

Trusted
Economy
Forum

ORGANIZATOR:

Trusted Economy Forum

WYDAWCA RAPORTU:



OBSERWATORIUM.BIZ

EUROPEJSKIE RAMY TOŻSAMOŚCI CYFROWEJ

- czym są i jak zmieniają rynek cyfrowy?



Raport przygotowany na rzecz
Trusted Economy Forum WEBINAR 2025

ZŁOTY PARTNER:

ASSECO
DATA SYSTEMS

SREBRNY PARTNER:

 **Authologic**

 **Poczta Polska**

HONOROWY PATRON STRATEGICZNY:

COI Centralny
Ośrodek
Informatyki

PATRONI HONOROWI:

PIIT

 **CYFROWA
POLSKA**

GŁÓWNE WNIOSKI RAPORTU

EUROPEJSKIE RAMY TOŻSAMOŚCI CYFROWEJ

- CZYM SĄ I JAK ZMIENIĄ RYNEK CYFROWY?

JAKIEGO RYNKU, USŁUG I PODMIOTÓW DOTYCZA EUROPEJSKIE RAMY TOŻSAMOŚCI CYFROWEJ?

- Notyfikowanych systemów elektronicznej identyfikacji.
- Dostawców usług zaufania mających siedzibę w Unii.
- Przedsiębiorców stosujących Silne Uwierzytelnienia Użytkownika.

JAKIE NOWE USŁUGI BĘDĄ WPROWADZONE W RAMACH EUROPEJSKICH RAM TOŻSAMOŚCI CYFROWEJ?

- Europejski Portfel Tożsamości Cyfrowej.
- Elektroniczne poświadczenia atrybutów.
- Elektroniczna archiwizacja danych i dokumentów.
- Rejestrowanie danych elektronicznych w rejestrze.
- Zarządzanie zdalnymi urządzeniami do składania podpisu elektronicznego i pieczęci.

JAKIE BĘDĄ OBOWIĄZKI DLA INTERESARIUSZY?

- Państwa członkowskie, administracja publiczna, strony ufające i dostawcy usług zaufania muszą wdrożyć procedury zgodne ze znowelizowanym rozporządzeniem eIDAS, w tym systemy rejestracji, interoperacyjności, ochrony danych, mechanizmy zgłaszania incydentów i audytów zgodności.

JAKIE NOWE SZANSE DLA RYNKU OTWIERAJĄ EUROPEJSKIE RAMY CYFROWEJ TOŻSAMOŚCI?

- Europejski Portfel Tożsamości Cyfrowej umożliwi wdrażanie zaawansowanych usług jak silne uwierzytelnienie klienta (SCA), cyfrowy onboarding (z uwzględnieniem Know Your Customer - KYC), bezpieczne płatności, potwierdzanie tożsamości w przelewach, cyfrową reprezentację firm i udostępnianie danych do procesów kredytowych – wszystko w sposób zgodny z unijnymi przepisami i z zachowaniem kontroli użytkownika nad danymi.

CZYM BĘDZIE EUROPEJSKI PORTFEL TOŻSAMOŚCI CYFROWEJ?

Stanie się kluczowym narzędziem tożsamości w całej UE. Portfel umożliwia bezpieczne przechowywanie i udostępnianie danych tożsamości, składanie kwalifikowanych podpisów elektronicznych oraz zarządzanie elektronicznymi poświadczeniami atrybutów. Będzie dostępny bezpłatnie dla obywateli i rezydentów UE do celów prywatnych i obowiązkowo wspierany przez wszystkie państwa członkowskie od końca 2026 r.

Polska implementuje portfel jako aplikację mObywatel, która przechodzi transformację do wersji 3.0.

Nowa wersja aplikacji będzie zgodna ze znowelizowanym rozporządzeniem eIDAS, umożliwi składanie kwalifikowanego podpisu elektronicznego oraz selektywne udostępnianie danych. Docelowo zakłada się objęcie usługą nawet 20 milionów obywateli.

Spis treści

1.	Główne założenia Europejskich Ram Tożsamości Cyfrowej	5
1.1	Czym są Europejskie Ramy Tożsamości Cyfrowej i jakie zmiany wprowadzą	5
1.2	Europejski Portfel Tożsamości Cyfrowej	9
1.3	Inne nowe usługi Europejskich Ram Tożsamości Cyfrowej	11
1.4	Obowiązki interesariuszy	13
1.5	Harmonogram obowiązywania	16
1.6	Pilotaże Europejskiego Portfela Tożsamości Cyfrowej	18
2.	Implementacja Europejskich Ram Tożsamości Cyfrowej w Polsce	19
2.1	Dostosowanie mObywatel 2.0 do Europejskiego Portfela Tożsamości Cyfrowej	19
2.2	Krajowy pilotaż kwalifikowanego podpisu elektronicznego zintegrowanego z mObywatel 2.0	21
2.3	Współpraca rynkowa w obszarze usług zaufania: onboarding stron ufających w celu dostępu do elektronicznych poświadczeń atrybutów	22
2.4	Model docelowy dla kwalifikowanego podpisu elektronicznego w oparciu o Europejski Portfel Tożsamości Cyfrowej	23
3.0	Korzyści i nowe możliwości dla rynku wynikające z Europejskich Ram Tożsamości Cyfrowej	25

1. Głównie założenia Europejskich Ram Tożsamości Cyfrowej

1.1 Czym są Europejskie Ramy Tożsamości Cyfrowej i jakie zmiany wprowadzają.

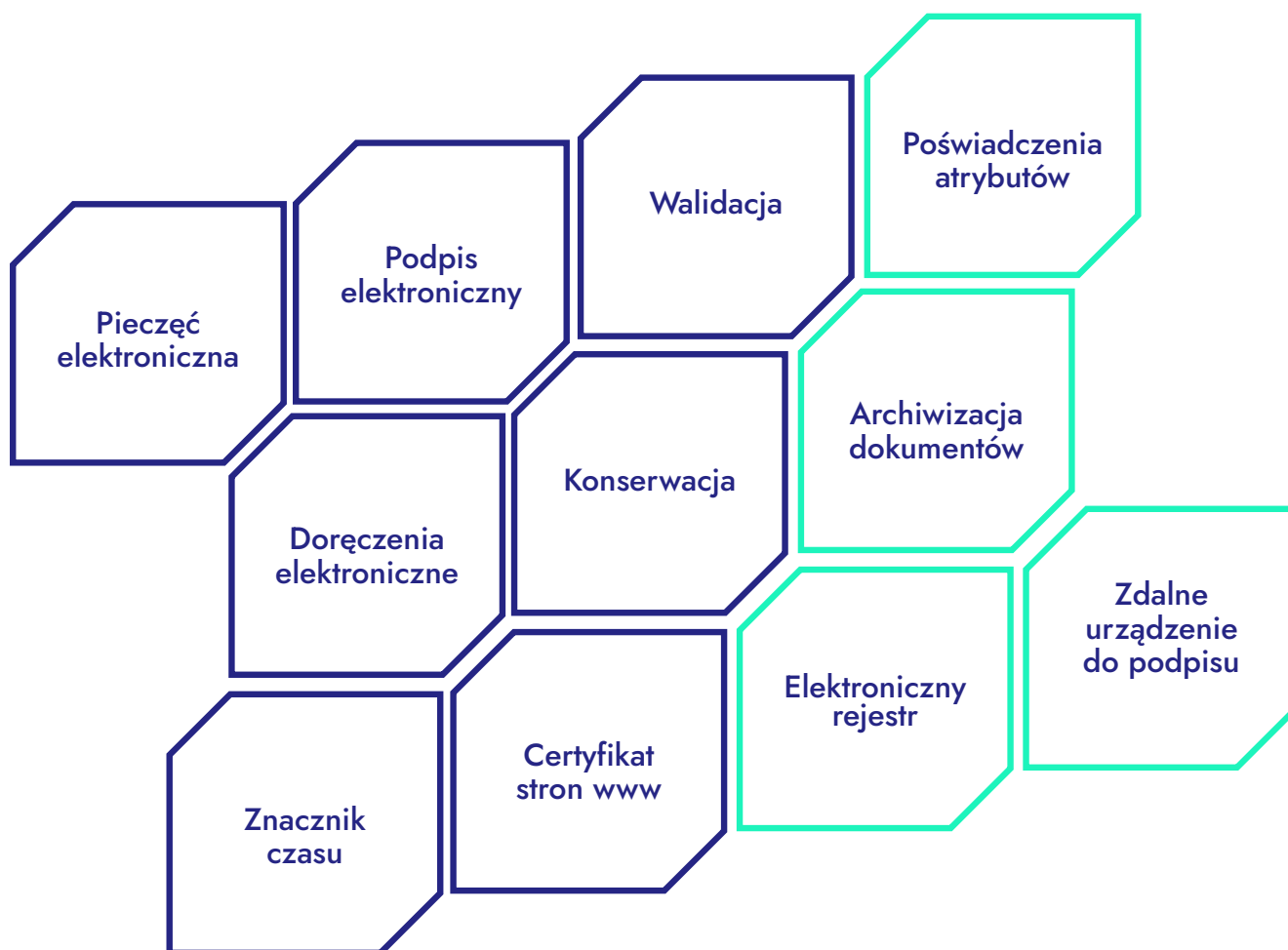
W lipcu 2025 roku przypada jedenasta rocznica opublikowania Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (tzw. rozporządzenie eIDAS). Celem rozporządzenia była harmonizacja rynku cyfrowego – stworzenie ujednoliconych ram prawnych i technicznych dla transakcji cyfrowych, na wspólnym rynku.

