

Rozdział 1

Weryfikowalne poświadczenia EBSI

EBSI Explained – edycja pierwsza.

Rozdziały w tej edycji:

01. Wyjaśniamy weryfikowalne poświadczenia

02. Weryfikowalne poświadczenia w akcji

03. Metody zdecentralizowanych identyfikatorów (DID)

04. Tożsamość cyfrowa

05. Model zaufania wydawców

06. OpenID Connect dla weryfikowalnych poświadczeń

07. Portfele cyfrowe

Weryfikowalne Poświadczenia – spis treści

Czego dowiesz się w tym rozdziale:

1.1

Dlaczego poświadczenia weryfikowalne?

1.2

Czym są weryfikowalne poświadczenia?

1.3

Jak działają poświadczenia weryfikowalne?

01.

**Dlaczego poświadczenia
weryfikowalne?**

Weryfikacja dokumentów i informacji pozostaje trudna.

Dlatego musimy inwestować w technologie umożliwiające łatwą weryfikację dokumentów i danych.

110 miliardów

wypranych poprzez fałszerstwa brudnych pieniędzy. Twierdzi się, że w Unii Europejskiej pierze się 110 miliardów euro poprzez fałszowanie dokumentów.

17 milionów

przedmiotów (np. podróbek) zatrzymano w zeszłym roku na granicach UE o łącznej wartości 740 mln euro.

30 milionów

skradzionych lub zagubionych dokumentów –tyle osiągnął wskaźnik w Europie w 2015 r. (Interpol szacuje, że do 2020 r. liczba ta wzrosła do 89 mln).

20 %

etykiet żywności w UE może być fałszywych, czyli niezgodnych z wymaganiami UE.

? Fałszywe testy na COVID-19

W obliczu ograniczeń podróży przestępcy produkują i sprzedają fałszywe certyfikaty testów na COVID-19. Wiele takich przypadków zostało wykrytych przez Europol.

**Dokumenty są łatwe
do podrobienia i trudne
do zweryfikowania.**

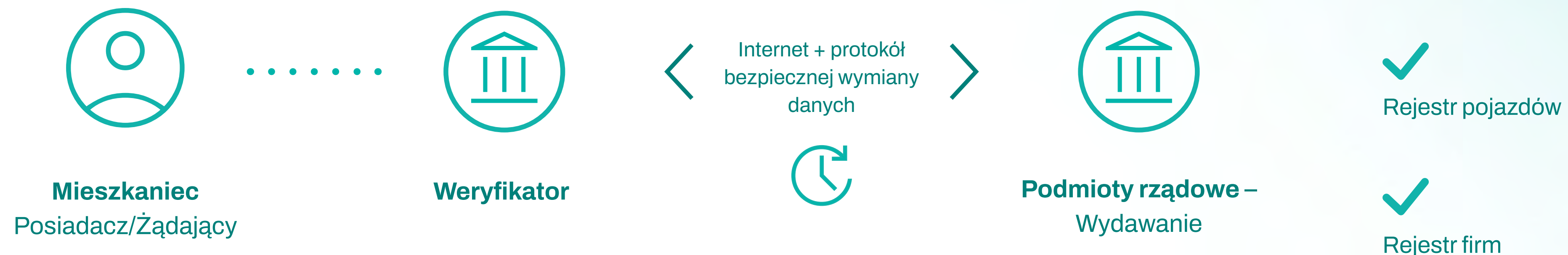
Wprowadzenie krajowych rejestrów
było dużym krokiem naprzód
w odróżnianiu informacji prawdziwych
od fałszywych.



Autentyczne źródła danych są obecnie cyfrowe i dostępne online.

