwają oraz współtworzą standaryzację, wymagania techniczne, polityki oraz stanowią wsparcie przy budowie Europejskiego Portfela Tożsamości Cyfrowej. Jej głównym celem w zakresie EUDI jest standaryzacja interfejsów z zaufanymi dostawcami usług i istniejącymi krajowymi dokumentami identyfikacji elektronicznej oraz opracowanie metodologii oceny prywatności w odniesieniu do tożsamości cyfrowej.

Na poziomie UE, Komisja Europejska otworzyła program „Cyfrowa Europa", którego owocem ma być EUDI, czyli prototyp cyfrowego portfela. W ramach programu powstały wieloskalowe pilotaże portfela cyfrowej tożsamości. Przed wprowadzeniem oficjalnego europejskiego cyfrowego portfela potrzebne jest środowisko testowe, dlatego rozpoczęto pilotaże w ramach czterech dużych projektów, które rozpoczęto w dniu 1 kwietnia 2023 r. Celem tych projektów jest przetestowanie cyfrowych portfeli tożsamości w rzeczywistych scenariuszach obejmujących różne sektory. W pilotażach bierze udział ponad 250 prywatnych przedsiębiorstw i organów publicznych z 25 państw członkowskich oraz Norwegii, Islandii i Ukrainy. Poniżej znajdują się nazwy pilotaży wraz z krótkim opisem obszaru, na którym skupiają się dane projekty.

1. NOBID (Nordic-Baltic eID Project): pilotaż koncentruje się na przypadkach użycia związanych z transgranicznymi transakcjami.

2. EUDI Wallet Consortium (EWC): skupia się na e-commerce, szczególnie w kontekście podóży, demonstrując potencjał eIDAS w poprawie bezpieczeństwa i wygody zakupów online. EWC tworzy dwa kluczowe moduły: płatności i cyfrową tożsamość organizacyjną (ODI).

3. Digital Credential for Europe (DC4EU): pilotaż zmienia podejście do danych tożsamości na zasadzie „raz na zawsze", działając w obszarze edukacji, pracy i zdrowia. Celem jest testowanie interoperacyjności i skalowalności.

4. POTENTIAL – European Consortium for Digital Identity: buduje przyszłość cyfrowej tożsamości w Europie, z naciskiem na użytkownika i ochronę danych. Celem jest zapewnienie bezpiecznej, autentycznej i weryfikowalnej cyfrowej tożsamości.

Opis przypadków użycia realizowanych w ramach wielkoskalowych pilotaży został opisany w rozdziale 2.1.

Dlaczego podjęto prace nad wspólnym rozwiązaniem tożsamości cyfrowej w Europie

3.1. Zalety jednolitego standardu

Europejski portfel tożsamości cyfrowej (ang. EU Digital Identity Wallet, EUDI) ma na celu ujednolicenie rynku identyfikacji elektronicznej zarówno na poziomie poszczególnych krajów członkowskich jak i całej Unii Europejskiej. Ma on usprawnić, zapewnić większe bezpieczeństwo i zwiększyć kontrolę nad przekazywanymi przez obywateli danymi w procesach realizowanych zarówno online, jak i offline.

Portfele docelowo mają się dzielić na państwowe i komercyjne. W kontekście tego raportu skupiamy się na omówieniu zakresu i potencjalnego wpływu wdrożenia portfeli narodowych. Każdy kraj członkowski zobowiązany będzie do wdrożenia własnego lub notyfikowania istniejącego portfela dedykowanego jako narodowy w ciągu 24 miesięcy od wejścia w życie aktów implementujących, określających wymagania wobec portfela, w praktyce państwa członkowie powinny wdrożyć swoje portfele nie później niż do końca 2026 roku. Portfele te będą samodzielnymi środkami identyfikacji elektronicznej powiązanymi z krajowymi środkami identyfikacji obywateli.

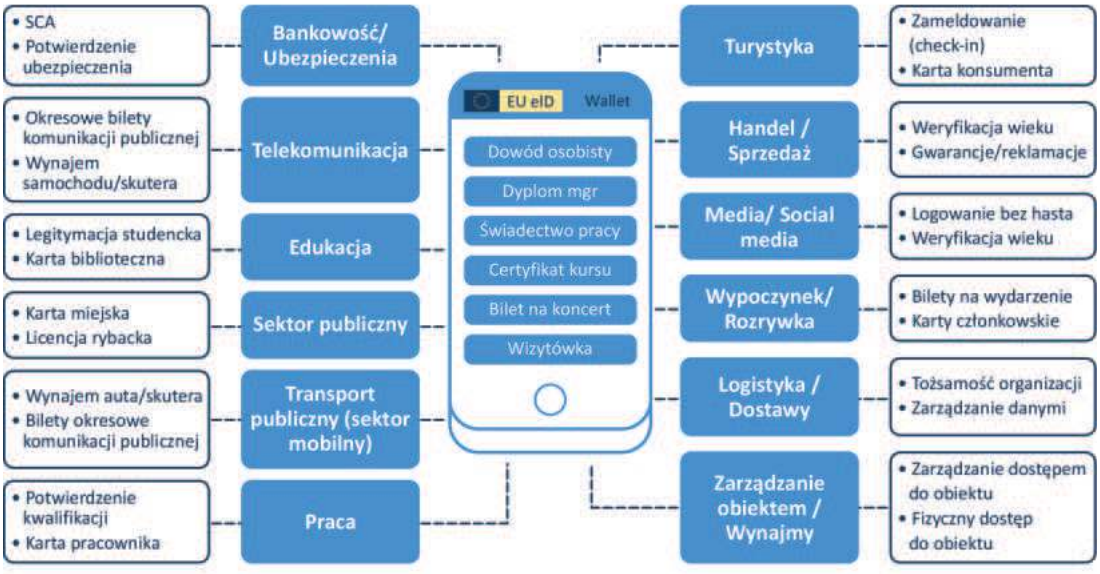
Poza samą warstwą „aplikacyjną" portfel ma zapewnić przede wszystkim bezpieczne i przejrzyste ramy regulacyjne i infrastrukturalne, które pozwolą na identyfikację i uwierzytelnienie użytkowników w ramach ujednoliconego, spójnego standardu na terenie całej Unii Europejskiej, niezależnie od kraju pochodzenia portfela i tego, w którym kraju jest on wykorzystywany tj. obywatele Polski będą mogli bez problemu wykorzystać portfel za granicą i vice versa. Portfel ma umożliwić interakcję obywateli z podmiotami publicznymi i prywatnymi ze szczególnym uwzględnieniem instytucji finansowych i dużych platform internetowych, ale także potencjalnie służyć potrzebom administracji publicznej – zarówno lokalnej jak i unijnej.

Funkcjonalności portfeli

Portfele tożsamości cyfrowej mają wesprzeć obywateli UE w realizacji czynności wymagających obecnie posłużenia się dokumentem tożsamości lub innym dokumentem takim jak na przykład dyplom czy potwierdzenie uprawnień lub kompetencji. Z funkcjonalności dowolnego portfela cyfrowej tożsamości skorzystać będzie można zarówno w kraju pochodzenia jak i w każdym kraju członkowskim.

Za jego pośrednictwem możliwe będą między innymi czynności takie jak:

- identyfikacja i potwierdzenie wieku,
- okazanie prawa jazdy,
- złożenie deklaracji podatkowej,
- uzyskanie dostępu do elektronicznych usług administracji publicznej,
- realizacja recept,
- otworzenie rachunku bankowego,
- złożenie dokumentów w procesie rekrutacji na studia,
- rejestracja i logowanie do mediów społecznościowych.



Rysunek 17. Zakresy użycia portfela cyfrowej tożsamości

Są to przykładowe funkcjonalności portfeli, których wdrożenie zagwarantowane jest w rozporządzeniu eIDAS 2.0, jednak docelowy potencjał rozwiązań opartych o unijne ramy prawne jest znacznie większy i prawdopodobnie będzie wykorzystywany w ramach rozwiązań, które zaoferowane zostaną przez podmioty komercyjne. Docelowy kształt rynku portfeli pozostaje dzisiaj jedynie w sferze spekulacji i predykcji, jednak możliwości jakie stworzył framework legislacyjny są bardzo duże. Ponadto wszystkie duże platformy internetowe będą zobowiązane do wprowadzenia możliwości logowania za pośrednictwem portfeli.

Portfele narodowe mają także udostępnić nieodpłatnie dostęp do podpisów kwalifikowanych dla obywateli do wykorzystania w celach prywatnych. Szczegóły dotyczące implementacji tego wymogu nie są jeszcze jasne, natomiast sam fakt, że każda osoba fizyczna uzyska dostęp do kwalifikowanych podpisów elektronicznych może mieć kolosalny wpływ na proces rozwoju cyfryzacji instytucji publicznych i komercyjnych. Potencjalnie cyfryzacji na masową skalę ulec będą mogły procesy, które do tej pory zarezerwowane były jedynie do realizacji w bezpośrednim fizycznym kontakcie klienta z instytucją lub w wybranych przypadkach z innymi modelami takimi jak podpis fizyczny przy obecności kuriera.

Atrybuty

Działanie portfeli tożsamości cyfrowej opierać się będzie o atrybuty wydawane na żądanie użytkownika. Będą one stanowiły potwierdzenie **cech** *(takich jak na przykład dane osobowe, wiek, stan cywilny, wykształcenie, kwalifikacje zawodowe czy pełnomocnictwa)* i **stanu posiadania** *(dokumenty podróży, własność nieruchomości, dostępu do budynków czy pokojów hotelowych)*.

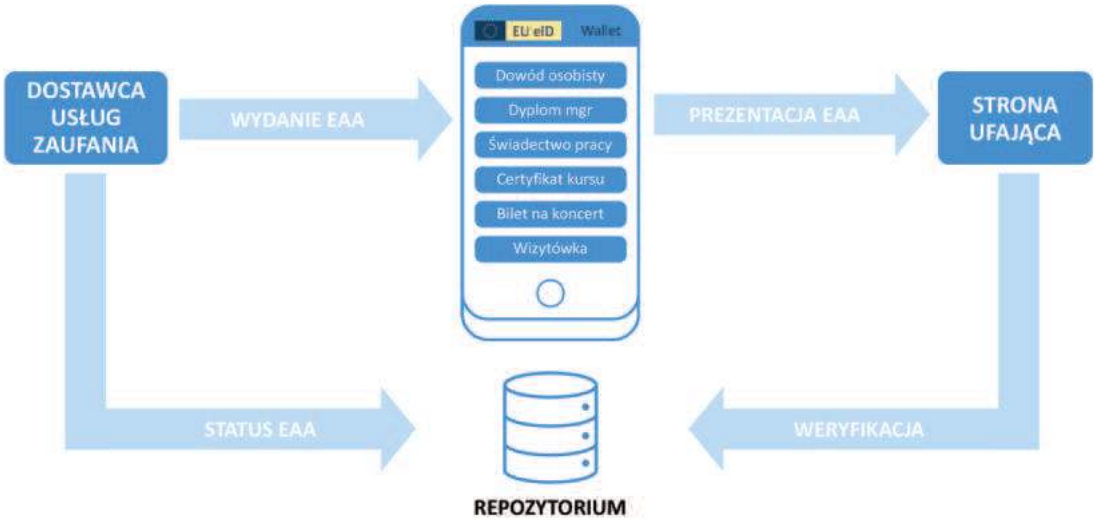
Atrybut oznacza cechę charakterystyczną, właściwość, prawo lub zezwolenie osoby fizycznej lub prawnej lub przedmiotu (art. 3 pkt 43 eIDAS2).

Rysunek 18. Przykład atrybutów przechowywanych w portfelu

Atrybuty udostępniane są przez administrację publiczną (przez podmioty odpowiedzialne za autentyczne źródła publiczne takie jak na przykład rejestr dowodów osobistych), inne podmioty stanowiące zaufane lub pierwotne źródło informacji. Przykładowo w Polsce źródło autentyczne będą stanowiły rejestry publiczne takie jak PESEL, Rejestr dowodów osobistych, Rejestr wydanych dokumentów paszportowych. Jednocześnie źródłem autentycznym dla atrybutu potwierdzającego numer konta bankowego jest sam bank, który prowadzi to konto.

Źródło autentyczne oznacza repozytorium lub system za prowadzenie którego odpowiedzialny jest podmiot sektora publicznego lub podmiot prywatny, które zawiera i udostępnia atrybuty dotyczące osoby fizycznej lub prawnej lub przedmiotu i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczne zgodnie z prawem Unii lub prawem krajowym w tym z praktykami administracyjnymi; (art. 3 pkt 47 eIDAS2)

Atrybuty wydawane są w sposób uwierzytelniony w postaci elektronicznego poświadczenia atrybutów. Poświadczenia te są wydawane przez kwalifikowanych i niekwalifikowanych dostawców usług zaufania. Dostawcy elektronicznych poświadczeń atrybutów zapewniają użytkownikom europejskiego portfela tożsamości cyfrowej możliwość żądania, otrzymywania i przechowywania elektronicznego poświadczenia atrybutów, a także zarządzania nim, niezależnie od państwa członkowskiego, w którym zapewniany jest europejski portfel tożsamości cyfrowej. To oznacza, że w portfelu będzie można przechowywać poświadczenia wystawiane przez różnych publicznych i prywatnych wystawców poświadczeń i posługiwanie się nimi w przekazywaniu danych stronom ufającym. Poświadczenia atrybutów wystawione przez kwalifikowanych dostawców będą miały takie same skutki prawne jak te wystawione przez organy administracji publicznej.



Rysunek 19. Model funkcjonowania Europejskiego Portfela Tożsamości Cyfrowej

Poza samymi możliwościami funkcjonalnymi oferowanymi przez portfele, najważniejszym aspektem z perspektywy klientów będzie możliwość kontroli nad przekazywanymi i przetwarzanymi danymi pochodzącymi z portfela. Użytkownik będzie miał bieżący wgląd w to, jakie dane w procesie są przekazywane drugiej stronie, w to kto i do jakich danych ma aktualnie dostęp i będzie mógł tym dostępem zarządzać. Jest to znacząca zmiana w stosunku do tego, jaki poziom kontroli nad swoimi danymi mają klienci.

Wykorzystanie europejskiego portfela cyfrowej tożsamości – kontekst PSD2

PSD2, czyli europejska dyrektywa dotycząca usług płatniczych, miała na celu rozwinięcie rynku płatniczego w kilku kluczowych obszarach tj. **bezpieczeństwo realizowanych transakcji płatniczych** (poprzez wprowadzenie procedur wielopoziomowego uwierzytelniania i innych narzędzi ograniczania ryzyka), **stymulowanie innowacyjności** i **zwiększenie konkurencyjności** głownie za pośrednictwem otwartej bankowości *(ang. open banking)*.

Europejskie portfele cyfrowej tożsamości, pośrednio i bezpośrednio, wpiszą się w rozwój powyższych aspektów. Mogą one mieć istotny wpływ na funkcjonowanie rynków płatniczych

1. **Bezpieczeństwo transakcji:** użytkownicy posiadający portfel cyfrowej tożsamości będą mogli korzystać za jego pośrednictwem z narzędzi autoryzujących *(SCA)* realizowane przez nich transakcje finansowe, w tym te opisane w dyrektywie PSD2.

2. **Ułatwienie dostępu do usług płatniczych**: za pośrednictwem portfela użytkownicy będą mogli dokonywać uwierzytelniania w ramach procesów rejestracji i logowania do dużych platform internetowych, utrzymując w tym samym czasie pełną kontrolę nad swoimi danymi. Może to bezpośrednio przełożyć się na wyższy komfort użytkowania i przekonać użytkowników korzystania z płatności elektronicznych.

3. **Zwiększenie konkurencyjności:** zastosowanie portfela i usprawnienie elektronicznych procesów identyfikacji i uwierzytelniania może ułatwić nowym graczom na oferowanie swoich usług online – zarówno tych finansowych, jak i innych.

Ponadto portfele mogą stać się narzędziem wykorzystywanym także bezpośrednio w procesie inicjowania płatności i wykroczyć poza powyższe ramy – dostarczania mocnego uwierzytelnienia użytkownika (Strong Customer Authentication – SCA), identyfikacji czy uwierzytelniania użytkowników. Informacje transakcyjne zapisane w portfelu będą mogły służyć do szybszego inicjowania i dokonywania transakcji online (np. przez szybkie przekazanie danych karty płatniczej czy przekazanie danych adresowych i kontaktowych klienta). Nietrudno też wyobrazić sobie, że portfele same w sobie zostaną wzbogacone o narzędzia inicjowania i potencjalnie przyjmowania płatności w oparciu o infrastrukturę kartową oraz open banking. Możliwość integracji kilku różnych procesów w ramach jednego narzędzia da rynkowi bodziec do jeszcze lepszej obsługi klienta i potencjalnie do budowania usług i produktów, które do tej pory realizowane były etapami, wymagały wykorzystania chociażby skanów dokumentów przesyłanych za pośrednictwem poczty e-mail czy nie były możliwe do realizacji w pełni online.