W dniu 29 lutego 2024 roku została przegłosowana przez Parlament Europejski nowelizacja rozporządzenia eIDAS wprowadzająca Europejskie Ramy Tożsamości Cyfrowej. 26 marca tego samego roku, Rada Unii Europejskiej również przyjęła tę nowelizację. Zaakceptowane, zmienione rozporządzenie, w kolejnych tygodniach zostało zamieszczone w Dzienniku Urzędowym UE, a po upływie dwudziestu dni od publikacji, czyli 20 maja 2024 roku, weszło w życie i oficjalnie obowiązuje. Pełne wdrożenie zaplanowane jest do końca 2026 roku.

Rozporządzenie eIDAS z 2014 roku określiło warunki uznawania przez państwa członkowskie środków identyfikacji elektronicznej osób fizycznych i prawnych oraz ustanowiło ramy prawne dla zdefiniowanych usług zaufania. Europejskie Ramy Tożsamości Cyfrowej gwarantują innowacyjne podejście do tożsamości cyfrowej w Europie, które ma zapewnić obywatelom i przedsiębiorcom Unii Europejskiej powszechny dostęp do bezpiecznej i wiarygodnej identyfikacji elektronicznej oraz uwierzytelniania elektronicznego.

Europejskie Ramy Tożsamości Cyfrowej rozszerzają zakres świadczonych usług zaufania, znanych z poprzedniego rozporządzenia, o dodatkowe elementy takie jak:

- **elektroniczne poświadczenia atrybutów,**
- **elektroniczną archiwizację danych elektronicznych i dokumentów elektronicznych,**
- **zarządzanie zdalnymi urządzeniami do składania podpisu elektronicznego i pieczęci,**
- **rejestrwanie danych elektronicznych w rejestrze elektronicznym.**



Rysunek 1. Istniejące oraz nowe usługi zaufania w ramach Europejskich Ram Tożsamości Cyfrowej

Pierwsze rozporządzenia wykonawcze (nazwane również aktami implementującymi) określające funkcje i wymagania bezpieczeństwa, a także kształt nowej infrastruktury zaufania wynikającej ze znowelizowanego rozporządzenia, weszły w życie w grudniu 2024 roku. Chociaż część zmian, które wchodzi w życie dzięki nowelizacji znalazły już odzwierciedlenie w brzmieniu odpowiednich przepisów, na inne trzeba poczekać do czasu pojawienia się odpowiednich rozporządzeń wykonawczych. Akty implementujące, które już obowiązują na dzień 20.05.2025 r., dotyczą funkcjonowania Europejskiego Portfela Tożsamości Cyfrowej:

- **CIR 2024/2977** Rozporządzenie wykonawcze Komisji (UE) 2024/2977 dotyczące PID (Dane Identyfikacyjne Osoby) oraz EAA – Elektroniczne Poświadczenia Atrybutów),
- **CIR 2024/2979** Rozporządzenie wykonawcze Komisji (UE) 2024/2979 dotyczące integralności i podstawowych funkcji,
- **CIR 2024/2980** Rozporządzenie wykonawcze Komisji (UE) 2024/2980 dotyczące powiadomień ekosystemowych,
- **CIR 2024/2981** Rozporządzenie wykonawcze Komisji (UE) 2024/2981 dotyczące certyfikacji rozwiązań portfela,
- **CIR 2024/2982** Rozporządzenie wykonawcze Komisji (UE) 2024/2982 dotyczące protokołów i interfejsów.

27 maja 2025 roku zaczną obowiązywać cztery kolejne rozporządzenia wykonawcze dotyczące takich aspektów jak:

- **CIR 2025/846** Transgraniczne dopasowanie tożsamości osób fizycznych,
- **CIR 2025/847** Incydenty i naruszenie bezpieczeństwa,
- **CIR 2025/848** Rejestracja stron ufających,
- **CIR 2025/849** Wykaz certyfikowanych europejskich portfeli tożsamości cyfrowej.

Natomiast od 15 kwietnia do 13 maja 2025 Komisja Europejska zebrała publiczne opinie dotyczące trzeciego zbioru projektów aktów wykonawczych obejmujących swym zakresem:

- Ustalenia proceduralne dotyczące wzajemnych ocen systemów identyfikacji elektronicznej, które mają być zgłaszane Komisji,
- Zgłoszenie i weryfikacja rozpoczęcia świadczenia kwalifikowanej usługi zaufania,
- Weryfikacja tożsamości i atrybutów przy wydawaniu kwalifikowanego certyfikatu lub kwalifikowanego poświadczenia atrybutów,
- Kwalifikowane certyfikaty podpisów elektronicznych i pieczęci elektronicznych,
- Zarządzanie urządzeniami do składania podpisu kwalifikowanego na odległość jako kwalifikowaną usługą zaufania,
- Powiadomienie o kwalifikowanych urządzeniach do składania podpisu elektronicznego i pieczęci elektronicznej, które zostały certyfikowane przez organy certyfikujące,
- Walidacja kwalifikowanych podpisów i pieczęci elektronicznych oraz zaawansowanych podpisów i pieczęci elektronicznych,
- Kwalifikowane usługi walidacji kwalifikowanych podpisów i pieczęci elektronicznych,

- Kwalifikowane usługi konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych,
- Świadczenie kwalifikowanych usług elektronicznego znakowania czasem,
- Wymogi dotyczące kwalifikowanych zarejestrowanych usług elektronicznych,
- Przekazywanie Komisji sprawozdań rocznych przez organy nadzorcze.

Przed publikacją projekty tych aktów będą przechodziły gruntowną modernizację.

EKSPERT RAPORTU

ROBERT POZNAŃSKI

ANALITYK, ASSECO DATA SYSTEMS

Rozporządzenie eIDAS 2.0 jest naturalną ewolucją względem przyjętego jeszcze w 2014 r. pierwszego rozporządzenia o identyfikacji elektronicznej oraz usługach zaufania.

Pierwsze Rozporządzenie skupione było przede wszystkim na usługach zaufania i dopiero wprowadziło identyfikację elektroniczną jako nową usługę. Europejskie Ramy Tożsamości Cyfrowej rozszerzają i porządkują mechanizmy identyfikacji elektronicznej, dzięki czemu usługi te powinny być bardziej przejrzyste a implementacje łatwiejsze do użycia przez obywateli.

Jedną z wielu nowości jest wprowadzenie europejskiego portfela identyfikacji cyfrowej, który mają być wyjściem naprzeciw zmieniającemu się stylowi życia, częstszym podróżom czy wykorzystaniu usług cyfrowych na poziomie transgranicznym.

W celu usprawnienia wdrożenia portfeli identyfikacji elektronicznej realizowane są pomiędzy różnymi krajami programy pilotażowe. Biorą w nich udział np. jednostki administracji publicznej oraz podmioty komercyjne, dzięki czemu możliwe będzie sprostanie oczekiwaniom zarówno podmiotów wdrażających jak i osób, które będą w przyszłości korzystały z tych rozwiązań.

