Rozdział 6

OpenID dla poświadczeń weryfikowalnych

Rozdziały pierwszego wydania

OpenID dla poświadczeń weryfikowalnych – spis treści

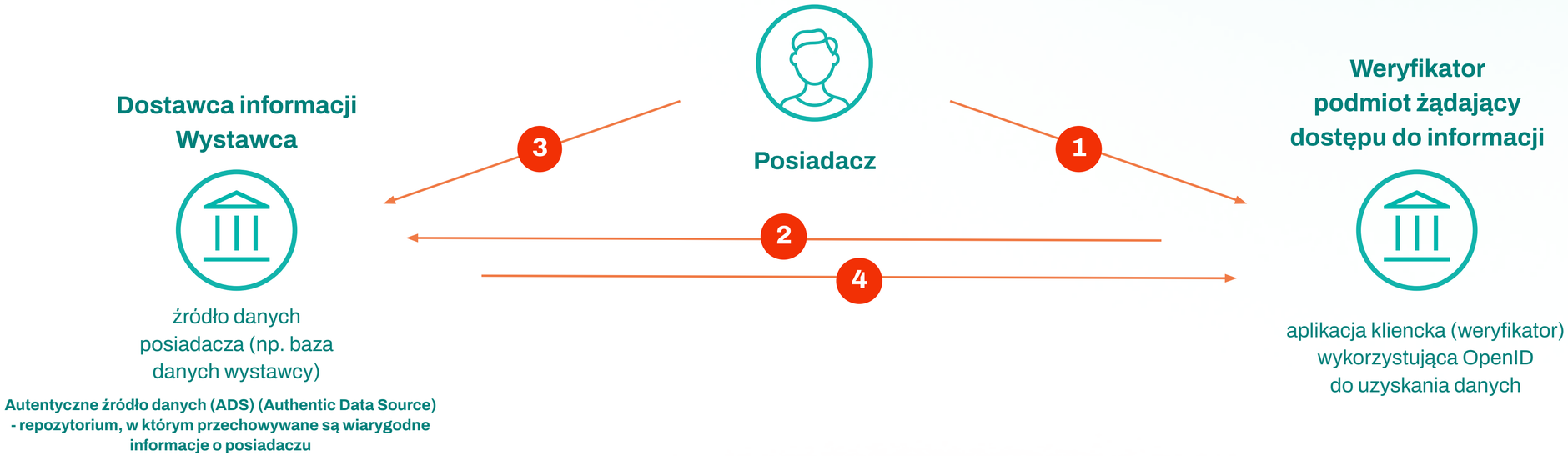
Czego dowiesz się w tym rozdziale?

6.1

Czym jest OpenID dla poświadczeń weryfikowalnych i dlaczego jest to ważne?

Wyzwanie związane z udostępnianiem informacji w oparciu o autoryzację

Większość protokołów umożliwia posiadaczom jedynie autoryzowanie weryfikatorów, którzy mają relację z wystawcą, aby ci mogli uzyskać nasze dane. W rezultacie posiadacz nie może udostępnić informacji dowolnie wybranemu przez siebie weryfikatorowi.



1. Żądanie dostępu - Weryfikator wysyła żądanie dostępu.
2. Żądanie informacji o posiadaczu - Usługa wystawcy żąda danych posiadacza.
3. Uwierzytelnienie posiadacza i autoryzacja weryfikatora - Posiadacz uwierzytelnia się i autoryzuje weryfikatora do pobrania swoich informacji z ADS (autentycznego źródła danych).
4. Udostępnienie informacji posiadacza - Następuje przekazanie danych posiadacza weryfikatorowi.

Nowy model suwerennej wymiany informacji

Trójstopniowa, samorządna wymiana informacji umożliwia posiadaczom dzielenie się swoimi informacjami z dowolnie wybranym podmiotem. W tym modelu posiadacz kontroluje, komu ujawnia swoje dane, bez konieczności istnienia wcześniejszej relacji między wystawcą a weryfikatorem.

1. Żądanie poświadczeń - Posiadacz inicjuje żądanie uzyskania poświadczeń od wystawcy.
2. Prezentacja poświadczeń - Posiadacz przekazuje otrzymane poświadczenia weryfikowalne wybranemu weryfikatorowi.
3. Weryfikacja poświadczeń - Weryfikator sprawdza otrzymane poświadczenia (np. porównując je z danymi w autentycznym źródle danych).

