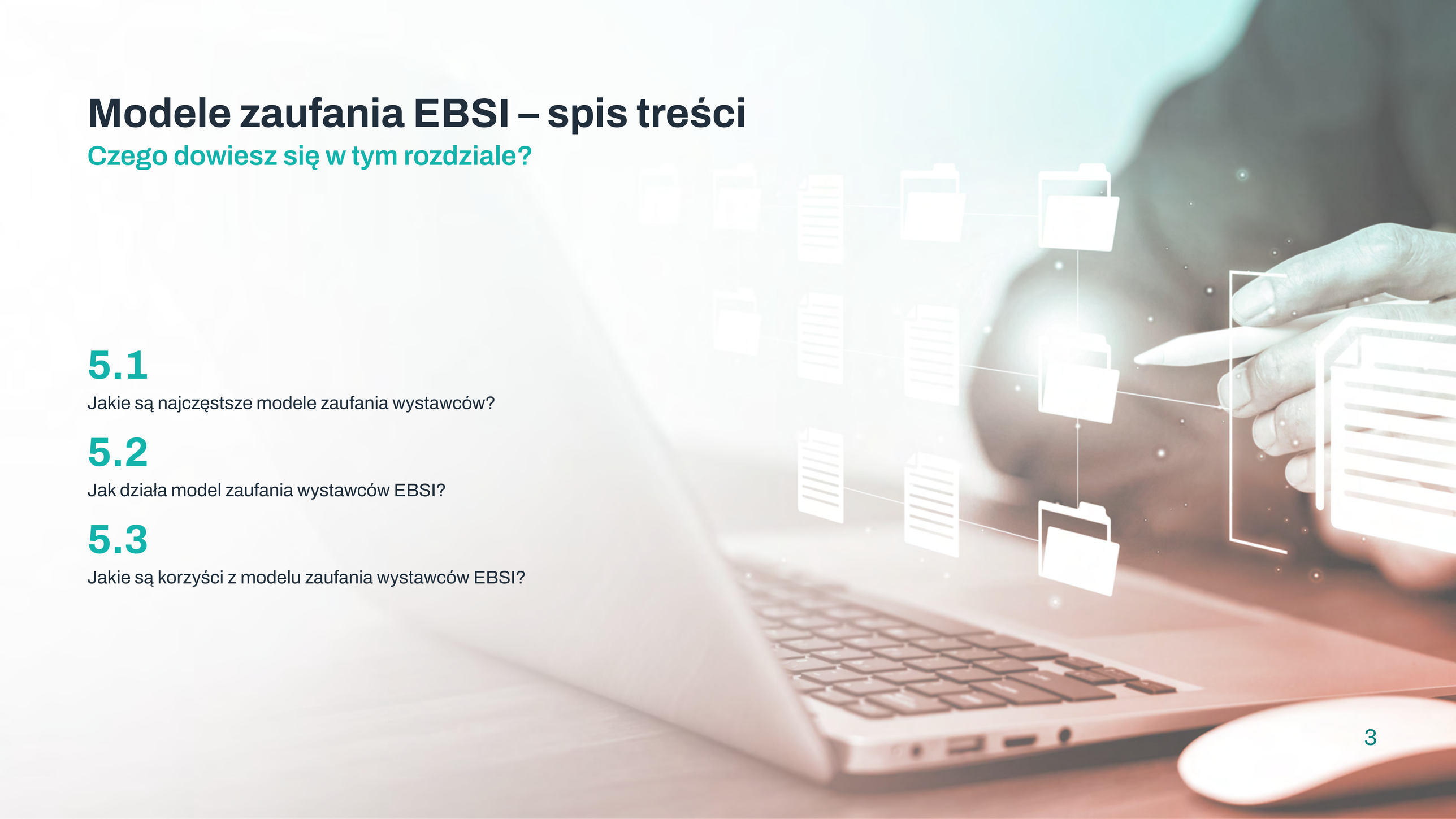
Rozdział 5

Model zaufania wystawców

Rozdziały pierwszego wydania

Modele zaufania EBSI – spis treści

Czego dowiesz się w tym rozdziale?



5.1

Jakie są najczęstsze modele zaufania wystawców?