1.2 Europejski Portfel Tożsamości Cyfrowej

Najbardziej rozpoznawalną i najbardziej istotną zmianą, którą wprowadzają Europejskie Ramy Tożsamości Cyfrowej jest wprowadzenie narzędzia o nazwie Europejski Portfel Tożsamości Cyfrowej.

Europejski Portfel Tożsamości Cyfrowej

to środek identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę, jak i elektronicznych poświadczeń atrybutów. Co więcej umożliwia on bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom Europejskich Portfeli Tożsamości Cyfrowej, które umożliwiają składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych.

Celem wprowadzenia portfela tożsamości jest umocnienie jednolitego rynku europejskiego przez umożliwienie obywatelom, mieszkańcom i przedsiębiorstwom identyfikację oraz uwierzytelnianie zarówno online, jak i offline. Zakłada się, że o Europejskim Portfelu Tożsamości Cyfrowej, będzie można mówić jako o narzędziu, które jest:

- bezpieczne – zapewni przechowywanie i udostępnianie danych przez bezpieczne protokoły komunikacji,
- zaufane – będzie traktowane jako wiarygodne źródło danych,
- przyjazne użytkownikowi, wygodne oraz dostępne – dzięki prostemu i intuicyjnemu interfejsowi, stworzonego z myślą o użytkownikach,
- rozpoznawalne w całej Unii Europejskiej – da możliwość identyfikacji we wszystkich krajach członkowskich UE.

W rozporządzeniu określono termin, który mówi o wprowadzeniu portfela i udostępnieniu go użytkownikom w sposób obligatoryjny – państwa członkowskie UE muszą posiadać swój portfel cyfrowy, który będzie służył obywatelom, przedsiębiorcom oraz innym instytucjom nie później niż 30 miesięcy od wejścia w życie Europejskich Ram Tożsamości

Cyfrowej. Użytkownicy będą mogli łatwo udowodnić swoją tożsamość i udostępniać dokumenty elektroniczne ze swoich portfeli cyfrowych za pomocą telefonu komórkowego i innych kanałów, a także potwierdzić swoje atrybuty (np. kwalifikacje zawodowe czy posiadanie prawa jazdy). Portfel będzie oficjalnym środkiem identyfikacji, który będzie miał zastosowanie w sektorze publicznym oraz prywatnym. Będzie też oferował wbudowany kwalifikowany podpis elektroniczny, który ma być dostępny dla każdej osoby fizycznej i nieodpłatny przy wykorzystaniu do celów prywatnych.

W Polsce rolę Europejskiego Portfela Tożsamości Cyfrowej będzie pełnić, znana już na polskim rynku, aplikacja mObywatel.

EKSPERT RAPORTU

MICHAŁ TABOR

Partner, Członek Zarządu, Obserwatorium.biz

Ekspert ds. identyfikacji, weryfikacji i podpisu elektronicznego, PIIT

Pomysł portfela tożsamości cyfrowej dla osób jest już dobrze znany. Zwykle działa on jako aplikacja mobilna, która pozwala użytkownikom udostępniać zweryfikowane dane tożsamości. Regulacja eIDAS wprowadza również portfel dla osób prawnych, nazywany portfelem biznesowym. Może on przyspieszyć cyfrowe zmiany zarówno w biznesie, jak i administracji. Jednym z pierwszych zastosowań portfela biznesowego będzie zarządzanie pełnomocnictwami i uprawnieniami, na przykład w procesach Know Your Business. Na początku dane dotyczące firm mogą pojawiać się w portfelach osób fizycznych, ale później zostaną przeniesione do portfela biznesowego. Taki portfel może pomóc przejść od wielu oddzielnych systemów do jednego, wspólnego sposobu zarządzania rolami i dostępem. Z czasem portfel biznesowy może pomóc zautomatyzować zadania biznesowe, umożliwiając bezpieczne udostępnianie danych firmy, przekazywanie przydatnych informacji i potwierdzanie wiarygodności danych o firmie. Jestem przekonany, że portfel biznesowy stanie się w najbliższych latach integralną częścią transakcji elektronicznych.

1.3 Inne nowe usługi Europejskich Ram Tożsamości Cyfrowej



Rysunek 2. Obecne oraz nowe rozwiązania bazujące na usługach zaufania

Europejskie Ramy Tożsamości Cyfrowej pozwalają na wprowadzenie szeregu nowych rozwiązań bazujących na usługach zaufania. Należą do nich archiwizacja elektroniczna danych elektronicznych i dokumentów, walidacja danych przekazywanych za pośrednictwem e-doręczeń, wydawanie elektronicznych poświadczeń atrybutów oraz ich walidacja, rejestrowanie danych elektronicznych w rejestrze elektronicznym, walidacja elektronicznych znaczników czasu, a także zarządzanie urządzeniami do składania podpisu elektronicznego na odległość. Poniżej przedstawione są opisy wybranych nowych usług:

Elektroniczne potwierdzenia atrybutów

Europejskie Ramy Tożsamości Cyfrowej wprowadzają kwalifikowane elektroniczne poświadczenie atrybutów, czyli elektroniczne poświadczenie atrybutów wydawane przez kwalifikowanego dostawcę usług zaufania i spełniające określone wymagania. Elektroniczne potwierdzenia atrybutów to cyfrowe dokumenty lub certyfikaty, które weryfikują określone właściwości, cechy lub uprawnienia przypisane do osoby, organizacji lub przedmiotu. Są one wydawane przez zaufane instytucje lub podmioty, które mogą potwierdzić prawdziwość i autentyczność tych atrybutów. Elektroniczne potwierdzenia atrybutów mogą być wykorzystywane w różnych kontekstach, m.in. takich jak:

- tożsamość cyfrowa: potwierdza dane identyfikacyjne osoby, takie jak imię, nazwisko, numer identyfikacyjny, czy adres,
- uprawnienia i kwalifikacje: weryfikują kwalifikacje zawodowe, uprawnienia do wykonywania określonych czynności czy posiadanie określonych licencji,
- atrybuty organizacyjne: potwierdzają role i stanowiska w organizacjach, np. status pracownika, członka zarządu czy pełnomocnika,
- właściwości produktów: potwierdzają cechy i specyfikacje produktów, np. certyfikaty jakości, zgodności z normami.

Elektroniczne potwierdzenia atrybutów są kluczowym elementem nowej infrastruktury zaufania, umożliwiającym bezpieczne i efektywne weryfikowanie informacji zarówno online, jak i offline. Przykłady zastosowania obejmują onboarding do usług finansowych, logowanie do systemów informatycznych, autoryzację transakcji, czy potwierdzanie kwalifikacji podczas rekrutacji. Dzięki Europejskim Ramom Tożsamości Cyfrowej, elektroniczne potwierdzenia atrybutów zyskują ujednolicone ramy prawne w Unii Europejskiej, co zwiększy ich wiarygodność i interoperacyjność na rynku europejskim. Elektroniczne potwierdzenie atrybutów będzie uznawane przez sądy i urzędy, a każdy użytkownik będzie mógł wykorzystywać Portfel Tożsamości Cyfrowej do otrzymywania, przechowywania i udostępniania elektronicznych poświadczeń atrybutów.

Archiwizacja elektroniczna jako usługa zaufania

Archiwizacja elektroniczna to usługa, która obejmuje odbiór, przechowywanie, odzyskiwanie i usuwanie danych oraz dokumentów elektronicznych, zapewniając ich trwałość, czytelność, integralność, poufność i dowód pochodzenia przez cały okres ich przechowywania. Obecnie elektroniczna archiwizacja w krajach Unii Europejskiej funkcjonuje na podstawie przepisów krajowych, co uniemożliwia świadczenie i uznawanie tego typu usług transgranicznie. Dzięki włączeniu tej usługi do Europejskich Ram Tożsamości Cyfrowej, powstaje jednolite europejskie podejście, które unika fragmentacji rynku i może zwiększyć zapotrzebowanie na tę usługę w całej UE. Wiąże się to jednak z konkretnymi wymaganiami dla dostawców usług zaufania. Muszą oni stosować procedury i technologie, które zapewniają trwałość i czytelność danych elektronicznych w czasie, a także ich integralność i dokładność od momentu przechowywania do pobrania.

