EBSI Verifiable Credentials explained

CHAPTER 5

Issuers trust model

June 2022

European Commission | ebsi European Blockchain

EBSI, explained – first edition

What are the different chapters of this first edition?

01.

Verifiable Credentials Explained

02.

Verifiable Credentials in action

03.

Decentralised Identifiers (DID) Methods

04.

Digital Identity

05.

Issuers Trust Model

06.

Open ID Connect for Verifiable Credentials

07.

Digital Wallets

05. EBSI Trust Models explained – Index

What are you going to learn in this chapter?

05.1

What are the most common Trust Models of Issuers?

05.2

How does EBSI's Issuers Trust Model work?

05.3

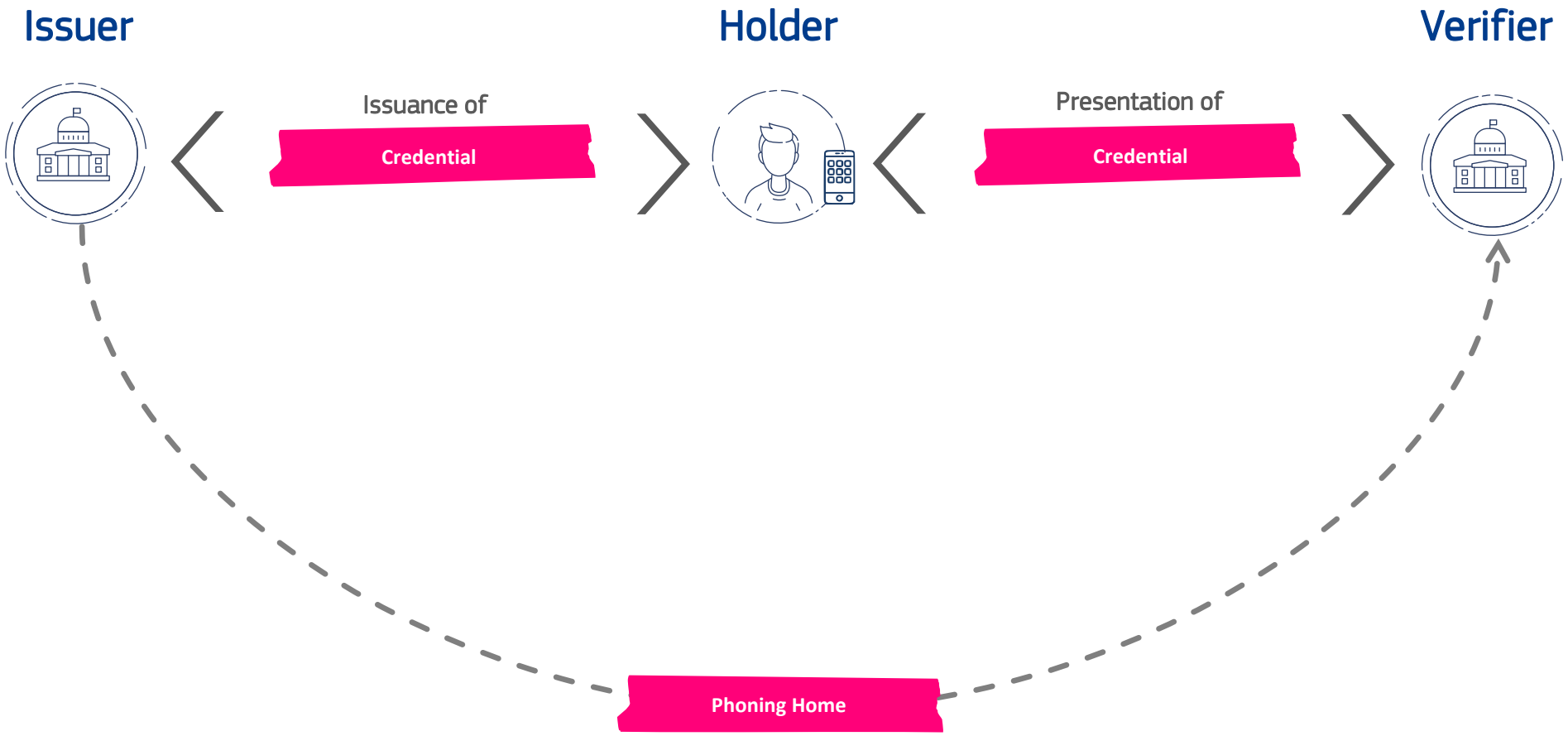
What are the benefits of EBSI's Issuers Trust Model?

05.1

What are the most common Trust Models of Issuers?

The classical trust model for Issuers

Classic solutions often require Verifiers to contact Issuers in order to ensure that the information they receive from Holders can be trusted. This pattern is called “phoning home”.



The “Phoning Home” problem

The need to “phone home” creates several challenges.

Challenge 01

Technical burdens

It places a technical burden on the credential Issuer, who needs to create and maintain APIs available to Verifiers and ensure that connectivity is available 24x7.

Challenge 02

Operational burdens

It requires the Verifier to create and maintain calls to all those APIs from every credential Issuer. In an open credential ecosystem, this could involve hundreds or thousands of integrations for every relying party.