Cztery standardy umożliwiające nową wymianę informacji

Nie istnieje jeden uniwersalny protokół wymiany poświadczeń weryfikowalnych – dostępnych jest kilka alternatyw:

OpenID for Verifiable Credentials (OID4VC)	ISO 18013-5 (mobilne prawo jazdy, mDL)	Credential Issuance and Present Proof	DIF Wallet and Credential Interaction (WACI)
Fundacja OpenID standaryzuje rodzinę otwartych specyfikacji OID4VC dla samorządnego wydawania i prezentowania poświadczeń weryfikowalnych. Uwaga: OpenID for VCs jest częścią standardów OpenID Connect.	ISO standaryzuje normę 18013-5 dla bezprzewodowej (offline) wymiany mobilnych dokumentów tożsamości (np. prawa jazdy) oraz normę 23220 dla wymiany poświadczeń online.	Hyperledger standaryzuje protokoły Credential Issuance (wydawania poświadczeń) oraz Present Proof (prezentowania dowodów) w ramach ekosystemu self-sovereign identity.	Decentralized Identity Foundation (DIF) standaryzuje protokół WACI do wydawania i prezentowania poświadczeń weryfikowalnych. Uwaga: Protokół WACI jest zbudowany na bazie protokołu komunikacyjnego DIDComm.

EBSI wybrało protokoły OpenID dla poświadczeń weryfikowalnych

W przypadkach użycia realizowanych w EBSI wybrano protokoły OpenID for Verifiable Credentials do obsługi wydawania i prezentacji poświadczeń weryfikowalnych w środowisku online.

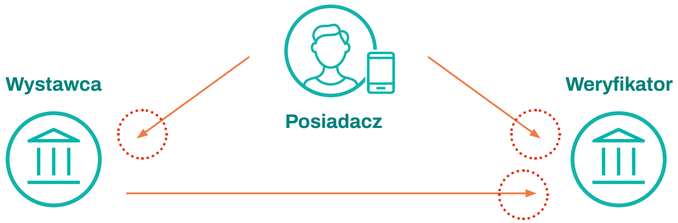
W przypadkach użycia realizowanych w EBSI wybrano protokoły OpenID for Verifiable Credentials do obsługi wydawania i prezentacji poświadczeń weryfikowalnych w środowisku online.

Fundacja OpenID standaryzuje rodzinę otwartych specyfikacji OpenID for Verifiable Credentials dla samorządnego wydawania i prezentowania poświadczeń weryfikowalnych.

Są to otwarte standardy, cechujące się wysoką dojrzałością, aktywną i szeroką społecznością, a także protokołami zbudowanymi na sprawdzonych standardach OpenID i OAuth.

Porównanie popularnego OIDC z OID4VC?

Wymiana oparta na autoryzacji kontra samorządna wymiana informacji – obie specyfikacje są komplementarne, ponieważ rozwiązują różne problemy.



OAuth i OpenID Connect (OIDC)

Protokół obsługuje wymianę poświadczeń opartą na autoryzacji, w której posiadacz upoważnia weryfikatora (klienta) do dostępu do swoich informacji w jego imieniu (weryfikator uzyskuje dane z bazy wystawcy za zgodą posiadacza).

OAuth i OpenID Connect (OIDC)

Protokół obsługuje wymianę poświadczeń opartą na autoryzacji, w której posiadacz upoważnia weryfikatora (klienta) do dostępu do swoich informacji w jego imieniu (weryfikator uzyskuje dane z bazy wystawcy za zgodą posiadacza).

OID4VC składa się z trzech standardów. Dwa z nich są używane przez EBSI

OpenID for Verifiable Credentials (OID4VCs) to zbiór trzech powiązanych standardów, które umożliwiają samorządne uwierzytelnianie użytkownika oraz wydawanie i prezentowanie poświadczeń weryfikowalnych. EBSI wykorzystuje te standardy, które dotyczą wydawania i prezentowania poświadczeń.

1

Uwierzytelnianie

SIOPv2 (Self-Issued OpenID Provider v2)

Definiuje sposób, w jaki posiadacze mogą uwierzytelniać się w samorządny sposób wobec dowolnego podmiotu. (Standard uwierzytelniania użytkownika.)

EBSI w kwestii uwierzytelniania posiadacza nie ogranicza się wyłącznie do SIOPv2 – wspiera również inne metody uwierzytelniania.