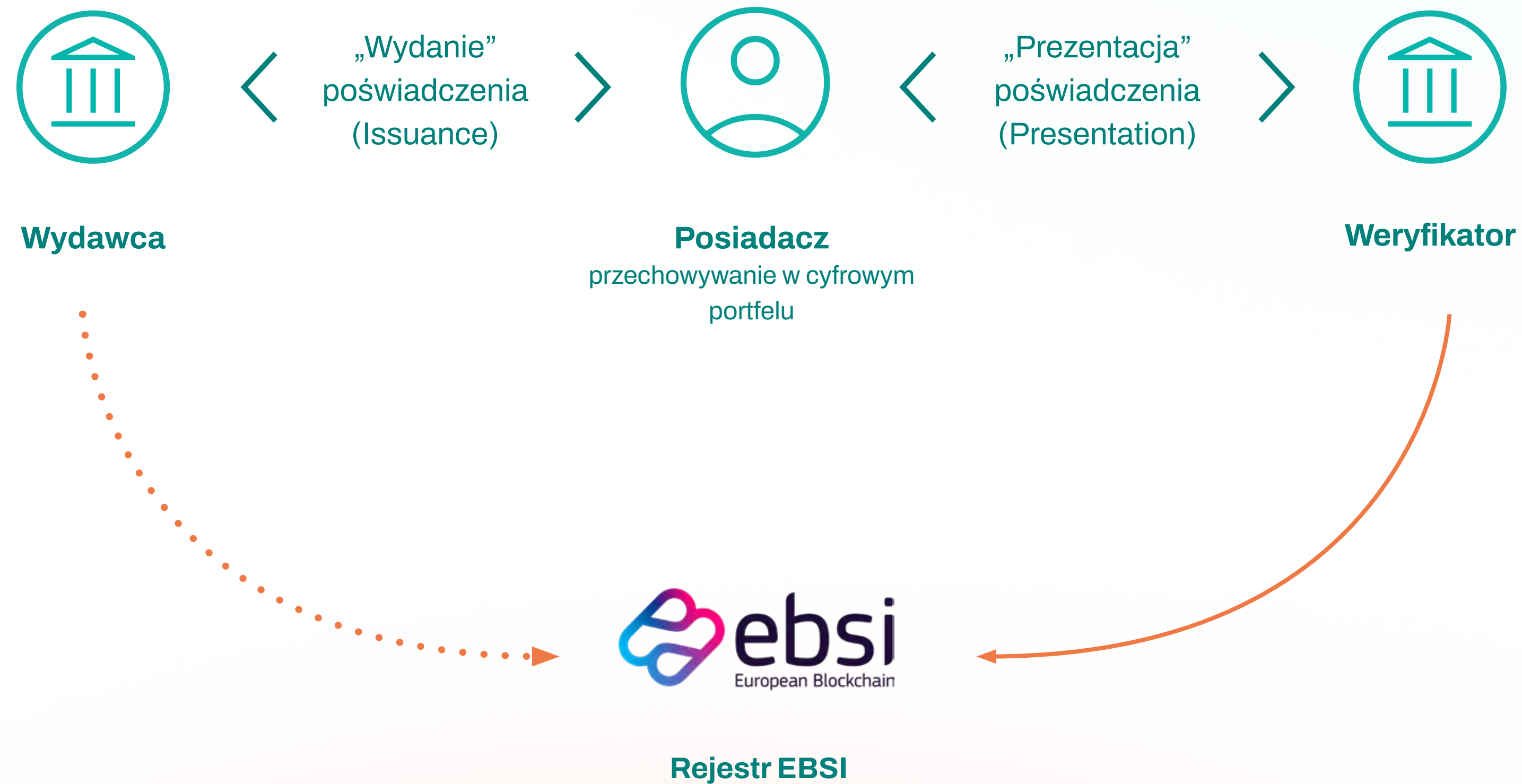
Jednak dostęp w czasie rzeczywistym często nie jest możliwy i odbywa się za pośrednictwem podmiotów trzecich.

Weryfikacja poprzez dostęp do autentycznych źródeł informacji jest często pośredniczona (tj. wykonywana przez jeden podmiot w imieniu innego).



Scenariusz bezpośredniej weryfikacji (suwerenny).