Wykorzystanie europejskiego portfela cyfrowej tożsamości – kontekst AML

Dyrektywa dotycząca przeciwdziałania praniu pieniędzy (Anti-Money Laundering – AML) to przepisy, które wprowadziły szereg procedur, standardów i narzędzi nałożonych na sektor finansowy mających za cel utrudnienie lub uniemożliwienie prania brudnych pieniędzy i sponsorowania terroryzmu. Najważniejszymi filarami dyrektywy AML w kontekście interakcji instytucji z klientami, są:

1. **Identyfikacja klienta (ang. Know Your Customer, KYC) -** instytucje, które zostały objęte obowiązkami narzuconymi przez dyrektywę AML zobowiązane są do identyfikacji swoich klientów, do przechowywania odpowiednich dokumentów i informacji, aby skutecznie móc weryfikować osoby, które za ich pośrednictwem realizują transakcje.

2. **Monitorowanie transakcji** – dyrektywa AML zobowiązuje instytucje finansowe także do bieżącego monitorowania transakcji realizowanych przez klientów. Celem monitorowania ma być identyfikowanie i raportowanie ryzykownych i niebezpiecznych transakcji.

3. **Transakcje anonimowe** – ograniczenie dopuszczalności transakcji anonimowych tj. bez skutecznej identyfikacji osoby zlecającej np. w przypadku popularnych niegdyś kart przedpłaconych.

Portfele cyfrowej tożsamości jako narzędzie usprawnią klientom korzystanie z usług online, pozwolą instytucjom na rozwój i wdrażanie procesów z łatwą, pełną i pewną identyfikacją klienta. Wykorzystanie tych nowych możliwości sprawi, że bezpieczeństwo klientów i zgodność instytucji z narzuconymi procedurami i standardami staną się jeszcze prostsze do spełnienia. W zakresie nakreślonych powyżej obszarów EUDI znajdą zastosowanie do:

1. Identyfikacji klienta.

2. Uwierzytelnienia klienta.

3. Autoryzacji realizowanych transakcji.

3.2. Problem jednolitych usług elektronicznych w ramach UE

Analiza w kontekście wdrożenia eIDAS 1.0

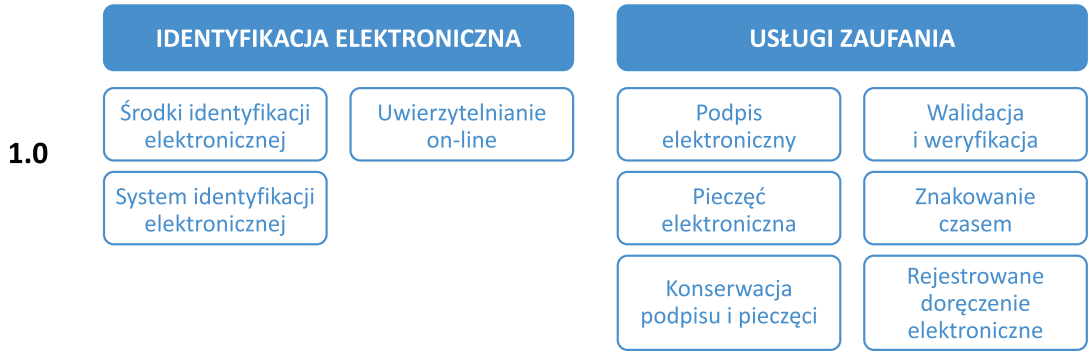
Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE [rozporządzenie eIDAS] obowiązuje od 2016 roku. Podstawowymi celami rozporządzenia było[35]:

- zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi,

- rozwój jednolitego rynku cyfrowego poprzez tworzenie odpowiednich warunków sprzyjających wzajemnemu transgranicznemu uznawaniu głównych aktywatorów, takich jak elektroniczna identyfikacja, dokumenty elektroniczne, podpisy elektroniczne i usługi doręczeń elektronicznych, oraz odpowiednich warunków sprzyjających interoperacyjności usług administracji elektronicznej w całej Unii Europejskiej

- zniesienie, przynajmniej w przypadku usług publicznych, istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach członkowskich w celu uwierzytelniania

[35] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32014R0910 (dostęp 14.03.2024 r.)



Rysunek 20. eIDAS 1.0 – co przyniósł?

U podstaw aktualnie obowiązującego rozporządzenia eIDAS (rozporządzenie 1.0) stały dwa pojęcia: identyfikacja elektroniczna, która miała zapewnić stronom bezpieczne uwierzytelnianie się w świecie online oraz usługi zaufania, których celem jest zawieranie bezpiecznych transakcji za pomocą takich jak narzędzi jak: podpis elektroniczny czy rejestrowane doręczenie elektroniczne.

Mimo że eIDAS 1.0 był ważnym krokiem naprzód w harmonizacji przepisów dotyczących identyfikacji elektronicznej i usług zaufania w UE, istnieją pewne czynniki, które wpłynęły na to, że nie doszło do pełnego wdrożenia jednolitych usług cyfrowych w UE. Oto kilka możliwych powodów:

1. Brak pełnej harmonizacji: Chociaż eIDAS 1.0 wprowadziło jednolite ramy prawne dla identyfikacji elektronicznej i usług zaufania w UE, niektóre obszary pozostają nieharmonizowane, takie jak interoperacyjność. W rezultacie, różnice w przepisach krajowych, w tym w wymaganiach interoperacyjności mogły utrudnić pełne wdrożenie jednolitych usług cyfrowych w skali UE.

2. Różnorodność rynków wewnętrznych: UE składa się z różnych rynków wewnętrznych, z różnymi językami, kulturami, zwyczajami i systemami administracyjnymi. Różnice te mogły wpłynąć na wdrożenie jednolitych usług cyfrowych, ponieważ wymagają dostosowania do lokalnych uwarunkowań.

3. Różnorodność interesariuszy: Wdrożenie jednolitych usług cyfrowych w UE wymaga współpracy różnych interesariuszy, takich jak państwa członkowskie, dostawcy usług cyfrowych, sektor prywatny i publiczny itp. Różnorodność interesariuszy mogła wpłynąć na proces wdrożenia, ze względu na różnice w interesach, priorytetach i podejściach.

4. Brak kompetencji cyfrowych i akceptacji społeczeństwa: Wprowadzenie jednolitych usług cyfrowych wymaga pełnego zaufania i akceptacji ze strony społeczeństwa, zarówno w kontekście prywatności, ochrony danych osobowych, jak i bezpieczeństwa cyfrowego. Brak pełnego zaufania społeczeństwa mogło wpłynąć na adopcję i wdrożenie jednolitych usług cyfrowych na szeroką skalę.

Status usług identyfikacji i usług zaufania

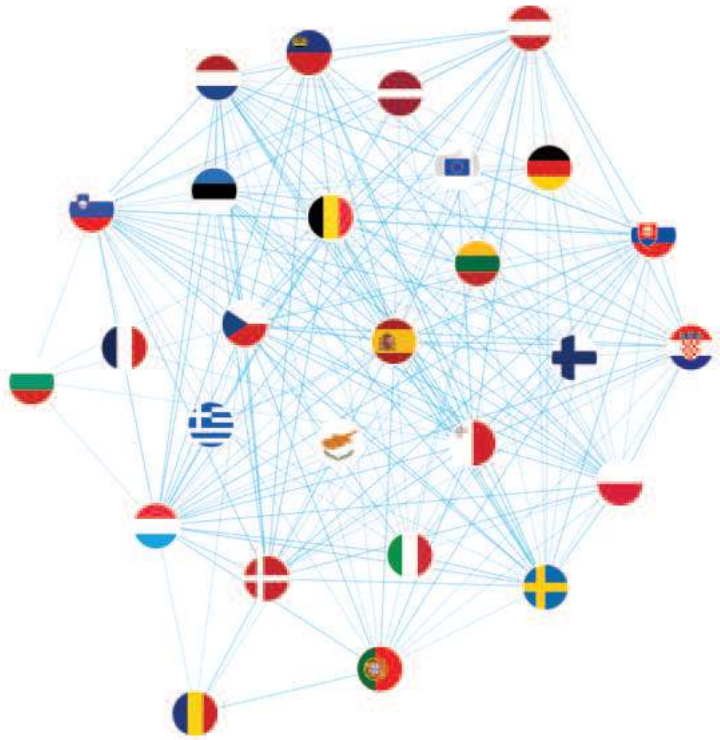
Z danych dostępnych na dzień 08 marca 2024, 24 z 27 krajów członkowskich notyfikowało przynajmniej jeden system identyfikacji elektronicznej. Są to systemy notyfikowane na najwyższym poziomie bezpieczeństwa (wysoki), jak i średnim poziomie bezpieczeństwa. W ten sposób, w ramach poszczególnych krajów, obywatele mają łatwy dostęp do usług administracji publicznej.

Natomiast jeśli chodzi o perspektywę paneuropejską, kraje członkowskie w założeniu mogą się ze sobą komunikować za pomocą węzłów eIDAS (eIDAS nodes). Sieć eIDAS składa się z połączonych ze sobą węzłów eIDAS, po jednym na kraj uczestniczący, które mogą żądać uwierzytelniania transgranicznego lub je zapewniać. Obowiązkiem każdego kraju jest:

- wdrożyć swój węzeł eIDAS oraz
- wspierać podłączenie krajowych dostawców tożsamości i dostawców atrybutów do węzła eIDAS, udostępniając w ten sposób ich krajowe systemy identyfikacji elektronicznej na potrzeby transgranicznych usług online.

Komisja Europejska prezentuje publicznie aktualne połączenia między węzłami eIDAS sieci eIDAS w oparciu o deklarację państw członkowskich[36]. Wybrane dane prezentują się następująco:

[36] https://eidas.ec.europa.eu/efda/browse/notification/eid-chapter-contacts (dostęp 15.03.2024 r.)



Rysunek 21. Powiązania notyfikowanych systemów identyfikacji elektronicznej UE (źródło: https://eidas.ec.europa.eu)

Tabela 2. Zestawienie krajów europejskich, które obsługują transgraniczny węzeł eIDAS

Kraj	Liczba państw, która obsługuje środki identyfikacji elektronicznej z danego kraju	Liczba państw, których środki identyfikacji elektronicznej są obsługiwane przez dany kraj
Austria	14	17
Belgia	17	17
Bułgaria	0	5
Chorwacja	12	14
Czechy	22	19
Cypr	0	3
Dania	15	15
Estonia	13	13
Finlandia	0	20
Francja	2	0
Grecja	0	9
Niemcy	13	0
Polska	14	17
Islandia	0	0
Węgry	0	0
Irlandia	0	0
Włochy	12	4

Tabela 2. cd.

Kraj	Liczba państw, która obsługuje środki identyfikacji elektronicznej z danego kraju	Liczba państw, których środki identyfikacji elektronicznej są obsługiwane przez dany kraj
Łotwa	11	0
Lichtenstein	14	10
Litwa	12	0
Luksemburg	21	14
Malta	16	13
Holandia	15	17
Portugalia	14	5
Hiszpania	17	19
Norwegia	0	0
Rumunia	2	5
Słowacja	16	16
Słowenia	15	20
Szwecja	15	17

Na podstawie dostępnych danych **(tabela 2)** można wywnioskować, że problem jednolitych usług elektronicznych rzeczywiście występuje. W kilku krajach są nawet przypadki, gdzie nie występuje integracja ż żadnym innym krajem w zakresie obsługi środków identyfikacji elektronicznej: Norwegia, Węgry, Irlandia.

Inne dane wskazują z kolei, że 19 z 27 krajów umożliwia logowanie się do portalu Komisji Europejskiej w domenie EU LOGIN[37].

Perspektywa polska

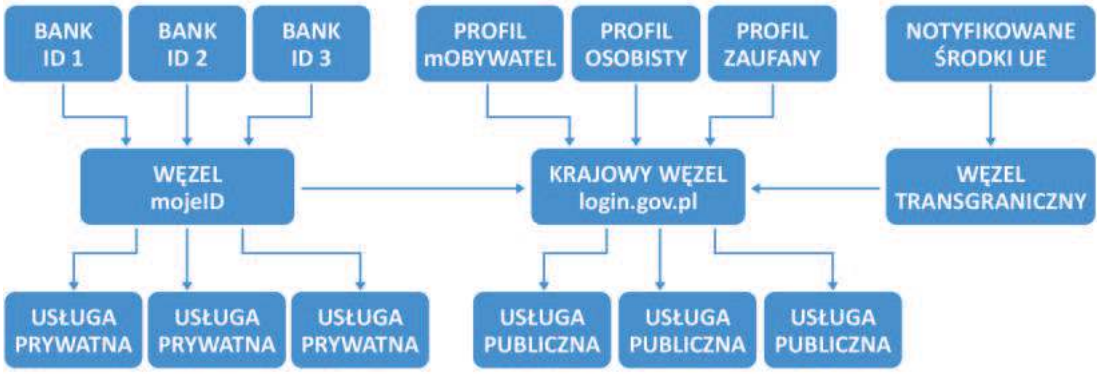
W Polsce funkcjonują następujące środki identyfikacji elektronicznej:

- profil zaufany
- profil osobisty
- profil mObywatel
- bankowe środki identyfikacji elektronicznej.

Podstawowym użytkownikiem środków identyfikacji elektronicznej są podmioty administracji publicznej, które za pomocą krajowego węzła login.gov.pl umożliwiają identyfikację z wykorzystaniem wszystkich dostępnych środków identyfikacji elektronicznej. Krajowy węzeł identyfikacji elektronicznej co do zasady umożliwia korzystanie z publicznych środków identyfikacji udostępnianych przez ministra cyfryzacji, tj. profile zaufany, osobisty oraz mObywatel. W ostatnim czasie Minister Cyfryzacji dopuścił także możliwość korzystania z profilu osobistego i profilu mObywatel dla podmiotów gospodarczych na podstawie jednostkowych decyzji. Węzeł krajowy udostępnia także bankowe środki identyfikacji elektronicznej – udostępnienie to jest realizowane tylko i wyłącznie na potrzeby podmiotów publicznych i realizowane jest z wykorzystaniem funkcjonalności sytemu mojeID. Sam system mojeID umożliwia obsługę podmiotów prywatnych i udostępnia im na podstawie umowy środki identyfikacji elektronicznej z systemów bankowych. System ten jest z powodzeniem stosowany przez podmioty gospodarcze, które spełniają kryteria dostępu do usługi. Należy nadmienić, że system mojeID nie jest udostępniany bankom i instytucjom finansowym do świadczenia usług objętych obowiązkami ustawy o przeciwdziałaniu praniu brudnych pieniędzy.

Poniższy graf prezentuje podstawowy model funkcjonowania krajowych środków identyfikacji elektronicznej, które stanowią podstawę krajowego schematu identyfikacji elektronicznej.

[37] https://webgate.ec.europa.eu/cas/login?loginRequestId=ECAS_LR-14628979-CWmVRoxqNaZ39pG2DbEWuHcXL1tWX2jWV78j-BZonWvjGTorzjnXa9qfE96cMnXoxojOxo95kDYk1cWKYl8sakO-r-S0vSrmBGYC7OPR31u7PsG-dcJ43zZOsoJJgxfkSggh7MGAYoskij-xabjjfwfbGxk2NBOpsjFzzJumzWcA0ACuAQYQTEziLtbiOsDQI-wDDzxb6G (dostęp 15.03.2024.)