2

Wydawanie

OpenID for Verifiable Credential Issuance (OID4VCI)

Definiuje interfejsy API oraz mechanizmy autoryzacji oparte na OAuth2 dla procesu wydawania poświadczeń weryfikowalnych.

3

Prezentowanie

OpenID for Verifiable Presentations (OID4VP)

Definiuje mechanizmy (rozszerzenia OAuth2) umożliwiające prezentowanie danych w formie poświadczeń weryfikowalnych.

EBSI korzysta z OID4VCI i OID4VP do wydawania i prezentacji poświadczeń.

OID4VCI odpowiada za wydawanie, OID4VP za prezentację, a SIOPv2 za uwierzytelnianie.

Uproszczony obraz zakresu każdego standardu

Jak wygląda scenariusz samorządnej wymiany informacji w ujęciu uproszczonym?

Standard SIOPv2 dotyczy uwierzytelniania posiadacza i może być wykorzystywany opcjonalnie przez portfel (nie jest wymagany przez EBSI, które dopuszcza inne sposoby uwierzytelniania).

A Standard OID4VP obejmuje interakcje pomiędzy wystawcą (OP) a posiadaczem (portfelem) związane z wydawaniem poświadczeń (część A na schemacie).

B Standard OID4VCI obejmuje interakcje pomiędzy posiadaczem (portfelem) a weryfikatorem (RP) związane z prezentacją poświadczeń (część B na schemacie).

6.2.

Jak działa OpenID dla wydawania poświadczeń weryfikowalnych?

Wydawanie poświadczenia weryfikowalnego składa się z czterech kluczowych etapów:

1. Żądanie poświadczenia (Request VC):

1.1 Posiadacz rozpoczyna proces wydania na stronie internetowej wystawcy, a portfel otrzymuje informacje o typie poświadczenia, o które wnioskuje posiadacz, poprzez skanowanie kodu QR lub przekierowanie do aplikacji portfela. (Ten krok jest pomijany, jeśli użytkownik zażądał poświadczenia bezpośrednio z poziomu portfela.)

1.2 Portfel pobiera metadane wystawcy (rozszerzone w ramach OID4VCI) w celu sprawdzenia obsługiwanych metod przepływu, formatów poświadczeń, rodzajów podpisów oraz dostępnych endpointów API.

1.3 Portfel inicjuje żądanie wydania poświadczenia weryfikowalnego. Żądanie autoryzacji jest rozszerzeniem standardowego OAuth2 - portfel może w nim określić typ i format żądanego poświadczenia oraz typ i format podpisu.

2. Uwierzytelnienie (Authentication):

2.1 Posiadacz uwierzytelnia się u wystawcy za pomocą metody uwierzytelniania wspieranej przez wystawcę (np. loguje się lub używa eID).

3. Wydanie poświadczenia (Issue VC):

3.1 Po pomyślnej autoryzacji, portfel otrzymuje kod autoryzacyjny OAuth2, który następnie wysyła do endpointu token (OAuth2 token endpoint) wystawcy, aby uzyskać token dostępu oraz wyzwanie kryptograficzne (challenge). Wyzwanie służy do potwierdzenia kontroli posiadacza nad kluczami powiązanymi z jego DID.

3.2 Posiadacz podpisuje otrzymane wyzwanie przy użyciu swojego klucza (kluczy) DID, udowadniając w ten sposób, że faktycznie kontroluje dany DID (jest właścicielem odpowiadających mu kluczy prywatnych).

3.3 Portfel wysyła do wystawcy podpisane wyzwanie jako dowód kontroli nad DID (Proof of DID ownership).

4. Odebranie poświadczenia (Collect VC):

4.1 Wystawca wystawia pożądane poświadczenie weryfikowalne* i powiadamia portfel (np. zwracając specjalny identyfikator lub URL), że może ono zostać odebrane. Portfel następnie łączy się z odpowiednim endpointem credential wystawcy i pobiera wystawione poświadczenie weryfikowalne.

(*) (Wystawca może opatrzyć poświadczenie podpisem elektronicznym lub pieczęcią elektroniczną zgodnie z eIDAS. Sam proces wydania może odbyć się od razu (just-in-time) lub zostać odroczony. W przypadku wydania odroczonego wystawca zwraca portfelowi token odbioru (tzw. acceptance token), który portfel może użyć później do pobrania gotowego poświadczenia.)

Co standaryzuje OpenID4VCI?