Nowy model wymiany informacji

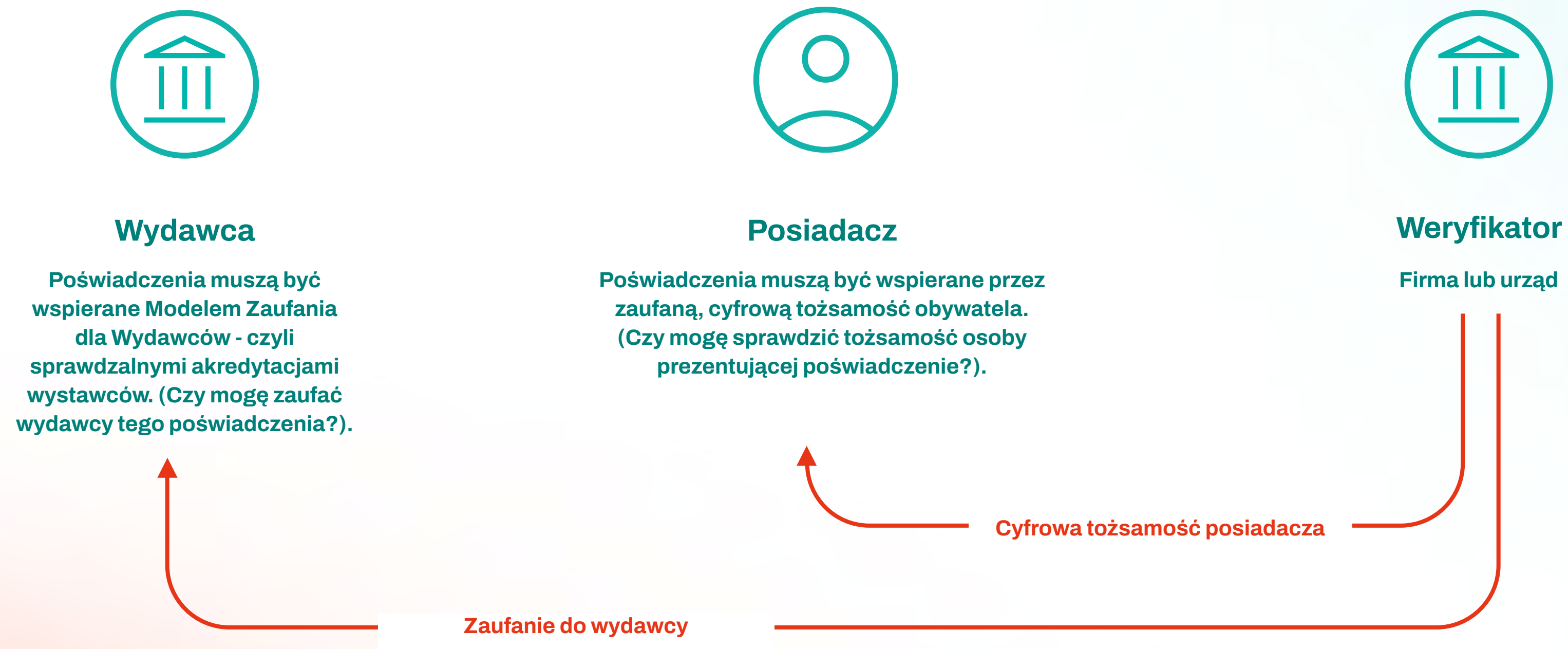


Wyzwania scenariusza bezpośredniej weryfikacji (samodzielności).

Technologia może pomóc

...

Celem jest znaczne ułatwienie weryfikacji informacji w relacjach mieszkaniec→firma (C2B) oraz mieszkaniec→urząd (C2G). Poświadczenia weryfikowalne są kluczowym, ale niewystarczającym elementem do osiągnięcia tego celu. Pozostają dwa inne wyzwania:

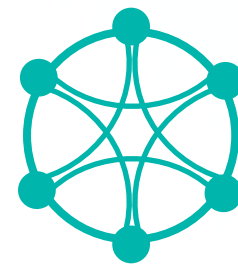


Trzy kluczowe komponenty nadchodzącej ewolucji Web3:



Poświadczenia weryfikowalne:

nowy sposób wyrażania informacji. Poświadczenia zawierają (poświadczenia zawierają metadane, twierdzenia i dowody/ podpisy).



Blockchain (rozproszony rejestr):

nowa zdecentralizowana infrastruktura.



Cyfrowy Portfel:

nowy sposób interakcji obywatela z systemem.

Dlaczego inwestować w te technologie?

Trudne do podrobienia, a łatwe do weryfikacji

Poświadczenia weryfikowalne stają się standardem de facto, ponieważ....