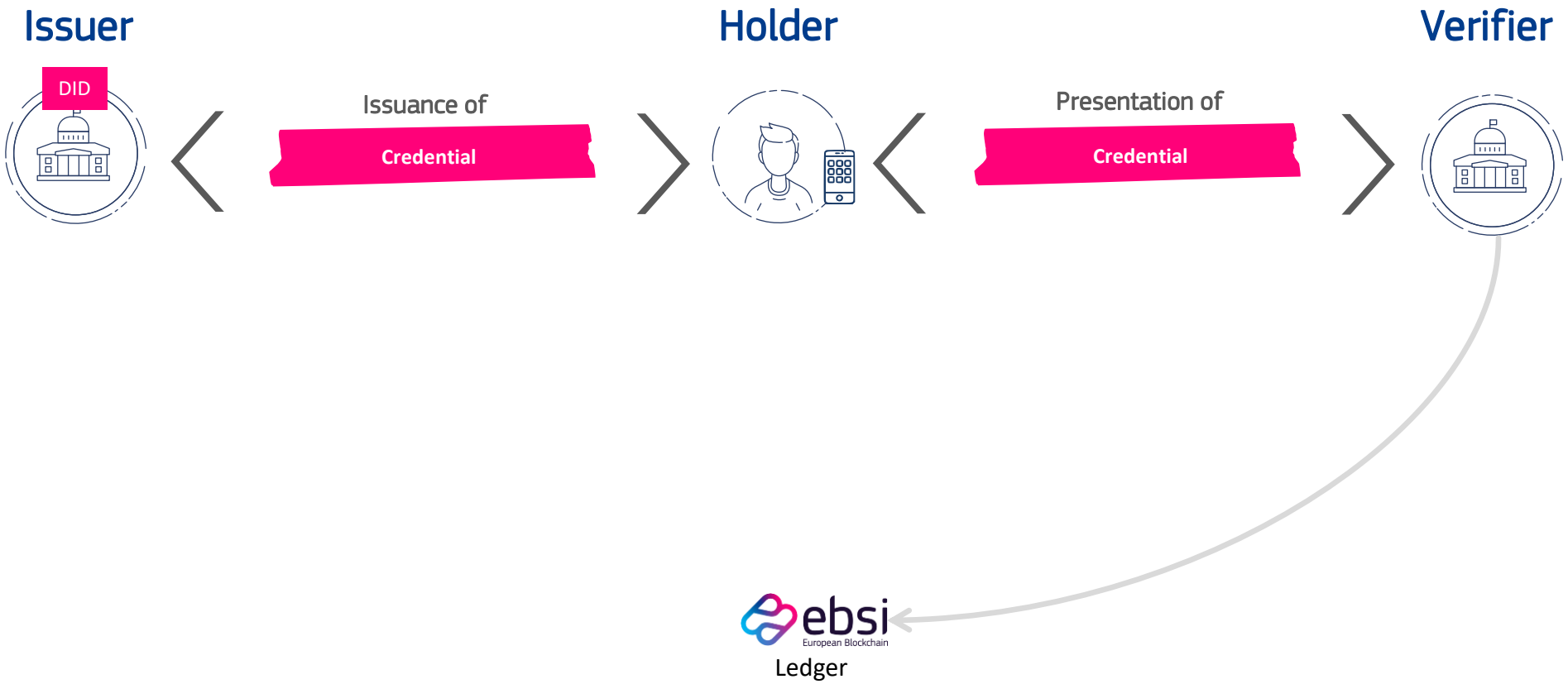
Challenge 03

Privacy challenges

It causes privacy challenges because it provides a way for issuers and Verifiers to correlate an identity holder’s usage of a credential across domains.

A new trust model for Issuers

According to EBSI's Verifiable Credentials model, EBSI enables Verifiers to trust Issuers without "Phoning home". Instead, Verifiers can retrieve the information required to trust Issuers from EBSI's ledger. This chapter provides detailed information about how this is achieved.



Conceptual Trust Models of Issuers that avoid “phoning home”

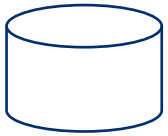
There are three basic Trust Models of Issuers of Verifiable Credentials, these models can be combined.

Scalability, flexibility and interoperability

Centralised Trust Model

For example:

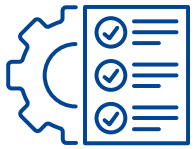
Certificates e.g. managed PKI



Federated Trust Model

For example:

Trusted Lists (*)



Distributed Trust Model

For example:

ebsi European Blockchain **Ledger**

- Public Keys of Issuers
- Registry of Issuers
- Trusted Schemas Registry

The **eIDAS Regulation** introduced the concept of Trusted List and the Commission Implementing Decision (EU) 2015/1505 specifies its technical specifications: https://europa.eu/!GRyHFF

How does EBSI's distributed Trust Model compare to others?

Trust models relevant in a C2G or C2B setting.

Centralised and Federated trust models usually rely on X.509 Certificates

This is hierarchical and not that flexible, as it requires many roles:

- **Certificate Authority** (CA) which stores, issues and signs the digital certificates.
- **Registration Authority** (RA) which verifies the identity of entities requesting their digital certificates to be stored at the CA.
- **Validation Authority** (VA) which can provide information for validation on behalf of the CA.
- **Distribution Authority** (DA) which is responsible for the distribution of certificates.

EBSI's distributed trust model leverages blockchain and DIDs

The use of DIDs alongside blockchain enables decentralisation and greater flexibility. Only two roles are required:

- **Trusted Accreditation Organisation (TAO)** verifies, accredits and manages the entities, i.e. Trusted Issuers, that issue electronic documents.
- **Trusted Issuer (TI)** is responsible to issue certain types of electronic documents and to manage their signing keys with the support of blockchain. In technical terms, it manages a DID document.