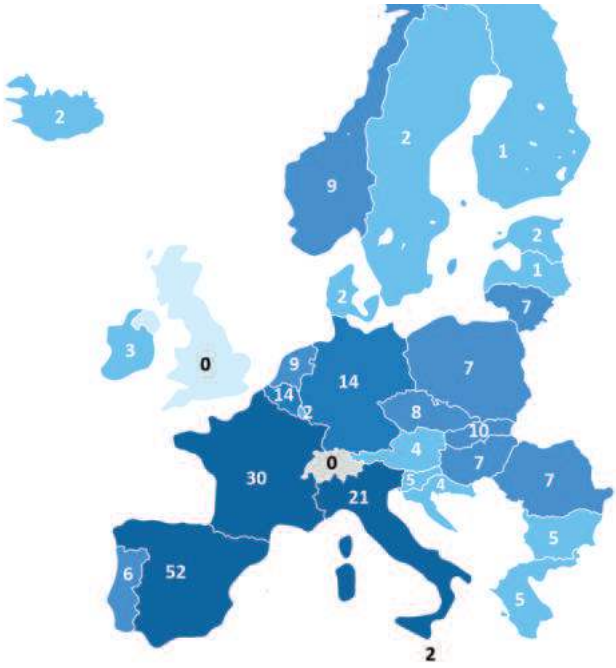
Rysunek 22. Środki identyfikacji elektronicznej funkcjonujące w Polsce

Rysunek 23. Rozpoznawanie polskich środków identyfikacji w UE (źródło: https://eidas.ec.europa.eu)

Polska notyfikowała dwa udostępniane przez ministra cyfryzacji środki identyfikacji elektronicznej profil zaufany i profil osobisty. Profil zaufany został notyfikowany na poziomie średnim bezpieczeństwa, natomiast profil osobisty na poziomie wysokim. Notyfikacja oznacza, że wskazane polskie środki są rozpoznawane w usługach publicznych w innych krajach Unii Europejskiej. Poniższy graf prezentuje informacje o krajach, w których profil zaufany i profil osobisty są rozpoznawane.

Jeżeli chodzi o usługi zaufania, światowy i europejski rynek usług zaufania, ze szczególnym uwzględnieniem podpisu elektronicznego rozwija się bardzo dynamicznie, przede wszystkim ze względu na aktywne użycie usług zaufania do procesów transformacji cyfrowej w przedsiębiorstwach oraz administracji publicznej. Rysunek 24 prezentuje mapę dostawców kwalifikowanych usług zaufania wg stanu na dzień 15 marca 2024[38].

[38] https://eidas.ec.europa.eu/efda/tl-browser/#/screen/statistics (dostęp 15.03.2024).



Rysunek 24. Liczba aktywnych dostawców kwalifikowanych usług zaufania – stan na 15.03.2024

Na koniec 2023 roku, największą liczbę usług zaufania stanowiła usługa kwalifikowanych certyfikatów podpisu elektronicznego – 168 dostawców z Europy dostarczało tę usługę[39].

Oczekiwania rozwojowe

Rozporządzenie eIDAS uchwalone w 2014 roku było rewolucją, jeżeli chodzi o dostarczenie prawnych narzędzi w postaci identyfikacji elektronicznej oraz usług zaufania. Wciąż jednak występują bariery w dostępie do transgranicznych usług online (niska interoperacyjność na poziomie krajów UE), jak i skorzystania z niektórych usług zaufania, takich jak doręczenia elektroniczne. Wciąż aktualne są następujące oczekiwania rozwojowe:

- Pełna interoperacyjność: jednym z głównych celów eIDAS jest zapewnienie pełnej interoperacyjności usług elektronicznej identyfikacji między różnymi krajami UE.
- Rozwój usług zaufania: powszechna dostępność do podpisu elektronicznego czy usług doręczeń elektronicznych.
- Integracja rozwiązań z sektorem prywatnym i publicznym: rozwój eIDAS powinien prowadzić do szerszego przyjmowania technologii identyfikacji elektronicznej zarówno przez sektor publiczny, jak i prywatny. To oznacza integrację tych rozwiązań w różnych obszarach, od usług rządowych po sektor bankowy i handel elektroniczny.
- Edukacja i świadomość: konieczne jest edukowanie użytkowników końcowych, przedsiębiorstw i instytucji na temat korzyści płynących z korzystania z usług identyfikacji elektronicznej i usług zaufania. Wzrost świadomości na temat eIDAS może przyczynić się do zwiększenia zaufania do transakcji elektronicznych.

Więcej o oczekiwaniach rozwojowych oraz zaletach jednolitego podejścia do cyfrowej tożsamości w kontekście nowelizowanego rozporządzenia eIDAS przedstawiono w rozdziale 3.1.

3.3. Zagadnienie bezpieczeństwa

Prace nad wspólnym rozwiązaniem tożsamości cyfrowej w Europie zostały podjęte z kilku kluczowych powodów, z których bezpieczeństwo jest jednym z najważniejszych. W preambule nowelizowanego rozporządzenia wskazano, że Europejskie ramy tożsamości cyfrowej mają na celu[40]:

- ulepszenie skuteczności aktualnego rozporządzenia eIDAS, w tym rozszerzenie korzyści wynikających

[39] Na podstawie opracowań własnych Obserwatorium.biz oraz źródeł dostępnych na https://eidas.ec.europa.eu

[40] https://www.europarl.europa.eu/doceo/document/A-9-2023-0038-AM-006-006_PL.pdf

z niego na sektor prywatny, a także promowanie zaufanych tożsamości cyfrowych dla wszystkich Europejczyków (motyw 1).

- zapewnienie kontroli nad tożsamością i danymi – jest to odpowiedź na wezwanie Rady Europejskiej do stworzenia ogólnounijnych ram bezpiecznej publicznej identyfikacji elektronicznej, które pozwolą obywatelom kontrolować ich tożsamość i dane w internecie oraz ułatwią dostęp do usług publicznych, prywatnych i transgranicznych (motyw 2).

- ochronę prywatności i bezpieczeństwo w cyberprzestrzeni. W Europejskiej deklaracji praw i zasad cyfrowych[41] podkreśla się prawo każdego do technologii, produktów i usług cyfrowych, które są bezpieczne i strzegą prywatności, a także ochronę przed cyberprzestępczością, w tym naruszeniami ochrony danych i kradzieżą tożsamości (motyw 4).

- zapewnienie zharmonizowanych ram tożsamości cyfrowych, które mają przyczynić się do większej integracji cyfrowej Unii, umożliwiając obywatelom i rezydentom korzystanie z cyfryzacji przy jednoczesnym zwiększeniu przejrzystości i ochrony ich praw (motyw 6).

- nowe podejście ma na celu redukcję ryzyka i kosztów wynikających z obecnej fragmentacji systemów identyfikacji elektronicznej i zwiększyć integrację rynku wewnętrznego poprzez bezpieczne, godne zaufania i zharmonizowane środki identyfikacji (motyw 7).

- zwiększenie odporności na cyberataki poprzez oparcie portfeli tożsamości cyfrowej o wspólne normy i specyfikacje techniczne w celu zapewnienia niezakłóconej interoperacyjności, ale również znaczącego zmniejszenia potencjalnego ryzyka związanego z postępującą cyfryzacją dla obywateli i rezydentów Unii oraz dla przedsiębiorstw (motyw 19).

- zapewnienie bezpieczeństwa już na etapie projektowania, uwzględniając przy tym zaawansowane zabezpieczenia służące ochronie przed kradzieżą tożsamości i innymi rodzajami kradzieży danych, atakami prowadzącymi do odmowy usługi (ang. denial of service) oraz wszelkimi innymi zagrożeniami cyberbezpieczeństwa; rozwiązania bezpieczeństwa powinny obejmować najnowocześniejsze metody szyfrowania i przechowywania danych, które dostępne są wyłącznie dla użytkownika i możliwe do odszyfrowania tylko przez niego, i które oparte są na pełnym szyfrowaniu komunikacji z innymi europejskimi portfelami tożsamości cyfrowej i stronami ufającymi (motyw 31).

W preambule rozporządzenia eIDAS 2.0 wielokrotnie podkreślono znaczenie bezpieczeństwa jako kluczowego elementu wspólnych europejskich ram tożsamości cyfrowej. Jest to odpowiedź na rosnącą potrzebę ochrony danych osobowych i prywatności obywateli w erze cyfryzacji oraz w obliczu wzrastających zagrożeń cybernetycznych.

W rozporządzeniu przyjęto mechanizm, który ma zapewnić weryfikację implementacji założeń przyjętych w preambule. Tym mechanizmem jest certyfikacja zgodności europejskich portfeli tożsamości cyfrowej, która wynika z art. 5c rozporządzenia, i która jest praktycznym walidatorem zasad bezpieczeństwa wynikających z preambuły. Każdy portfel musi być certyfikowany przez akredytowane jednostki oceniające zgodność, co ma zagwarantować i potwierdzić wysoki poziom jego bezpieczeństwa. W tym kontekście Komisja Europejska jest zobowiązana do przyjęcia aktów wykonawczych, które ustanowią wykaz norm referencyjnych oraz specyfikacje i procedury certyfikacji.

W artykule 12a dotyczącym certyfikacji systemów identyfikacji elektronicznej zadbano także o wymóg cyklicznej (co 2 lata) oceny podatności na zagrożenia, która ma być też podstawą do utrzymania ważności certyfikatu zgodności (ważność certyfikatu zgodności ma wynosić 5 lat). Europejskie portfele tożsamości cyfrowej mają podlegać regularnym ocenom podatności, które mają na celu wykrywanie wszelkich podatności i zagrożeń związanych z cyberbezpieczeństwem. W przypadku gdy zostaną stwierdzone podatności na zagrożenia i nie zostaną one wyeliminowane, certyfikacja zostaje odwołana.

Poza aspektami bezpieczeństwa, wynikającymi bezpośrednio z rozporządzenia eIDAS 2.0, należy wskazać na prowadzone prace komitetu technicznego CEN/TC 224 pod Europejskim Komitetem Standaryzacyjnym (CEN). Celem prac komitetu jest wypracowanie jasnych wytycznych dotyczących procesu włączenia danych identyfikacyjnych użytkownika (osoby fizycznej lub prawnej) do portfela. Wytyczne uwzględniają wymaganie wynikające z rozporządzenia z art. 5 lit d., stanowiące, że portfele muszą spełniać wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa, w szczególności w zakresie wymogów dotyczących potwierdzania i weryfikacji tożsamości, zarządzania środkami identyfikacji elektronicznej oraz uwierzytelniania. Opracowywane wytyczne mają w szczególności uwzględniać zalecenia dotyczące[42]:

[41] https://digital-strategy.ec.europa.eu/pl/library/european-declaration-digital-rights-and-principles (dostęp 10.04.2024)

[42] Źródło: CEN TC 224 WG20, dokument roboczy opracowania CEN TC 224, 10/2023. Dostęp za pośrednictwem zasobów ETSI w ramach członkostwa Obserwatorium.biz

- sprawdzenia kompatybilności portfela oraz urządzenia przechowującego portfel z wymaganiami dostawcy danych identyfikujących oraz właściciela schematu tożsamości;
- sprawdzenia powiązania między portfelem a urządzeniem przechowującym portfel z wnioskodawcą;
- rejestracji portfela oraz urządzenia przechowującego portfel.

Jednocześnie w oparciu o będące w opracowaniu normy techniczne i wytyczne, państwa członkowskie będą musiały ustanowić wewnętrzne procedury krajowe, które będą respektowały wydawanie portfeli na wysokim poziomie bezpieczeństwa. Na stan 21 marca 2023, następujące przykładowe państwa członkowskie posiadają systemy identyfikacji elektronicznej notyfikowane na poziomie średnim lub wysokim:

Kraj	Poziom średni	Poziom wysoki
Polska	Profil zaufany	Profil osobisty (dowód osobisty z warstwą elektroniczną)
Francja	Tak	**Nie**
Dania	Tak	**Nie**
Włochy	Tak	Tak
Czechy	Tak	Tak
Bułgaria	Tak	Tak
Szwecja	Tak	Tak
Łotwa	Tak	Tak
Holandia	Tak	Tak

Fakt, że dany kraj posiada system identyfikacji elektronicznej na poziomie wysokim wcale nie oznacza, że jego wykorzystanie jest powszechne i umożliwi łatwe uruchomienie procesu aktywacji portfela.

Z drugiej strony kraj, który nie posiada żadnego systemu identyfikacji elektronicznej na poziomie wysokim, musi się przygotować na procedurę stworzenia lub podwyższenia poziomu bezpieczeństwa z średniego na wysoki. W tym celu w ramach komitetu normalizacyjnego ETSI oraz standardu technicznego TS *119 461 Policy and security requirements for trust service components providing identity proofing of trust service subjects*[43], trwają pracę nad wypracowaniem mechanizmów podniesienia poziomu bezpieczeństwa środka identyfikacji elektronicznej z poziomu średniego na wysoki.

3.4. Zagadnienia kosztów

Przy okazji wdrożenia projektów o tak dużej skali jak europejski portfel tożsamości cyfrowej naturalnie pojawia się zagadnienie kosztów inwestycyjnych i kosztów utrzymania oraz potencjalnych strumieni przychodu. Podobnie jest i w przypadku EUDI, jednak tutaj do czynienia mamy z bardziej skomplikowaną sytuacją. Wszystkie państwa członkowskie będą zobowiązane do wdrożenia portfela narodowego i spełnienia szeregu warunków zawartych w rozporządzeniu eIDAS 2.0 między innymi dotyczących darmowego dostępu do portfeli i zawartych w nich funkcjonalności, takich jak dostęp do PID, autoryzacji transakcji czy wreszcie podpisów kwalifikowanych dla osób fizycznych.

Oczywistym komponentem wdrożenia portfeli są bezpośrednie koszty developmentu, wdrożenia, utrzymania czy nawet koszt dotarcia do użytkowników czy to w postaci reklam w mediach tradycyjnych i społecznościowych czy materiałów edukacyjnych. Koszt samego stworzenia aplikacji mitygowany jest tym, że każde państwo nie będzie musiało tworzyć własnej nowej aplikacji, ale będzie mogło wykorzystać do tego celu istniejące już rozwiązania własne, zewnętrzne lub skorzystać z kodu Open Source wypracowanego w ramach

[43] https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf (dostęp 21.03.2024 r.) – jest to aktualna wersja standardu. W opracowaniu jest rewizja dokumentu. Planowana publikacja czerwiec 2024.

wielkoskalowych pilotaży (European Digital Identity · GitHub). W związku z powyższym każde z państw członkowskich będzie mogło, przynajmniej częściowo, zredukować koszty związane z wdrożeniem, natomiast do obsłużenia pozostaną pozostałe składniki kosztowe związane z komunikacją, utrzymaniem czy udostępnieniem dodatkowych funkcjonalności.

Najważniejszą funkcjonalnością, jaka przychodzi na myśl w tym kontekście, jest zawarte w rozporządzeniu zobowiązanie dotyczące dostarczenia bezpłatnych kwalifikowanych podpisów elektronicznych dla osób fizycznych do wykorzystania do czynności innych niż profesjonalne. Motyw 20 rozporządzenia jednoznacznie wskazuje, że użycie kwalifikowanego podpisu elektronicznego powinno być nieodpłatne dla wszystkich osób fizycznych do celów innych niż profesjonalne. Państwa członkowskie powinny móc ustanowić środki zapobiegające nieodpłatnemu użyciu kwalifikowanych podpisów elektronicznych przez osoby fizyczne do celów profesjonalnych, przy jednoczesnym zapewnieniu, aby wszelkie takie środki były proporcjonalne do zidentyfikowanego ryzyka oraz uzasadnione.

Rozporządzenie w tym zakresie, mówi jedynie o tym, że usługa taka ma zostać bezpłatnie udostępniona osobom fizycznym, natomiast oczywistym jest, że jej wdrożenie i dostarczenie nie będzie możliwe bezkosztowo, niezależnie czy dostawcą certyfikatu do podpisu będzie podmiot publiczny czy prywatny, z którym dane państwo podpisze umowę na świadczenie tego typu usługi. Na początku funkcjonowania EUDI być może nie będzie to problematyczne ze względu na organiczną liczbę użytkowników, o tyle wraz z rozwojem i popularyzacją portfeli koszt utrzymania usługi będzie coraz wyższy. Poszczególne państwa członkowskie powinny już teraz przygotować się na konieczność zmierzenia się z takim kosztem i spróbować zoptymalizować koszty w tym zakresie wedle swoich możliwości technicznych i przewidywanej skali użycia portfeli.

Powyższa lista kosztów, z którymi przyjdzie się mierzyć wszystkim państwom członkowskim, nie jest oczywiście listą zamkniętą. Wciąż pozostaje szereg kwestii wymagających rozstrzygnięcia, kwestii infrastrukturalnych jak na przykład sieć akceptacji portfeli cyfrowej tożsamości – online i offline czy też relacji portfela z innymi obszarami dotykającymi cyfryzacji na poziomie europejskim jak eDelivery, podpisami elektronicznymi w kontekstach komercyjnych/służbowych, open bankingiem czy też planowanym cyfrowym euro.

Jak pozycjonować polskie rozwiązania na tle wspólnych rozwiązań europejskich

4.1. Zakres zbieżności i rozbieżności polskich rozwiązań w odniesieniu do koncepcji europejskiej e-tożsamości

Notyfikacja polskich środków identyfikacji elektronicznej stanowiła pewien kamień milowy na polskim rynku usług zaufania. Poniżej została zaprezentowana tabela, w której krajowe rozwiązania (profil mObywatel, profil zaufany oraz profil osobisty) zostały porównane z europejskim profilem e-tożsamości.