1.4 Obowiązki interesariuszy

Nowelizacja omawianego rozporządzenia nie tylko wprowadza nowe usługi i rozwiązania, ale też określa szczegółowe zobowiązania na poszczególnych interesariuszy europejskiego rynku cyfrowego. Obecni, jak i nowi gracze rynkowi, państwa członkowskie i ich administracja, będą musieli sprostać wyzwaniom jakie stawiają przed nimi Europejskie Ramy Tożsamości Cyfrowej. Po stronie użytkowników pozostanie dużo wyzwań w postaci akceptacji i zrozumienia dla nowych usług i warunków ich funkcjonowania.

Obowiązki państw członkowskich

Państwa członkowskie Unii Europejskiej są odpowiedzialne za zapewnienie swoim obywatelom i rezydentom dostępu do co najmniej jednego Europejskiego Portfela Tożsamości Cyfrowej, który spełnia zharmonizowane unijne standardy w zakresie bezpieczeństwa, interoperacyjności i ochrony danych osobowych. Obowiązek ten obejmuje zarówno stworzenie krajowych mechanizmów certyfikacji i nadzoru nad dostawcami portfeli, jak i zapewnienie ich wzajemnej uznawalności w ramach całej Unii. Państwa członkowskie muszą także zagwarantować równy dostęp do usług identyfikacji elektronicznej dla wszystkich obywateli i rezydentów – niezależnie od ich pochodzenia, statusu społecznego czy lokalizacji – eliminując bariery cyfrowe i techniczne. Co istotne, korzystanie z portfela nie może być obowiązkowe; państwa członkowskie zobowiązane są do zapewnienia alternatywnych sposobów identyfikacji w kontaktach z administracją publiczną. Na państwach członkowskich ciąży również obowiązek ustanowienia elektronicznych rejestrów stron ufających portfelom, wraz z krajowymi politykami rejestracji, które określają m.in. proces zgłoszenia, dokumentację, sposób weryfikacji, procedury aktualizacji danych

oraz mechanizmy odwoławcze. Ponadto państwa powinny również prowadzić działania edukacyjne i informacyjne, wspierać rozwój kompetencji cyfrowych obywateli oraz inicjować pilotaże innowacyjnych rozwiązań poprzez tzw. piaskownice regulacyjne, które umożliwiają bezpieczne testowanie nowych technologii w ograniczonym środowisku.

Obowiązki administracji publicznej

Instytucje administracji publicznej, zarówno na szczeblu krajowym, jak i lokalnym, mają obowiązek pełnego uznawania i wspierania użycia europejskich portfeli tożsamości cyfrowej jako środka identyfikacji i uwierzytelniania w elektronicznych usługach publicznych. Oznacza to konieczność dostosowania infrastruktury informatycznej i procedur administracyjnych do obsługi portfela w kontaktach z obywatelami oraz zapewnienia zgodności z unijnymi zasadami minimalizacji danych i poszanowania prywatności. Administracja publiczna nie może odmówić dostępu do usług z powodu niekorzystania przez obywatela z portfela ani faworyzować użytkowników portfeli cyfrowych względem innych. Jednocześnie powinna aktywnie współpracować z ich dostawcami, zapewniając skuteczny proces rejestracji stron ufających oraz kontrolę nad ich zgodnością z przepisami prawa. W przypadku stwierdzenia nieprawidłowości administracja ma obowiązek podjęcia działań nadzorczych i korygujących.

Obowiązki stron ufających (przedsiębiorstw i platform cyfrowych)

Przedsiębiorstwa świadczące usługi cyfrowe, zwłaszcza w sektorach regulowanych lub wymagających silnego uwierzytelnienia, mają obowiązek akceptowania europejskich portfeli tożsamości cyfrowej w sytuacjach, gdy takie uwierzytelnienie jest wymagane przez prawo unijne, krajowe lub na podstawie zawartej umowy. Dotyczy to w szczególności bardzo dużych platform internetowych, które zgodnie z rozporządzeniem DSA (2022/2065) są zobowiązane do umożliwienia użytkownikom korzystania z Europejskiego Portfela Tożsamości Cyfrowej jako metody logowania, jeśli użytkownik tego zażąda. Przedsiębiorcy muszą zadbać, aby żądania udostępnienia danych przez użytkowników były zgodne z zasadą proporcjonalności i konieczności oraz jasno określały, jakie dane są wymagane i do jakiego celu. Obowiązkiem stron ufających (prywatnych firm) jest także rejestracja w krajowych rejestrach, prowadzenie oceny skutków dla ochrony danych i zapewnienie zgodności z RODO – w tym także przy przetwarzaniu danych szczególnych kategorii, takich jak dane zdrowotne. Rejestracja musi być przejrzysta, niedyskryminująca i dostosowana do różnych modeli działalności – zarówno online, jak i offline. Rejestry mają umożliwić użytkownikowi weryfikację strony ufającej i jej uprawnień. Strony ufające powinny korzystać z portfela wyłącznie w zakresie, który wcześniej zgłosiły i który został zatwierdzony przez podmiot rejestrujący.

Obowiązki dostawców Europejskich Portfeli Tożsamości Cyfrowej

Dostawcy Europejskich Portfeli Tożsamości Cyfrowej, niezależnie od tego, czy są to podmioty publiczne, prywatne, działające z upoważnienia państwa członkowskiego czy niezależnie, ponoszą odpowiedzialność za wdrożenie najwyższych standardów bezpieczeństwa i prywatności już na etapie projektowania usługi. Muszą zagwarantować pełne oddzielenie logiczne (a preferencyjnie także fizyczne) danych związanych z obsługą portfeli od pozostałych danych przetwarzanych przez organizację. Dostawcy nie mogą zbierać danych o transakcjach użytkownika, ich treści ani historii, chyba że użytkownik wyrazi na to uprzednią, świadomą i wyraźną zgodę. Funkcjonalność musi obejmować przejrzysty panel zarządzania, selektywne ujawnianie danych, możliwość zarządzania pseudonimami i domyślne włączenie śledzenia historii transakcji, w tym opcji ich usunięcia. Dostawcy muszą także zapewnić, że użytkownik może przenieść swoje dane do innego portfela bez ponoszenia dodatkowych kosztów, a ich oprogramowanie musi być interoperacyjne z urządzeniami mobilnymi i platformami (np. NFC, secure elements, SIM).

Obowiązki dostawców usług zaufania

Dostawcy usług zaufania, zwłaszcza ci wydający kwalifikowane certyfikaty i elektroniczne poświadczenia atrybutów, zostają objęci nowymi, precyzyjnie określonymi obowiązkami wynikającymi zarówno z rozporządzenia eIDAS, jak i dyrektywy NIS2. Muszą wdrażać adekwatne środki techniczne i organizacyjne w celu zarządzania ryzykiem w obszarze cyberbezpieczeństwa i zgłaszać incydenty, które mogą mieć wpływ na jakość świadczonych usług. Szczególny nacisk położono na konieczność zapewnienia „całkowitej pewności” przy weryfikacji tożsamości osób, którym wydawane są kwalifikowane certyfikaty lub poświadczenia. W tym celu dopuszcza się różne metody uwierzytelniania, w tym łączenie środków identyfikacji elektronicznej średniego poziomu z dodatkowymi mechanizmami weryfikacyjnymi. W przypadku kwalifikowanych poświadczeń atrybutów, dostawcy muszą umożliwiać weryfikację tych atrybutów względem źródeł autentycznych, zgodnie z przepisami prawa unijnego lub krajowego. Ponadto, Europejskie Ramy Tożsamości Cyfrowej wprowadzają nowe regulacje dotyczące kar dla dostawców usług zaufania w przypadku naruszenia bezpieczeństwa świadczonych przez nich usług. Dodatkowe wymagania i kary dotyczą zarówno kwalifikowanych, jak i niekwalifikowanych dostawców usług zaufania.