05.2

How does EBSI’s Issuers Trust Model work?

Key actors of EBSI's Issuers Trust Model

What are the key actors of EBSI's Issuers Trust Model?

Trusted Accreditation Organisation (TAO)

TAOs are the organisations responsible for **accrediting Trusted Issuers**, of a specific sector/ domain in a specific geography, to issue certain types of Verifiable Credentials (VCs).

For example, in the education domain, **the Ministry of Education of a Country** is responsible for **accrediting the Universities of that country**. TAOs also **register the Trusted Schemas associated to the Verifiable Credential,** e.g. Diploma.

EBSI Ledger

EBSI acts as a **public registry of Issuers, containing the list of trusted Legal Entities that are accredited by TAOs to issue certain types of credentials**. In other words, accredited entities become Trusted Issuers via a simple accreditation process.

For example, in the education sector, in addition to the DID documents of registered Universities, EBSI makes available to Verifiers the accreditation given by a TAO, itself a Verifiable Credential, and the link to the associated Trusted Schema.

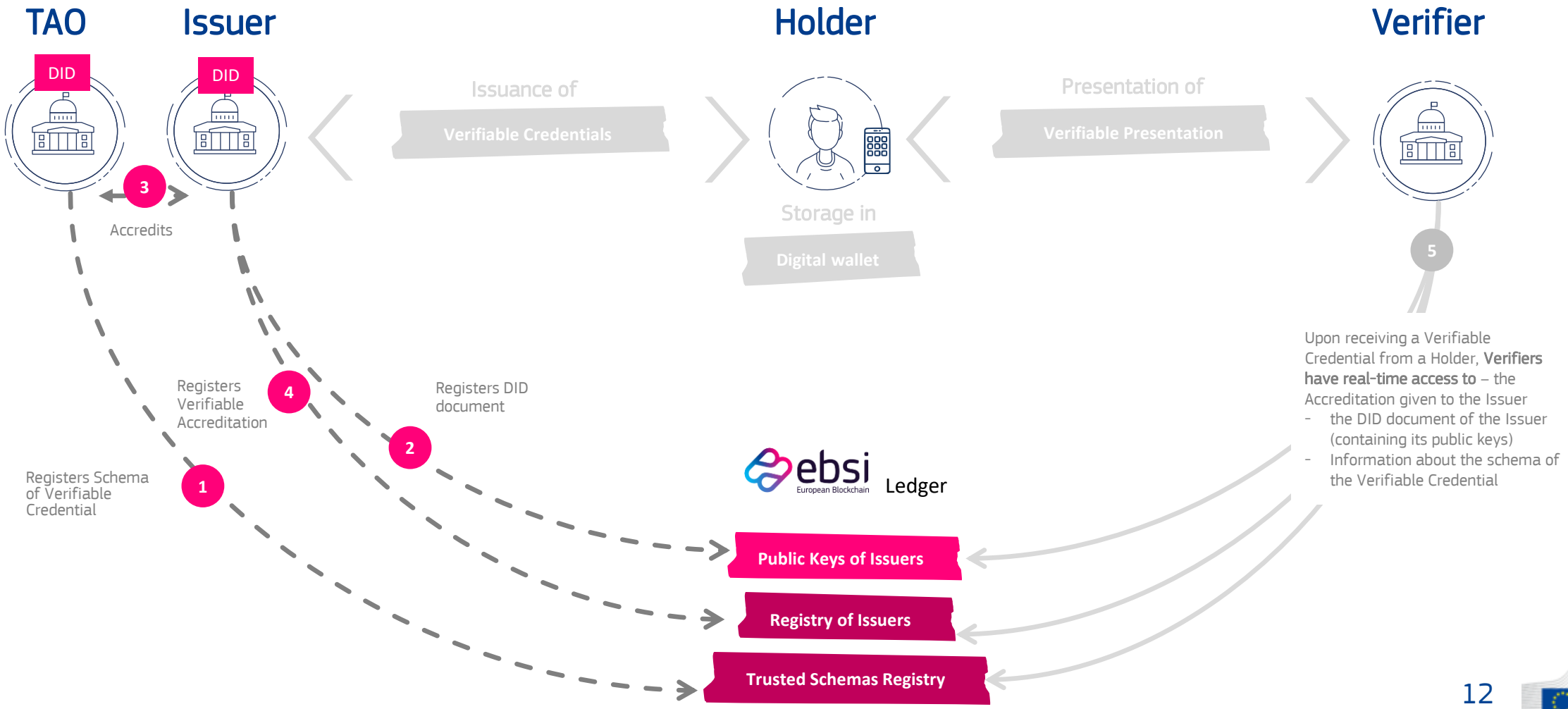
Furthermore, EBSI also makes available **the schemas of the Verifiable Credentials**. A schema supports the verification p**rocess and ensures that Issuers respect the agreed data models defined by each domain**.

Trusted Issuers (TI)

The **legal entities authorised to issue certain types of credentials**, e.g. A university is trusted to issue diplomas according to a specific Trusted Schema.

How to establish trust between Issuers and Verifiers?