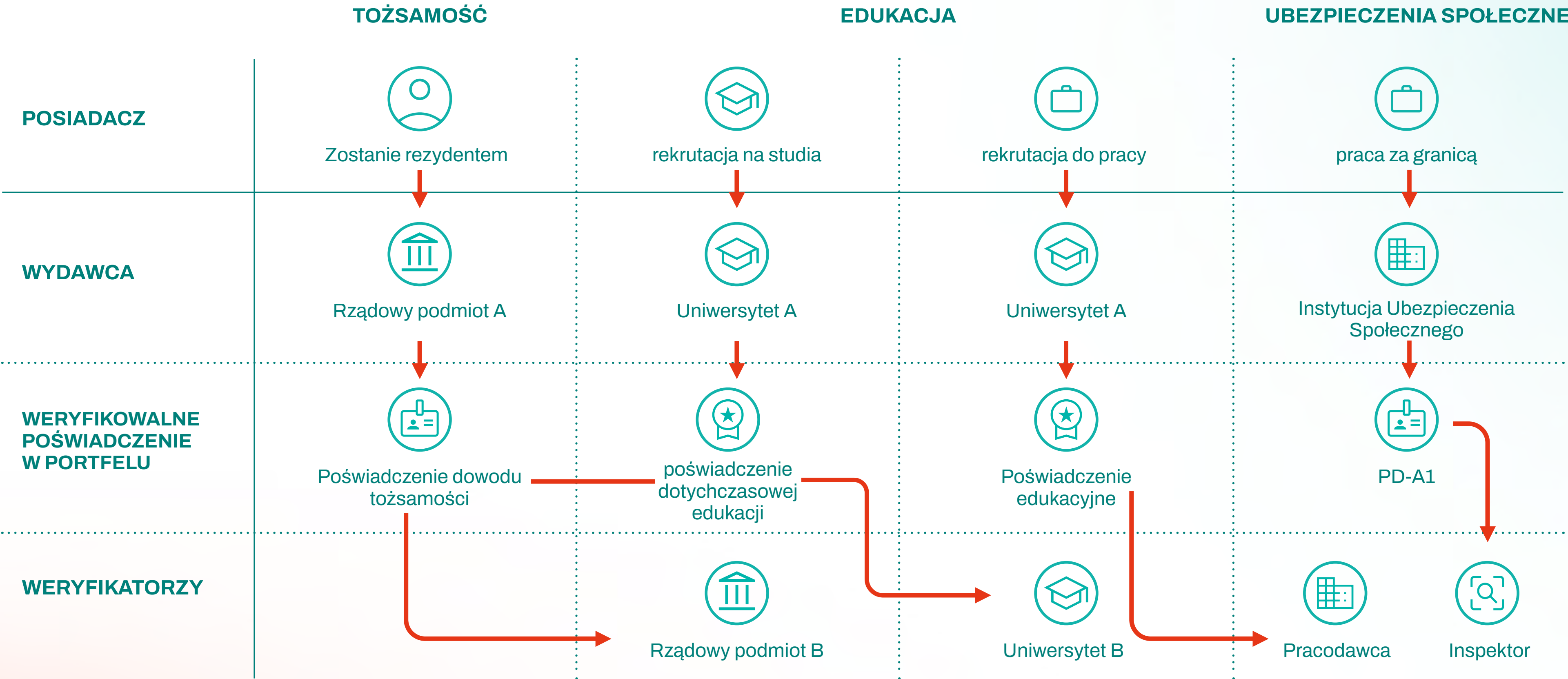
- Wysoka pewność, że posiadacz poświadczenia jest faktyczną osobą, której poświadczenie zostało wydane.
- Wysoka pewność, że wydawca poświadczenia jest zaufany (wraz z weryfikacją daty wystawienia, ważności itp.).
- Weryfikatorzy mają łatwy dostęp do informacji, a posiadacz zachowuje kontrolę nad swoimi danymi z możliwością ujawniania tylko wybranych fragmentów.



02.

**Czym są
poświadczenia weryfikowalne?**

Weryfikowalne poświadczenia mogą być użyte niemal we wszystkich scenariuszach działań obywateli.

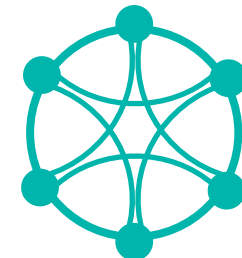


Trzy składniki zdecentralizowanej tożsamości:



Poświadczenia weryfikowalne:

nowy sposób wyrażania informacji.



Weryfikowalne rejestry danych:

nowa zdecentralizowana infrastruktura zapewniająca zaufanie.



Cyfrowy portfel:

nowy sposób interakcji obywatela z systemem.

TAO – zaufana organizacja akredytacyjna

Wdrożenie uczestników:

- Tworzenie portfeli oraz DIDów
- Rejestracja DIDów na EBSI
- Akredytacja Wydawców w rejestrze EBSI

Wydawca

Wydanie i przechowywanie poświadczeń:

- przygotowuje portfel i klucze,
- rejestruje DID w EBSI,
- uzyskuje akredytację (TAO);

Posiadacz

Prezentacja i weryfikacja:

- Żądanie Weryfikowalnej Prezentacji
- Udostępnienie Weryfikowalnej Prezentacji
- Weryfikacja Twierdzeń

Weryfikator

- przygotowuje i udostępnia weryfikowalną prezentację, poświadczenia,
- sprawdza otrzymaną prezentację

Podstawowy scenariusz udostępniania informacji:

Nowy scenariusz wymiany informacji C2B i C2G

Poświadczenia weryfikowalne umożliwiają wdrożenie nowego modelu wymiany informacji:



Całość oparta jest na cyfrowej tożsamości posiadacza i modelu zaufania wydawców (akredytacje).