1. Profil mObywatel	
Definicja	Środek identyfikacji elektronicznej, o którym mowa w art. 3 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, obsługiwany w aplikacji mObywatel. Identyfikacja działa z wykorzystaniem certyfikatu podstawowego Obywatela, przechowywanym w szyfrowanym kontenerze aplikacji mObywatel; wydawany zgodnie z art. 14 ust. 1-3 ustawy o aplikacji mObywatel
Zakres danych	Imię (imiona), nazwisko, datę urodzenia, dane z Rejestru PESEL, zdjęcie z Rejestru Dowodów Osobistych, a także informacje o numerze, serii, dacie wydania i ważności dokumentu mObywatel
Użycie	Usługi dostępne na terytorium RP Obowiązek przyjmowania dokumentu mObywatel w celach identyfikacji i weryfikacji swoich klientów, jednak wyłącznie przy fizycznej obecności stron
Sposób wykorzystania	Załatwianie spraw urzędowych online. Dostęp do danych dostępnych w ramach usługi portalu i aplikacji mObywatel.
Poziom wiarygodności	Średni poziom bezpieczeństwa
Sposób rejestracji	Aplikacja mObywatel: 1. Pobranie aplikacji. 2. Akceptacja regulaminu i ustawienie hasła. 3. Potwierdzenie tożsamości profilem zaufanym, e-dowodem lub bankowością elektroniczną. Portal mObywatel: 1. Wejście na stronę mObywatel.gov.pl (nastąpi przekierowanie do login.gov.pl) 2. Zalogowanie się do usługi poprzez: bankowość elektroniczną, profil zaufany, e-dowód, USE eID, aplikacja mObywatel).
Sposób utworzenia środka	Profil mObywatel jest wydawany użytkownikowi aplikacji mObywatel automatycznie z certyfikatem podstawowym.

2. Profil zaufany	
Definicja	Środek identyfikacji elektronicznej. zestaw danych identyfikujących i opisujących osobę fizyczną, która posiada pełną albo ograniczoną zdolność do czynności prawnych, który został wydany w sposób, o którym mowa w art. 20c albo art. 20cb ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne
Zakres danych	Imię (imiona), nazwisko, data urodzenia, numer PESEL
Użycie	Usługi dostępne na terytorium RP oraz UE Użycie jest ralizowane po uwierzytelnieniu użytkownika jedną z metod: login+ hasło+sms lub bankowe środki uwierzytelniajace
Sposób wykorzystania	Potwierdzenie tożsamości w Internecie do usług administracji publicznej. Składanie i podpisywanie dokumentów podpisem elektronicznym (jeśli jest to niezbędne do załatwienia twojej sprawy). Możliwość logowania do systemów informatycznych administracji publicznej, np: Platforma Usług Elektronicznych Zakładu Ubezpieczeń Społecznych (PUE ZUS), Internetowe Konto Pacjenta (IKP), e-Urząd Skarbowy itd.
Poziom wiarygodności	Średni poziom bezpieczeństwa
Sposób rejestracji	Profil zaufany jest darmowy, a rejestracja może zostać wykonana za pomocą następujących metod: • bank lub inny dostawca tożsamości, • rozmowa wideo z urzędnikiem, • e-dowód, • w placówce.
Sposób utworzenia środka	Środek tworzony jest jako zapis w systemie bazodanowym Ministra Cyfryzacji. Z profilem tworzone są środki uwierzytelniające w postaci identyfikatora, hasła oraz przypisanego numeru telefonu. Dostęp do profilu zaufanego może być realizowany z wykorzystaniem bankowych metod uwierzytelnienia, przypisanych do profilu.

3. Profil osobisty	
Definicja	Środek identyfikacji elektronicznej; Zestaw danych zapisanych wewnątrz e-dowodu, umożliwia logowanie do portali administracji publicznej. Profil osobisty jest zamieszczony w dowodzie osobistym każdej osoby mającej pełną lub ograniczoną zdolność do czynności prawnych (powyżej 13 roku życia).
Zakres danych	Imię (imiona), nazwisko, obywatelstwo, numer PESEL, datę i miejsce urodzenia
Użycie	Usługi dostępne na terytorium RP oraz UE, W celu użycia konieczne jest podanie numeru PIN przypisanego do profilu
Sposób wykorzystania	Umożliwia logowanie do portali administracji publicznej oraz pozwala na jednoznaczne zidentyfikowanie osoby korzystającej z usługi internetowej.
Poziom wiarygodności	Certyfikat identyfikacji i uwierzytelnienia, zamieszczony w warstwie elektronicznej dowodu osobistego Wysoki poziom bezpieczeństwa
Sposób rejestracji	Wniosek o wydanie e-dowodu składa się osobiście w Urzędzie gminy.
Sposób utworzenia środka	Profil osobisty jest umieszczony w e-dowodzie i stanowi jego funkcję.

4. Europejski portfel cyfrowej tożsamości	
Definicja	Środek identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych;
Zakres danych	Imię (imiona), nazwisko, zdjęcie, informacje o dokumencie tożsamości, adres, płeć, wiek, stan cywilny, skład rodziny, narodowość lub obywatelstwo, wykształcenie, tytuły i licencje, kwalifikacje zawodowe, tytuły i licencje, pełnomocnictwa i upoważnienia do reprezentowania osób fizycznych lub prawnych, publicznoprawne zezwolenia i licencje, w odniesieniu do osób prawnych – dane finansowe i dane dotyczące przedsiębiorstwa.
Użycie	Usługi publiczne i prywatne dostępne na terytorium UE Użycie wymaga uwierzytelnienia dynamicznego spełniającego wymagania wysokiego poziomu bezpieczeństwa środka identyfikacji.
Sposób wykorzystania	Ma umożliwić identyfikację elektroniczną do usług publicznych i prywatnych, zapewnić brak możliwości śledzenia jego użycia (w tym przez instytucje państwowe), a jednocześnie pozwolić na bezpieczną rejestrację do usług bankowych, mediów oraz kwalifikowanych usług zaufania. Przechowywanie i udostępnianie cyfrowych dokumentów tożsamości, atrybutów oraz stosowanie i rozpoznawanie podpisów kwalifikowanych na terenie Unii Europejskiej
Poziom wiarygodności	Wysoki poziom bezpieczeństwa
Sposób rejestracji	Każdy kraj członkowski UE opracuje własny sposób rejestracji spełniający wymagania wysokiego poziomu wiarygodności.
Sposób utworzenia środka	Środek będzie tworzony za pomocą PID (danych identyfikujących osobę) umieszczanego w portfelu cyfrowej tożsamości wraz z kluczami kryptograficznymi i zabezpieczonego silnymi mechanizmami portfela.

Ryzyko używania na rynku krajowym rozwiązań odmiennych do europejskiej e-tożsamości

5.1. Ograniczenia w rozwoju usług krajowych

Ryzyko używania na rynku krajowym rozwiązań odmiennych od europejskiej e-tożsamości jest wielowymiarowe. Przede wszystkim, takie działania mogą prowadzić do fragmentacji, zwiększając ryzyko i koszty związane ze stosowaniem rozbieżnych rozwiązań krajowych. Ponadto, niespójność w systemach identyfikacji elektronicznej może osłabić rynek wewnętrzny i utrudniać obywatelom i rezydentom Unii identyfikowanie się i potwierdzanie swojej tożsamości w sposób bezpieczny, godny zaufania, przyjazny dla użytkownika oraz zharmonizowany w całej Unii. Zharmonizowane podejście do identyfikacji elektronicznej, jakie proponuje europejski portfel tożsamości cyfrowej, ma na celu zmniejszenie tych ryzyk poprzez stworzenie bardziej zintegrowanej cyfrowo Unii. Ma to sprzyjać czerpaniu korzyści z cyfryzacji przy jednoczesnym zwiększeniu przejrzystości i ochrony praw obywateli i rezydentów UE.

Brak uznawania europejskiego portfela tożsamości cyfrowej przez krajowe systemy może skutkować utrudnieniem dostępu do różnych usług, co może prowadzić do izolacji cyfrowej i nierówności społecznych na tle Europy. Warto również zwrócić uwagę na aspekty związane z bezpieczeństwem i prywatnością, gdyż niespójne systemy mogą nie zapewniać takiego samego poziomu ochrony danych, co systemy zharmonizowane na poziomie UE. Europejskie portfele tożsamości cyfrowej mają również przyczyniać się do zwiększenia ochrony użytkowników przed oszustwami oraz zapewnić wysoki poziom ochrony danych, co może być trudniejsze do osiągnięcia w przypadku rozwiązań krajowych, które nie będą zintegrowane z europejską infrastrukturą i które nie będą respektowały tożsamych rozwiązań na rzecz bezpieczeństwa.

Na polskim rynku funkcjonują liczne rozwiązania służące identyfikacji elektronicznej, których przykłady przedstawiono w rozdziale 4.1. Administracja publiczna udostępnia środki identyfikacji, które co do zasady służą do identyfikacji w podmiotach publicznych, są to profil zaufany i profil osobisty. Jako główne ograniczenie krajowych rozwiązań autorzy raportu wskazują na ich zamknięty charakter, który jest ściśle powiązany z kwestią administrowania danymi osobowymi użytkowników przez podmioty gospodarcze. W Polsce dominującym administratorem danych są banki. Przeprowadzona przez banki procedura AML zapewnia bezpieczeństwo danych osobowych i przywiązanych do nich danych uwierzytelniających, jednocześnie obsługa bankowego środka identyfikacji elektronicznej jest oparta o te same metody co logowanie do konta. W ramach bankowej współpracy istnieje komercyjny system identyfikacji elektronicznej mojeID, który obejmuje zasięgiem większość klientów bankowych na polskim rynku, udostępnia on dane na potrzeby usług prywatnych oraz jest połączony z systemem krajowym.

Ograniczeniem polskiego modelu jest jego centralny charakter, w którym to dostawca usługi identyfikacji elektronicznej decyduje o możliwości udostępnienia środków identyfikacji elektronicznej stronom ufającym. Strony ufające w celu korzystania ze środków identyfikacji elektronicznej korzystają z usług węzłów identyfikacji elektronicznej. Dane użytkownika w procesie identyfikacji zawsze są przekazywane za pośrednictwem węzła tożsamości elektronicznej, którym może być:

- komercyjny – Krajowa Izba Rozliczeniowa, pełniąca rolę właściciela biznesowego i technicznego systemu mojeID,
- krajowy – Ministerstwo Cyfryzacji, będące właścicielem biznesowym systemu udostępniającego uznane krajowo środki identyfikacji elektronicznej.

Kolejnym ograniczeniem dla rynku krajowego jest konieczność utrzymywania przez dostawców tożsamości własnych systemów, rozwiązań oraz narzędzi do potwierdzenia tożsamości, jak i uwierzytelniania. Przykładowo, uzyskanie środka identyfikacji elektronicznej wymaga utrzymywania przez dostawcę rozwiązań takich jak:

- punkty potwierdzania tożsamości,
- systemy do wideo identyfikacji w celu zdalnej weryfikacji tożsamości,
- integracji z bazami dokumentów np. zastrzeżonych,
- integracji z systemami centralnymi w celu sprawdzenia istnienia tożsamości.

Z powyższym wiążą się koszty operacyjne, które każda z instytucji musi ponosić samodzielnie, natomiast nie utworzono rozwiązań, które umożliwiłby finansowanie utrzymywania i użytkowania środków identyfikacji elektronicznej. To także ograniczenia związane z bezpieczeństwem – każdy indywidualny dostawca tożsamości (przykładowo bank) musi posiadać umiejętności w zakresie rozpoznawania autentyczności dokumentów tożsamości oraz wykrywania różnych ataków na tożsamość (więcej opisano w rozdziale 2.2).

Mechanizmy uwierzytelniania są kluczowymi elementami bezpieczeństwa systemów informatycznych, w tym bankowości internetowej, usług online i innych

platform wymagających ochrony danych użytkowników. Istnieje kilka podstawowych rodzajów mechanizmów uwierzytelniania:

- hasła – jest to najbardziej podstawowa forma uwierzytelniania, gdzie użytkownik wprowadza swoje hasło, aby uzyskać dostęp do systemu. Zarządzanie hasłami wymaga od wydawcy stosowania procedur pozwalających na ich bezpieczne przechowywanie, a także umożliwianie użytkownikom zmiany hasła lub odzyskania dostępu w przypadku jego zapomnienia.

- Jednorazowe hasła (One-Time Passwords, OTP) wysyłane są do użytkownika za pośrednictwem wiadomości SMS. Metoda ta wymaga od wydawcy posiadania systemu zdolnego do generowania i wysyłania unikatowych kodów, które są ważne tylko przez krótki okres.

- Komunikaty PUSH wysyłane na aplikację mobilną – to rodzaj uwierzytelnienia dwuskładnikowego, gdzie użytkownik otrzymuje powiadomienie push w zainstalowanej na urządzeniu mobilnym aplikacji. Użytkownik musi potwierdzić próbę zalogowania się, klikając w komunikat. Wydawcy muszą zapewnić niezawodność i bezpieczeństwo przesyłania tych komunikatów.

- Tokeny sprzętowe – są to fizyczne urządzenia generujące kod dostępu (zazwyczaj OTP) w regularnych odstępach czasu. Użytkownik musi wprowadzić wyświetlony na tokenie kod, aby uzyskać dostęp. Zarządzanie tokenami sprzętowymi wymaga logistyki dystrybucji, obsługi i czasem wymiany urządzeń.

Każdy z tych mechanizmów wymaga od ich wydawców nie tylko zapewnienia wysokiego poziomu bezpieczeństwa i ochrony przed atakami, takimi jak phishing czy inne próby oszustwa, ale także zapewnienia odpowiedniej infrastruktury technologicznej i obsługi klienta. Ponadto, wydawcy muszą regularnie aktualizować i testować swoje systemy, aby sprostać rosnącym wymaganiom bezpieczeństwa oraz zmieniającym się zachowaniom i oczekiwaniom użytkowników w zakresie ergonomii.

Szanse w rozwoju rynku

Na polskim rynku funkcjonuje portfel cyfrowej tożsamości o randze krajowej – to aplikacja mObywatel. W aplikacji mobilnej dostępny jest m.in. dokument mObywatel czyli dokument mobilny pozwalający stwierdzić tożsamość i obywatelstwo polskie użytkownika aplikacji mObywatel na terytorium RP w relacjach wzajemnej fizycznej obecności stron[44]. Z danych z listopada 2023, dokument aktywowało 5 mln Polaków[45]. Liczba pobrań aplikacji przekroczyła 16 mln. Inną z ważnych funkcjonalności aplikacji mObywatel jest możliwość uwierzytelnienia do usług administracji publicznej w sposób bardzo wygodny (wymagane jest skanowanie kodu QR oraz podanie 4 cyfrowego PIN).