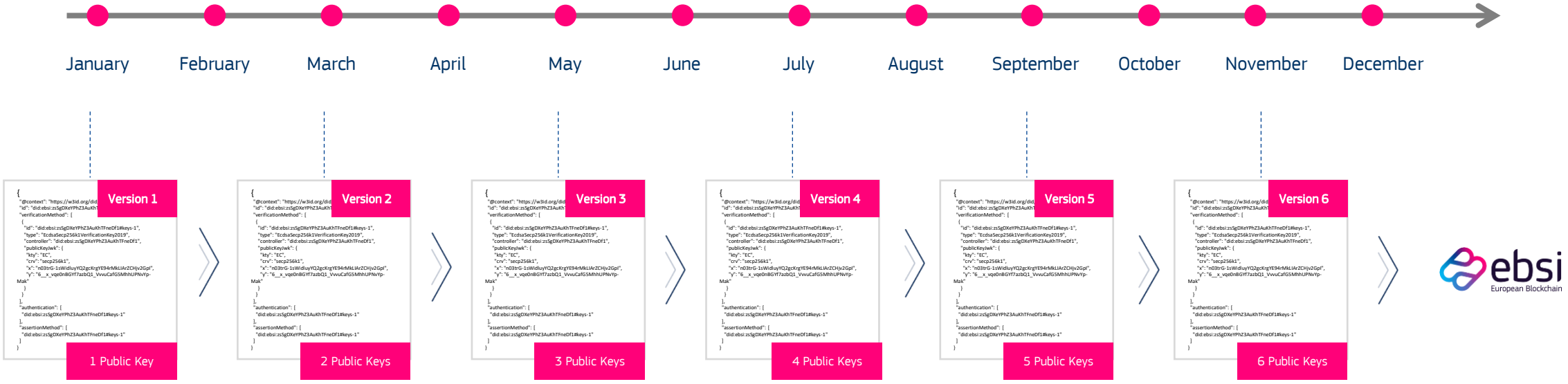
Understanding trust establishment in EBSI where numbers explain the sequence of events



Issuers can then manage their keys independently of the TAO

Once accredited, EBSI enables Issuers to manage their keys, according to EBSI's DID method, independently of the TAO

By rotating/updating keys frequently, Issuers **minimise the impact of an eventual compromise of their (private) key as less Verifiable Credentials will be signed with the same key**. Technically speaking, the use of DIDs and DID documents enables Issuers to rotate their keys, i.e., to update their cryptographic keys regularly (e.g. every other month) without impacting the Verifiers as they can easily retrieve the right version of the DID document from EBSI. This enables a much **smoother and secure management of keys in large ecosystems**. Issuers can have multiple active keys bound to their DID.



In this case, the Issuer decides to update its keys every other month. This is done by registering a new version of the (Issuer's) DID document on EBSI. Each version will therefore contain an additional public key. The Verifier knows the DID of the Issuer and therefore it can resolve the latest DID Document from EBSI with the updated keypair.

What is registered on the EBSI ledger?

What is registered on the EBSI ledger?

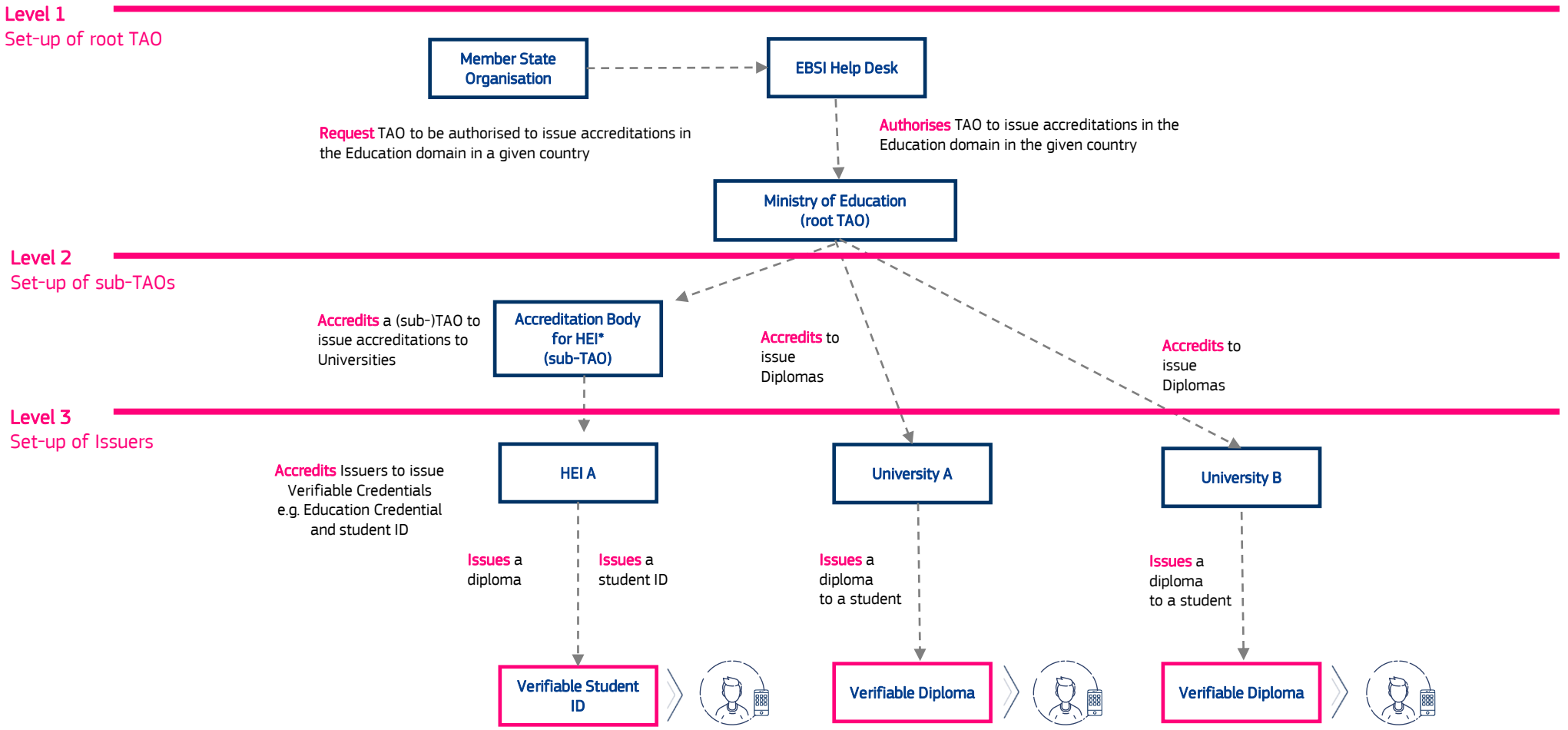
	Registry of Issuers	Trusted Schemas Registry