Wsparcie EBSI:
Rejestr wydawców, klucze publiczne wydawców i lista unieważnień (CRL) tworzą infrastrukturę weryfikacji.

Poświadczenia weryfikowalne - wyzwania:

Nowy model wymiany informacji C2B i C2G.

...

Celem poświadczeń jest znaczne ułatwienie weryfikacji danych w tych scenariuszach.

Poświadczenia weryfikowalne są istotnym, ale niewystarczającym elementem.

Pozostają dwa wyzwania:



Czemu Weryfikowalne poświadczenia?

Prawie niemożliwe do podrobienia, a łatwe do weryfikacji

Weryfikowalne Poświadczenia stają się de facto standardem, ponieważ:

- Wysoki poziom pewności, że wydawca jest zaufany wraz z atrybutami czasu wydania, datą ważności itp.
- Wysoki poziom pewności, że posiadacz jest tym komu Weryfikowalne poświadczenie zostało wydane.
- Weryfikatorzy mają łatwy dostęp do informacji, a posiadacz wciąż posiada dane wraz z kontrolą nad nimi z możliwością udostępnienia jedynie części informacji.

03.

**Jak działają poświadczenia
weryfikowalne?**

Weryfikowalne poświadczenia - scenariusz:

Nowy, rozproszony model wymiany informacji.