Uprawnienia i możliwości dla użytkowników (obywateli i rezydentów UE)

Użytkownicy Europejskich Portfeli Tożsamości Cyfrowej, czyli obywatele i rezydenci Unii Europejskiej nie będą mieli żadnych nowych obowiązków, zyskują tu natomiast szereg praw oraz możliwości kontroli nad swoimi danymi osobowymi. Portfel cyfrowy musi pozostawać pod ich wyłączną kontrolą, a korzystanie z niego ma być całkowicie dobrowolne. Użytkownicy mają prawo łączyć, przechowywać, selektywnie udostępniać, a także usuwać dane zawarte w portfelu. Powinni mieć również możliwość tworzenia pseudonimów i zarządzania nimi oraz dostęp do pełnej historii transakcji przeprowadzanych z użyciem portfela. Domyślnie portfel ma umożliwiać składanie kwalifikowanych podpisów elektronicznych bez konieczności przechodzenia dodatkowych procedur administracyjnych i bez opłat (w zastosowaniach nieprofesjonalnych). W przypadku wykrycia nadużycia lub niezgodnego z prawem żądania danych, użytkownik powinien mieć możliwość zgłoszenia incydentu do organu ochrony danych bezpośrednio z poziomu aplikacji portfela. Ponadto Europejskiego Portfela Tożsamości Cyfrowej będzie można używać także poza granicami swojego kraju na terenie całej UE. Obywatele i rezydenci Unii będą mieli w sposób bezpieczny oraz z zapewnieniem wysokiego stopnia ochrony danych możliwość dokonywania transgranicznej wymiany informacji cyfrowych związanych z ich tożsamością, takich jak ich adres, wiek, kwalifikacje zawodowe, prawo jazdy i inne zezwolenia oraz dane dotyczące płatności.

1.5 Harmonogram obowiązywania

Jak zostało wspomniane powyżej, rozporządzenie wprowadzające Europejskie Ramy Tożsamości Cyfrowej weszło oficjalnie w życie 20 maja 2024 roku, a pierwszych pięć aktów implementujących weszło w życie 24 grudnia 2024 roku. Każde państwo członkowskie zobowiązane jest do zapewnienia swoim obywatelom co najmniej jednego Europejskiego Portfela Tożsamości Cyfrowej w terminie 24 miesięcy od dnia opublikowania w/w aktów wykonawczych, co w praktyce oznacza 24 grudnia 2026 roku.

Aktualni kwalifikowani dostawcy usług zaufania muszą dostosować swoją infrastrukturę i świadczone usługi do wymogów znowelizowanego rozporządzenia oraz przedstawić stosowny raport z audytu na zgodność nie później niż w dniu 21 maja 2026 roku.

Od 24 grudnia 2027 roku regulowane branże muszą akceptować Europejskie Portfele Tożsamości Cyfrowej jako metodę uwierzytelniania. Dotyczy to przedsiębiorstw działających w sektorach, w których prawo wymaga silnego uwierzytelniania, m.in. w sektorze bankowym, telekomunikacyjnym i usługach rządowych.



Rysunek.3. Harmonogram wprowadzania Europejskich Ram Tożsamości Cyfrowej

1.6 Pilotáže Europejskiego Portfela Tożsamości Cyfrowej

W 2023 roku Komisja Europejska zleciła realizację zadania o nazwie Wielkoskalowe Pilotáže Europejskiego Portfela Tożsamości Cyfrowej (Large Scale Pilots (LSPs)) for EU Digital Identity Wallet). Pilotáže te zostały uruchomione w celu przetestowania w praktyce, na dużą skalę i w rzeczywistych warunkach, tego, jak będzie działać portfel w ekosystemie realnych usług, dostawców i przypadków użycia. W pierwszej fazie programu, przewidzianej na okres dwóch lat (2023-25) utworzono cztery międzynarodowe realizujące pilotáže, w których wzięło udział kilkadziesiąt organizacji komercyjnych, podmiotów z administracji publicznej jak również świata naukowego z całej Europy:

- POTENTIAL,
- EU Digital Wallet Consortium (EWC),
- NOBID Consortium,
- DC4EU (Digital Credentials for Europe).

Zadaniem tych przedsięwzięć jest wdrożenie i przetestowanie realnych scenariuszy biznesowych z wykorzystaniem portfela, w takich obszarach jak m.in.:

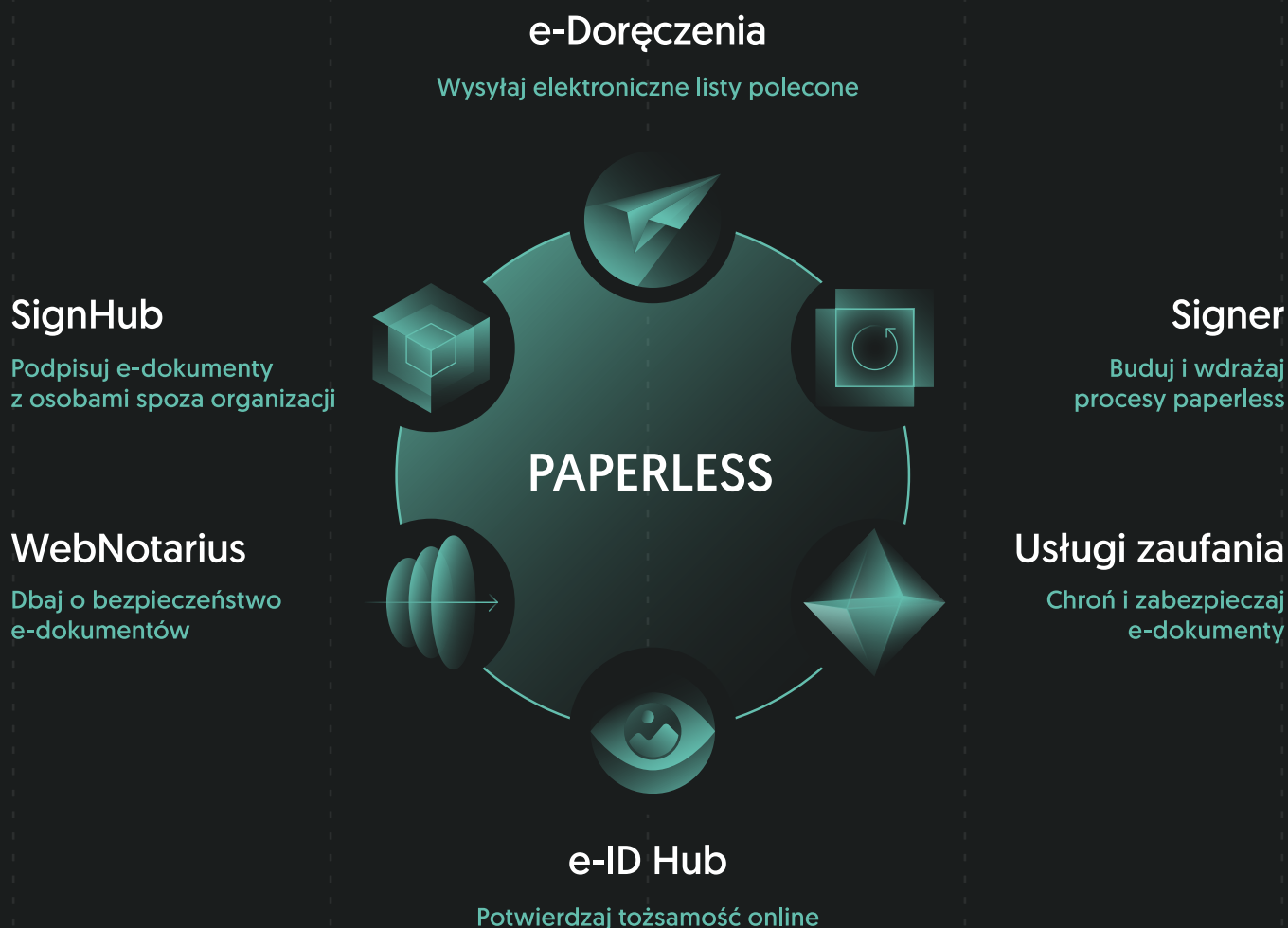
- podróże i odprawy lotniskowe,
- otwieranie konta bankowego,
- podpisywanie dokumentów,
- dostęp do usług zdrowotnych i edukacyjnych,
- potwierdzanie uprawnień zawodowych i reprezentacji prawnej.