Na przykładzie mObywatela można zauważyć, że pomimo mnogości rozwiązań (profil zaufany, środki bankowe, e-Dowód) na polskim rynku wciąż było miejsce na narzędzie portfelowe. Aplikacja mObywatel wypełnia pewną lukę jeżeli chodzi o wygodę dot. onboardingu i użycia. Natomiast wciąż aplikacja nie pozwala na jej wykorzystanie poza granicami kraju, jak również nie spełnia przykładowych wymagań wynikających z eIDAS 2.0 jeżeli chodzi o:

- onboarding do portfela na poziomie wysokim – obecnie wystarczającym jest poziom średni;

- nielinkowalność – aktualnie, wszystkie dane przechodzą przez Węzeł Krajowy co umożliwia właścicielowi węzła na śledzenie zapytań przychodzących i wychodzących;

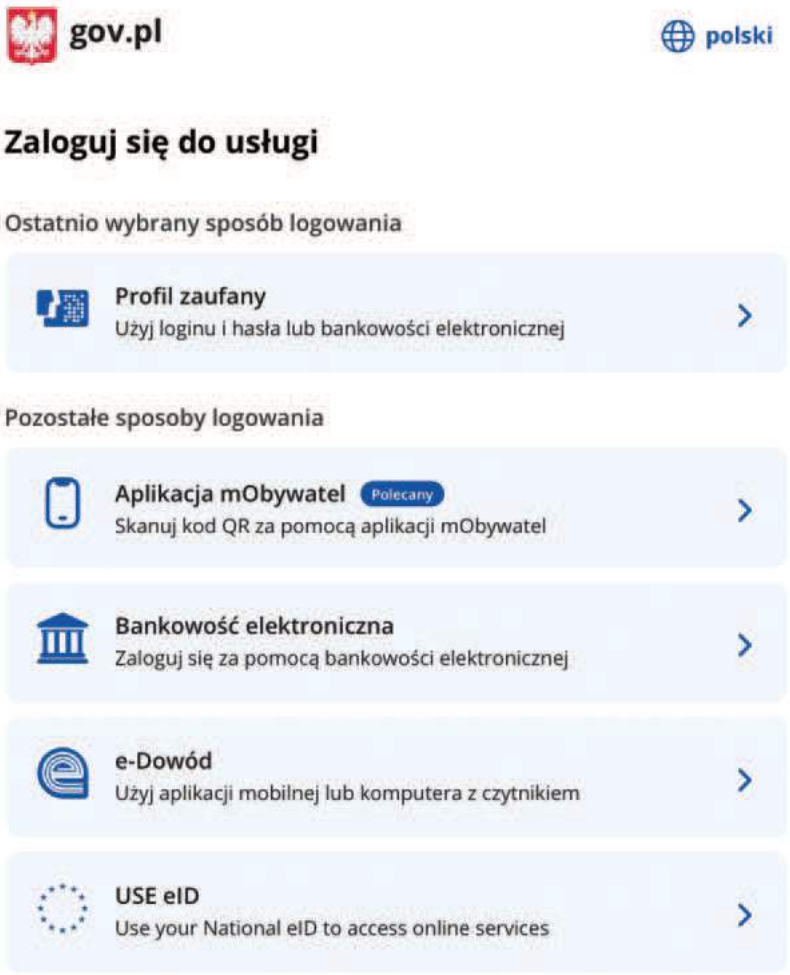
- bezpośrednią kontrolę nad danymi udostępnianymi przez użytkownika – użytkownik nie może wybrać jakie dane chciałby przekazać stronie ufającej. Aktualnie, są to sztywno zdefiniowane kontenery danych przez rozwiązanie techniczne, np.

  - imię, nazwisko, PESEL
  - imię, nazwisko, PESEL, zdjęcie
  - imię, nazwisko, PESEL, obywatelstwo
  - imię, nazwisko, PESEL, numer dowodu osobistego

- interoperacyjność z sektorem prywatnym – nie odnotowano szerokiego wdrożenia z użyciem mObywatela w sektorze prywatnym w procesach online. Wyjątkiem jest tutaj wskazywany na rysunku 25, przykład z domeny gov.pl

Głównymi czynnikami dla rozwoju usług opartych o systemy identyfikacji elektronicznej jest dostępność i łatwość użycia. Systemy identyfikacji elektronicznej muszą być dostępne i łatwe w użyciu dla wszystkich użytkowników, niezależnie od ich

[44] Art. 2 pkt 8 Ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz.U. 2023 poz. 1234).
[45] Dane z konferencji CommonSign pochodzące z prezentacji „03_mObywatel-2.0-kierunki-rozwoju__R.Orlik_COI".



Rysunek 25. Ekran logowania na portalu login.gov.pl

umiejętności technicznych. Przyjazne dla użytkownika interfejsy i procesy mogą zwiększyć adopcję tych technologii wśród szerszego grona odbiorców. Kolejnym czynnikiem jest współpraca międzysektorowa, w tym między sektorem publicznym a prywatnym – ważna dla promowania standardów i praktyk w zakresie identyfikacji elektronicznej. Partnerstwa te mogą prowadzić do innowacji i ulepszeń w systemach identyfikacji. Ważnym czynnikiem jest świadomość i akceptacja społeczna. Rosnąca świadomość korzyści płynących z cyfryzacji i bezpiecznej identyfikacji elektronicznej wśród społeczeństwa jest kluczowa dla promowania jej akceptacji i użytkowania. Edukacja i kampanie informacyjne mogą przyczynić się do zwiększenia zaufania do elektronicznych metod identyfikacji.

Europejski portfel tożsamości cyfrowej ma na celu ograniczenie ryzyk związanych z wykorzystywaniem z rozwiązań krajowych, jak i wykorzystanie istniejących czynników rozwoju rynku usług dla wszystkich obywateli UE.

5.2. Bariery w rozwoju usług transgranicznych

Nowelizacja rozporządzenia eIDAS 1.0 podkreśla, że pomimo podjętych działań wciąż napotykamy na bariery hamujące rozwój usług transgranicznych w Unii Europejskiej. Te przeszkody są zróżnicowane i obejmują przynajmniej następujące aspekty:

- **regulacyjne** wynikające z istnienia różnych przepisów krajowych, które dotyczą między innymi akceptacji różnorodnych metod identyfikacji, co komplikuje procesy transgraniczne,
- **technologiczne** związane z brakiem interoperacyjności systemów i usług, co ogranicza możliwość ich wzajemnego połączenia i efektywnego wykorzystania na skalę europejską,
- **edukacyjne** polegające na niskiej świadomości lub braku zaufania, spowodowane niedostatecznym systemem edukacji w zakresie korzystania

z elektronicznych środków identyfikacji i usług zaufania.

Do tej listy należy dodać barierę opisaną w rozdziale 5.1, dotyczącą braku interoperacyjności pomiędzy sektorem prywatnym a publicznym, szczególnie w zakresie udostępniania publicznych systemów identyfikacji elektronicznej dla ogólnego użytku. Gdyby przedsiębiorstwa i organizacje pozarządowe miały możliwość wykorzystywania państwowych systemów identyfikacji elektronicznej do weryfikacji tożsamości swoich klientów, użytkowników czy partnerów biznesowych, przyniosłoby to znaczące korzyści, takie jak:

- uproszczenie procesów biznesowych, które wymagają weryfikacji tożsamości, co pozwoliłoby na szybszą i bardziej efektywną realizację wielu operacji,
- wzmocnienie bezpieczeństwa poprzez opieranie się na sprawdzonych i bezpiecznych rozwiązaniach, co zwiększyłoby zaufanie użytkowników do transakcji online,
- ułatwienie dostępu do usług online dzięki zwiększeniu dostępności i ułatwieniu procesu logowania oraz weryfikacji tożsamości,
- uproszczenie i zwiększenie przejrzystości procesów compliance, co umożliwiłoby łatwiejsze dostosowanie się do przepisów prawa i norm regulacyjnych.

Współczesna gospodarka oraz administracja publiczna coraz częściej opierają się na procesach cyfrowych, które wymagają skutecznej i bezpiecznej identyfikacji osób fizycznych. To właśnie w tym kontekście pojawia się wyzwanie związane z koniecznością legitymowania się jednolitym identyfikatorem – numerem, który jednoznacznie pozwala na identyfikację obywatela w różnorodnych systemach i usługach. Ta wymagana unifikacja, choć na pierwszy rzut oka wydaje się być rozwiązaniem przynoszącym wiele korzyści, niesie ze sobą również szereg wyzwań i barier, szczególnie widocznych w kontekście prowadzenia działalności gospodarczej oraz zarządzania procesami administracyjnymi na poziomie międzynarodowym.

Na przykładzie Polski, można stwierdzić, że numer PESEL stał się fundamentem dla identyfikacji obywateli, będąc kluczowym elementem w obsłudze wielu procesów biznesowych oraz administracyjnych. Jego uniwersalność i powszechne zastosowanie ułatwiają wiele operacji, od rejestracji w urzędach po procesy bankowe. Niemniej, kiedy próbujemy przenieść te mechanizmy na płaszczyznę międzynarodową, napotykamy na istotne trudności. Kraje takie jak Belgia czy Holandia, podobnie do Polski, utrzymują centralne ewidencje ludności, co ułatwia wewnętrzną organizację i wymianę danych między różnymi instytucjami na poziomie krajowym. Jednakże, systemy te mogą się różnić w zakresie gromadzonych danych, sposobu ich przetwarzania oraz poziomu dostępu dla różnych podmiotów, co komplikuje międzynarodową współpracę i wymianę informacji.

Z drugiej strony mamy przykłady krajów takich jak Niemcy, które nie posiadają bezpośredniego odpowiednika polskiego PESEL. W Niemczech do identyfikacji wykorzystywane są inne dane, jak np. informacje dotyczące miejsca zamieszkania. Ten brak jednolitego systemu identyfikacji na poziomie europejskim prowadzi do tzw. fragmentaryzacji – sytuacji, w której każde państwo członkowskie posiada własny, odrębny system identyfikacji obywateli. Fragmentaryzacja ta jest jednym z głównych wyzwań dla rozwoju usług transgranicznych, gdyż każda próba integracji czy współpracy napotyka na bariery prawne i techniczne wynikające z różnic między krajowymi systemami identyfikacji. Brak harmonijnych przepisów prawa oraz ograniczona interoperacyjność systemów informatycznych to kolejne aspekty, które wywodzą się właśnie z problematyki jednolitego identyfikatora.

Rozdział 3.2 omawia wyzwania związane z wdrażaniem jednolitych usług cyfrowych, wskazując na rozporządzenie eIDAS z 2014 roku, które miało na celu ujednolicenie rynku transgranicznego w UE poprzez wprowadzenie bezpiecznych i jednolitych ram dla usług identyfikacji elektronicznej. Mimo ambitnych celów, główną barierą okazała się niska interoperacyjność między systemami identyfikacji różnych krajów. Problemy te obejmują różnice w regulacjach, standardach technologicznych oraz w akceptacji środków identyfikacji, co utrudnia transgraniczny dostęp do usług cyfrowych i hamuje integrację cyfrowego rynku w Europie. Rozbieżności pomiędzy systemami krajowymi nie tylko komplikują proces identyfikacji dla użytkowników końcowych, ale również stwarzają dodatkowe bariery dla przedsiębiorstw pragnących rozszerzyć swoje usługi na nowe rynki w Unii Europejskiej.

Ponadto, identyfikowane są problemy związane z akceptacją transgraniczną środków identyfikacji elektronicznej. Chociaż rozporządzenie eIDAS ma na celu zapewnienie wzajemnego uznawania środków identyfikacji elektronicznej między państwami członkowskimi, w praktyce proces ten napotyka na liczne przeszkody. Te trudności wynikają częściowo z technicznych aspektów wdrożenia, a częściowo z niejednolitego podejścia do zarządzania tożsamością cyfrową w różnych krajach.

Rezultatem jest sytuacja, w której pełny potencjał rynku transgranicznego pozostaje niewykorzystany,

a obywatele i przedsiębiorstwa nie mogą w pełni korzystać z korzyści płynących z cyfryzacji. Aby sprostać tym wyzwaniom, niezbędne jest rzeczywiste wdrożenie przepisów wynikających z rozporządzenia eIDAS 2.0, tak aby faktyczna interoperacyjność miała możliwość zaistnieć. Oznacza, to że dwa warunki muszą zaistnieć:

#1 Polski portfel cyfrowej tożsamości będzie uznawany i akceptowany przez wszystkie kraje członkowskie bez wyjątku.

#2 Polska jako państwo nie odmówi akceptacji dowolnego portfela z danego kraju UE, o ile został on wydany w schemacie opracowanym przez eIDAS 2.0.

W ramach rozporządzenia eIDAS 2.0, ustanowiono mechanizmy egzekwowania przepisów, w tym wprowadzenie systemu kar dla podmiotów naruszających jego zasady. Zgodnie z art. 16, państwa członkowskie zobowiązane są do wypracowania systemu sankcji, które mają charakter skuteczny, proporcjonalny i odstraszający. Cel ten ma na zapewnić, że wszelkie działania sprzeczne z regulacjami eIDAS 2.0 będą spotykać się z adekwatną reakcją prawną, mającą na celu nie tylko ukaranie za naruszenie, ale także zapobieganie przyszłym wykroczeniom poprzez działanie prewencyjne.

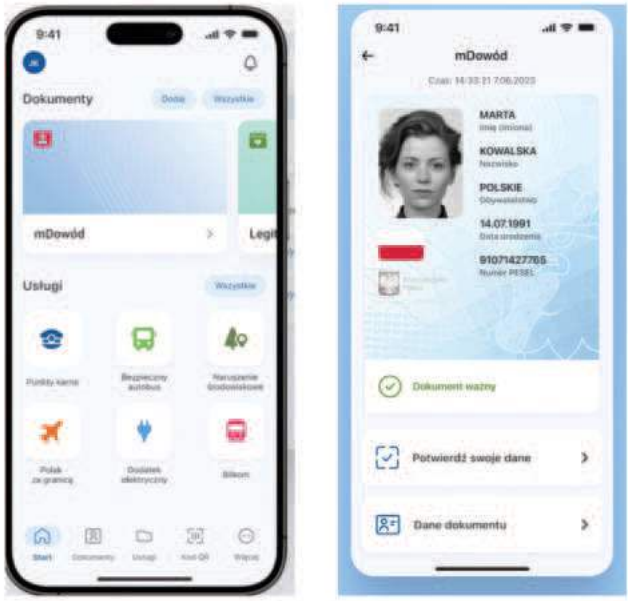
Równolegle, art. 5f pkt 5 rozporządzenia podkreśla znaczenie monitorowania i oceny wprowadzenia europejskich portfeli tożsamości cyfrowej. Przewiduje się, że w ciągu 24 miesięcy od ich wprowadzenia Komisja Europejska przeprowadzi szczegółową analizę, mającą na celu ocenę, jak europejskie portfele tożsamości cyfrowej są przyjmowane przez użytkowników i jak wpływają na rynek. Analiza ta będzie uwzględniać różne aspekty, takie jak popularność portfeli wśród użytkowników, ich transgraniczne wykorzystanie, wpływ na rozwój technologiczny, zmiany w sposobach użytkowania przez konsumentów oraz ogólny popyt na te usługi. Takie kompleksowe podejście ma na celu nie tylko ocenę skuteczności i funkcjonalności portfeli tożsamości cyfrowej, ale także identyfikację potencjalnych obszarów do dalszego rozwoju i udoskonalenia.

Pozostaje mieć nadzieję, że te działania przysłużą się osiągnięciu głównemu celowi eIDAS 2.0, jakim jest zwiększenie zaufania i bezpieczeństwa w cyfrowej przestrzeni transgranicznej w Unii Europejskiej, promując jednocześnie innowacje i cyfrową integrację rynku.

5.3. Zagadnienia bezpieczeństwa

Na rynku europejskim funkcjonuje wiele przykładów portfeli tożsamości. Są one stworzone dla celów danego kraju, dostarczają różnych możliwości, ale przede wszystkim różny jest ich model bezpieczeństwa, ponieważ nie jest on oparty o żaden dostępny standard w tym zakresie, zwłaszcza jeżeli chodzi o model interoperacyjności i bezpiecznej wymiany danych.

Pierwszym z przykładów jest mObywatel. Jest to aplikacja mobilna stworzona przez polski rząd, umożliwiająca obywatelom dostęp do cyfrowych wersji dokumentów tożsamości, takich jak dowód osobisty czy prawo jazdy, a także umożliwiająca korzystanie z różnych usług publicznych.



Rysunek 26. Widok z aplikacji mObywatel

Bezpieczeństwo rozwiązania oparte jest o następujące aspekty:

- dane pochodzą z rejestrów publicznych, co gwarantuje integralność oraz autentyczność danych,
- dane są zabezpieczone kryptograficznie (pieczęć elektroniczna Ministra Cyfryzacji),
- onboarding do aplikacji oparty jest o węzeł krajowy (co najmniej poziom średni),
- dane z aplikacji można przekazać tylko do innego użytkownika aplikacji lub systemu dziedzinowego podłączonego do infrastruktury Ministra.

Powyższe informacje nie zostały jednak niezależnie potwierdzone. Stąd w przypadku aspiracji mObywatela do spełnienia wymagań eIDAS 2.0 niezbędna będzie jego certyfikacja na zgodność z wymaganiami i standardami technicznymi.

Kolejnym przykładem jest portfel Diia dostarczony przez państwo ukraińskie. Portfel umożliwia posługiwanie się mobilnym dokumentem tożsamości, jak również usprawnia dostęp do usług online z sektora publicznego oraz prywatnego. Portal Diia (jeden z komponentów ekosystemu portfela) ma ponad 21,7 miliona użytkowników — dostępnych jest online ponad 70 usług rządowych. Aplikacja mobilna Diia umożliwia Ukraińcom dostęp do 14 cyfrowych dokumentów (dowód osobisty, biometryczny paszport zagraniczny, legitymacja studencka, prawo jazdy, świadectwo rejestracyjne pojazdu, polisa ubezpieczenia pojazdu, numer podatkowy, akt urodzenia, certyfikat przesiedlenia wewnętrznego) oraz łącznie 21 usług[46].