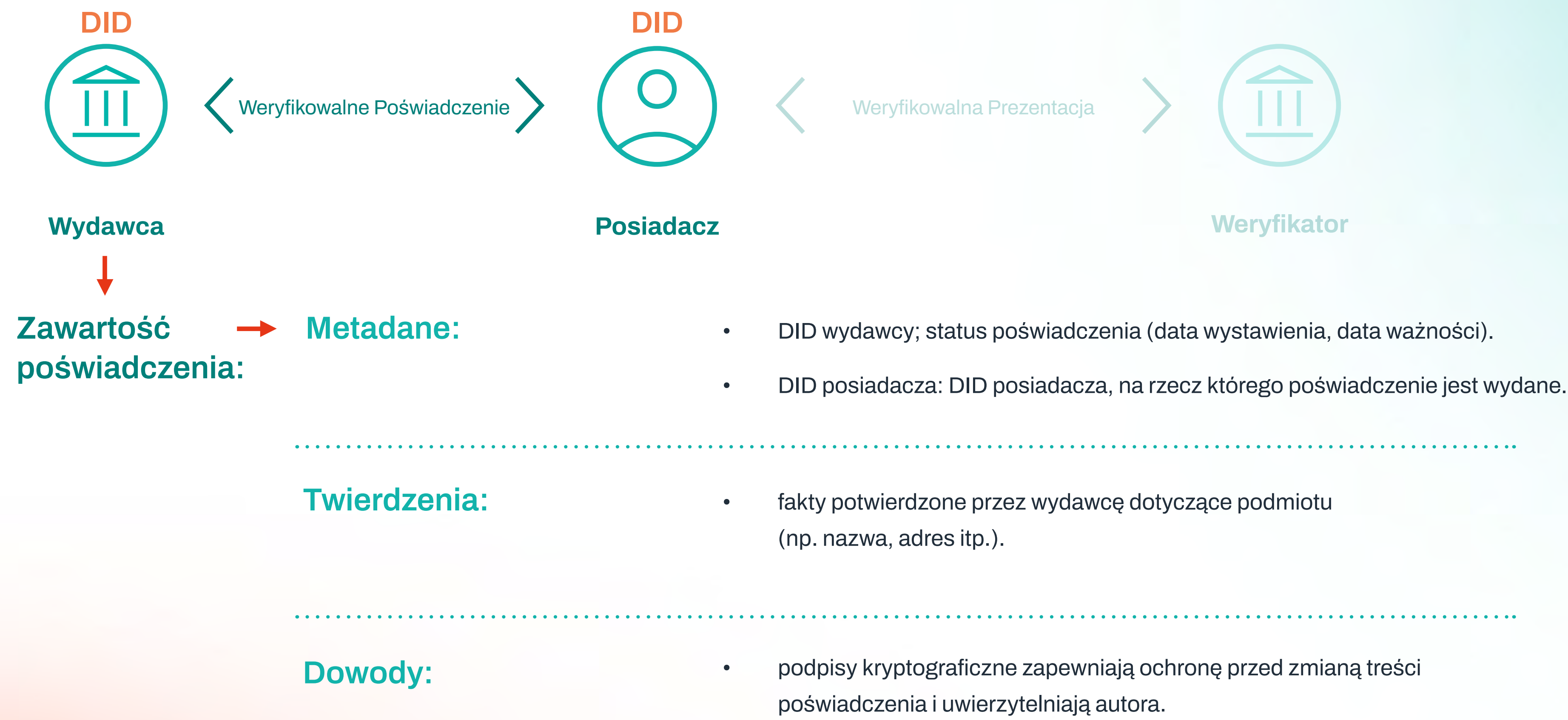
Jak to działa

Krok 0. Wystawcy zostają włączeni do systemu, portfele są skonfigurowane, a środowiska weryfikatorów utworzone.



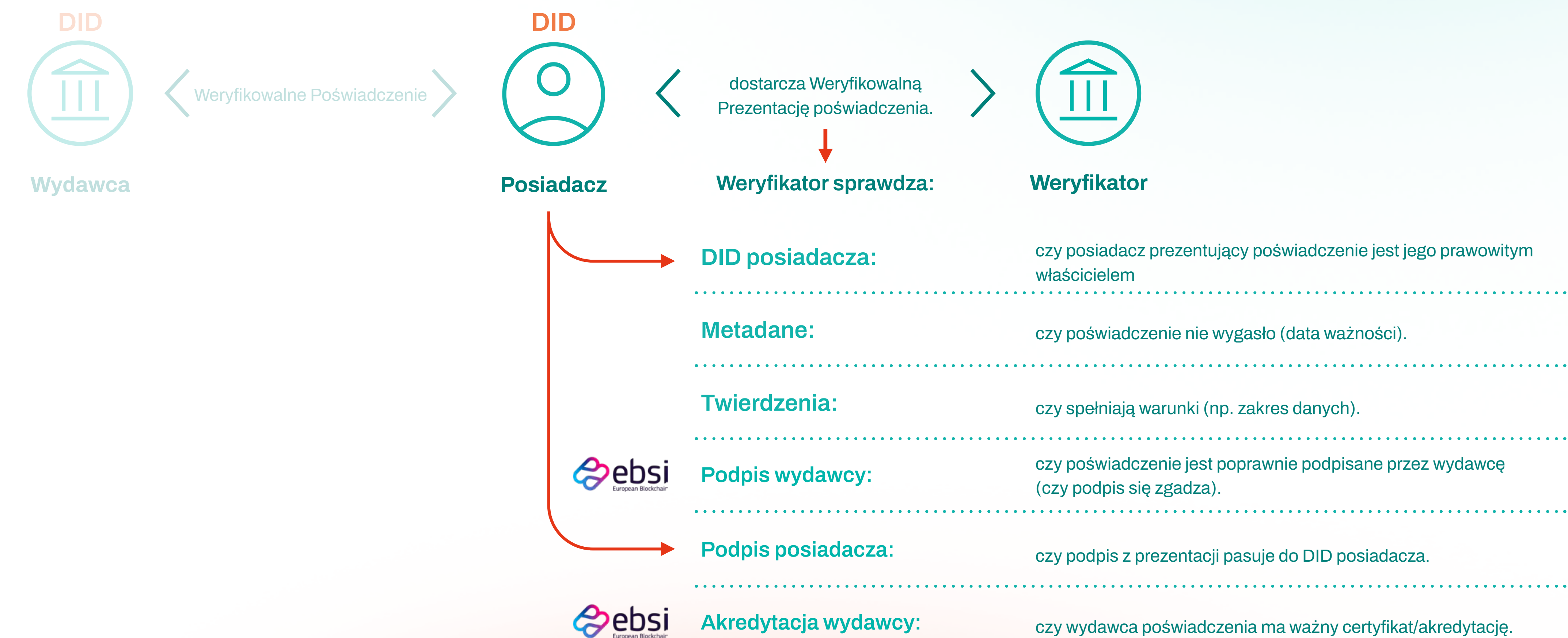
Jak to działa

Krok 1. Wydanie poświadczenia, które następnie przechowywane jest w portfelu zgodnym z EBSI



Jak to działa

Weryfikacja poświadczenia:



Standardy i rekomendacje

EBSI propaguje uznane w branży standardy



Standardy i rekomendacje W3C:

- Zdecentralizowane Identyfikatory v1
- Model Danych Poświadczeń Weryfikowalnych v1.1
- Wymiana Prezentacji v2



OpenID Connect:

- OpenID Connect SIOP v2
- OpenID Connect dla Prezentacji Weryfikowalnych
- OpenID Connect dla Wydawania Poświadczeń Weryfikowalnych



eIDAS:

- JAdES (JSON Advanced Electronic Signatures)
- Uwierzytelnianie i identyfikacja eID



Rodzina standardów JWT (RFC):

- IETF RFC 7515-7520

Modele zaufania wydawców

Skalowalność, elastyczność oraz interoperacyjność

Model scentralizowany:

Centralny urząd (np. „EU Gateway” – bramka UE)

zarządza certyfikatami wydawców.