Wyżej wymienione konsorcja zakończą działalność latem 2025 roku. Na początku 2025 roku, wyniku kolejnego przetargu, wyłoniono dwa nowe konsorcja, a mianowicie: WE BUILD (Wallet Ecosystem for Business & Payment Use cases, Identification, Legal person representation, and Data sharing) oraz Aptitude. Oczekuje się, że oba nowe projekty rozpoczną się we wrześniu 2025 r. i potrwać dwa lata.

Zgodnie ze znowelizowanym Rozporządzeniem eIDAS, państwa członkowskie będą zobowiązane do wydania portfela do 2026 r. Pilotáže służą jako etap przejściowy, umożliwiający testowanie i zbieranie doświadczeń przed pełnym wdrożeniem.

Używaj narzędzi ekosystemu #EnterprisePaperless!

Transformacja cyfrowa zwiększa efektywność, ale wymaga gotowości do zmian w procesach i sposobie myślenia. Dzięki nam odkryjesz korzyści z przejścia na paperless i przeniesiesz swoją organizację do cyfrowej przyszłości, gdzie papier przestaje być nośnikiem dokumentów.



Dołącz do świadomych przedsiębiorców.
Sprawdź jak na: paperless.asseco.com

ASSECO

2. Implementacja Europejskich Ram Tożsamości Cyfrowej w Polsce

2.1 Dostosowanie mObywatel 2.0 do Europejskiego Portfela Tożsamości Cyfrowej

Aplikacja mObywatel 2.0 stanowi kluczowy element polskiej strategii cyfrowej, oferując obywatelom możliwość wygodnego dostępu do szeregu oficjalnych dokumentów w wersji elektronicznej za pośrednictwem smartfona. Obecnie w ramach aplikacji dostępne są m.in. mDowód (mobilny dokument tożsamości), prawo jazdy, dane rejestracyjne pojazdów (mPojazd), legitymacje studenckie i emeryckie oraz Karta Dużej Rodziny. Dokumenty te są honorowane zarówno przez administrację publiczną, jak i przez podmioty sektora prywatnego.

Weryfikacja dokumentów w aplikacji mObywatel 2.0 została zaprojektowana z myślą o bezpieczeństwie, wygodzie użytkownika i uniwersalności zastosowania. Użytkownik może potwierdzić swoje dane na dwa sposoby: poprzez weryfikację wizualną (sprawdzenie wyglądu dokumentu, obecności elementów zabezpieczających, takich jak hologramy i tło dynamiczne) lub za pomocą weryfikacji kryptograficznej. Ta druga, najbardziej bezpieczna metoda opiera się na infrastrukturze klucza publicznego (PKI), a proces rozpoczyna się od zeskanowania jednorazowego kodu QR, który inicjuje bezpieczne połączenie i wymianę danych z podmiotem weryfikującym. Dane te nie są przechowywane po stronie odbiorcy, co istotnie zwiększa poziom ochrony prywatności.

Wszystkie dane użytkownika są szyfrowane i przechowywane wraz z kluczami kryptograficznymi w chronionym środowisku urządzenia mobilnego. Udostępniane dane wyświetlane są tylko przez krótki czas i nie mogą być zapisane przez podmiot weryfikujący, co zapewnia prywatność i minimalizuje ryzyko nadużyć.

Pomimo wysokiego poziomu dojrzałości technologicznej oraz szerokiego zakresu funkcjonalności, aplikacja mObywatel 2.0 nie jest jeszcze w pełni zgodna ze znowelizowanym rozporządzeniem eIDAS. Poniżej zaprezentowano porównanie mObywatel 2.0 z docelową aplikacją w wersji 3.0.

Cecha	mObywatel 2.0	mObywatel 3.0 (Polski portfel Tożsamości Cyfrowej)
Poziom bezpieczeństwa	Średni	Wysoki lub średni
Certyfikacja bezpieczeństwa	Nie jest wymagana	Wymagana na zgodność z Common Criteria
Kwalifikowany podpis elektroniczny	Nie wspierany	Wspierany
Dokumenty mobilne	Stacyczny zestaw danych	Selektywne ujawnianie przez użytkownika
Integracja stron ufających	Procedura administracyjna	Automatyczna integracja na podstawie wcześniejszej rejestracji

Centralny Ośrodek Informatyki (COI) prowadzi już prace nad dostosowaniem aplikacji mObywatel 2.0 w Europejski Portfel Tożsamości Cyfrowej. Dzięki realizacji projektu wewnętrznie, COI ogranicza zależność od dostawców zewnętrznych i wzmacnia długoterminową niezależność technologiczną państwa. Rozwiązanie opracowywane przez COI jest w pełni zgodne z przyjętymi unijnymi aktami wykonawczymi oraz powiązanymi specyfikacjami technicznymi. Wspiera ono formaty poświadczeń zdefiniowane w Architecture Reference Framework.

W celu zapewnienia interoperacyjności transgranicznej, COI aktywnie uczestniczy w unijnych projektach pilotażowych. W szczególności brał udział w wydarzeniu Warsaw Interop Event w lutym 2025 roku, podczas którego przeprowadzono międzynarodowe testy mające na celu weryfikację zgodności technicznej i prawnej z innymi krajowymi implementacjami Europejskiego Portfela Tożsamości Cyfrowej. Działania te potwierdzają gotowość polskiego rozwiązania do funkcjonowania w europejskim ekosystemie zaufanych usług tożsamości cyfrowej.

2.2 Krajowy pilotaż kwalifikowanego podpisu elektronicznego zintegrowanego z mObywatel 2.0

Ministerstwo Cyfryzacji prowadzi pilotaż z udziałem portfela mObywatel 2.0 w ramach którego tożsamość osoby podpisującej dokument potwierdzana jest za pośrednictwem portfela tożsamości cyfrowej. Proces podpisu opiera się na wykorzystaniu jednorazowego kwalifikowanego podpisu elektronicznego. Od października 2025 roku pilotaż obejmie wszystkich polskich kwalifikowanych dostawców usług zaufania i zakłada udostępnienie obywatelom kwalifikowanego podpisu elektronicznego bez opłat – do użytku prywatnego, niezwiązanego z działalnością zawodową.

Pilotaż zakłada wykorzystanie aplikacji mObywatel 2.0 do procesu onboardingu, natomiast wydanie certyfikatu i złożenie podpisu realizowane jest przez kwalifikowanych dostawców usług zaufania (QTSP) zintegrowanych z portfelem. Po uwierzytelnieniu się za pomocą e-dowodu i aplikacji mObywatel, użytkownik wybiera jednego z dostawców z losowo generowanej listy, co zapewnia równe szanse wszystkim dostawcom kwalifikowanym e-podpisu. Podpis składany jest z użyciem jednorazowego certyfikatu, zgodnie ze standardem PAdES, a podpisany dokument natychmiast przekazywany jest na platformę, z której zainicjowano proces.

Podstawą wspomnianej współpracy są formalne porozumienia zawarte pomiędzy Ministerstwem Cyfryzacji a wszystkimi uczestniczącymi w pilotażu dostawcami, precyzujące zasady współdziałania, podział odpowiedzialności oraz sposób przetwarzania danych. Państwo zapewnia zarówno koordynację prawną, jak i techniczną, dążąc do wypracowania modelu usługi, który będzie skalowalny i zgodny z przyszłymi wymogami regulacyjnymi.

Pilotaż stanowi fundament dla długofalowej integracji kwalifikowanego podpisu elektronicznego z Europejskim Portfelem Tożsamości Cyfrowej. Jego celem jest nie tylko weryfikacja gotowości technologicznej i zgodności prawnej rozwiązania, lecz także przygotowanie gruntu pod powszechne wdrożenie odpowiadające potrzebom obywateli i wymaganiom Unii Europejskiej. Inicjatywa ta wzmacnia również zaufanie do krajowych usług cyfrowych i promuje ich wykorzystanie.