Standard OID4VCI definiuje następujące elementy procesu wydawania poświadczeń weryfikowalnych:

1. Żądanie poświadczenia (Request VC):

- Mechanizm pozwalający wystawcy publikować metadane dotyczące obsługiwanych typów poświadczeń, formatów i rodzajów podpisów.
- Dwa sposoby inicjowania procesu wydania poświadczenia: poprzez stronę internetową wystawcy oraz bezpośrednio z poziomu portfela.
- Dwa tryby przepływu procesu wydania poświadczeń: tryb pre-autoryzowany (pre-authorised flow) oraz tryb z autoryzacją użytkownika (authorisation flow).
- Rozszerzone żądanie autoryzacji, które umożliwia portfelowi uzyskanie zgody (autoryzacji) na wydanie poświadczenia weryfikowalnego.

2. Uwierzytelnienie (Authentication):

3. Wydanie poświadczenia (Issue VC):

- Nowy endpoint chroniony protokołem OAuth2 (tzw. credential endpoint), pod którymi wystawca udostępnia portfelowi wydane poświadczenia do odbioru.
- Mechanizm powiązania kryptograficznego wydanego poświadczenia z kluczem lub certyfikatem posiadacza (tzw. holder binding - dzięki temu poświadczenie jest przypisane do tożsamości posiadacza).

4. Odebranie poświadczenia (Collect VC):

- Mechanizm umożliwiający natychmiastowe lub odroczone wydanie poświadczenia (just-in-time vs deferred issuance).

A. Kryptograficzne powiązanie posiadacza

Cel: zapewnić, że wydawane poświadczenie zostanie przypisane do posiadacza kontrolującego określony identyfikator (DID) i klucze.

1

Kim jest posiadacz wnioskujący o poświadczenie?

to ustala się poprzez uwierzytelnienie posiadacza

2

Czy posiadacz kontroluje podany DID?

(to ustalane jest poprzez wyzwanie i podpis posiadacza

3

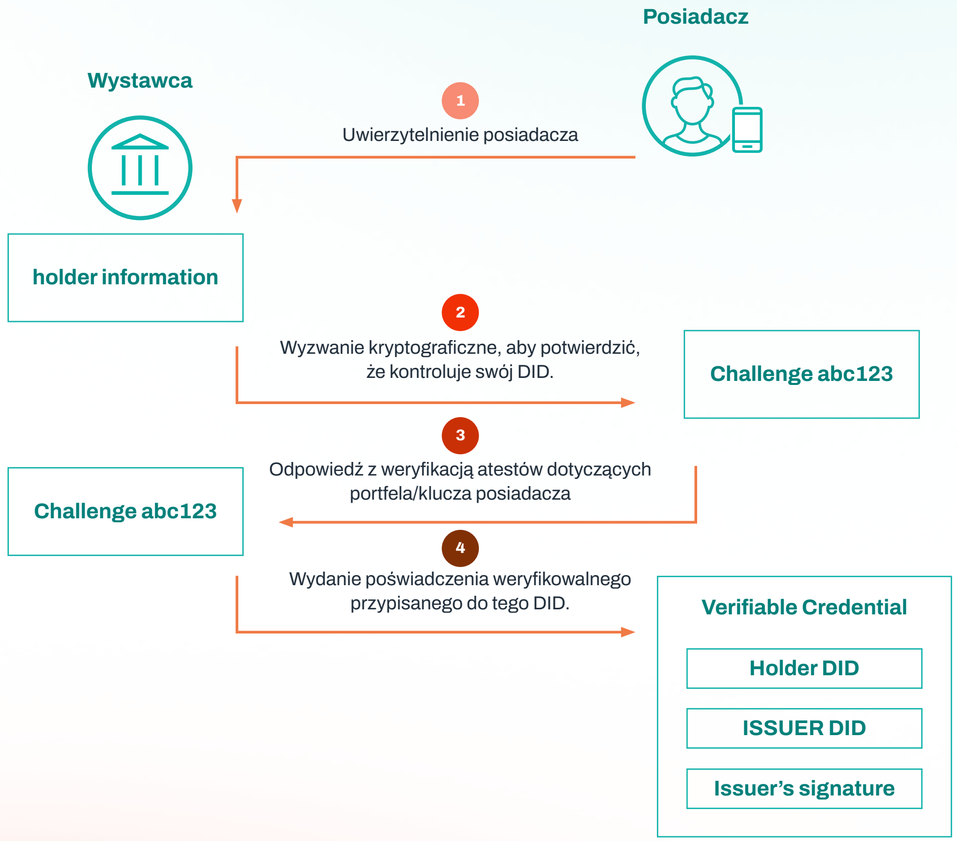
Czy portfel i klucze posiadacza są bezpieczne?