Klasyczny model zaufania dla wystawców

Klasyczne rozwiązania często wymagają, aby weryfikatorzy kontaktowali się z wystawcami, aby upewnić się, że informacje otrzymane od posiadaczy są wiarygodne. Ten schemat określa się potocznie jako „phoning home” („telefonowanie do domu”).

Problem „telefonowania do domu”

Potrzeba „telefonowania do domu” generuje zatem szereg powyższych wyzwań.

Obciążenia techniczne:	Obciążenia operacyjne:	Wyzwania prywatności:
Powoduje to obciążenie po stronie wystawcy poświadczenia, który musi utworzyć i utrzymywać interfejsy API dostępne dla weryfikatorów oraz zapewnić dostępność połączenia 24/7.	Wymaga od weryfikatora utworzenia i utrzymania wywołań do wszystkich tych API dla każdego wystawcy. W otwartym ekosystemie poświadczeń może to oznaczać setki lub tysiące integracji dla każdego usługobiorcy.	Taki model powoduje problemy z prywatnością, ponieważ umożliwia wystawcom i weryfikatorom śledzenie, jak posiadacz korzysta z poświadczenia w różnych domenach (istnieje możliwość korelowania aktywności posiadacza między różnymi usługami).

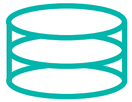
Nowy model zaufania dla wystawców

Zgodnie z modelem poświadczeń zaufanych w EBSI, weryfikatorzy mogą zaufać wystawcom bez tzw. „telefonowania do domu”. Zamiast tego weryfikatorzy mogą pobrać informacje potrzebne do weryfikacji zaufania do wystawcy z rejestru EBSI. Niniejszy rozdział wyjaśnia szczegółowo, jak to działa.

Koncepcyjne modele zaufania wystawców bez „telefonowania do domu”

Istnieją trzy podstawowe modele zaufania dla wystawców weryfikowalnych poświadczeń – modele te mogą być ze sobą łączone w praktyce. Są to:

RÓŻNIĄ SIĘ ONE SKALOWALNOŚCIĄ, ELASTYCZNOŚCIĄ I INTEROPERACYJNOŚCIĄ.

Model Zaufania Scentralizowany	Model Zaufania Federacyjny	Model Zaufania Rozproszony
		ebsi European Blockchain
Certyfikaty, np. zarządzane listy zaufania PKI (*) – tradycyjne podejście oparte na infrastrukturze klucza publicznego.	Listy Zaufane (*) (*) Rozporządzenie eIDAS wprowadziło koncepcję list zaufanych, a decyzja wykonawcza Komisji (UE) 2015/1505 określa jej specyfikacje techniczne: https://europa.eu/!GRyHFF	• Klucze publiczne wystawców • Rejestr wystawców • Rejestr zaufanych schematów – rejestr schematów (struktur danych) używanych przez poświadczenia;

Czym różni się rozproszony model zaufania EBSI od innych?

Modele zaufania w relacjach obywatel-administracja (C2G) lub obywatel-biznes (C2B)

Centralne i federacyjne modele zaufania	Rozproszony model zaufania EBSI
Zazwyczaj opierają się na certyfikatach X.509. Jest to podejście hierarchiczne i mało elastyczne, ponieważ wymaga zaangażowania wielu podmiotów: • Urząd Certyfikacji (CA) – przechowuje, wydaje i podpisuje certyfikaty cyfrowe. • Urząd Rejestracji (RA) – weryfikuje tożsamość podmiotów ubiegających się o certyfikat przechowywany następnie w CA. • Urząd Walidacji (VA) – na żądanie dostarcza informacji niezbędnych do walidacji certyfikatu w imieniu CA. • Urząd Dystrybucji (DA) – odpowiada za dystrybucję certyfikatów.	Wykorzystuje łańcuch bloków oraz zdecentralizowane identyfikatory (DID), zapewniając decentralizację i większą elastyczność. Wymagane są tylko dwie role: • Zaufana Organizacja Akredytacyjna (TAO) – weryfikuje, akredytuje i zarządza podmiotami (tzw. zaufanymi wystawcami) uprawnionymi do wydawania elektronicznych dokumentów. • Zaufany Wystawca (TI) – odpowiada za wydawanie określonych typów elektronicznych dokumentów oraz zarządzanie kluczami służącymi do ich podpisywania z wykorzystaniem blockchain. Technicznie rzecz biorąc, zarządza on dokumentem DID.