2.3 Współpraca rynkowa w obszarze usług zaufania: onboarding stron ufających w celu dostępu do elektronicznych poświadczeń atrybutów

Zgodnie z rozporządzeniem eIDAS 2.0, wszystkie państwa członkowskie UE, które wdrażają Europejski Portfel Tożsamości Cyfrowej są zobowiązane do ustanowienia krajowego systemu rejestracji stron ufających. Są to podmioty, które chcą wykorzystywać portfel do weryfikacji tożsamości użytkowników lub pozyskiwania od nich danych w postaci różnych poświadczeń atrybutów. System rejestracji musi obejmować m.in. sposób rejestrowania podmiotów w państwie ich siedziby, zasady wydawania certyfikatów dostępowych potwierdzających ich uprawnienia dostępowe oraz mechanizmy zarządzania tymi certyfikatami w czasie. Informacje o zarejestrowanych podmiotach powinny być publicznie dostępne – zarówno w formie czytelnej dla człowieka, jak i możliwej do przetwarzania automatycznie (np. poprzez stronę internetową lub interfejs API). Każde państwo członkowskie powinno opublikować krajową politykę w tym zakresie. Polityka ta powinna umożliwiać szybki i zautomatyzowany proces rejestracji. Całość musi być przyjazna użytkownikowi i dostępna online. Zgodnie z projektem unijnego aktu wykonawczego, proces ten powinien być niedrogi i proporcjonalny do poziomu ryzyka.

Projekt europejskiej normy ETSI TS 119 475 przewiduje dwa modele realizacji tego procesu:

- Pierwszy model opiera się na obsłudze procesu przez administrację publiczną – całość procesu rejestracji i wydawania certyfikatów dostępowych prowadzona jest bezpośrednio przez instytucję państwową, taką jak np. Ministerstwo Cyfryzacji. Państwo zachowuje pełną kontrolę nad procesem weryfikacji podmiotów, jednak model ten wymaga budowy dedykowanej infrastruktury oraz zaangażowania odpowiednich zasobów kadrowych.
- Drugi model zakłada delegację zadań na kwalifikowanych dostawców usług zaufania. To oni, na podstawie umów i w oparciu o krajowe przepisy, prowadzą proces rejestracji i wydawania certyfikatów dostępowych w imieniu państwa. Model ten pozwala na wykorzystanie istniejącej infrastruktury oraz doświadczenia QTSP, odciążając tym samym administrację publiczną i ograniczając koszty operacyjne.

Decyzja dotycząca wyboru konkretnego modelu w Polsce nie została jeszcze podjęta. Trwają prace nad ustaleniem docelowego rozwiązania.

2.4 Model docelowy dla kwalifikowanego podpisu elektronicznego w oparciu o Europejski Portfel Tożsamości Cyfrowej

Docelowy model stosowania kwalifikowanego podpisu elektronicznego w ramach Europejskiego Portfela Tożsamości Cyfrowej w Polsce zakłada zapewnienie tej usługi wszystkim obywatelom – bezpłatnie i w sposób powszechny. Usługa będzie dostępna wyłącznie poprzez krajowy portfel cyfrowy mObywatel 3.0 i ma umożliwiać proste, bezpieczne oraz prawnie uznawane podpisywanie dokumentów w relacjach prywatnych, administracyjnych i biznesowych inicjowanych przez państwo.

Model obejmuje trzy podstawowe scenariusze użycia:

- Obywatel–Obywatel (C2C) – podpisywanie dokumentów w kontaktach prywatnych, w oparciu o krótkoterminowe certyfikaty wydawane zdalnie na czas jednej sesji podpisu;
- Obywatel–Administracja (C2A) – podpisywanie dokumentów urzędowych, z pełną integracją procesu identyfikacji i składania podpisu z platformami administracji publicznej
- Obywatel–Biznes (C2B) – wykorzystanie podpisu w kontaktach z podmiotami prywatnymi z pełną integracją procesu identyfikacji i składania podpisu z platformami komercyjnymi.

W zależności od przyjętego modelu finansowania, mogą zostać wprowadzone ograniczenia liczby podpisów możliwych do złożenia w określonym czasie. Aktualnie zakłada się, że scenariusze C2C pozostaną całkowicie bezpłatne. W przypadku pozostałych zastosowań analizowane są różne warianty finansowania, takie jak: roczna subskrypcja użytkownika, ryczałtowe dopłaty dla dostawców usług zaufania lub opłaty za pojedynczy podpis. W relacjach C2A koszty mogą zostać pokryte przez państwo, natomiast w scenariuszach C2B – przez podmioty gospodarcze inicjujące proces.

Celem jest osiągnięcie masowego wykorzystania rozwiązania – do 2031 roku planuje się objęcie usługą 20 milionów obywateli. Model ten ma uczynić kwalifikowany podpis elektroniczny podstawową usługą w przestrzeni cyfrowej, zwiększyć dostęp obywateli do e-administracji i wspierać zaufane interakcje cyfrowe we wszystkich sektorach, przy jednoczesnym zachowaniu konkurencyjności na rynku usług zaufania.

EKSPERT RAPORTU

RAFAŁ SIONKOWSKI

ZASTĘPCA DYREKTORA DEPARTAMENTU KANAŁÓW CYFROWYCH,
CENTRALNY OŚRODEK INFORMATYKI (COI)

W odpowiedzi na wymogi europejskiego rozporządzenia eIDAS 2.0 budujemy nową wersję aplikacji mObywatel – cyfrowy portfel tożsamości, który będzie zgodny z najnowszymi standardami identyfikacji elektronicznej i usług zaufania. To przedsięwzięcie stanowi duże wyzwanie zarówno pod względem technologicznym, jak i organizacyjnym – zwłaszcza że Polska już dysponuje rozbudowanym i szeroko wykorzystywanym rozwiązaniem. W wielu aspektach mierzymy się z większymi trudnościami niż państwa, które budują swoje systemy od podstaw – chociażby w zakresie migracji danych i doświadczenia ponad 9 milionów aktywnych użytkowników.

Kompleksowe wdrożenie europejskiej cyfrowej tożsamości może przynieść wymierne korzyści nie tylko dla administracji publicznej, lecz również dla całej gospodarki. Nowe mechanizmy identyfikacji i uwierzytelniania cyfrowego przyczynią się do przyspieszenia cyfryzacji procesów, zwiększenia bezpieczeństwa usług online oraz uproszczenia interakcji obywateli z instytucjami.

Aby wdrożenie eIDAS 2.0 przyniosło oczekiwane efekty, konieczne jest ścisłe współdziałanie wielu podmiotów – zarówno instytucji publicznych, jak i prywatnych. Szczęólnego znaczenia nabiera zapewnienie interoperacyjności między rozwiązaniami państwowymi a ofertą rynku, w tym w zakresie kwalifikowanych podpisów elektronicznych. W środowisku, w którym funkcjonuje podpis zaufany jako narzędzie publiczne, potrzebne jest szerokie porozumienie pomiędzy kwalifikowanymi dostawcami usług zaufania, sektorem prywatnym oraz organami państwa, aby zapewnić spójność, bezpieczeństwo i szeroką dostępność usług tożsamości cyfrowej.



CZY WIESZ, ŻE...

e-Polecony do księgowej
wyślesz na luzie w czasie pracy?

Załącz adres do doręczeń elektronicznych i korzystaj z e-Poleconego:

wygodna wysyłka
z dowolnego
miejsca i urządzenia

bez awizo,
bez kolejek

gwarancja
bezpiecznego
szyfrowania

automatyczne
generowanie
dokumentów

możliwość
monitorowania
listu

ochrona
środowiska przez
redukcję papieru

Dowiedz się więcej na www.e-polecony.com

3. Korzyści i nowe możliwości dla rynku wynikające z Europejskich Ram Tożsamości Cyfrowej

Europejskie Ramy Tożsamości Cyfrowej z założenia mają zrewolucjonizować sposób, w jaki obywatele i firmy funkcjonują w środowisku cyfrowym. Centralnym elementem znowelizowanego rozporządzenia jest opisywany w szczegółach w poprzedniej części raportu, Europejski Portfel Tożsamości Cyfrowej. Dzięki niemu, użytkownicy zyskają narzędzie, które umożliwia bezpieczne i łatwe zarządzanie swoją tożsamością cyfrową, a także umożliwia realizację szeregu procesów zarówno on-line, jak i on-site, które dotychczas były czasochłonne i obarczone ryzykiem błędów. Portfel zaoferuje szeroki wachlarz korzyści oraz realne możliwości zastosowania w praktyce biznesowej i administracyjnej na cyfrowym, zintegrowanym rynku UE. Jego efektywne funkcjonowanie objawi się w pełni jednak dopiero w kontekście całego ekosystemu, w którym będzie on funkcjonował razem ze źródłami atrybutów, siecią akceptacji portfela oraz transakcjami, które będzie umożliwiał.