to weryfikują atesty portfela/kluczy dostarczone wystawcy

4

Czy mogę teraz wydać poświadczenie na ten DID?

jeśli odpowiedzi na powyższe są pozytywne - tak

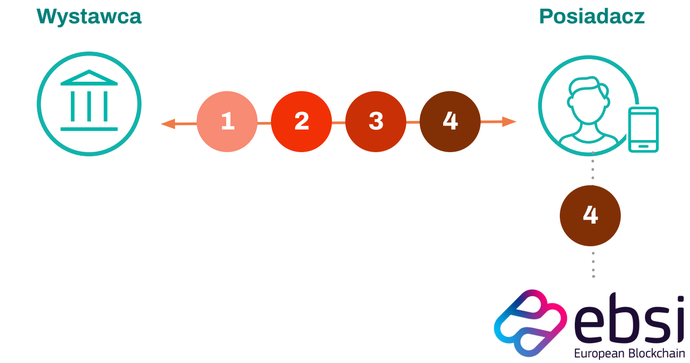


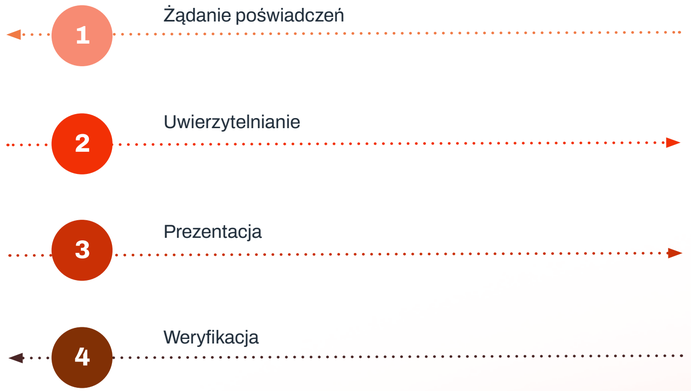
6.3.

Jak działa OpenID dla prezentacji poświadczeń weryfikowalnych?

B. Jak działa prezentacja poświadczeń weryfikowalnych?

Prezentowanie poświadczeń weryfikowalnych składa się z czterech głównych kroków:





1 Żądanie poświadczeń

Weryfikator inicjuje prośbę o jedno lub więcej poświadczeń weryfikowalnych od posiadacza. Odbywa się to poprzez zeskanowanie przez posiadacza kodu QR za pomocą aplikacji portfela (gdy posiadacz korzysta z innego urządzenia niż weryfikator) lub poprzez przekierowanie w przeglądarce (gdy oba podmioty są na tym samym urządzeniu) do aplikacji portfela posiadacza.

2 Uwierzytelnienie posiadacza

Posiadacz uwierzytelnia się u weryfikatora za pomocą metody uwierzytelniania udostępnionej przez weryfikatora. (Weryfikator może również zażądać poświadczeń po uwierzytelnieniu posiadacza, w ramach już nawiązanej sesji.)

3 Prezentacja poświadczeń

Portfel posiadacza przetwarza otrzymane żądanie, wybiera odpowiednie poświadczenia spełniające wymagania weryfikatora i przygotowuje weryfikowalną prezentację. Następnie portfel przekazuje tę prezentację (zawierającą wymagane poświadczenia) do weryfikatora.

4 Weryfikacja poświadczeń

Weryfikator sprawdza otrzymaną weryfikowalną prezentację oraz zawarte w niej poświadczenia weryfikowalne (np. przy pomocy usług EBSI, które potwierdzają ważność podpisów, status poświadczeń itp.).

B. Co standaryzuje OpenID4VP?

Standard OID4VP definiuje następujące elementy procesu prezentacji poświadczeń:

1 **Żądanie poświadczeń**

Mechanizm umożliwiający weryfikatorom publikowanie metadanych dotyczących obsługiwanych typów poświadczeń, formatów i rodzajów podpisów.

Mechanizm inicjowania wymiany weryfikowalnej prezentacji (rozpoczęcie procesu przekazania poświadczeń od posiadacza do weryfikatora).