Rysunek 27. Portfel Diia UA

Kolejnym przykładem jest grecki portfel Gov.gr. Gov.gr Wallet to oficjalna grecka aplikacja portfelowa, która jest dostępna za pośrednictwem oficjalnego konta Republiki Greckiej, umożliwia tworzenie, przechowywanie i kontrolę nowych cyfrowych dowodów osobistych i cyfrowych praw jazdy. Nowe cyfrowe dowody tożsamości i prawo jazdy są dokumentami cyfrowymi wydawanymi za pośrednictwem gov.gr i są w pełni równoważne dokumentom papierowym, do dowolnego legalnego użytku na terytorium Grecji. Nie są one międzynarodowym dokumentem podróży.

Rysunek 28. Grecki portfel

Innym przykładem jest holenderski portfel DigiD app, który jest rodzajem cyfrowego paszportu. Jest to jeden z nielicznych portfeli tożsamości, który jest na liście europejskich systemów identyfikacji elektronicznej. **Został notyfikowany na poziomie średnim oraz wysokim.**

Rysunek 29. DigiID

Możemy wyróżnić występowanie portfeli cyfrowej tożsamości w co najmniej następujących pozostałych krajach UE:

- MitID (Dania)
- Belgia (Itsme)

[46] https://ukraine.ua/invest-trade/digitalization/ (dostęp 21.03.2024 r.)

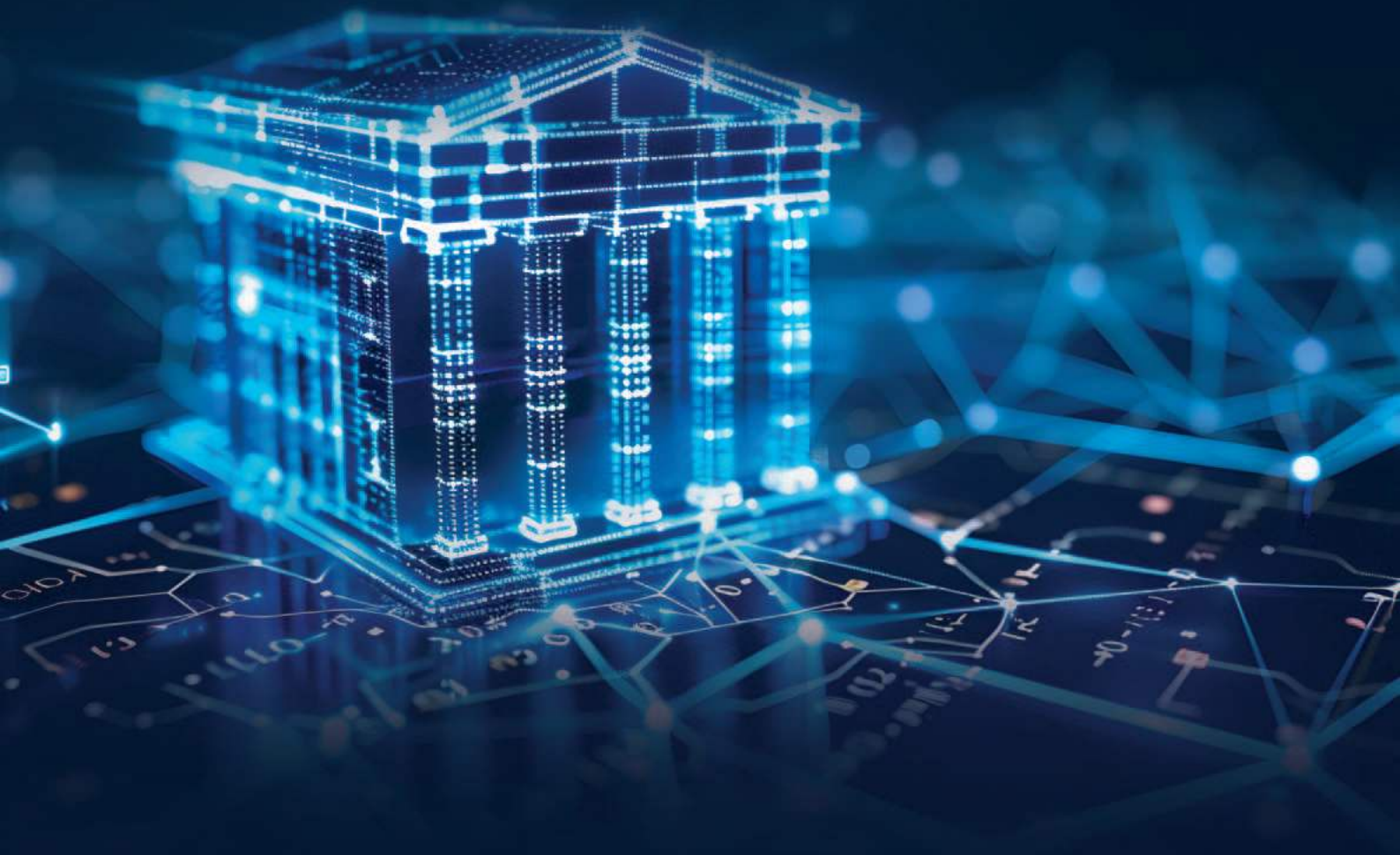
- Czechy (mojeID)
- Estonia (SmartID)
- Francja (FranceConnect)

Poza holenderskim rozwiązaniem, który przeszedł procedurę notyfikacji i jest znana publicznie jego wiarygodność, autorom niniejszego opracowania nieznane są szczegóły dot. modelów bezpieczeństwa pozostałych portfeli. Ryzyko wynikające z zastosowania na rynkach krajowych rozwiązań identyfikacji elektronicznej różniących się od ustalonych standardów europejskiej e-tożsamości, a także obecność różnorodnych portfeli cyfrowej tożsamości na rynku europejskim, stwarza liczne wyzwania dla bezpieczeństwa. Takie wyzwania są ważne nie tylko dla pojedynczych użytkowników, ale również dla ogólnego stanu bezpieczeństwa systemów cyfrowych na szczeblu krajowym oraz europejskim.

Fragmentacja systemów identyfikacji wywołana przez różnice w krajowych rozwiązaniach może znacznie utrudniać ich interoperacyjność oraz współpracę transgraniczną, podnosząc zagrożenie cyberatakami. Różnice w poziomach zabezpieczeń poszczególnych systemów mogą stanowić potencjalną lukę, którą mogą wykorzystać cyberprzestępcy. Ponadto, brak jednolitych standardów bezpieczeństwa pomiędzy poszczególnymi systemami identyfikacji elektronicznej w Europie prowadzi do zwiększonego ryzyka dla ochrony danych użytkowników i utrudnia zapewnienie skutecznej ochrony przed zagrożeniami cybernetycznymi. W związku z tym, istotne jest dążenie do harmonizacji i interoperacyjności rozwiązań identyfikacji elektronicznej w całej Europie, aby zwiększyć poziom bezpieczeństwa i zaufania do cyfrowych usług transgranicznych, jednocześnie promując rozwój jednolitego cyfrowego rynku wewnętrznego.

Rozporządzenie eIDAS 2.0 stanowi krok w tym kierunku, proponując ramy dla wzajemnego uznawania elektronicznych środków identyfikacji i usług zaufania. Współpraca na poziomie międzynarodowym, rozwój jednolitych standardów bezpieczeństwa oraz edukacja użytkowników na temat zarządzania tożsamością cyfrową i ochrony danych osobowych mogą przyczynić się do zwiększenia bezpieczeństwa i zaufania do cyfrowych usług transgranicznych.

Jakie działania powinny podjąć polskie banki, aby sprostać wymogom europejskiej e-tożsamości



6.1. Zagadnienia techniczne

Przygotowanie się banków na akceptację Europejskiego Portfela Cyfrowej Tożsamości wymaga przeprowadzenia analizy technicznej oraz ustalenie odpowiednich etapów działania. Zgodnie z wcześniej omawianymi przepisami banki będą do końca 2027 roku zobowiązane uznawać portfel cyfrowej tożsamości wszędzie tam, gdzie realizowane są procesy silnego uwierzytelnienia klienta, w szczególności oznaczać będzie to zobowiązania wynikające z wdrożenia dyrektywy płatniczej.

Europejski eID Wallet oparty jest na standardach technicznych określonych w znowelizowanym rozporządzeniu eIDAS 2.0, dokumencie architektury referencyjnej oraz innych europejskich standardach, takich jak standardy ETSI (Europejski Instytut Norm Telekomunikacyjnych), CEN (Europejski Komitet Normalizacyjny) oraz CENELEC (Europejski Komitet Normalizacji Elektrotechnicznej). Instytuty te podjęły już działania mające na celu stworzenie standardów technicznych umożliwiających wykorzystanie portfela cyfrowej tożsamości przez strony ufające, w tym banki. Jednocześnie banki nie tylko będą mogły korzystać z portfela cyfrowej tożsamości w celu uwierzytelnienia i identyfikacji klienta, ale także będą mogły stanowić autentyczne źródło dla poświadczeń atrybutów tj. potwierdzenia posiadania rachunku bankowego lub potwierdzenia salda. Sektor bankowy w tym zakresie powinien podjąć działania w celu pełnego rozpoznania standardów, ustalenia metod stosowania tych standardów przez banki. Może także okazać się konieczne wypracowanie standardów sektorowych dla akceptacji oraz udostępniania danych przez portfele cyfrowej tożsamości.

W momencie, w którym będzie znany ostateczny zakres standardów dostępu do portfeli, sektor bankowy powinien dokonać oceny zgodności swoich istniejących systemów informatycznych z wymaganiami technicznymi oraz weryfikacji procesów organizacyjnych opartych o tę technologie. Może to obejmować analizę istniejących protokołów uwierzytelniania, integracji z systemami zewnętrznymi, obsługi kryptografii, zarządzania certyfikatami, zabezpieczeń sieciowych i innych aspektów technicznych. Jeśli istniejące systemy bankowe nie będą spełniały wymagań technicznych dla europejskiego portfela, banki mogą potrzebować aktualizacji swoich systemów, w tym oprogramowania, infrastruktury sieciowej, zabezpieczeń, protokołów komunikacyjnych i innych elementów technicznych, aby umożliwić akceptację europejskich portfeli.

Banki powinny przygotować procedury obsługi europejskich portfeli w swoich systemach, w tym procesy uwierzytelniania, obsługi transakcji, zarządzania certyfikatami, zarządzania błędami i innymi procedurami związanymi z akceptacją. Jednocześnie należy zwrócić uwagę, że wdrożenie portfela wymagać może stosowania reguł związanych z rozpoznawaniem nie tylko tożsamości opartej o numery PESEL oraz dane identyfikacyjne typowe dla polskich obywateli, a także rozpoznawanie tożsamości osób z innych krajów UE w oparciu o przyjęte schematy identyfikacji osób. Dane te powinny móc być zapisane w systemach bankowych w celu jednoznacznej identyfikacji klienta usług bankowych.

Portfel cyfrowej tożsamości w zakresie identyfikacji elektronicznej ma umożliwiać przekazanie tożsamości w sposób bezpośredni, poufny i uniemożliwiający śledzenie oraz późniejsze linkowanie tożsamości. Wobec takich założeń funkcjonowania portfela należy przyjąć, że najlepszym modelem korzystania z jego funkcjonalności będzie wdrożenie rozwiązania pozwalającego bezpośrednio w banku na użycie funkcjonalności portfela. Portfel ma umożliwiać integrację za pomocą połączenia internetowego oraz NFC.

Połączenie internetowe portfela cyfrowej tożsamości będzie przebiegało w scenariuszu, w którym użytkownik portfela cyfrowej tożsamości skanuje jednorazowy kod QR, a następnie czynności związane z akceptacją zapytania o dane realizuje za pomocą posiadanego urządzenia mobilnego. Przy takiej integracji należy podjąć działania umożliwiające bankowi wyświetlenie jednorazowego kodu QR, który w sposób bezpieczny będzie mógł być zeskanowany urządzeniem mobilnym użytkownika, jednocześnie należy ze strony banku zapewnić aby użytkownik urządzenia mobilnego miał dostęp do sieci internet, np. za pomocą udostępnionej mu sieci WiFi.

W przypadku użycia kanału NFC, kanał ten może być użyty, aby nastąpiło tylko powiązanie portfela z systemem banku a następnie cała komunikacja odbywa się przez internet, lub całość komunikacji może być przekazana w kanale NFC. W przypadku korzystania z kanału NFC konieczne będzie dysponowanie przez placówkę bankową odpowiednimi czytnikami NFC umożliwiającymi komunikację z urządzeniami mobilnymi.

Bank korzystający z portfela zgodnie z rozporządzeniem eIDAS 2.0 staje się stroną ufającą, która w celu żądania danych z portfela cyfrowej tożsamości będzie posługiwała się dedykowanym certyfikatem potwierdzającym jej uprawnienia do korzystania z portfela cyfrowej tożsamości. Certyfikaty pozwalające na realizacje zadań strony ufającej będą wydawane zapewne przez kwalifikowanych dostawców usług zaufania i będą wymagały wcześniejszej rejestracji

w kraju, w którym strona ufająca ma siedzibę. Na moment pisania niniejszego raportu szczegóły, jak takie procesy będą przebiegały nie są znane, mają zostać określone w aktach implementujących pod koniec 2024 roku.

Integracja banku będzie mogła przebiegać z wykorzystaniem operatora technicznego, instytucji, która w imieniu banku będzie zarządzać kluczami certyfikatami umożliwiającymi dostęp do portfela cyfrowej tożsamości oraz przeprowadzi proces żądania i udostępnienia danych. Operatorzy techniczni prawnie są zobowiązani do nieprzetwarzania danych związanych z użyciem portfela cyfrowej tożsamości, nie mogą linkować tożsamości, przechowywać historii, która by umożliwiała jakiekolwiek śledzenie użytkowników portfeli cyfrowej tożsamości.

Portfel cyfrowy będzie przechowywał rożne poświadczenia atrybutów, zakres danych w tych poświadczeniach może dotyczyć bardzo wielu informacji, cech i uprawnień osób fizycznych i prawnych. O ile w zakresie podstawowych danych identyfikacyjnych będziemy dysponowali jednolitymi formatami i zakresami danych, to na poziomie unijnym nie powstały zunifikowane słowniki i wymagania formatów danych stosowanych w różnych sektorach. Prowadzi to do konieczności opracowania takich formatów na poziomie sektora finansowego, aby informacje, które będą akceptowane przez banki były jednoznaczne.

Banki poza faktem występowania w roli strony ufającej, takiej, która jest konsumentem danych o tożsamości i atrybutów, są także autentycznym źródłem danych dla wielu informacji. W tym zakresie banki udostępniają informacje o posiadanych kontach, udostępniają dane finansowe, historię transakcji, historię kredytową. Wszystkie te informacje w postaci poświadczeń atrybutów mogą być kolekcjonowanie w portfelach cyfrowej tożsamości. Jak wskazano wyżej wystawcami elektronicznych poświadczeń atrybutów będą dostawcy usług zaufania, którzy zabezpieczą poświadczenie zawierające atrybuty pochodzące z banku oraz umożliwią ich pobranie do portfela cyfrowej tożsamości. Dostawcy usług zaufania wydawania elektronicznych poświadczeń atrybutów podlegają szczególnym wymaganiom prawnym, norm i audytów. Bank, będąc źródłem danych, nie wystawia poświadczenia, jednie na zasadzie umownej dostarcza dane, którego jest pierwotnym źródłem powstania.

Poza europejskim portfelami na rynku może pojawić się wiele portfeli komercyjnych, spełniających te same standardy techniczne i posługujące się tymi samymi formatami. Modele i zasady posługiwania się portfelami prywatnymi, w szczególności akceptacja tych portfeli nie jest opisana prawnie i może być zależna od przyjętych zasad sektorowych. Portfele te będą mogły przetwarzać i przechowywać kwalifikowane poświadczenia atrybutów – które są prawnie uznane i niosą wiarygodną informację. Ze względu na zastosowanie jednolitych standardów technicznych, korzystanie z portfeli komercyjnych może być bardzo powszechne i stanowić alternatywę dla przechowywania wszystkich danych w portfelu unijnym wydawanym przez kraj członkowski. W tym zakresie możliwe, że powstanie portfela sektorowego wydawanego przez banki mogłoby stanowić ważne uzupełnienie funkcji realizowanych przez portfel unijny.