Rys.4. Ekosystem Europejskich Ram Tożsamości Cyfrowej

Nowy ekosystem pozwoli na pojawienie się następujących korzyści i nowych wartości dla jego uczestników:

Powszechna, transgraniczna i bezpieczna identyfikacja osób i firm w środowisku online i offline

Portfele tożsamości cyfrowej będą zgodne z ustalonymi unijnymi standardami technicznymi i zapewnią takie samo doświadczenie użytkownika oraz zestaw funkcjonalności niezależnie od kraju wydania. Umożliwią one bezpieczne uwierzytelnianie i identyfikację w usługach publicznych i prywatnych — zarówno w kraju, jak i za granicą. Wprowadzenie rozwiązań takich jak automatyczne wypełnianie formularzy elektronicznych i zasada „once-only” (jednorazowego przekazywania danych) skróci czas obsługi i zmniejszy ryzyko błędów.

Portfel będzie mógł przechowywać i udostępniać atrybuty tożsamości, takie jak status zatrudnienia, miejsce zamieszkania, prawo do ulg, ważne bilety, informacje o płatnościach podatkowych czy potwierdzenia praw własności. W przyszłości możliwe będzie także bezpieczne przechowywanie dokumentów podróжных (np. paszportów, wiz), co ułatwi odprawy lotniskowe i meldunki w hotelach.

W odróżnieniu od obecnych systemów eID, użytkownik portfela będzie miał pełną kontrolę nad swoimi danymi — będzie wiedział, kto i w jakim celu otrzymał określone informacje, a także będzie mógł wycofać zgodę na ich dalsze udostępnianie.

Europejski Portfel Tożsamości Cyfrowej umożliwi identyfikację użytkownika wobec usługodawców prywatnych (np. banków), autoryzację płatności online oraz zdalne otwieranie kont bankowych bez konieczności wizyty w placówce. Dodatkowo użytkownik będzie mógł potwierdzić reprezentację podmiotu (np. firmy) w kontaktach biznesowych.

Portfel będzie również zawierać mechanizmy potwierdzania tożsamości drugiej strony oraz rejestrowania historii udostępnień danych. Wszystkie transakcje będą zgodne z rozporządzeniem eIDAS, co istotnie zwiększy bezpieczeństwo i zaufanie w środowisku cyfrowym.

Kwalifikowany podpis elektroniczny dla każdego

Każdy użytkownik portfela będzie miał dostęp do kwalifikowanego podpisu elektronicznego, umożliwiającego podpisywanie dokumentów — w tym umów o pracę — z pełną mocą prawną. Podpis ten będzie dostępny bez dodatkowych kosztów i zbędnych formalności administracyjnych.

Wzrost cyberbezpieczeństwa i spójność z polityką cyfrową UE

Rozporządzenie eIDAS jest częścią szerszej strategii UE „Droga ku cyfrowej dekadzie 2030”, zakładającej budowę bezpiecznego, zaufanego i zintegrowanego środowiska cyfrowego. Portfel będzie wspierać użytkowników w ochronie ich danych i tożsamości przed nadużyciami, zapewniając zgodność z RODO oraz innymi unijnymi regulacjami dotyczącymi cyberbezpieczeństwa.

Nowe możliwości dla użytkowników i biznesu

Dzięki Europejskim Ramom Cyfrowej Tożsamości, przedsiębiorstwa zyskują możliwość zgodnego z prawem świadczenia usług o wysokim poziomie zaufania na całym jednolitym rynku, przy minimalizacji kosztów związanych z krajowymi różnicami w identyfikacji elektronicznej. Przykładowe scenariusze wykorzystania portfela będą obejmować:

- silne uwierzytelnianie klienta (SCA) – portfel może pełnić rolę narzędzia umożliwiającego silne uwierzytelnienie zgodne z wymogami PSD2 oraz eIDAS, co będzie kluczowe przy autoryzacji płatności elektronicznych i logowaniu do usług bankowych,
- realizację funkcji KYC (Know Your Customer) przy procesach finansowych – onboardingu do usług finansowych (bankowych czy ubezpieczeniowych), czy weryfikacji klientów dokonujących wpłat gotówkowych do urządzeń samoobsługowych czy POS gdzie użytkownik będzie mógł potwierdzić swoją tożsamość cyfrowo, bez konieczności okazywania dokumentu fizycznego,
- realizacja płatności przy użyciu portfela z wykorzystaniem atrybutów takich jak wiek, prawo do wstępu (np. bilety komunikacyjne czy na wydarzenia sportowe, kulturalne),
- Weryfikacja danych odbiorcy przelewu – portfel będzie mógł pomóc w potwierdzeniu tożsamości oraz poprawności danych odbiorcy przy transakcjach finansowych, co ograniczy ryzyko błędów i oszustw,
- Przekazywanie danych do procesu kredytowego – dane niezbędne do oceny zdolności kredytowej (np. o zatrudnieniu, dochodach, zobowiązaniach) będą mogły być przekazywane za pośrednictwem portfela w sposób bezpieczny i potwierdzony,
- Portfel tożsamości dla firm – przedsiębiorstwa będą mogły korzystać z wersji portfela przeznaczonej dla podmiotów prawnych, co pozwoli np. pracownikom na potwierdzenie reprezentacji firmy w transakcjach handlowych lub administracyjnych.

EKSPERT RAPORTU

PIOTR STERCZAŁA

PARTNER, CZŁONEK ZARZĄDU, OBSERWATORIUM.BIZ

Wejście w życie Europejskich Ram Tożsamości Cyfrowej będzie radykalną zmianą nie tylko w zakresie identyfikacji elektronicznej, ale także innych procesów biznesowych i administracyjnych realizowanych online i offline. Nowe przepisy, a raczej ich implementacja, stosowanie w praktyce i budowanie w ich oparciu procesów to zupełnie nowy rozdział cyfryzacji Unii Europejskiej.

Na bazie rozporządzenie powstaną Europejskie Portfele Tożsamości Cyfrowej, które pozwolą na bezpieczną i wygodną identyfikację na terenie UE. Portfele stały się symbolem zmian wprowadzanych przez Europejskie Ramy Tożsamości Cyfrowej zamiast eIDAS 2.0 ponieważ mają dać powszechny dostęp do identyfikacji, podpisów kwalifikowanych i do posługiwania się atrybutami. I to właśnie one, w mojej opinii, będą prawdziwą rewolucją. Dzięki atrybutom dowolne osoby (docelowo także prawne) będą mogły w prosty, bezpieczny i w pełni kontrolowany sposób przekazywać niemal dowolne informacje o sobie innym podmiotom.

Możliwość digitalizacji niemal dowolnych informacji za pośrednictwem atrybutów będzie bodźcem do niespotykanego do tej pory rozwoju transakcyjności w skali lokalnej i europejskiej. Powstawać będą procesy, które do tej pory były niemal niemożliwe do scyfryzowania a te, które już istnieją staną się jeszcze wygodniejsze, efektywniejsze, ale przede wszystkim bezpieczniejsze.

Autorzy raportu:

Sławomir Hadryan,
Dominika Rzęsa,
Michał Tabor,
Piotr Sterczała,
Miłosz Brakoniecki,
Marcin Wolski.

Nota prawna

Informacje i opinie zawarte w raporcie zostały przygotowane na podstawie wiedzy pozyskanej z badań desk research oraz doświadczenia profesjonalnego autorów raportu. Autorzy nie biorą odpowiedzialności za decyzje podjęte na podstawie raportu „Europejskie Ramy Cyfrowej Tożsamości - czym są i jak zmieniają rynek cyfrowy?”.



DORADZAMY SZKOLIMY BADAMY

www.obserwatorium.biz

#podpis_elektroniczny

#uslugi_zaufania

#elektroniczna_identyfikacja

#ergonomia_uslug_cyfrowych

#transformacja_cyfrowa_biznesu_i_administracji



OBSERWATORIUM.BIZ