2 **Uwierzytelnienie posiadacza**

Posiadacz uwierzytelnia się u weryfikatora za pomocą metody uwierzytelniania udostępnionej przez weryfikatora

3 **Prezentacja poświadczeń**

Przebieg prezentacji poświadczeń - zdefiniowanie kroków i protokołu wymiany weryfikowalnej prezentacji między portfelem a weryfikatorem.

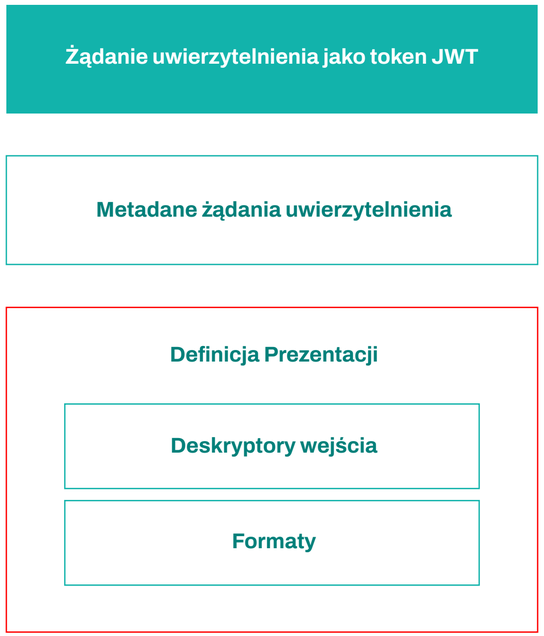
Endpointy API do przekazywania poświadczeń weryfikowalnych - określenie, w jaki sposób portfel udostępnia weryfikatorowi weryfikowalne prezentacje (np. przez odpowiedź na żądanie na określony adres URL).

4 **Weryfikacja poświadczeń**

Weryfikator sprawdza otrzymaną weryfikowalną prezentację oraz zawarte w niej poświadczenia weryfikowalne

B. Jak portfel wie, które poświadczenia udostępnić?

Aby określić, które poświadczenia weryfikowalne powinny zostać przedstawione w odpowiedzi na żądanie weryfikatora, wykorzystywane są dwa kluczowe elementy:



Żądanie poświadczeń

Metadane żądania uwierzytelnienia - żądanie przedstawienia poświadczeń jest przekazywane w formie rozszerzonego żądania uwierzytelnienia OAuth2 (tokenu JWT). Metadane tego żądania zawierają standardowe parametry (claims) OAuth2 opisujące weryfikatora i jego wymagania - dzięki temu portfel posiadacza poznaje wszystkie potrzebne informacje o weryfikatorze (adresy endpointów, obsługiwane formaty i rodzaje podpisów, itp.) oraz zapewniona jest ochrona całego procesu prezentacji (np. przed manipulacją).