W EU funkcjonuje też Lista zaufanych list eIDAS – spis dostawców kwalifikowanych certyfikatów, używany do weryfikacji wydawców.

Model federacyjny:

Sieć wspólnych reguł między wieloma organizacjami (każdy kraj/branża zarządza swoimi wydawcami)

Przykładem są krajowe listy eIDAS jako wspólne repozytorium informacji. elektronicznych dokumentów.



Możliwe jest łączenie modeli zaufania - np. rozproszony model EBSI może korzystać z certyfikatów X.509 w razie potrzeby.

Model rozproszony (EBSI):

W pełni zdecentralizowany, każdy wydawca publikuje akredytacje w blockchainie EBSI (DID).

EBSI wykorzystuje blockchain oraz standard zdecentralizowanego identyfikatora W3C, aby stworzyć w pełni rozproszony model zaufania gdzie każdy sektor lub państwo członkowskie określa i zarządza akredytacjami wydawców do wydawania poświadczeń.

Ważne! Kombinacja wielu modeli zaufania jest możliwa

Czy możemy porównać modele zaufania wydawców?

	Zcentralizowany model zaufania	Federacyjny model zaufania	Rozproszony model zaufania
Koncepcja:	Centralny organ (np. Komisja) zarządza scentralizowaną usługą odpowiedzialną za zarządzanie i dystrybucję certyfikatów wystawców dokumentów elektronicznych.	Rozporządzenie eIDAS wprowadziło paneuropejską listę wszystkich dostawców certyfikatów kwalifikowanych. Lista ta może być wykorzystana do weryfikacji informacji o wystawcach dokumentów elektronicznych.	Wykorzystanie technologii blockchain oraz standardu DID (Decentralized Identifiers, W3C) do stworzenia w pełni rozproszonego modelu zaufania, w którym każdy sektor lub państwo członkowskie/region definiuje i zarządza własnymi wystawcami dokumentów elektronicznych, bez potrzeby istnienia centralnego organu.
Przykład:	EU Gateway	Zaufane listy eIDAS	EBSI
Technologia:	Certyfikaty X.509	Certyfikaty X.509	Dokumenty DID / weryfikowalne akredytacje (możliwość połączenia z certyfikatami X.509)
Zarządzanie:	Model hierarchiczny, mało elastyczny, wymagający wielu ról: Urząd Certyfikacji (CA), Urząd Rejestracji (RA), Urząd Walidacji (VA) i Urząd Dystrybucji (DA).	Model ten to federacja scentralizowanych modeli zaufania spełniających wspólne wymagania. Podstawy pozostają podobne, jednak podejście oferuje większą skalowalność i interoperacyjność.	Model umożliwia decentralizację i większą elastyczność. Wymagane są tylko dwie role: Zaufana Organizacja Akredytacyjna (TAO) oraz Zaufany Wystawca (TI).
Zalety:	Kontrola usługi: Dostarczanie usługi skoncentrowane wokół podmiotu centralnego, co pozwala na znacznie szybsze wdrożenie niż w innych modelach.	Interoperacyjność: Lista zaufanych list eIDAS zapewnia solidny fundament umożliwiający bezpieczny dostęp do wszystkich zaufanych list UE, wspierając interoperacyjność transgraniczną.	Elastyczność: Rotacja kluczy pozwala wystawcom minimalizować liczbę unieważnionych weryfikowalnych poświadczeń w przypadku odwołania kluczy podpisujących wystawcy. Możliwość połączenia z klasycznym systemem X.509/PKI. Może również wspierać zarówno scentralizowane, jak i federowane modele zaufania.

Weryfikacja cyfrowej tożsamości posiadacza

Istnieją trzy podejścia:



Podejście scentralizowane:

krajowe środki e-ID (np. krajowy dowód elektroniczny)

federacyjny model:

sieć powiązanych systemów e-ID (np. węzły eIDAS do wzajemnego uwierzytelniania).