Trusted Accreditation Organisations (TAO)	• **DID and DID Document of TAO**
	• **TAO's Verifiable Authorisation**
	• **TAO's Verifiable Accreditation** (including reference to DID, applicable jurisdiction & organisations they are allowed to accredit for which VC(s), and corresponding schema(s)).
		• **Accreditation Credential schema** – describes data model for:
		  • Organisations they are allowed to accredit;
		  • Applicable jurisdiction;
		  • type of Verifiable Credential.

Trusted Issuers (TI)	• **DID and Document of Trusted Issuer**
	• **Issuer's Verifiable Accreditation** (including reference to DID, VCs they are allowed to issue and applicable jurisdiction, and corresponding schema).
		• **Verifiable Credential schema** – describes data model for:
		  Verifiable Credentials they are allowed to issue.
		  Note: the VC schema is determined at Use case/policy level.

How to setup EBSI's (multilevel) Issuers Trust Model?

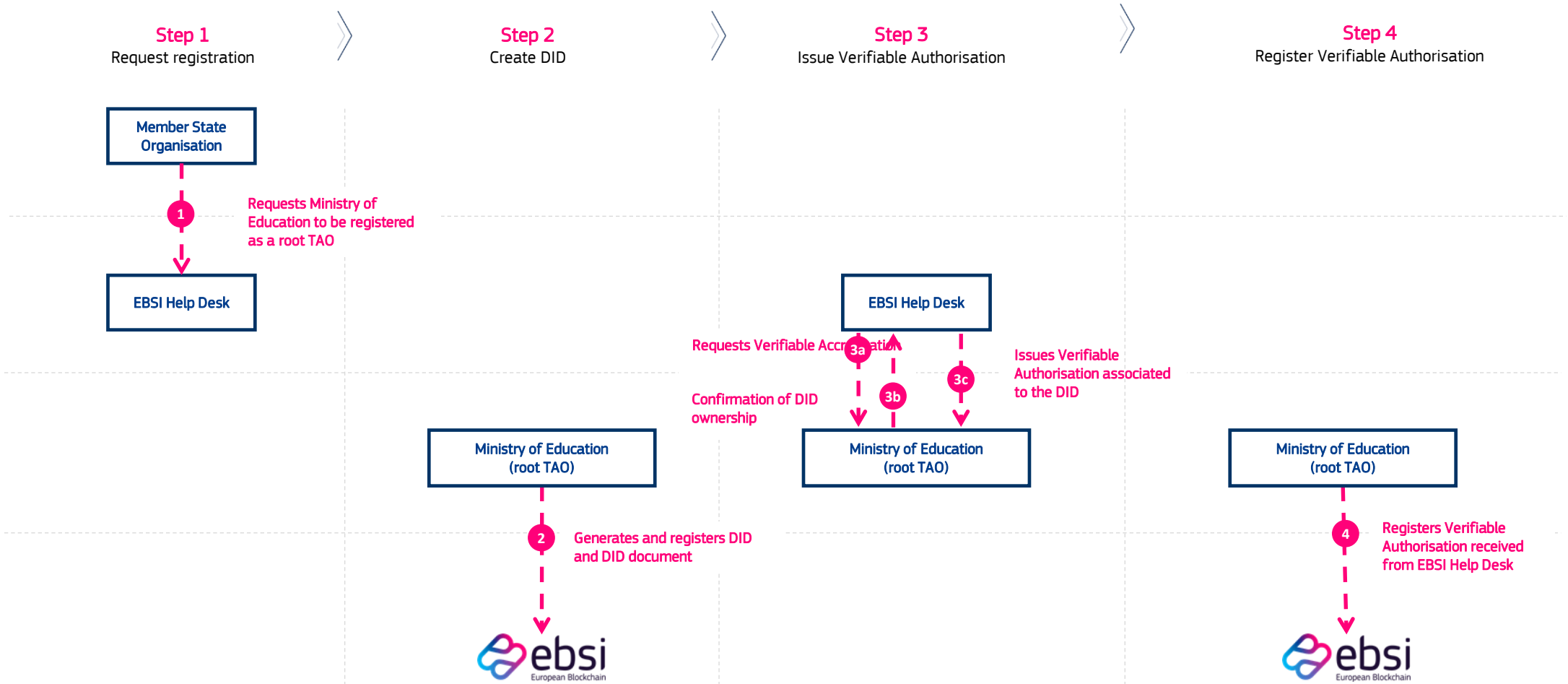
Example: Education domain in Member State X