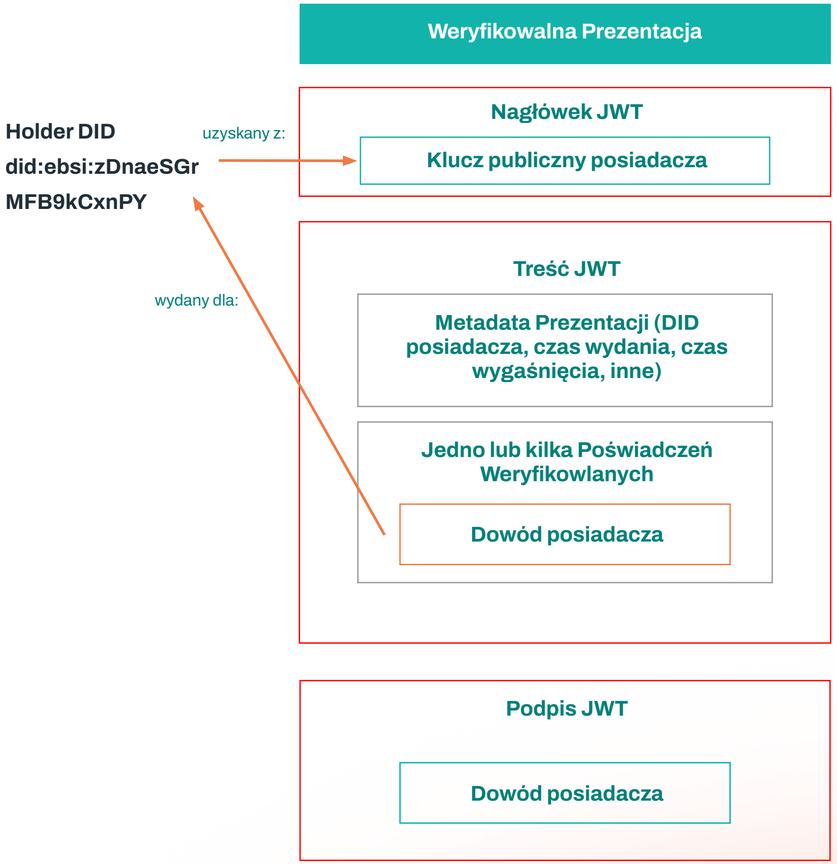
Definicja Prezentacji

Definicja Prezentacji (Presentation Definition) - jest to część specyfikacji Presentation Exchange, pozwalająca zadać warunki dotyczące wymaganych poświadczeń. Weryfikator może zażądać poświadczeń określonego typu (np. odwołując się do schematu JSON z zaufanego rejestru schematów EBSI) lub poświadczeń spełniających pewne kryteria (np. zawierających pola: imię, nazwisko, adres). Definicja prezentacji opisuje jedno lub więcej wymaganych poświadczeń na podstawie typu lub zawartości. Składa się ona m.in. z:

- Deskryptorów wejściowych (input descriptors) - definiują, jakich informacji żąda weryfikator. Każdy deskryptor może odnosić się do konkretnego schematu poświadczenia lub do zbioru wymagań co do zawartości poświadczenia (np. że poświadczenie musi zawierać pola takie jak nazwisko i adres).
- Formatów - określają wymagany format poświadczeń weryfikowalnych i prezentacji (np. JWT, JSON-LD itp.), jakie weryfikator akceptuje.

B. Jak weryfikatorzy weryfikują weryfikowalne prezentacje?

Weryfikowalna Prezentacja (VP) jest tworzona i podpisywana przez posiadacza (self-issued) i zawiera wszelkie niezbędne informacje do weryfikacji. Struktura weryfikowalnej prezentacji obejmuje:



Nagłówek

Klucz publiczny posiadacza - umieszczony w nagłówku prezentacji, jest to klucz publiczny powiązany z DID posiadacza. Służy on do weryfikacji podpisu posiadacza.

Treść

Metadane prezentacji - informacje o prezentacji, w tym DID posiadacza, czas wystawienia prezentacji, czas wygaśnięcia (jeśli dotyczy) oraz inne standardowe atrybuty. DID posiadacza w metadanych musi odpowiadać (być wyprowadzony z) kluczowi publicznemu umieszczonemu w nagłówku prezentacji.

Dowód wystawcy - podpis cyfrowy wystawcy obecny w każdym weryfikowalnym poświadczeniu zawartym w prezentacji (potwierdza autentyczność i integralność poświadczenia).

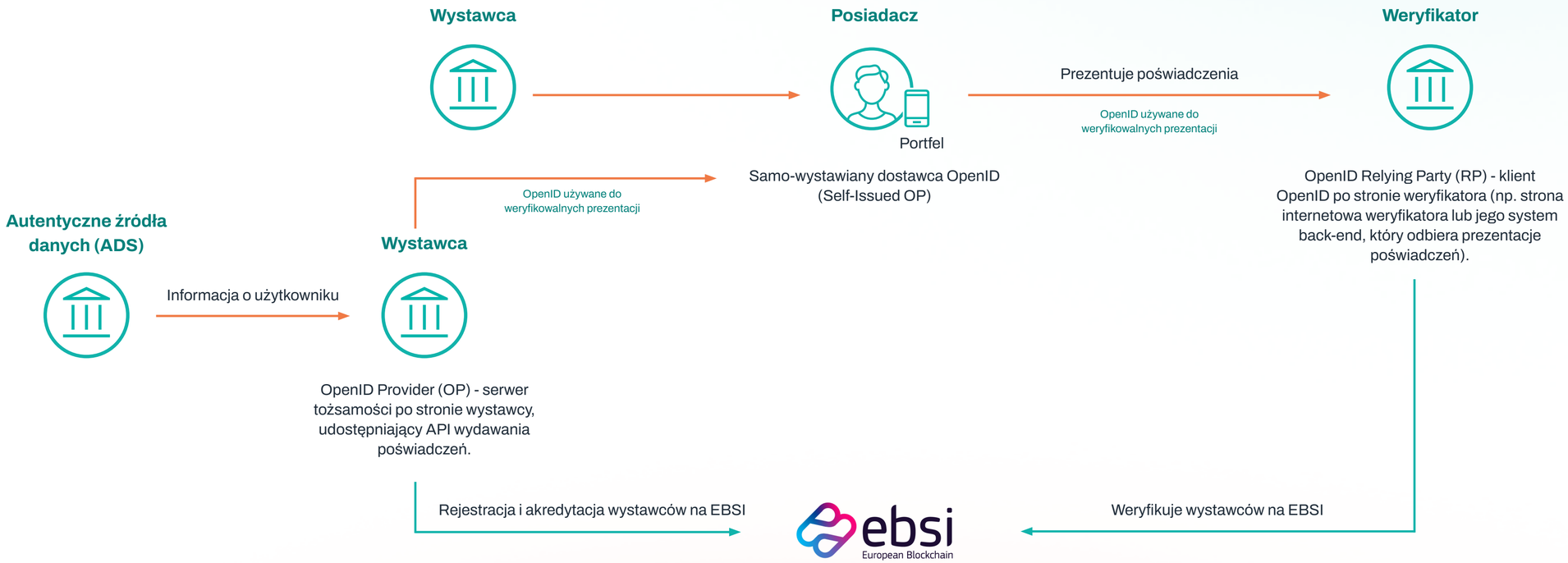
Podpis

Dowód posiadacza - podpis cyfrowy posiadacza złożony na całości weryfikowalnej prezentacji, stanowiący potwierdzenie, że to posiadacz przedkłada prezentację. Podpis ten jest weryfikowany za pomocą powyższego klucza publicznego posiadacza.

Ostatnie pytanie?

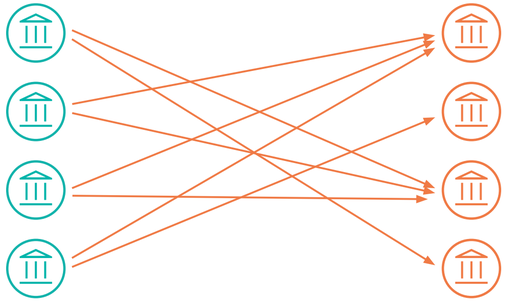
OID4VC można zastosować w dowolnym sektorze

Role i komponenty pozostają takie same we wszystkich sektorach. Oznacza to, że model oparty na OID4VC jest uniwersalny i może zostać zaadaptowany niezależnie od branży:



OID4VC jest zgodny z modelem zaufania wystawców EBSI

W ekosystemie EBSI wystawcy i weryfikatorzy mogą ustanowić zaufaną relację na dwa sposoby: poprzez dwustronne umowy lub za pomocą kotwic zaufania w ramach szerszego modelu zaufania.



Podejście 1

Dwustronne umowy między wystawcą a weryfikatorem:

- \+ Dobre rozwiązanie, gdy liczba wystawców i weryfikatorów jest niewielka (para instytucji może bezpośrednio się porozumieć).
- \+ Proste do zaprojektowania (wymaga jedynie uzgodnienia warunków między dwiema stronami).
- − Wymaga niestandardowej konfiguracji i integracji dla każdej pary podmiotów.
- − Specyficzne dla danego przypadku użycia - nie stanowi uniwersalnego rozwiązania.
- − Trudne do skalowania - przy większej liczbie podmiotów liczba umów rośnie wykładniczo.

Podejście 2

Kotwice zaufania / model zaufania opartego na centralnych autorytetach:

- \+ Dobre rozwiązanie, gdy występuje wielu wystawców i weryfikatorów (wprowadzony jest centralny lub rozproszony punkt zaufania).
- − Trudniejsze do zaprojektowania - wymaga stworzenia lub uzgodnienia wspólnego modelu zaufania (np. listy zaufanych wystawców, schematu akredytacji).
- \+ Nie wymaga niestandardowej konfiguracji dla każdej pary - podmioty ufają centralnym kotwicom zaufania (np. certyfikatom lub rejestrom zaufanych podmiotów).
- \+ Uniwersalne - można zastosować w szerokim zakresie przypadków użycia i sektorów.
- \+ Łatwe do skalowania - dodanie kolejnych wystawców lub weryfikatorów jest proste (zwiększanie skali zarówno horyzontalnie, jak i wertykalnie).

Chcesz wiedzieć więcej?

Kluczowe zasoby

Strona internetowa EBSI

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

Podręcznik poświadczeń weryfikowalnych EBSI

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

Demonstracje EBSI (Demo Day)

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


ebsi
European Blockchain