Europejskie portfele cyfrowej tożsamości będą umożliwiały złożenie kwalifikowanego podpisu elektronicznego, który będzie powszechnie dostępnym narzędziem dla każdej osoby fizycznej. Portfel umożliwi bankowi wystawienie dokumentu do złożenia kwalifikowanego podpisu za pomocą portfela cyfrowej tożsamości. Wystawcami kwalifikowanych certyfikatów dla podpisów elektronicznych w portfelu cyfrowej tożsamości będą kwalifikowani dostawcy usług zaufanych, którzy także będą wystawiali środowisko aplikacji do składania podpisu pozwalające na utworzenie podpisów jednorazowych w oparciu o portfel. Integracja z takim środowiskiem pozwoli na złożenie podpisu przez posiadacza każdego portfela cyfrowej tożsamości.

Przygotowanie techniczne do wdrożenia europejskiego portfela jest procesem, który wymaga współpracy pomiędzy dostawcami portfeli, dostawcami usług atrybutów oraz stronami ufającymi. Na poziomie europejskim przygotowania techniczne są realizowane w ramach wielkoskalowych pilotaży, które łączą ze sobą wszystkie zainteresowane strony. W ramach testów zostaną przeprowadzone badania przypadków użycia, testy, wypracowane rozwiązania. Doświadczenie i wzory wypracowane przez wielkoskalowe pilotaże będą miały wpływ na stosowane rozwiązania krajowe, jednakże zakres opracowanych przypadków użycia nie obejmie całościowo potrzeb polskiego rynku, w tym zakresie będą powstawały krajowe inicjatywy mające na celu wypracowanie standardów na potrzeby sektora finansowego.

6.2. Zagadnienia organizacyjne

Przygotowanie się do wprowadzenia w życie zmian związanych z wejściem w życie rozporządzenia eIDAS 2.0 wymagać będzie od banków dużego zaangażowania w zakresie aktualizacji i tworzenia nowych procesów, procedur, regulaminów czy polityk eIDAS 2.0. To jednak nie wszystko, bo ogrom wprowadzanych zmian będzie także wymagał odpowiedniego przygotowania pracowników banków, jak i ich klientów.

6.2.1. Faza przygotowawcza i działania ciągłe po wdrożeniu eIDAS 2.0

Przygotowanie do wprowadzania odpowiednich zmian w powyższych aspektach wymagać będzie od banków realizacji szeregu czynności. Ustanowienie regulaminów, polityk i procedur związanych z eIDAS 2.0 w banku wymagać będzie przeprowadzenia analiz i audytów, wdrożenia procedur w tym procedur monitorowania i raportowania, szkoleń pracowników oraz monitorowania i zarządzania ryzykiem. Wdrażanie eIDAS 2.0 w bankach i innych dużych instytucjach będzie procesem skomplikowanym i dynamicznym, wymagającym ciągłego monitorowania. W zakres działań przygotowawczych wchodzić będą:

Pierwszym krokiem w przygotowaniu się do wdrożenia eIDAS 2.0 będzie przeprowadzenie analizy przepisów prawa – zarówno tych bezpośrednio związanych z tożsamością cyfrową, ale także przepisów, które są powiązane pośrednio lub bezpośrednio, takie jak AML czy RODO. Analiza powinna obejmować zarówno przepisy na poziomie krajowym, jak i unijnym. Warto wziąć pod uwagę, że wdrażanie eIDAS 2.0 nie będzie procesem jednorazowym i wymagać będzie ciągłego doskonalenia.

Monitoring zewnętrzny: w zakresie implementacji, interpretacji i praktyk związanych z rozporządzeniem mogą na bieżąco pojawiać się zmiany. Dlatego istotne będzie bieżące ich monitorowanie w zakresie prawa, technologii i funkcjonowania biznesowego. Zmiany wprowadzanie przez rozporządzenie w zakresie tożsamości cyfrowej docelowo mogą fundamentalnie zmienić model komunikacji i interakcji banku z klientami i innymi podmiotami gospodarczymi, dlatego bieżący monitoring będzie kluczowym elementem w zakresie zdolności banków do utrzymania swoich usług na najwyższym poziomie.

Instytucje finansowe będą zobowiązane do uznawania portfela cyfrowej tożsamości, wobec czego uzyskanie statusu i uprawnień strony ufającej, która prawidłowo może się zidentyfikować wobec portfela i zażądać danych z tego portfela, będzie jednym z podstawowych wymagań organizacyjnych. Procedury w tym zakresie po stronie krajowej nie zostały jeszcze opracowane ani nie został desygnowany urząd, który będzie odpowiedzialny za rejestrację stron ufających.

Proces ewaluacji i doskonalenia wewnątrz instytucji będzie równie istotnym aspektem dopasowywania się do zachodzących zmian. Banki będą musiały na bieżąco prowadzić ewaluację wdrożonych procesów i regulaminów na bazie feedbacku ze strony klientów, pracowników i z innych źródeł, jak audyty i analizy wewnętrzne. Proces samodoskonalenia powinien stanowić element zapewniania w banku ciągłej zgodności z obowiązującymi przepisami i najlepszymi praktykami, ale też dostosowywania się do oczekiwań klientów.

Kolejnym ważnym elementem wdrażania eIDAS 2.0 będą audyty wewnętrzne i zewnętrzne. Ich realizacja w procesie przygotowania do wdrożenia rozporządzenia, a później także utrzymania jest istotna, ponieważ pozwoli na przygotowanie procesów oraz procedur związanych z cyfrowymi tożsamościami w zgodzie z regulaminami, politykami i innymi wymogami. Realizowane audyty powinny dotyczyć aspekty techniczne, proceduralne jak i ocenę ich zgodności z przepisami prawymi. Już dziś banki podłączone do krajowego schematu identyfikacji elektronicznej i węzła mojeID przechodzą raz na dwa lata audyty potwierdzające zgodność ze standardami. Jeżeli nadal banki będą świadczyły podobną rolę w zakresie dostarczania atrybutów tożsamości, zakres audytów będzie musiał być dostosowany do znowelizowanych przepisów.

Kolejnym procesem, który powinien zostać wdrożony przez banki to proces monitorowania i zarządzania ryzykiem związanym z eIDAS 2.0. Jego celem powinny być: identyfikacja, ocena, i zarządzanie ryzykami związanymi z cyfrowymi tożsamościami, zabezpieczeniami technicznymi, danymi osobowymi i innymi aspektami związanymi z eIDAS 2.0.

Obecnie systemy bankowe, zarówno te wykorzystywane wewnętrznie, jak i systemy udostępniane klientom, są tworzone i utrzymywane we współpracy z dostawcami zewnętrznymi. Dostarczają oni bankom zasobów ludzkich, narzędzi, a niejednokrotnie – także całych komponentów oprogramowania, w związku z tym w celu przygotowania pod eIDAS 2.0 koniecznym może być przegląd systemów i procesów działających na styku z tożsamością cyfrową i podjęcie działań z dostawcami poszczególnych elementów. Celem uwzględnienia dostawców w pracach przygotowawczych powinno być zapewnienie zgodności i odpowiedniego poziomu bezpieczeństwa systemów banku oraz przygotowanie procedur i reguł współpracy, aby uwzględniały zmieniające się regulacje, przepisy prawa i procedury wewnętrzne banków.

Wdrożenie założeń rozporządzenia wymagać będzie także szerokiej komunikacji z klientami banku. Komunikacja powinna objąć standardowe, wymagane prawem elementy, takie jak informacja o zmianach w regulaminach, politykach czy procesach banku dotykających klientów. Docelowo jednak zakres działań komunikacyjnych powinien być znacznie szerszy i dotknąć także aspektów takich jak:

a. Elementy edukacyjne – informacje na temat zasad weryfikacji tożsamości i procesów bankowych.

b. Korzyści płynące z wdrożenia eIDAS 2.0.

c. Informacje o działaniach banku w zakresie ochrony klienta – jego środków w banku i danych osobowych.

d. Potencjalne zagrożenia po stronie klienta i jak mogą się przed nimi uchronić.

e. Jak zachować się w przypadku podejrzeń lub zaistnienia groźnych zdarzeń po stronie klienta.

Komunikacja powinna być realizowana w możliwie szerokim wachlarzu kanałów bankowych i zewnętrznych, takich jak strony internetowe banku, systemy bankowości elektronicznej, bankowość oddziałowa, media społecznościowe czy nawet media lokalne czy krajowe.

6.2.2. Regulaminy

Wdrożenie rozporządzenia eIDAS 2.0 i wprowadzenie lub rozszerzenie akceptacji tożsamości cyfrowych w bankach, z uwzględnieniem europejskiego portfela cyfrowej tożsamości, wymagać będzie zmiany szeregu regulaminów. Poniżej wymienione zostały aspekty, które banki będą musiały zmodyfikować lub uwzględnić w regulaminach, aby móc działać w zgodności z wymogami rozporządzenia:

Wszystkie banki posiadają regulaminy dotyczące weryfikacji tożsamości klientów w środowisku online i offline. Odpowiednie regulaminy będą musiały opisywać w jaki sposób dokonywana jest weryfikacja tożsamości, jakie dane są wymagane, w jakich przypadkach klient może z nich korzystać, jakie dane będą przekazywane w przypadku skorzystania ze środka identyfikacji cyfrowej. Regulamin ten powinien także określić zasady i ograniczenia związane z wykorzystaniem przez klienta EUDI w zakresie onboardingu, uwierzytelniania, zakupu produktów, autoryzacji transakcji cyfrowych czy zakres odpowiedzialności poszczególnych stron w przypadku korzystania z tego narzędzia.

Banki będą musiały uwzględnić w swoich regulaminach zapisy dotyczące transakcji elektronicznych takich jak przelewy, płatności online czy zakup produktów w celu umożliwienia klientom korzystania z europejskiego portfela tożsamości cyfrowej jako narzędzia do uwierzytelniania i autoryzacja określonych przez rozporządzenie transakcji. Doprecyzowane powinny zostać procedury dotyczące korzystania z EUDI, w tym aspekty takie jak limity, procedury odwoławcze czy zakresy odpowiedzialności.

Banki, aby pozostać w zgodzie ze wszystkimi obowiązującymi przepisami dotyczącymi ochrony danych osobowych klientów, będą musiały dostosować regulaminy związane z tym aspektem, aby uwzględnić wykorzystanie EUDI jako narzędzia weryfikacji, uwierzytelniania i przetwarzania danych klientów.

Kolejnym aspektem, który będzie wymagał aktualizacji będzie temat reklamacji, odwołań i rozwiązywania sporów związanych z wykorzystaniem tożsamości cyfrowych. Regulaminy będą musiały uwzględnić zasady rozstrzygania reklamacji związanych z korzystaniem z europejskiego portfela cyfrowej tożsamości oraz zakres odpowiedzialność za ewentualne straty klientów oraz opisywać procedury w przypadku wystąpienia sporów między klientem a bankiem.

Banki będą musiały zabezpieczyć także aspekty związane z bezpieczeństwem takie jak obowiązki i wymagania stawiane klientom w zakresie korzystania z tożsamości cyfrowej, stosowane przez bank zabezpieczenia czy procedury awaryjne w przypadku wystąpienia incydentu.

6.2.3. Polityki

Polityki, czyli zbiory zasad, procedur i standardów określających zakres dozwolonych i/lub zabronionych działań w danym kontekście, to kluczowy element funkcjonowania dojrzałych instytucji i przedsiębiorstw. Po uprzednim zrealizowaniu analizy prawnej, audytów i analiz biznesowych banki będą musiały dokonać przeglądu polityk i dokonać odpowiednich zmian na podstawie wniosków z ww. analiz. Po dokonaniu zmian w politykach banki powinny także dopilnować ich wdrożenia w procedurach, systemach i procesach biznesowych, przeprowadzenia odpowiednich szkoleń pracowników oraz ustanowenie procedur bieżącego monitorowania i raportowania wewnątrz instytucji. Procedury powinny podlegać realizacji regularnych przeglądów i aktualizacji zgodnie ze zmieniającymi się praktykami rynkowymi, regulacjami i oczekiwaniami klientów oraz innymi czynnikami zewnętrznymi i wewnętrznymi.

1. **uwierzytelniania klienta** – Uzupełnienie polityk o procedury związane z akceptacją portfeli tożsamości cyfrowej z naciskiem na realizację procesów uwierzytelniania za pośrednictwem EUDI.

2. **Polityka monitorowania i wykrywania zagrożeń** – W związku ze skalą zmian wprowadzanych

w obszarze tożsamości cyfrowych przez rozporządzenie eIDAS 2.0 konieczne będzie zaktualizowanie polityk monitorowania i wykrywania zagrożeń. Wraz z pojawianiem się nowych narzędzi, procesów i produktów cyfrowych powstawać będą zapewne nowe rodzaje zagrożeń i nowe wektory ataku zarówno na klientów, jak i na same banki.

3. **Polityka zarządzania ryzykiem** – Podobnie jak w przypadku polityk dotyczących zagrożeń, ważnym elementem prawidłowego funkcjonowania tożsamości cyfrowych w środowisku bankowym będę identyfikacja, ocena i zarządzanie ryzykami.

4. **Polityka prywatności i ochrony danych** – Zgodność z przepisami dotyczącymi ochrony danych osobowych zabezpieczana jest przez polityki i regulaminy. Wprowadzenie tożsamości cyfrowych jako elementu interakcji z klientami wymusi na bankach bardzo dokładne przejrzenie obecnych dokumentów i procedur oraz dostosowanie ich do wyzwań związanych z obsługą EUDI. Banki będą musiały nie tylko zapewnić odpowiednie procesy i zabezpieczenia techniczne, ale także przygotować pracowników w zakresie znajomości procedur oraz do obsługi i wsparcia klientów.

5. **Polityka jakości obsługi** – Odpowiednie przygotowanie procesów i pracowników do odpowiedniej obsługi potrzeb i oczekiwań klientów będzie kluczowym elementem do sukcesu tożsamości cyfrowych. Instytucje finansowe w Polsce cieszą się dość dużym zaufaniem klientów i można oczekiwać, że to one będą stanowiły jeden z pierwszych punktów styczności z tożsamościami cyfrowymi, banki będą zatem nie tylko źródłem wiedzy dla klienta, ale także potencjalnymi pierwszymi beneficjentami gotowości klientów do pełnej migracji na procesy cyfrowe.

6.2.4. Procesy

Po wcześniejszym zabezpieczeniu obszarów związanych z regulaminami, procedurami i politykami, konieczna będzie realizacja przeglądu i aktualizacji procesów – zarówno wewnętrznych po stronie banku, jak i tych, z którymi na co dzień stykają się klienci. Wdrożenie akceptacji tożsamości cyfrowej w procesach banku powinno rozpocząć się od dogłębnej analizy obejmującej aspekty biznesowe, technologiczne, prawne i te związane z bezpieczeństwem. Odpowiednie zadbanie o procesy wykorzystujące tożsamości cyfrowe może być nie tylko spełnieniem wymogów regulacyjnych, ale być bodźcem do zwiększenia efektywności procesów bankowych oraz jeszcze lepszej obsługi klientów.

Realizacja analizy procesów mogłaby odbyć się zgodnie z poniższym schematem:

1. Identyfikacja obszarów działalności banku, w których realizowana jest weryfikacja tożsamości klientów np. obszary:

   - pozyskania i utrzymania klienta,
   - sprzedaży produktów,
   - obsługi klienta,
   - przyjmowania i obsługi reklamacji.

2. Identyfikacja wymagań prawnych i regulacyjnych, do których banki muszą się dostosować. To będzie zakres minimum konieczny do wprowadzenia, aby banki operowały w zgodzie z dyrektywami i innymi przepisami prawa w zakresie identyfikacji klientów (m.in. eIDAS, AML, RODO, PSD2, a w przyszłości też PSD3).

3. Inwentaryzacja i ocena procesów w ramach wymienionych obszarów. Warto zwrócić uwagę, że portfele cyfrowej tożsamości wykorzystywane mogą być zarówno w środowisku online, jak i w placówkach bankowych czy partnerskich. Celem tego kroku jest zidentyfikowanie wszystkich procesów:

- w których obecnie realizowana jest weryfikacja tożsamości klienta,
- w których wymagane będzie akceptacja tożsamości cyfrowej,
- w których akceptacja cyfrowej tożsamości mogłaby stanowić wartość dodaną.

W ramach tego kroku przeanalizowane i zweryfikowane powinny zostać procedury, wymagane dane, dokumentacja i inne aspekty poszczególnych procesów.