* Higher Education Institution

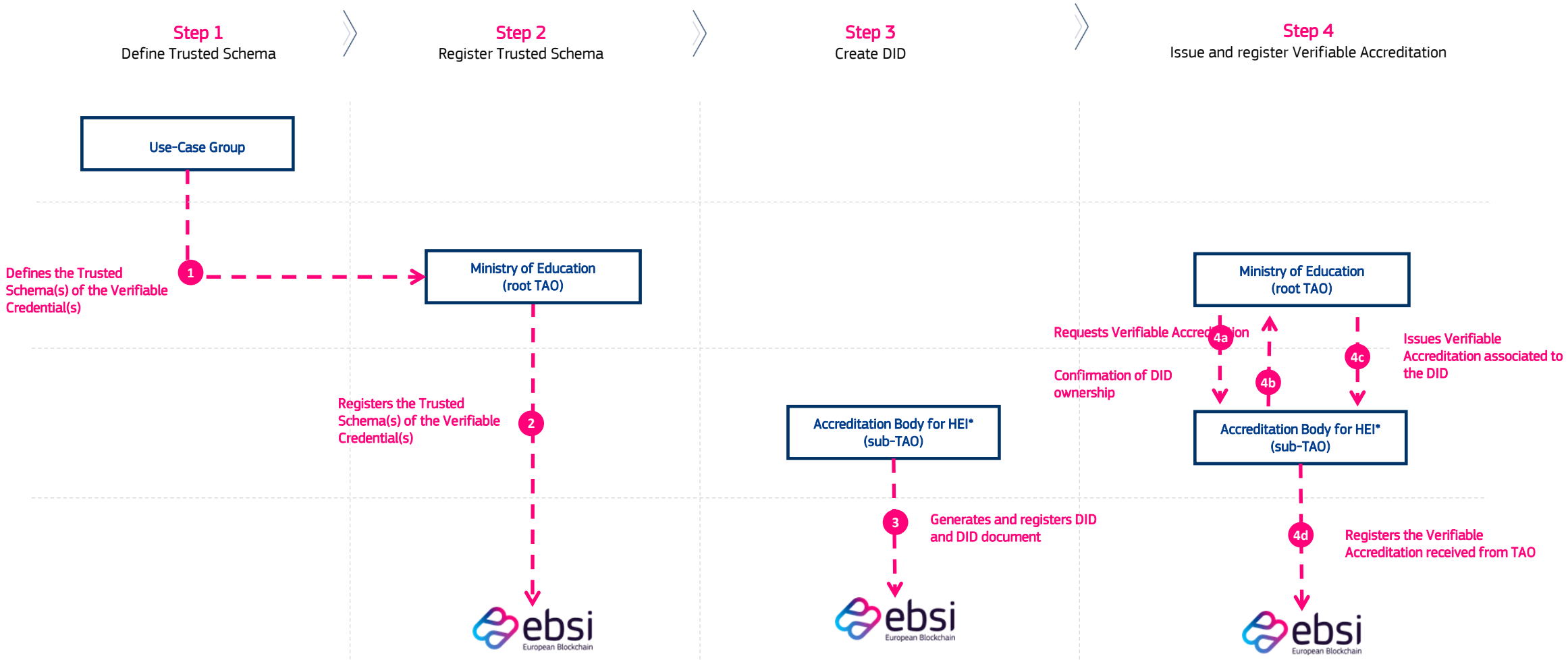
Workflow associated to Level 1 - Set-up of root TAO

Onboarding of root TAO



Workflow associated to Level 2 - Set-up of (sub-)TAO

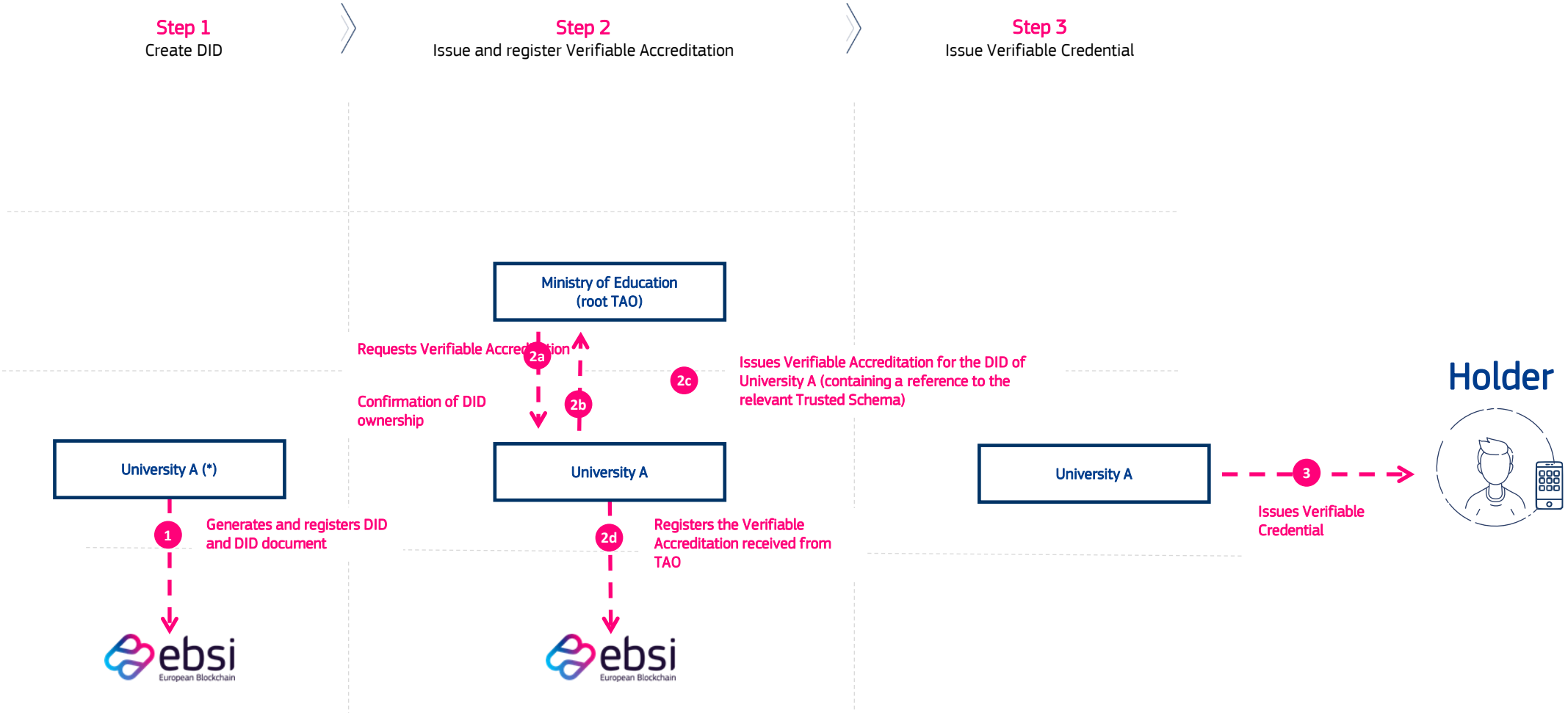
Onboarding of (sub-)TAOs, this is optional