5.2.

Jak działa model zaufania wystawców EBSI?

Kluczowe podmioty modelu zaufania wystawców EBSI

Jakie są kluczowe podmioty modelu zaufania wystawców EBSI?

Zaufana Organizacja Akredytacyjna (TAO)

Organizacja odpowiedzialna za akredytowanie zaufanych wystawców (Trusted Issuers) w określonym sektorze/domenie na danym obszarze geograficznym, upoważniając ich do wydawania określonych typów poświadczeń weryfikowalnych (VC).

Przykład: w domenie edukacji ministerstwo edukacji danego kraju pełni rolę TAO akredytującego uniwersytety w tym kraju. TAO rejestruje również Zaufane Schematy powiązane z danym rodzajem poświadczenia (np. schemat danych dyplomu).

Rejestr EBSI

EBSI pełni rolę publicznego rejestru wystawców, zawierającego listę zaufanych podmiotów prawnych akredytowanych przez TAO do wydawania określonych typów poświadczeń. Innymi słowy, podmioty uzyskujące akredytację stają się zaufanymi wystawcami (TI) poprzez prosty proces akredytacji.

Przykład: w sektorze edukacji, poza dokumentami DID zarejestrowanych uniwersytetów, EBSI udostępnia weryfikatorom także akredytację nadaną przez TAO (będącą weryfikowalnym poświadczeniem) oraz link do powiązanego Zaufanego Schematu. Ponadto EBSI udostępnia same schematy weryfikowalnych poświadczeń. Schemat wspiera proces weryfikacji i zapewnia, że wystawcy przestrzegają uzgodnionych modeli danych zdefiniowanych dla danej domeny.

Zaufany Wystawca (TI)

Akredytowany podmiot prawny uprawniony do wydawania określonych typów poświadczeń. Np. akredytowana uczelnia (uniwersytet) staje się zaufanym wystawcą dyplomów zgodnie z określonym Zaufanym Schematem. Podmioty akredytowane przez TAO uzyskują status Zaufanego Wystawcy w wyniku procesu akredytacji opisanego powyżej. Z chwilą akredytacji ich identyfikator (DID) i dokument DID zostają zarejestrowane na rejestrze EBSI, a weryfikowalna akredytacja wydana przez TAO powiązana z tym DID jest dostępna do wglądu dla weryfikatorów.

Jak ustanowić zaufanie między wystawcami a weryfikatorami?

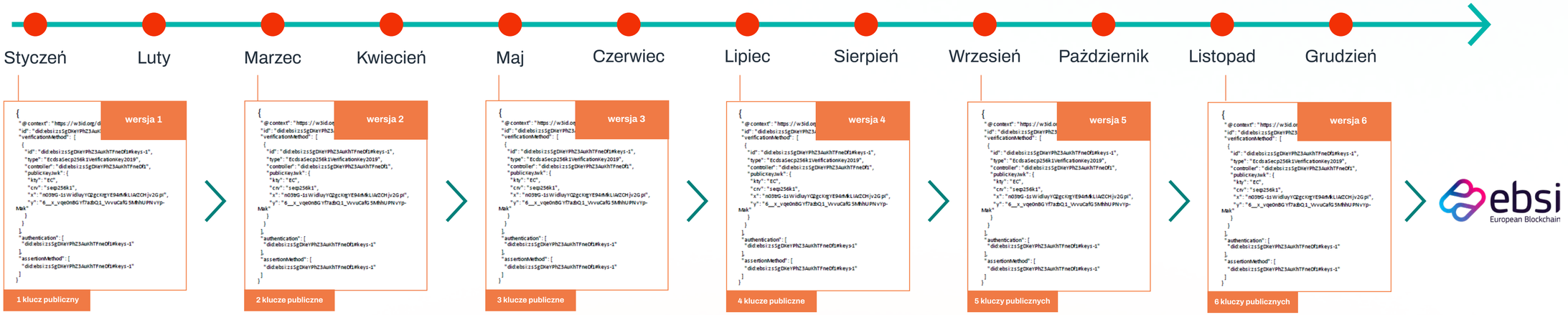
Poniżej przedstawiono proces ustanawiania zaufania w EBSI - numery wskazują kolejność zdarzeń:

Wystawcy mogą zarządzać kluczami niezależnie od TAO

Po uzyskaniu akredytacji EBSI umożliwia wystawcom samodzielne zarządzanie swoimi kluczami kryptograficznymi (zgodnie z własną metodą DID EBSI), niezależnie od TAO. Poniższy przykład ilustruje mechanizm rotacji kluczy przez wystawcę poprzez aktualizację dokumentu DID w kolejnych wersjach.

DID

DID: Przy częstym rotowaniu/aktualizowaniu kluczy wystawcy minimalizują skutki ewentualnego kompromitacji swojego klucza prywatnego, ponieważ mniej poświadczeń będzie podpisanych tym samym kluczem. Technicznie rzecz biorąc, użycie DID i dokumentów DID umożliwia wystawcom rotację kluczy, tj. regularne aktualizowanie kluczy kryptograficznych (np. co dwa miesiące) bez wpływu na weryfikatorów – mogą oni łatwo pobrać z EBSI właściwą wersję dokumentu DID. Umożliwia to znacznie płynniejsze i bezpieczniejsze zarządzanie kluczami w dużych ekosystemach. Wystawcy mogą mieć wiele aktywnych kluczy powiązanych ze swoim DID jednocześnie.



W tym przykładzie wystawca postanawia aktualizować swoje klucze co dwa miesiące. Odbywa się to poprzez rejestrację nowej wersji dokumentu DID wystawcy w EBSI. Każda kolejna wersja dokumentu DID zawiera dodatkowy klucz publiczny. Weryfikator znając DID wystawcy może zawsze uzyskać z EBSI najnowszą wersję dokumentu DID z zaktualizowaną parą kluczy.

Co jest rejestrowane w rozproszonym rejestrze EBSI?

Na rejestrze EBSI rejestrowane są informacje potrzebne do zaufania łańcuchowi wydawców i weryfikacji poświadczeń. Obejmują one:

	Rejestr Wystawców:	Rejestr Zaufanych Schematów:
Zaufana Organizacja Akredytacyjna (TAO)	• DID TAO i odpowiadający mu dokument DID; • Weryfikowalne Upoważnienie TAO (Verifiable Authorisation); • Weryfikowalna Akredytacja TAO - poświadczenie akredytacji (zawiera odniesienie do DID, właściwej jurysdykcji oraz organizacji, które TAO może akredytować, dla jakich poświadczeń oraz odpowiedniego schematu).	Schemat poświadczenia akredytacji - opis modelu danych akredytacji, zawierający m.in.: • organizacje, które TAO ma prawo akredytować; • właściwą jurysdykcję; • rodzaj poświadczenia weryfikowalnego (którego dotyczy akredytacja).
Zaufani Wystawcy (TI):	• DID zaufanego wystawcy i jego dokument DID; • Weryfikowalna Akredytacja wystawcy – poświadczenie akredytacji wystawcy (zawiera odniesienie do DID, typów poświadczeń, które może wydawać, właściwej jurysdykcji oraz odpowiedniego schematu).	• Schemat weryfikowalnego poświadczenia - opis modelu danych dla weryfikowalnych poświadczeń, jakie mogą być wydawane. (Uwaga: konkretny schemat poświadczenia jest ustalany na poziomie polityki dla danego przypadku użycia.)

Jak skonfigurować wielopoziomowy model zaufania wystawców w EBSI?

Przykład: domena edukacji w Państwie Członkowskim X

Poziom 1:
Ustanowienie głównego TAO (np. Ministerstwa Edukacji).

Ministerstwo Edukacji (pełni rolę głównego TAO) akredytuje organ akredytacyjny (pod-TAO) do akredytowania uniwersytetów.

Poziom 2:
Ustanowienie podległych TAO (sub-TAO) - opcjonalne (np. organu akredytacyjnego dla uczelni).

Organ akredytacyjny dla instytucji szkolnictwa wyższego (sub-TAO) akredytuje uniwersytety do wydawania dyplomów.

Poziom 3:
Ustanowienie zaufanych wystawców (np. uniwersytetów).

- Organ akredytacyjny (TAO) także akredytuje wydawców do wydawania innych weryfikowalnych poświadczeń (np. poświadczeń edukacyjnych, legitymacji studenckich).
- Uniwersytet A wydaje weryfikowalny dyplom studentowi.
- Uniwersytet B wydaje studentowi weryfikowalną legitymację studencką (Verifiable Student ID).

Przepływ działań - poziom 1 (ustanowienie głównego TAO)

Wdrożenie głównego TAO (Onboarding of root TAO)

Krok 1	Krok 2	Krok 3	Krok 4
Złożenie wniosku o rejestrację. Podmiot z ramienia państwa członkowskiego (Member State Organisation) zgłasza w EBSI prośbę o zarejestrowanie Ministerstwa Edukacji jako głównej Zaufanej Organizacji Akredytacyjnej (root TAO).	**Utworzenie DID.** Ministerstwo Edukacji generuje swój zdecentralizowany identyfikator (DID) i rejestruje dokument DID w systemie EBSI.	**Wydanie weryfikowalnego upoważnienia.** Helpdesk EBSI (EBSI Help Desk) wydaje Ministerstwu Edukacji Weryfikowalne Upoważnienie (Verifiable Authorisation) powiązane z jego nowo utworzonym DID. Jest to poświadczenie autoryzujące Ministerstwo jako TAO	**Rejestracja weryfikowalnego upoważnienia.** Ministerstwo Edukacji zapisuje w rejestrze EBSI otrzymane od Helpdesku EBSI weryfikowalne upoważnienie. Od tego momentu Ministerstwo figuruje w rejestrze jako główny TAO.

Przepływ działań - poziom 2 (ustanowienie sub-TAO)

Wdrożenie (sub)TAO - etap opcjonalny (np. ustanowienie organu akredytacyjnego niższego szczebla)

Krok 1	Krok 2	Krok 3	Krok 4
Zdefiniowanie Zaufanego Schematu. Grupa ds. danego przypadku użycia (Use-Case Group) definiuje Zaufany Schemat dla weryfikowalnego poświadczenia, które będzie wydawane w danej domenie (np. schemat danych dyplomu w edukacji).	**Rejestracja Zaufanego Schematu.** Ministerstwo Edukacji (jako root TAO) rejestruje zdefiniowany schemat poświadczenia w EBSI (dodaje go do rejestru schematów).	**Utworzenie DID przez sub-TAO.** Organ akredytacyjny dla instytucji szkolnictwa wyższego (sub-TAO) generuje swój DID i rejestruje odpowiadający mu dokument DID w EBSI.	**Wydanie i rejestracja weryfikowalnej akredytacji.** Ministerstwo Edukacji (TAO) wydaje dla DID podległego organu akredytacyjnego Weryfikowalną Akredytację (Verifiable Accreditation) potwierdzającą jego uprawnienia jako sub-TAO. Sub-TAO rejestruje otrzymaną akredytację w EBSI (w rejestrze wystawców). W efekcie organ akredytacyjny staje się zaufaną organizacją akredytacyjną sub-TAO, która może dalej akredytować innych zgodnie z zasadami przypadku użycia.

Przepływ działań – poziom 3 (wdrożenie wystawców)

Wdrożenie zaufanych wystawców (np. uczelni wydających dyplomy)

Krok 1	Krok 2	Krok 3
Utworzenie DID przez wystawcę. Uniwersytet A generuje swój DID i rejestruje dokument DID w EBSI.	**Wydanie i rejestracja weryfikowalnej akredytacji dla wystawcy.** Uniwersytet A zwraca się do TAO (Ministerstwa Edukacji) o nadanie mu akredytacji. TAO potwierdza posiadanie DID przez uniwersytet, a następnie wydaje dla DID Uniwersytetu A Weryfikowalną Akredytację zawierającą odniesienie do odpowiedniego Zaufanego Schematu (np. schematu dyplomu). Uniwersytet A rejestruje otrzymaną akredytację w EBSI, stając się oficjalnie zaufanym wystawcą.	**Wydanie weryfikowalnego poświadczenia.** Uniwersytet A jako zaufany wystawca może teraz wystawić studentowi Weryfikowalne Poświadczenie (np. dyplom) podpisane swoim kluczem. Posiadacz otrzymuje poświadczenie w portfelu cyfrowym.

Uwaga: Wdrożenie instytucji A oraz uniwersytetu B przebiegałoby podobnie według tego schematu.

Podsumowanie łańcucha zaufania EBSI dla wystawców

Weryfikowalne Akredytacje określają, jakie poświadczenia weryfikowalne dany wystawca może wydawać i zgodnie z jakimi zasadami (politykami). Poniżej przedstawiono podsumowanie zależności w łańcuchu zaufania:

A Akredytacja główna (root) - promuje daną jednostkę prawną do roli pierwszej Zaufanej Organizacji Akredytacyjnej (TAO). Zarejestrowanie weryfikowalnego upoważnienia (Verifiable Authorisation) dla tej jednostki rozpoczyna nowy łańcuch zaufania. Tylko upoważnione (akredytowane) podmioty prawne mogą akredytować kolejne podmioty zgodnie z zasadami i politykami danego przypadku użycia.

B Określenie Zaufanych Schematów dla danej domeny - dokonywane przez grupę ds. danego przypadku użycia lub właściwe państwo członkowskie. (Definiuje się schematy poświadczeń specyficzne dla danej dziedziny, które stanowią podstawę zaufania).

C Akredytacja do akredytowania – awansuje daną jednostkę prawną do roli Zaufanej Organizacji Akredytacyjnej (sub-TAO), która może następnie akredytować inne podmioty, zgodnie z politykami danego przypadku użycia.

D Akredytacja do poświadczania – awansuje daną jednostkę prawną do roli Zaufanego Wystawcy (TI), który może wydawać weryfikowalne poświadczenia zgodnie z politykami danego przypadku użycia.

W łańcuchu uczestniczą także:

Helpdesk EBSI – inicjuje akredytację pierwszego TAO (punkt A); grupa ds. przypadku użycia / państwo członkowskie - definiuje schematy (punkt B); oraz posiadacz – otrzymuje poświadczenie od zaufanego wystawcy.)

Uwaga techniczna

Dotyczy rejestrowania weryfikowalnych upoważnień i akredytacji w rejestrze EBSI:

TAO oraz zaufani wystawcy rejestrują upoważnienia i akredytacje za pośrednictwem powyższych interfejsów EBSI API

Krok 1:

Przedstawienie weryfikowalnego upoważnienia lub akredytacji (przez aplikację) za pomocą interfejsów API autoryzacji:

Krok 2:

Otrzymanie tokenu dostępu (po pomyślnej weryfikacji uprawnień).

Krok 3:

Podpisanie transakcji blockchain (zawierającej dane do rejestracji)
za pomocą klucza wystawcy lub TAO.

API: /authorisation/v2/siop-sessions

https://api.preprod.ebsi.eu/docs/apis/authorisation/latest#/

API: trusted-issuers-registry/v3/jsonrpc (Method: insertIssuer, updateIssuer)

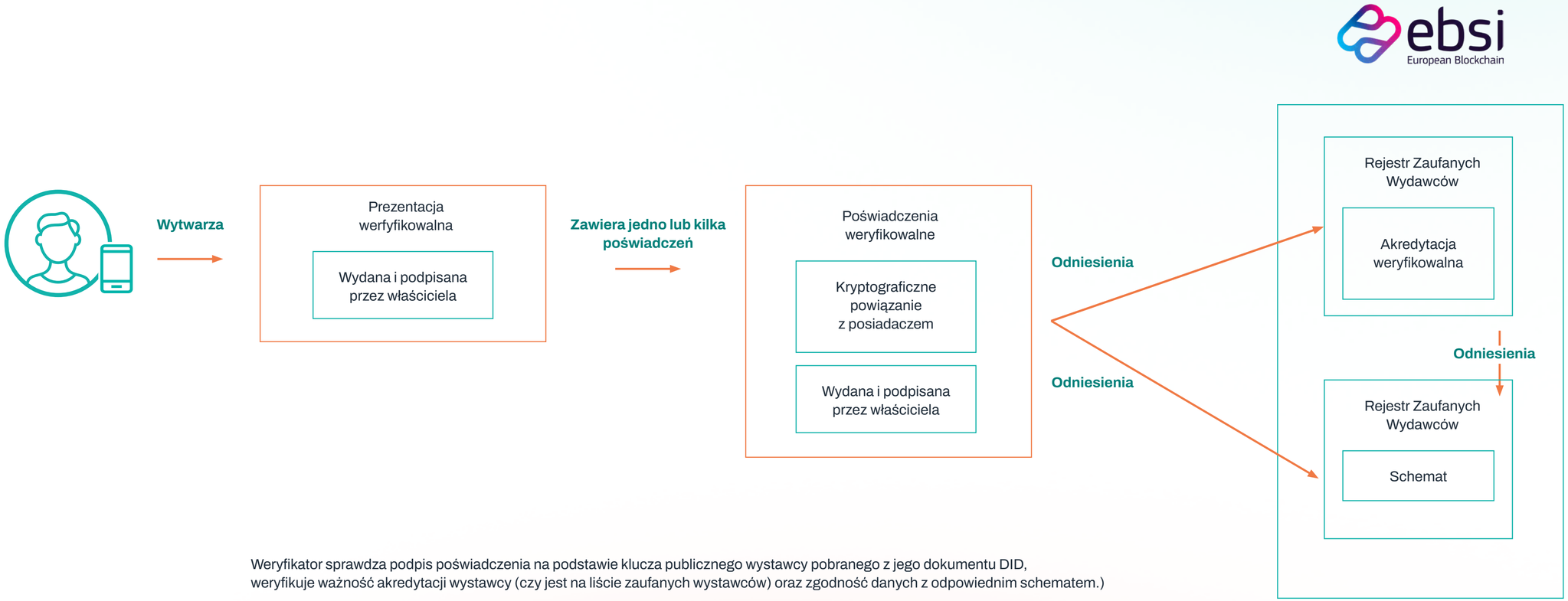
https://api.preprod.ebsi.eu/docs/apis/trusted-issuers-registry/latest

Krok 4:

Przesłanie podpisanej transakcji wraz z tokenem dostępu do sieci EBSI (zapis w rejestrze).

Co się dzieje po ustanowieniu łańcucha zaufania?

Gdy łańcuch zaufania jest już ustanowiony, EBSI umożliwia weryfikatorom łatwe sprawdzenie, czy wystawca danego weryfikowalnego poświadczenia jest zaufany.



Weryfikator sprawdza podpis poświadczenia na podstawie klucza publicznego wystawcy pobranego z jego dokumentu DID, weryfikuje ważność akredytacji wystawcy (czy jest na liście zaufanych wystawców) oraz zgodność danych z odpowiednim schematem.)

5.3.

Jakie są korzyści z modelu zaufania wystawców EBSI?

Obsługa wielu łańcuchów zaufania

Obsługa wielu łańcuchów zaufania

Projekt umożliwiający obsługę wielu łańcuchów zaufania o strukturze i zasadach specyficznych dla danego przypadku użycia. EBSI wspiera istnienie równolegle wielu niezależnych „łańcuchów” zaufania dostosowanych do różnych domen czy sektorów.

EBSI pozwala na utrzymywanie wielu takich łańcuchów jednocześnie – w przedstawionym wcześniej przykładzie pokazano łańcuch zaufania dla domeny edukacji.

Analogicznie można zdefiniować oddzielny łańcuch zaufania dla innej domeny (np. ubezpieczeń społecznych), z własnymi Zaufanymi Organizacjami Akredytacyjnymi i Zaufanymi Wystawcami, ustanowionymi zgodnie z politykami obowiązującymi w tej dziedzinie (podobnie jak to miało miejsce w przypadku domeny edukacji). Dzięki temu architektura EBSI jest elastyczna i może zostać dostosowana do różnych obszarów zastosowań, w których struktura łańcucha zaufania oraz reguły mogą się różnić

Zalety rozproszonego modelu zaufania EBSI

1. Łatwy do zarządzania: zaprojektowany tak, aby Zaufane Organizacje Akredytacyjne (TAO) i zaufani wystawcy mogli łatwo nim zarządzać.

2. Łatwy do zweryfikowania: zaprojektowany tak, aby wielu weryfikatorów mogło z łatwością sprawdzić autentyczność przedstawianych informacji.

3. Trudny do podrobienia: zaprojektowany w sposób uniemożliwiający kopiowanie i duplikowanie poświadczeń (utrudniający fałszerstwo).

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