Rozproszony model zaufania:

np. Europejska suwerenna tożsamość ESSIF (oparta na blockchain i wspólnych standardach).

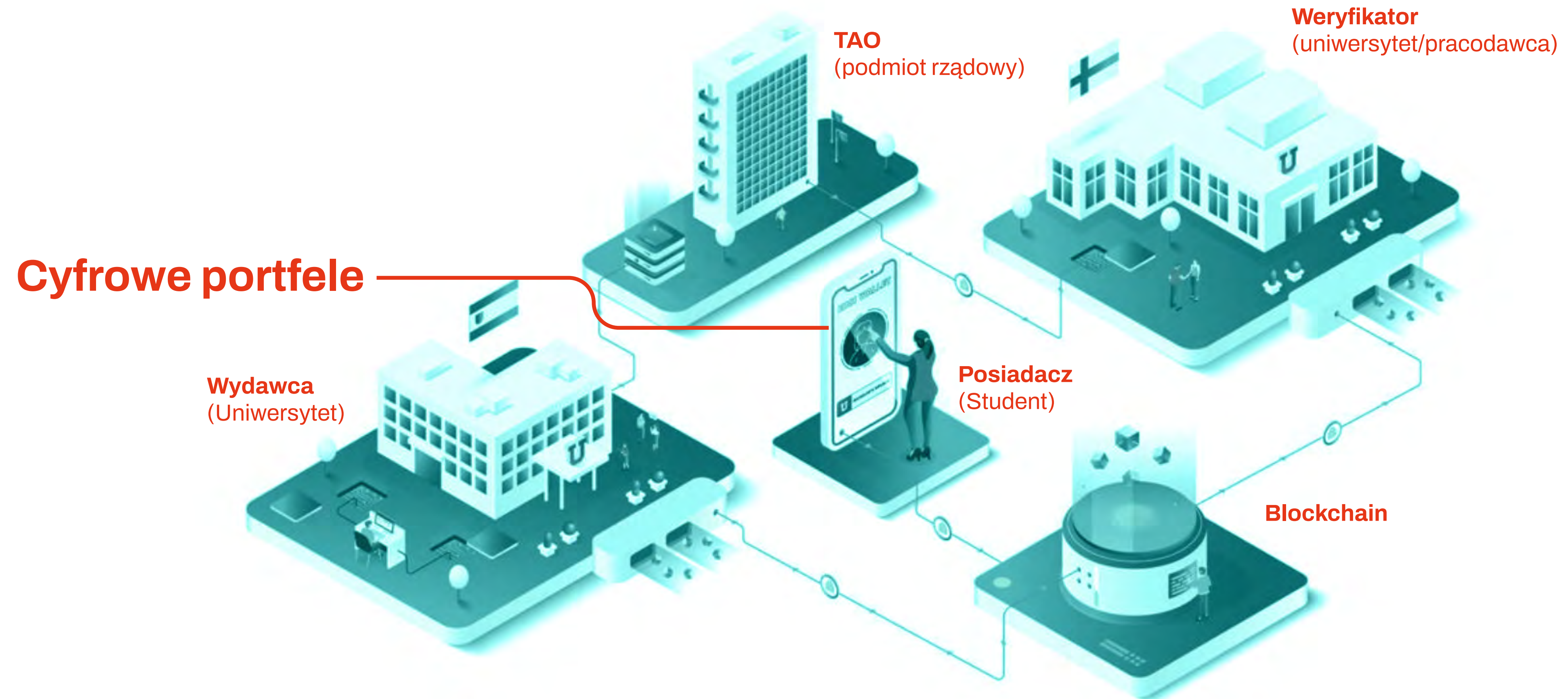
Weryfikowalna tożsamość: np. użycie Weryfikowalnych poświadczeń z danymi eIDAS (wspólny model eIDAS).

Ważne!

Jest zalecane, aby portfele zgodne z EBSI oraz aplikacje dla weryfikatorów wspierały kilka podejść do weryfikacji tożsamości cyfrowej.

Portfele pośredniczą w niemal wszystkich interakcjach użytkowników.

Zdecydowana większość interakcji związanych z wymianą poświadczeń (VC) zależy od portfela.



Chcesz wiedzieć więcej?

Kluczowe zasoby

Odkryj EBSI

Sprawdź stronę EBSI

<https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>

Odkryj technikalia

Sprawdź {playbook} EBSI

<https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Playbook>

Obejrzyj filmiki demonstracyjne

Zobacz EBSI Demo Day

<https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Demo+Day>