* Higher Education Institution

Workflow associated to Level 3 - Set-up of Issuers

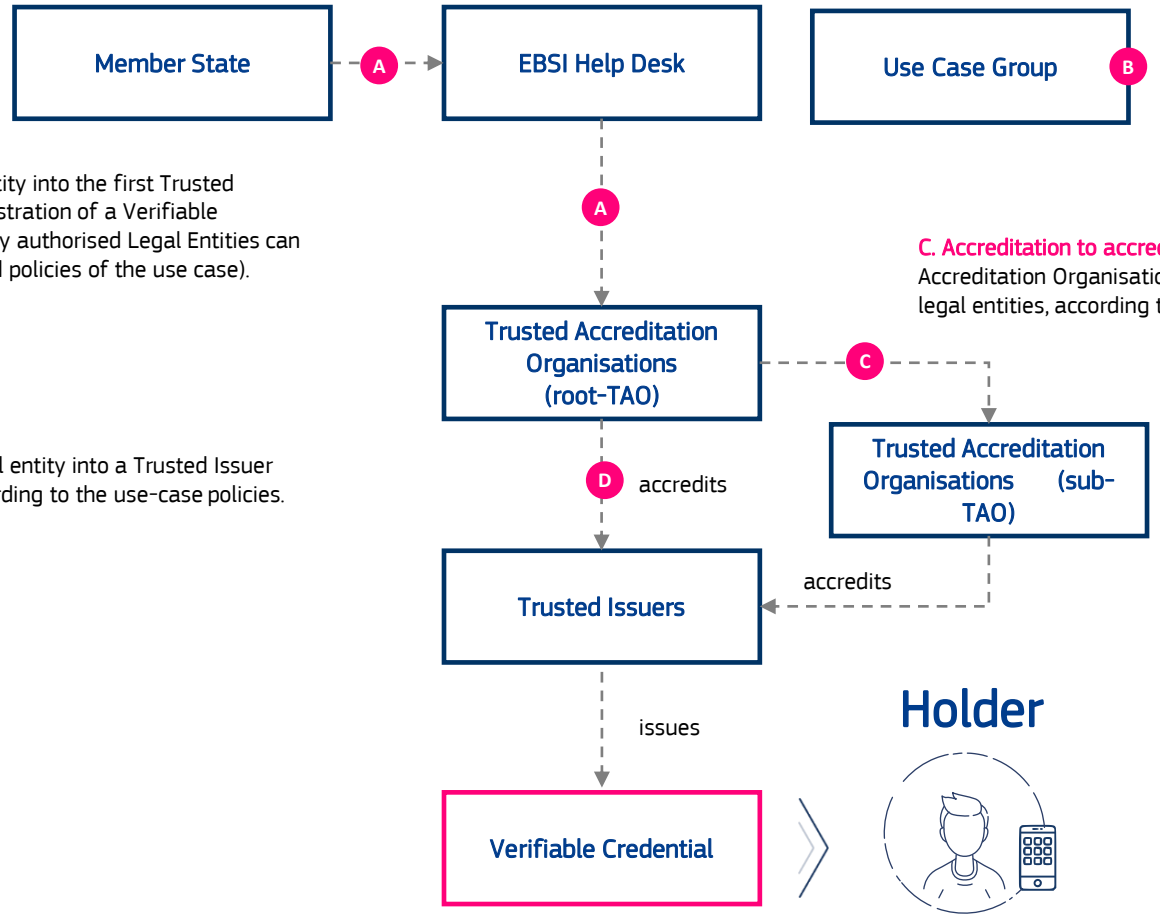
Onboarding of Issuers



* The onboarding of HEI A and University B would follow a similar process

Summary of EBSI Issuers' trust chain

Verifiable Accreditations tell us which Verifiable Credentials an issuer can issue and under which policies



A. Root-accreditation promotes a legal entity into the first Trusted Accreditation Organisation (TAO). The registration of a Verifiable Authorisation starts a new trust chain. Only authorised Legal Entities can accredit others (according to the rules and policies of the use case).