4. Analiza, ocena i docelowo zarządzanie ryzykami związanymi z wdrożeniem akceptacji tożsamości cyfrowej. Analiza objąć powinna takie obszary jak:

- ryzyka związane z wyłudzeniami i innymi działaniami przestępców *(np. pojawienie się nowych rodzajów ataków wykorzystujących tożsamość cyfrową)*,
- ryzyka związane z błędami klientów *(np. niedostateczne przygotowanie czy kompetencje klientów w zakresie identyfikacji elektronicznej)*,

- ryzyka prawne lub związane z compliance *(np. niedostosowanie się do regulacji i innych wymogów prawa)*,
- ryzyka biznesowe *(np. utrata klientów ze względu na uproszczenie procesów onboardingu w innych bankach, rezygnacja z produktów przez uproszczone procesy)*,
- ryzyka operacyjne i techniczne (np. *błędy i/lub przerwy techniczne związane z niedostatecznym procesem testowania),*
- ryzyka reputacyjne *(np. gorsze przygotowanie w zakresie obsługi klienta niż banki konkurencyjne)*,
- innych ryzyk właściwych dla danego obszaru działalności banku.

5. W ramach rozwoju procesów banki będą musiały podjąć decyzje dotyczące technologii jakie zostaną zaimplementowane – od tych wymaganych jak obsługa EUDI po te dobrowolne czyli np. zastosowanie wybranych modeli biometrii, modeli autentykacji czy innych aspektów technicznych. Będzie to też dobra okazja do rozszerzenia procesów banku o podpisy elektroniczne czy inne usługi zaufania.

6. Na bazie przeprowadzonych analiz potrzeb biznesowych, wymagań regulacyjnych i analizie potrzeb klientów należy dokonać przeglądu i projektowania lub przeprojektowania procesów. W procesach powinny zostać uwzględnione wybrane technologie, procedury i polityki banku oraz inne elementy operacyjne i biznesowe oraz aspekty bezpieczeństwa.

7. Po przeprojektowaniu procesów należy przeprowadzić testy wewnętrzne, aby sprawdzić funkcjonowanie procesów od strony technicznej i operacyjnej. Warto także testy wzbogacić o badania z użytkownikami końcowymi, aby zadbać też o aspekty związane z użytecznością i ergonomią. Ważne także, aby dokonana została walidacja procesów i systemów, aby ostatecznie potwierdzić ich zgodność z wymogami eIDAS 2.0.

8. Przed ostatecznym wdrożeniem produkcyjnym należy zadbać o przygotowanie pracowników banku, tych bezpośrednio obsługujących poszczególne procesy oraz tych zajmujących się obsługą i wsparciem klientów. Pracownicy powinni zostać odpowiednio przeszkoleni zarówno w zakresie funkcjonowania procesów, jak i w odniesieniu do obsługi tożsamości cyfrowej. Pracownicy poza szkoleniami powinni także dostać do dyspozycji odpowiednie materiały informacyjne oraz ewentualny kontakt do osób które będą w stanie pomóc w sytuacjach awaryjnych.

6.3. Przepisy prawa

Analiza prawna w kontekście eIDAS 2.0 jest kluczowa dla banków działających w ramach Unii Europejskiej, które muszą zarządzać cyfrowymi tożsamościami zgodnie z obowiązującymi regulacjami. Taka analiza powinna być kompleksowa i uwzględniać szeroki zakres aspektów prawnych. Konieczne jest zrozumienie istotnych zasad, wymagań i obowiązków związanych z cyfrowymi tożsamościami, w tym identyfikacji elektronicznej, uwierzytelnienia, autoryzacji, ochrony danych osobowych, a także zgodności z regulacjami AML/KYC oraz innymi przepisami dotyczącymi bezpieczeństwa, prywatności i ochrony konsumentów.

Ważne jest także ocenienie, w jakim stopniu obecne procesy, procedury, polityki oraz inne działania banku są zgodne z wymaganiami eIDAS 2.0. Należy zidentyfikować potencjalne obszary niezgodności i określić potrzebne zmiany czy dostosowania, które zapewnią pełną zgodność z przepisami, szczególnie w kontekście uwierzytelnienia, identyfikacji, autoryzacji, zarządzania danymi osobowymi oraz zabezpieczeń.

Analiza powinna również objąć potencjalne ryzyka związane z implementacją eIDAS 2.0, takie jak zagrożenia dotyczące ochrony danych osobowych, bezpieczeństwa technicznego czy zgodności z przepisami AML/KYC. Rozpoznanie tych ryzyk umożliwi ich efektywne zarządzanie i minimalizowanie potencjalnych negatywnych skutków.

Analiza musi dokładnie rozważyć wprowadzenie europejskiego portfela cyfrowej tożsamości. Jest to kluczowy element dla instytucji finansowych, gdyż wpływa na sposób, w jaki realizowane są procedury AML (Anti-Money Laundering). Banki muszą dostosować swoje systemy w taki sposób, aby zapewnić zgodność z nowymi wymaganiami dotyczącymi weryfikacji i uwierzytelnienia tożsamości klienta, co ma bezpośredni wpływ na skuteczność działań przeciwdziałających praniu pieniędzy oraz finansowaniu terroryzmu.

Kolejnym istotnym aspektem są elektroniczne poświadczenia atrybutów oraz kwalifikowane elektroniczne poświadczenia atrybutów. Umożliwiają one uwierzytelnienie atrybutów dotyczących zarówno osób fizycznych, jak i prawnych, co z kolei wpływa na transakcje finansowe oraz wiarygodność i bezpieczeństwo procesów biznesowych. Analiza powinna uwzględnić, jak te poświadczenia będą akceptowane

w procedurach bankowych i jakie zmiany są konieczne do ich wdrożenia.

Równie ważna jest analiza możliwości udostępniania przez bank informacji o atrybutach klientów usług bankowych w postaci elektronicznego poświadczenia atrybutów. Wymaga to zrozumienia zarówno technicznych aspektów przekazywania tych danych, jak i prawnych implikacji ochrony danych osobowych. Należy ocenić, jakie zmiany w infrastrukturze IT banku są konieczne oraz jak będą one wpływać na relacje z klientami.

Osobną kwestią są nowe usługi zaufania, w szczególności elektroniczne archiwum i elektroniczny rejestr, które zaczynają odgrywać znaczącą rolę w usługach bankowych i finansowych. Stosowanie usług zaufania może adresować wiele ryzyk, ale konieczne jest zbadanie, jak wdrożenie tych usług wpłynie na istniejące procesy oraz jakie zabezpieczenia prawne należy wdrożyć, aby wniosły one nową wartość i możliwości dla sektora finansowego.

Ponadto, analiza prawna powinna dostarczyć bankowi konkretne rekomendacje i kierunki działań, które pomogą sprostać wymaganiom eIDAS 2.0. Obejmuje to aktualizacje polityk, procedur, procesów biznesowych, a także zarządzanie danymi osobowymi i zabezpieczeń technicznych. Niezbędne mogą okazać się również kwalifikowane usługi zaufania oraz audyty związane z eIDAS 2.0.

Istotne jest, aby analiza prawna uwzględniała konieczność monitorowania zmian prawnych związanych z eIDAS 2.0 i odpowiedniego aktualizowania polityk, procedur i działań banku, aby na bieżąco odpowiadać na ewolucję przepisów prawnych.

W kwestii komunikacji, zarówno wewnętrznej, jak i zewnętrznej, analiza powinna zwrócić uwagę na strategie dotyczące wdrażania eIDAS 2.0. Bank powinien zapewnić jasny przekaz zmian wewnętrznych oraz dostosować komunikację z klientami i innymi zainteresowanymi stronami zewnętrznymi.

Ocena zabezpieczeń prawnych również nie powinna zostać pominięta. Bank powinien zagwarantować, że regulaminy, umowy, polityki i procedury są aktualne i odzwierciedlają wprowadzane zmiany prawne.

Należy podkreślić, że analiza prawna w kontekście eIDAS 2.0 zależy od specyfiki danego banku, jego procesów biznesowych, istniejących polityk i procedur, jak również od krajowych regulacji prawnych. Dlatego zaleca się konsultacje z doświadczonym zespołem specjalizującym się w prawie cyfrowym i ochronie danych osobowych.

6.4. Przygotowanie własnych pracowników

Banki przygotowując się do eIDAS 2.0 muszą wykonać ogrom prac audytowych, analitycznych, projektowych i wdrożeniowych. Szerokie wykorzystanie tożsamości cyfrowych będzie bardzo dużym wyzwaniem, jednak odpowiednie przygotowanie pozwoli bankom zlewarować technologię, która może znacząco zwiększyć efektywność, wygodę i dostępność usług cyfrowych oferowanych klientom. Wyzwania techniczne i biznesowe nie są jednak jedynymi z którymi przyjdzie się bankom zmierzyć.

Bardzo ważnym elementem sukcesu będzie przygotowanie pracowników do nowej rzeczywistości, w przeciwieństwie do innych regulacji, które zwykle dotykały jedynie wybranych departamentów czy obszarów w instytucjach finansowych, eIDAS wpłynie na funkcjonowanie w zasadzie każdego z nich, stąd wyzwanie związane z przygotowaniem kadry będą znacząco większe niż dotychczas. Szkolenia dotyczyć będą musiały, zapewne w różnym zakresie, niemal wszystkich pracowników banku, bez względu na obszar czy zajmowane stanowisko. Przygotować będzie trzeba pracowników działających w pierwszej linii kontaktu z klientami, jednostki techniczne, biznesowe, prawne, aż po najwyższą kadrę zarządzającą.

Zakres realizowanych szkoleń będzie różnił się zapewne między departamentami i stanowiskami, jednak warto podejść do wyzwań związanych ze szkoleniami całościowo. Obszary, w których wymagana będzie aktualizacja lub pozyskanie zupełnie nowej wiedzy:

1. **eIDAS 2.0 i Europejki Portfel Cyfrowej Tożsamości (EUDI)** – podstawowe szkolenie, np. w formie online powinno być przeprowadzone pośród wszystkich pracowników banku. Świadomość zmian i możliwości jakie wprowadza eIDAS 2.0 powinno stanowić element nie tylko bieżącej wiedzy, ale także dać pracownikom narzędzie do myślenia w przyszłości o procesach i produktach banku z uwzględnieniem zagadnień tożsamości cyfrowej. Szkolenie powinno obejmować zarówno teorię i zagadnienia regulacyjne, jak i aspekty praktyczne związane z weryfikacją tożsamości, funkcjonalnościami portfela oraz najważniejszymi procedurami i regulaminami wdrożonymi w banku. Szkolenie mogłoby także zostać uzupełnione o podstawowe aspekty związane z bezpieczeństwem klientów i banku, w tym tematami najważniejszych typów bieżących zagrożeń.

2. **Procedury weryfikacji tożsamości** to podstawowy obszar związany z obsługą tożsamości cyfrowej. Pracownicy, którzy będą mieć bezpośrednią

styczność z procesami identyfikacji klienta (bezpośrednio w kontakcie z klientem, ale także np. przy projektowaniu procesów, procedur czy materiałów edukacyjnych) będą musieli dogłębnie poznać szczegóły dotyczące weryfikacji tożsamości. Wiedza ta powinna objąć wszystkie najważniejsze aspekty – zasady przeprowadzania weryfikacji tożsamości, ocena autentyczności dokumentów klienta, aspektów bezpieczeństwa czy technicznej obsługi odpowiednich procesów.

3. **Obsługa i komunikacja** to obszary kluczowe z punktu widzenia klientów. To pracowników call center, oddziałów czy np. czatów klienci będą dopytywać o nowe rozwiązania oferowane przez bank – jak z nich skorzystać, jak założyć oraz czy są bezpieczne. Szkolenia w zakresie obsługi klienta powinny zgłębiać zagadnienia związane z bezpieczeństwem, weryfikacją tożsamości, ale także uzupełnić wiedzę pracowników o rzeczy istotne z perspektywy klienta np. jak założyć EUDI, jak zmienić formę uwierzytelniania w czasie realizacji transakcji cyfrowych czy jak bezpiecznie obchodzić się ze swoimi danymi osobowymi zgromadzonymi w portfelu. Pracownicy Ci powinni być w stanie wesprzeć klienta w jego pierwszych krokach oraz pomóc mu rozwiązać bardziej wymagające problemy, jak obsługę incydentów czy wsparcie w realizacji procesów cyfrowych.

4. **Obsługa incydentów i awarii** jest kolejnym obszarem kluczowym z perspektywy klienta, jednak jego obsługa wykracza poza samych pracowników, z którymi kontaktuje się klient. W rozwiązywanie problemów związanych z bezpieczeństwem i aspektami technicznymi zaangażowani są zarówno pracownicy oddziałów i call center jako osoby przyjmujące zgłoszenia od klienta, jak i pracownicy departamentów obsługujących IT oraz często jednostki biznesowe. Szkolenia w tym zakresie powinny mieć praktyczny charakter i skupić się na tym, aby przekazać pracownikom wiedzę i narzędzia niezbędne do sprawnego rozwiązywania wszystkich problemów, z którymi zgłoszą się klienci.

5. **Ochrona prywatności i danych osobowych klientów**. Szkolenie w tym zakresie powinno uzupełniać wiedzę pracowników, którą pozyskiwali przy okazji przepisów takich jak RODO czy AML i skupić się na zmianach procesowych i proceduralnych jakie niesie za sobą przetwarzanie danych klientów pozyskiwanych za pośrednictwem nowych lub zmienionych procesów i z nowych, wcześniej niewykorzystywanych źródeł.

Podsumowanie i wnioski końcowe

Raport koncentruje się na analizie obecnych ram regulacyjnych i technologicznych dotyczących cyfrowej tożsamości w kontekście Unii Europejskiej. Przegląd obejmuje kluczowe zagadnienia związane z identyfikacją i uwierzytelnieniem, a także usługi zaufania, takie jak elektroniczne poświadczenia atrybutów, certyfikaty oraz podpisy cyfrowe. W szczególności, raport kładzie nacisk na inicjatywy Unii Europejskiej w zakresie rozwoju wspólnych standardów cyfrowej tożsamości, które mają na celu ułatwienie dostępu do usług cyfrowych przy jednoczesnym zachowaniu prywatności i bezpieczeństwa danych.

Raport prezentuje założenia koncepcji cyfrowej tożsamości, która opiera się o europejski portfel cyfrowej tożsamości. Projektowany portfel zapewni spójny standard identyfikacji elektronicznej na terenie całej Unii Europejskiej, umożliwiający obywatelom korzystanie z cyfrowej tożsamości w różnych krajach członkowskich. Cyfrowe portfele tożsamości mają umożliwić realizację szerokiego zakresu czynności, od identyfikacji i uwierzytelniania, przez złożenie podpisów elektronicznych, po dostęp do usług administracyjnych, finansowych i biznesowych.

W raporcie omówiono szanse oraz ryzyka związane z wdrażaniem europejskiej cyfrowej tożsamości. Zwrócono uwagę na zwiększenie bezpieczeństwa i interoperacyjności, a także uproszczenie dostępu do transgranicznych usług elektronicznych. Omówione ryzyka obejmują zagrożenia związane z prywatnością danych, phishingiem, kradzieżą tożsamości oraz błędami w onboardingu użytkowników .

Rozporządzenie eIDAS oraz jego nowelizacja eIDAS 2.0 są kluczowymi elementami, wspierającymi wdrożenie europejskich ram cyfrowej tożsamości. Wprowadzenie wspólnych standardów ma na celu zmniejszenie fragmentacji systemów identyfikacji elektronicznej oraz poprawę integracji cyfrowej w UE.

Przedstawione poniżej wnioski i rekomendacje mają na celu ułatwienie adaptacji europejskich rozwiązań cyfrowej tożsamości, jednocześnie minimalizując ryzyka i maksymalizując korzyści dla obywateli oraz instytucji na terenie całej Unii Europejskiej

- Wdrażanie wspólnych europejskich standardów cyfrowej tożsamości jest kluczowe dla zminimalizowania fragmentacji i zapewnienia spójności usług na terenie całej UE. Harmonizacja systemów identyfikacji elektronicznej powinna być priorytetem dla wszystkich krajów członkowskich.

- Kluczowe znaczenie ma edukacja użytkowników w zakresie bezpiecznego korzystania z cyfrowych tożsamości oraz wprowadzenie mechanizmów zapobiegających phishingowi i kradzieży tożsamości. Należy również zwrócić uwagę na zróżnicowany poziom onboardingu, co może wpływać na bezpieczeństwo całego systemu.

- Efektywna implementacja europejskiego portfela cyfrowej tożsamości wymaga ścisłej współpracy międzynarodowej w zakresie regulacji, technologii i standardów operacyjnych, co zapewni spójne i bezpieczne środowisko dla wszystkich użytkowników .

- Banki oraz inne instytucje powinny przygotować się na wdrożenie nowych technologii, takich jak zaawansowane metody uwierzytelniania i biometrii, aby sprostać wymogom europejskiej e-tożsamości i zapewnić zgodność z regulacjami takimi jak eIDAS 2.0.

Raport przygotowany na zlecenie Fundacji
Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY