Rozdział 3

Zdecentralizowane identyfikatory EBSI (metody DID)

EBSI, wyjaśnione – pierwsza edycja

Jakie są poszczególne rozdziały tej pierwszej edycji?

01. Weryfikowalne poświadczenia wyjaśnione

02. Weryfikowalne poświadczenia w praktyce

03. Zdecentralizowane identyfikatory EBSI (metody DID)

04. Tożsamość cyfrowa

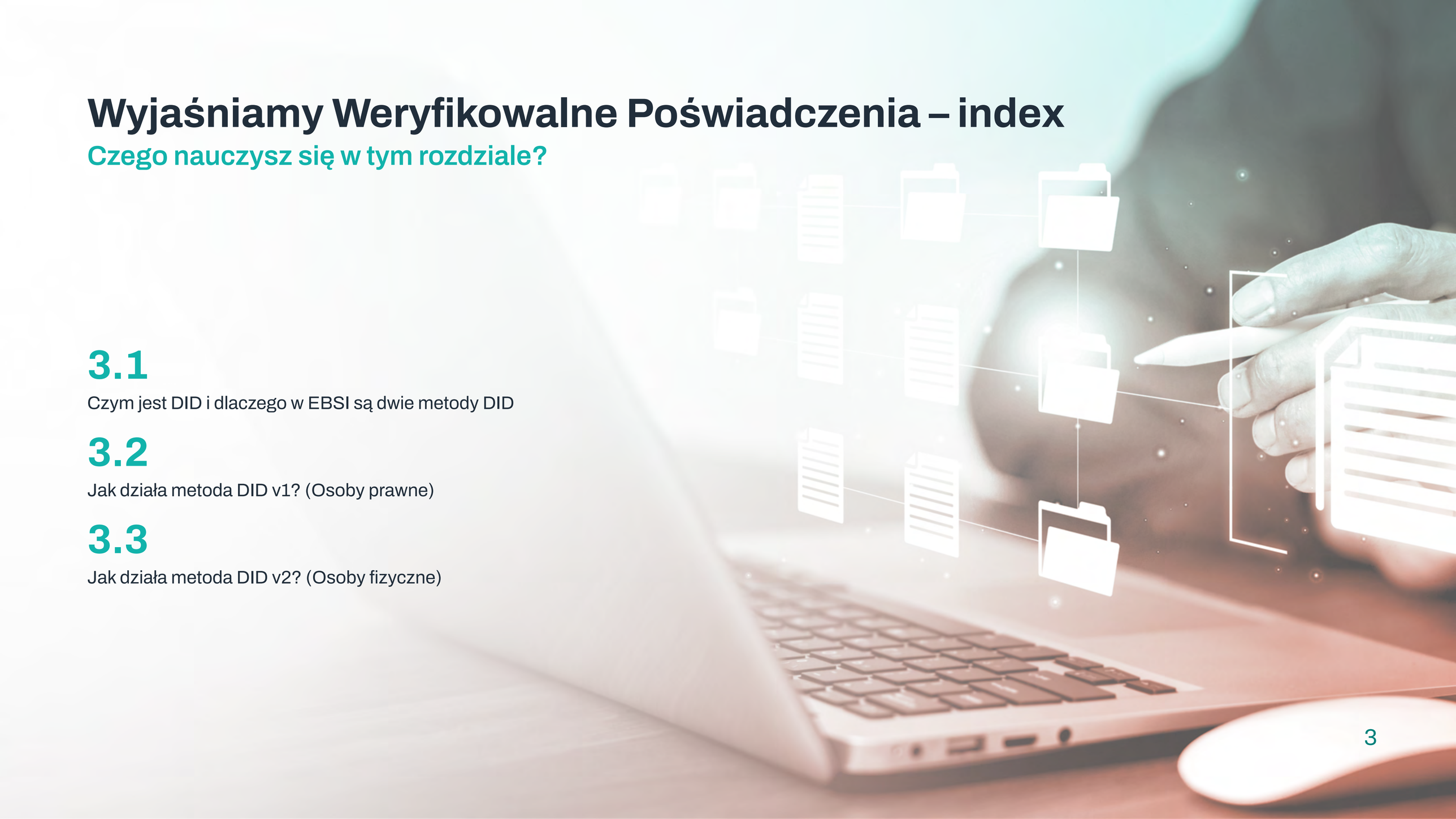
05. Model zaufania wystawców tożsamości cyfrowej

06. OpenID Connect dla weryfikowalnych poświadczeń

07. Cyfrowe portfele

Wyjaśniamy Weryfikowalne Poświadczenia – index

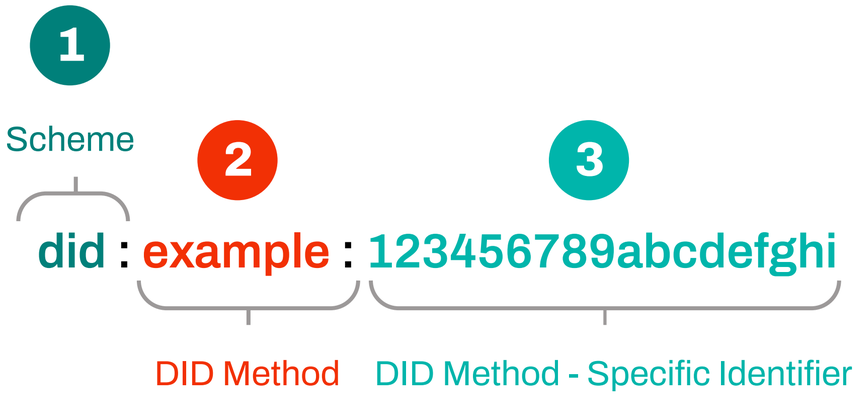
Czego nauczysz się w tym rozdziale?



3.1
Czym jest DID i dlaczego w EBSI są dwie metody DID?

Czym jest zdecentralizowany identyfikator (DID) według W3C?

DID to po prostu długi ciąg znaków, który nie dostarcza żadnej znaczącej informacji o osobie fizycznej ani prawnej. Identyfikatory DID oraz dokumenty DID są generowane przez ich właścicieli za pomocą portfela lub systemów back-office.



1. pierwsza część to zawsze trzy litery **„did”**;
2. druga część określa identyfikator metody DID;
3. trzecia część to całkowicie unikalny losowy ciąg znaków generowany zgodnie ze specyficznymi zasadami dla danej metody.

Dlaczego to ważne?

Identyfikatory DID są używane do zapewnienia autentyczności wystawców i posiadaczy w weryfikowalnych maszynowo dokumentach znanych jako poświadczenia weryfikowalne (VC).

Weryfikowalne poświadczenia w portfelu cyfrowym

Przykład weryfikowalnego poświadczenia w portfelu – specyfikacja W3C

{
„@context”: [
„https://www.w3.org/2018/credentials/v1”,
„https://essif.europa.eu/schemas/vc/2020/v1”
],
„id”: „https://essif.europa.eu/tsr/53”,
„type”: [
„VerifiableCredential”,
„VerifiableAttestation”,
„VerifiableAccreditation”,
„DiplomaVerifiableAccreditation”
],
„issuer”: „did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1”,
„issuanceDate”: „2020-06-22T14:11:44Z”,
„credentialSubject”: {
„id”: „did:ebsi:zDnaeSGrMFB9kCxnPYWaeMrRyun2HLVHjDNUf76ccy4ZfHU24”,
(….)

DID wystawcy

DID posiadacza

EBSI ma dwie metody DID

Jakie są poszczególne metody DID obsługiwane przez EBSI i dlaczego?

v1

Specyfikacja metody DID EBSI v1

ukierunkowana na osoby prawne. Zaprojektowana z myślą o częstej rotacji kluczy.

Dokumenty DID są przechowywane na rozproszonej księdze EBSI.

v2

Specyfikacja metody DID EBSI v2

ukierunkowana na osoby fizyczne. Zaprojektowana w celu pełnego zachowania prywatności.

Dokumenty DID przechowywane są wyłącznie w portfelu.

Jakie są różnice między metodami DID?

Jedna metoda jest ukierunkowana na osoby prawne (Wystawcy), a druga na osoby fizyczne (Posiadacze).

	v1 Specyfikacja metody DID EBSI v1	v2 Specyfikacja metody DID EBSI v2
Przez kogo jest używana?	Metoda v1: Stosowana przez osoby prawne (Wystawcy).	Metoda v2: Stosowana przez osoby fizyczne (Posiadacze).
Jak jest generowana?	Metoda v1: DID i dokument DID są generowane przez aplikację (back-office) lub aplikację działającą jak portfel.	Metoda v2: DID i dokument DID są generowane i przechowywane w portfelu.
Gdzie jest rejestrowana?	Metoda v1: Dokument DID jest zarejestrowany na rozproszonej księdze EBSI. Brak powiązania między DID a kluczem publicznym, co umożliwia częstą rotację kluczy przez wystawców.	Metoda v2: Dokument DID nie jest rejestrowany na rozproszonej księdze EBSI, ponieważ posiadanie DID może zostać zweryfikowane kryptograficznie dzięki zawartemu w nim skrótowi JWK klucza publicznego – zatem jeśli posiadacz udowodni posiadanie klucza prywatnego, udowodni tym samym posiadanie DID.
Jak to działa?	Metoda v1: Weryfikatorzy pobierają dokument DID z EBSI, aby potwierdzić własność DID oraz zweryfikować podpis weryfikowalnego poświadczenia (VC) przy użyciu klucza publicznego wystawcy służącego do potwierdzeń.	Metoda v2: Portfel dołącza DID i dokument DID podczas przedstawiania informacji weryfikatorom lub gdy zostanie poproszony przez weryfikatorów albo wystawców o potwierdzenie posiadania DID.

Przegląd metod DID EBSI

Jedna metoda jest ukierunkowana na osoby prawne (Wystawcy), a druga na osoby fizyczne (Posiadacze).

Specyfikacja metody DID EBSI v1

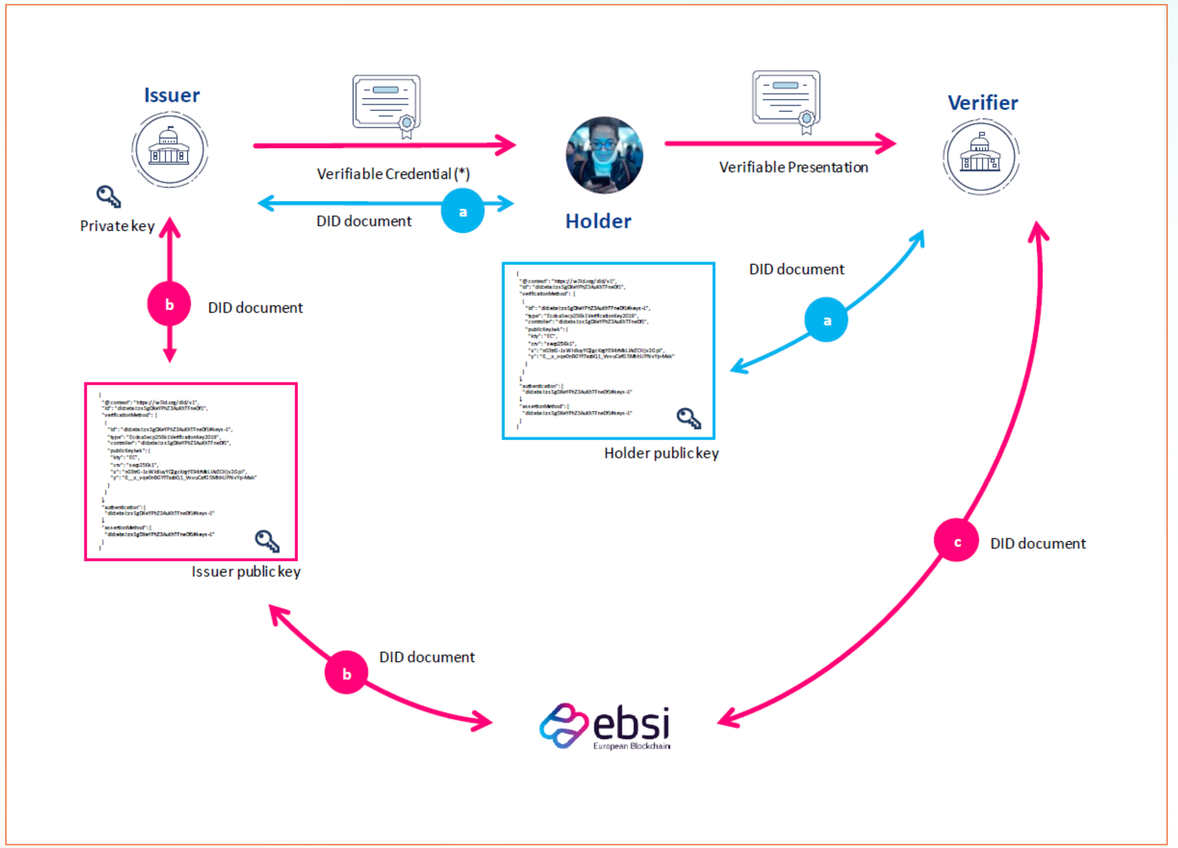
a. Dokumenty DID osób fizycznych są dostarczane przez portfel.

   Dokumenty DID ani same identyfikatory DID osób fizycznych nie są rejestrowane na EBSI.

b. Dokumenty DID podmiotów prawnych są rejestrowane na EBSI (patrz specyfikacja metody DID EBSI v1).

c. Weryfikatorzy pobierają dokumenty DID wystawców/ osób prawnych z EBSI, używając linku takiego jak:

   https://api.test.intebsi.xyz/did-registry/v2/identifiers/did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1



* Wystawcy muszą również mieć możliwość otrzymania dokumentów DID z portfeli użytkowników/posiadaczy w momencie wystawiania weryfikowalnych poświadczeń, aby potwierdzić posiadanie DID.

Przyjrzyjmy się ponownie identyfikatorom DID w EBSI

Struktura DID składa się z trzech części w obu metodach, jednak metoda DID v2 wykorzystuje ustandaryzowany sposób wyliczania skrótu klucza publicznego.

Metoda DID v1

1 2 3

did : ebsi : zk4bhCepWSYp9RhZkRPiwUL

Scheme DID Method DID Method - Specific Identifier

transformacja z użyciem base58bt	wersja 1	idetyfikator losowy, losowe 16 bajtów

Metoda DID v2

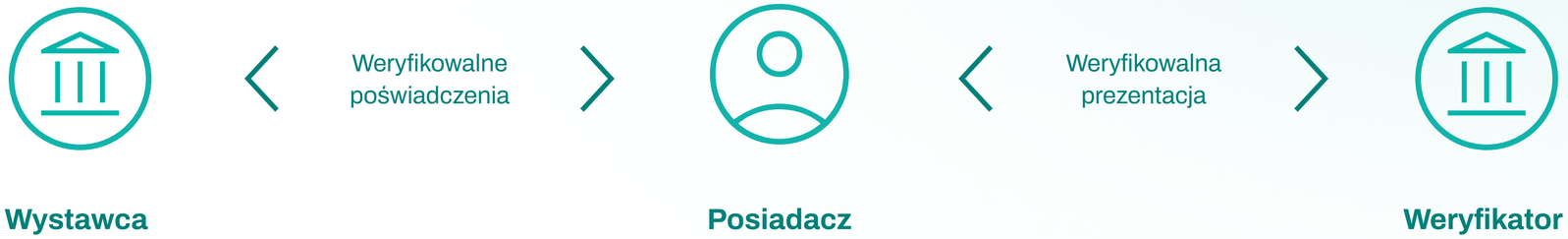
did : ebsi : zDnaeSGrMFB9kCxnPYWaeMrRyun2HLVHjDNUf76ccy4ZFU24

transformacja z użyciem base58bt	wersja 2	idetyfikator losowy, zakodowany klucz publiczny

JWK thumbprint – ustandaryzowana metoda obliczania skrótu klucza publicznego

Zastosowanie metod DID EBSI

Metody DID w podstawowym scenariuszu wymiany informacji



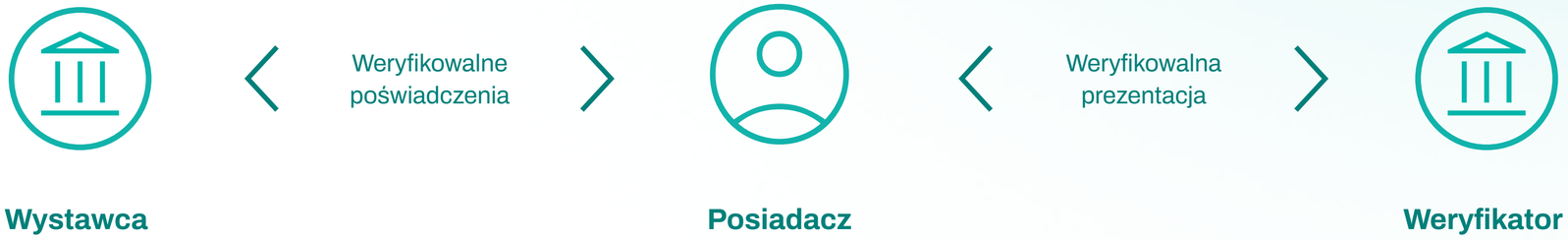
ebsi
European Blockchain

- Cyfrowy portfel
- Rejestr wystawców
- Klucze publiczne wystawców
- CRL *

* Weryfikacja autentyczności wystawcy oraz statusu jego akredytacji

Jak to działa?

Krok 0. Wystawcy przechodzą procedurę onboarding w EBSI, portfele są skonfigurowane, a aplikacje weryfikatorów utworzone.



Metoda DID v1

- Rejestracja samodzielnie wygenerowanych kluczy publicznych i DID (jako części dokumentu DID) na EBSI.
- Akredytacja wystawców weryfikowalnych poświadczeń (VC) przez Zaufane Organy Akredytacyjne (TAO).
- Rejestracja wystawców w rejestrze wystawców EBSI.

Metoda DID v2

- Wybiera portfel zgodny z EBSI
- Portfel generuje DID, klucz publiczny i klucz prywatny. Wszystkie te elementy są częścią dokumentu DID przechowywanego w portfelu
- Żąda poświadczeń (VC) od wystawców

- Brak specjalnego procesu wdrożenia ani konfiguracji poza utworzeniem aplikacji Weryfikatora, która może korzystać z interfejsów API EBSI i współdziałać z portfelami zgodnymi z EBSI

* Weryfikacja autentyczności wystawcy oraz statusu jego akredytacji

Jak to działa?

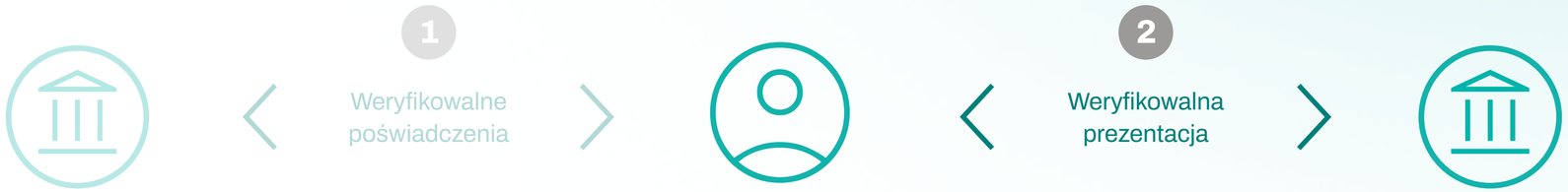
Krok 1. Wydanie weryfikowalnego poświadczenia (VC), które jest następnie przechowywane w portfelu zgodnym z EBSI.

Co zawiera takie poświadczenie?

Metadane Poświadczeń	• DID podmiotu, który wystawia poświadczenie (wystawcy). • Status poświadczenia (data wystawienia, data wygaśnięcia).
Oświadczenia (claims)	• DID posiadacza poświadczenia. • Twierdzenia o podmiocie (co wystawca potwierdza na temat tego podmiotu).
Dowód (podpis wystawcy)	• Cyfrowy dowód (podpis), dzięki któremu poświadczenie jest odporne na manipulacje (jeden lub więcej kryptograficznych dowodów pozwalających wykryć ingerencję w treść i zweryfikować autorstwo poświadczenia).

Jak to działa?

Krok 2. Prezentacja weryfikowalnego poświadczenia do weryfikacji.



Co zawiera takie poświadczenie?

- Metadane Poświadczeń
- Oświadczenia (claims)
- Dowód (podpis wystawcy)

Co jest sprawdzane?

DID Posiadacza	Czy posiadacz poświadczenia (VC) jest tą samą osobą, która je przedstawia.
Metadane Poświadczenia	Czas wystawienia poświadczenia oraz to, czy poświadczenie nie wygasło.
Oświadczenia (claims)	Twierdzenia dotyczące podmiotu (informacje, które wystawca potwierdził).
Dowód (podpis wystawcy)	Podpis wystawcy na poświadczeniu.
Dowód (podpis) posiadacza	Podpis posiadacza na prezentacji.
Sprawdzenie akredytacji wystawcy	Akredytacja wystawcy.

3.2.

Jak działa metoda DID v1?

Specyfikacja metody DID EBSI v1 dla osób prawnych (Wystawcy)

Koncepcyjny uproszczony przepływ

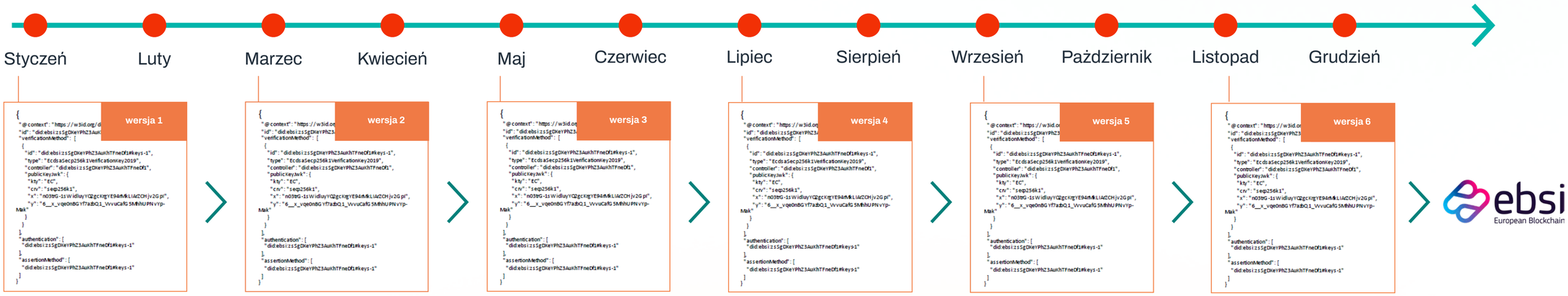
- Wystawca tworzy identyfikator DID zgodnie z profilem schematu DID EBSI (np. did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1).
- Wystawca tworzy także klucze kryptograficzne powiązane z danym DID.
- Wystawca rejestruje te informacje na EBSI w postaci dokumentu DID.
- Dokument DID może zostać pobrany z EBSI przez wystawców i weryfikatorów za pomocą prostego adresu URL.

Metoda DID v1 umożliwia wystawcom elastyczne zarządzanie kluczami i zapewnia weryfikatorom dostęp do nich w czasie rzeczywistym.

Metoda DID v1 a rotacja kluczy

Wystawca

Wykorzystanie identyfikatorów DID oraz dokumentów DID zarejestrowanych na EBSI (zgodnie z definicją metody DID v1) umożliwia wystawcom regularną rotację kluczy (np. co dwa miesiące) bez wpływu na pracę weryfikatorów, ponieważ mogą oni łatwo pobrać z EBSI właściwą wersję dokumentu DID. Zapewnia to znacznie płynniejsze i bezpieczniejsze zarządzanie kluczami w rozległych ekosystemach. Ponadto wystawcy mogą mieć wiele aktywnych kluczy powiązanych ze swoim DID.



Ważna uwaga: Rotacja kluczy minimalizuje liczbę weryfikowalnych poświadczeń, które muszą zostać unieważnione z powodu unieważnienia kluczy podpisujących wystawcy.

Unieważnienie kluczy wystawcy

Załóżmy, że wystawca wydaje 20 poświadczeń każdego miesiąca (240 rocznie) i zmienia parę kluczy co dwa miesiące. Gdyby para kluczy z okresu marzec/kwiecień została skompromitowana, wystawca musiałby ponownie wydać około 40 poświadczeń podczas unieważnienia tej pary kluczy zamiast 240 poświadczeń, gdyby używał tej samej pary kluczy przez cały rok.

Cykl życia DID dla osób prawnych

Krok 1:

Utworzenie DID. Wykonywane w tle przez aplikację zaplecza lub aplikację portfelową.

- Tworzenie identyfikatora DID oraz
- pary kluczy (publiczny i prywatny) dla klucza kontrolnego DID.
- Tworzenie adresu w sieci EBSI wyprowadzonego z klucza publicznego klucza kontrolnego DID.
- Tworzenie dodatkowych kluczy oraz dokumentu DID (zawierającego klucz publiczny klucza kontrolnego DID).

Krok 2:

Rejestracja skrótu dokumentu DID.

Portfel rejestruje na EBSI skrót dokumentu DID. W tym celu:

- dokument DID jest przekazywany do EBSI, aby platforma mogła sprawdzić, czy wystawca posiada wszystkie klucze prywatne odpowiadające kluczom publicznym zawartym w dokumencie DID (sam dokument DID nie jest utrwalany na EBSI);
- jeśli wszystkie kontrole zakończą się pomyślnie, dokument DID zostaje zarejestrowany na EBSI.

Krok 3:

Aktualizacja dokumentu DID.

Dokument DID jest aktualizowany o nowe klucze publiczne za pomocą aplikacji zaplecza lub aplikacji portfelowej.

Krok 4:

Rejestracja zaktualizowanego dokumentu DID.

Zaktualizowany dokument DID zostaje ponownie zarejestrowany na EBSI po przeprowadzeniu podobnych kontroli jak w kroku 1.

Krok 5:

Dezaktywacja DID, aktualizacja dokumentu DID w celu dezaktywacji identyfikatora.

Utworzenie nowej wersji dokumentu DID bez żadnych kluczy (przy użyciu aplikacji zaplecza lub portfelowej).

Krok 6:

Zarejestrowanie dokumentu DID.

Dokument DID bez klucza publicznego na EBSI z zastosowaniem podobnych kontroli jak w kroku 1.

ebsi
European Blockchain

3.3.

Jak działa metoda DID v2?

Specyfikacja metody DID EBSI v2 dla osób fizycznych

Uproszczony przepływ koncepcyjny:

- Portfel generuje klucze kryptograficzne i na ich podstawie wywodzi identyfikator DID zgodnie z profilem schematu DID EBSI v2, kodując klucz publiczny (np. did:ebsi:zDnaeSGrMFB9kCxnPYWaeMrRyun2HLVHjDNUf76ccy4ZfHU24) – wykorzystuje do tego tzw. skrót JWK (ustandaryzowany sposób obliczania haszu klucza publicznego).
- W procesie wydawania weryfikowalnego poświadczenia (VC) posiadacz udostępnia swój dokument DID (klucz publiczny) i potwierdza posiadanie DID poprzez wykazanie kontroli nad odpowiadającym mu kluczem prywatnym przed weryfikatorem.
- W procesie wymiany weryfikowalnej prezentacji (VP) posiadacz udostępnia swój dokument DID (klucz publiczny) i potwierdza posiadanie DID poprzez wykazanie kontroli nad odpowiadającym mu kluczem prywatnym przed weryfikatorem.

Chcesz wiedzieć więcej?

Uproszczony przepływ koncepcyjny:

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

Aneks

Kluczowe akronimy i terminy użyte w tym dokumencie

- **Zdecentralizowany identyfikator (DID)** – przenośny identyfikator oparty na adresie URL, znany także jako DID, powiązany z podmiotem. Takie identyfikatory są najczęściej używane w weryfikowalnych poświadczeniach i powiązane z podmiotami w ten sposób, że samo weryfikowalne poświadczenie może być łatwo przenoszone z jednego repozytorium do innego bez potrzeby ponownego wystawiania poświadczenia.
- **Dokument zdecentralizowanego identyfikatora (dokument DID)** – dokument zawierający informacje związane z konkretnym identyfikatorem DID, takie jak powiązane repozytorium oraz informacje o kluczach publicznych.
- **Wystawca (Issuer)** – rola, jaką może pełnić podmiot poprzez stwierdzanie pewnych faktów (claims) o jednym lub kilku podmiotach, tworzenie na tej podstawie weryfikowalnego poświadczenia oraz przekazywanie tego poświadczenia posiadaczowi.
- **Poświadczenie weryfikowalne (VC)** – zestaw jednego lub więcej oświadczeń (claims) dokonanych przez wystawcę. Poświadczenie weryfikowalne to odporne na manipulacje poświadczenie, którego autorstwo może zostać zweryfikowane kryptograficznie. Poświadczenia weryfikowalne mogą posłużyć do zbudowania weryfikowalnych prezentacji, które również można zweryfikować kryptograficznie.
- **Prezentacja weryfikowalna (VP)** – dane wywiedzione z jednego lub wielu weryfikowalnych poświadczeń wystawionych przez jednego lub wielu wystawców, które są udostępniane określonemu weryfikatorowi. Weryfikowalna prezentacja to odporna na manipulacje prezentacja, zakodowana w sposób umożliwiający zaufanie do autorstwa danych po przeprowadzeniu kryptograficznej weryfikacji.
- **Weryfikowalny rejestr danych (verifiable data registry)** – rola systemu polegająca na pośredniczeniu w tworzeniu i weryfikacji identyfikatorów, kluczy oraz innych istotnych danych (takich jak schematy weryfikowalnych poświadczeń, rejestry unieważnień, publiczne klucze wystawców itp.), które mogą być wymagane do korzystania z weryfikowalnych poświadczeń.
- **Weryfikator (Verifier)** – rola, jaką pełni podmiot, otrzymując jedno lub więcej weryfikowalnych poświadczeń (opcjonalnie wewnątrz weryfikowalnej prezentacji) do weryfikacji. Inne specyfikacje mogą określać tę rolę jako stronę ufającą (relying party).

Źródło: W3C

Czym w ujęciu technicznym jest dokument DID?

Każdemu identyfikatorowi DID odpowiada pojedynczy, unikalny dokument DID, który może podlegać wersjonowaniu.

- Każdy zdecentralizowany identyfikator (DID) jest powiązany z kluczami publicznymi używanymi przez weryfikatorów do weryfikacji podpisów elektronicznych – są one umieszczone w dokumencie DID.
- Dokument DID zawiera kryptograficzne klucze publiczne używane do weryfikacji poświadczeń weryfikowalnych.
- Zgodnie z metodą DID v1 wystawcy muszą mieć dokument DID przechowywany na EBSI, nad którym sprawują kontrolę.
- Zgodnie z metodą DID v2 posiadacze nie mają dokumentu DID na EBSI. Ich dokument DID jest przechowywany w portfelu i udostępniany przez portfel.

Przykład dokumentu DID w EBSI (fragment JSON):

```
{
 „@context”: „https://w3id.org/did/v1”,
 „id”: „did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1”,
 „verificationMethod”: [
  {
   „id”: „did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1#keys-1”,
   „type”: „EcdsaSecp256k1VerificationKey2019”,
   „controller”: „did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1”,
   „publicKeyJwk”: { ... }
  }
 ],
 „assertionMethod”: [
  „did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1#keys-1”
 ]
}
```

Klucz publiczny powiązany z DID

Odwołanie do klucza publicznego

Czym jest klucz publiczny i prywatny i kiedy się ich używa?

Kryptografia z kluczem publicznym i prywatnym wykorzystuje parę kluczy:

- klucz publiczny i klucz prywatny, które są matematycznie ze sobą powiązane (ale nie są powiązane z danym DID);
- klucz prywatny musi pozostać tajny i nie może być udostępniany (np. powinien pozostać w portfelu posiadacza);
- klucz publiczny używany przez wystawców i posiadaczy jest ujawniany w dokumencie DID, nie zmniejszając bezpieczeństwa całego procesu.

Podpisy elektroniczne wykorzystują pary kluczy publiczny/prywatny, aby zapewnić zaufanie zarówno między wystawcami a weryfikatorami, jak i między posiadaczami a weryfikatorami:

- Podczas tworzenia weryfikowalne poświadczenia są podpisywane przez wystawców (ich kluczem prywatnym) i sprawdzane przez weryfikatorów (przy użyciu klucza publicznego z dokumentu DID odpowiedniego wystawcy) w celu zapewnienia integralności i autentyczności.
- Podczas udostępniania informacji weryfikowalne prezentacje są podpisywane przez posiadaczy (ich kluczem prywatnym) i sprawdzane przez weryfikatorów (przy użyciu klucza publicznego z dokumentu DID posiadacza) w celu zapewnienia integralności i autentyczności.

Czym jest rejestrator DID / weryfikowalny rejestr DID?

Użycie DID wymaga istnienia systemu rejestratora, którym może być rozproszona księga (np. blockchain), zdecentralizowany system plików, baza danych lub inna forma zaufanego magazynu danych. EBSI jest rejestratorem wszystkich identyfikatorów DID w EBSI.

Rejestrator DID jest używany tylko w metodzie DID v1 do obsługi dokumentów DID wystawców.

Schemat DID i metoda DID

EBSI definiuje schemat DID oraz specyfikację metody DID, która określa m.in. w jaki sposób:

1. Weryfikatorzy mogą rozwiązać identyfikator DID i pobrać dokument DID wystawcy z EBSI, tak aby:
   - uzyskać jego najnowszą wersję,
   - uzyskać dowolną wcześniejszą wersję dokumentu DID.
2. Sprawdzić, czy identyfikatory DID są zgodne ze schematem EBSI.
3. Rejestrować dokumenty DID (włącznie z późniejszymi aktualizacjami).
4. Dezaktywować identyfikatory DID.

Schemat DID i metoda DID – co to zapewnia?

- Unikalność identyfikatorów DID wystawców.
- Niezaprzeczalność i niezmienność identyfikatorów DID oraz dokumentów DID wystawców.
- Gwarancję, że ten sam klucz kontrolny **nie** zarejestruje dwóch różnych identyfikatorów DID.
- Gwarancję, że tylko klucz kontrolny danego wystawcy może zarządzać jego DID.

Czym jest klucz kontrolny DID?

Czym jest klucz kontrolny DID, kto go używa i dlaczego?

Klucz kontrolny DID jest wykorzystywany tylko w metodzie DID v1 do zarządzania dokumentami DID wystawców.

Klucz kontrolny DID to para kluczy używana przez...

- **Wystawcy:** do rejestracji, aktualizacji lub dezaktywacji swoich dokumentów DID (które zawierają klucz publiczny klucza kontrolnego DID).
- **Osoby fizyczne**: nie poiadają klucza kontrolnego DID, ponieważ ich dokument DID nie jest rejestrowany na EBSI.

Dlaczego używa się klucza kontrolnego DID?

Prywatne klucze kontrolne DID służą do podpisywania transakcji, które rejestrują, aktualizują i dezaktywują identyfikatory DID na rozproszonej księdze EBSI. Skrót publicznego klucza kontrolnego DID jest zawsze przechowywany na tej księdze w ramach transakcji. Ważne jest, aby zauważyć, że:

- Jeden klucz kontrolny DID może zarządzać tylko jednym identyfikatorem DID.
- Jeden identyfikator DID może być zarządzany przez wiele kluczy kontrolnych DID.
- Kluczy kontrolnych DID wolno używać wyłącznie do zarządzania identyfikatorami DID.


ebsi
European Blockchain