B. Defines the Trusted Schemas of the specific domain

C. Accreditation to accredit promotes a legal entity into a Trusted Accreditation Organisation (sub-TAO) who can accredit other legal entities, according to the use-case policies.

D. Accreditation to attest promotes a legal entity into a Trusted Issuer who can issue Verifiable Credentials according to the use-case policies.

Technical note

On registration of Verifiable Authorisations and Verifiable Accreditations

TAO and Trusted Issuers register authorisations and accreditations on ebsi European Blockchain

Trusted Accreditation Organisation (TAO) or Trusted Issuer (TI)

Step I
Present Verifiable Authorisation or Accreditation

Step II
Receive access token

Step III
Sign blockchain transaction

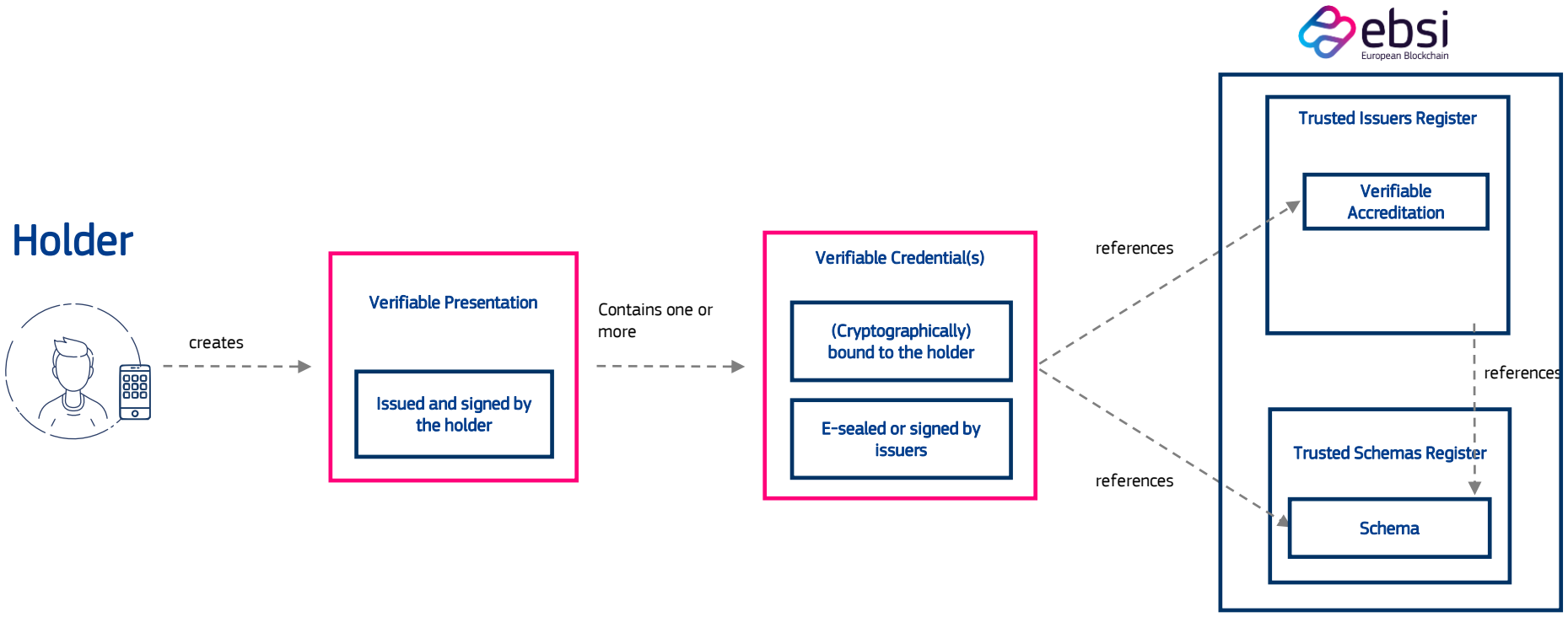
Step IV
Submit the signed transaction with access token

Authorisation API
API: /authorisation/v2/siop-sessions
link

Trusted Issuers Registry API
API: trusted-issuers-registry/v3/jsonrpc
Method: insertIssuer, updateIssuer
link

What happens when the trust chain is set up?

Once the chain is set-up, EBSI enables Verifiers to easily verify whether the Issuer of a VC can be trusted



05.3

What are the benefits of the EBSI Issuers Trust Model?

A design that supports multiple trust-chains with use-case specific structure and policies

EBSI has support for multiple trust-chains

As explained in the example

Accredits one or more TAOs and Trusted Issuers, according to the Social Security policies, similar to the education domain

Benefits of the EBSI's distributed Trust Model

Easy to manage and to verify by design

01

Easy to manage

Designed in a way that is easy to manage for the Trusted Accreditation Organisations (TAOs) and the Issuers.

02

Easy to verify

Designed in a way that is easy for many verifiers to easily check the authenticity of information.

03

Difficult to fake

Designed in a way that prohibits their copying and duplication.

Want to know more?

Key resources

Explore EBSI

Explore the EBSI website

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

Discover the specs

Discover the EBSI Playbook

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

Watch the demos

Watch the EBSI Demo Day

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

https://ec.europa.eu/ebsi