EBSI-VECTOR
Education and work reloaded

D3.7: Specification for the business registries on EBSI and pilot scenarios

Project title:	**EBSI-VECTOR** - EBSI enabled VErifiable Credentials & Trusted Organisations Registries
Grant Agreement No.	101102512 - DIGITAL-2022-DEPLOY-02-EBSI-SERVICES
Deliverable Title	D3.7: Specification for the business registries on EBSI and pilot scenarios
Version:	1.1
Date:	05/07/2024
Responsible Partner:	IDunion SCE
Authors:	Christian Klugow (IDunion SCE), Jonas Žalinkevicius (SKS)
Contributing Partners:	Goldman, INAIL, Hashnet, NASK, Bolagsverket, BRC
Reviewers:	Philipp Friedl (DRV-Bund) Tadej Slapnik , Tali Rezun (Hashnet)
Dissemination Level:	PU – Public

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Document Change History

Version	Date	Author (organisation)	Description
0.1	16/01/2024	Christian Klugow (IDunion SCE), Jonas Zalinkevicius (SKS), et. al.	Scope, Data model, BPMN Diagram, Sequential flows
0.2	17/01/2024	Christian Klugow (IDUnion SCE)	Draft for internal review
0.3	20/02/2024	EBSI-VECTOR: Task 3.3 participants	Internal review among task members finished
0.4	16/04/2024	EBSI-Vector: Task 3.3 participants	Pilot scenario described, external review finished
0.5	26/04/2024	DRV-Bund and IDunion	Final review completed
1.0	30/04/2024	IDUnion	Final release
1.1	05/07/2024	Christian Klugow (IDunion SCE)	Response to feedback from external experts • Update on 4.3.7 • New: Annex II

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

List of Figures

List of Tables

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

List of Terms and Abbreviations

Terms and Abbreviations	Definition
Business registry	○ can include records of legal entities such as companies or other corporations ○ can also include non-profit organizations, foundations, government bodies or sole entrepreneurs in a broader sense ○ Four types of business registries were identified in this document in chapter 3
Decentralized Identifier (DID)	an identifier that is created, owned, and (co-)controlled by the subject of the identifier (such as an individual or an entity) rather than being issued and managed by a centralized authority
DID Controller	○ refers to the entity or entities that have the authority to manage and control a particular DID. ○ is typically the entity that has the right to update, revoke, or otherwise manage the associated DID and its associated cryptographic keys.
DID Document	contains details about a DID, its associated cryptographic material, and metadata necessary for interaction
DID Subject	refers to the entity, whether it be an individual, organization, device, to which a Decentralized Identifier (DID) is assigned
Early Adopters Program	an initiative by the European Commission aimed at encouraging and supporting the adoption of the European Blockchain Service Infrastructure (EBSI)
EBSI	European Blockchain Service Infrastructure
EDIC	name of the future organization that operates the European Blockchain Service Infrastructure
Enterprise Wallet	a Digital Wallet design to serve the needs of legal entities in their role as issuer, holder and/or verifier

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Identity check	a technical gateway at which the identity of an individual or legal entity is confirmed by conducting a pre-defined process
Implementing developer	a generalist with IT know-how who is responsible for implementing and testing IT-processes
Issuer	a legal entity that issues Verifiable Credentials
Legal PID (ODI)	Legal Person identification data or Organizational Digital Identity – a data set uniquely identifying a legal entity
MVP	Minimum viable product - initial version of a product that includes only the essential features needed to satisfy early adopters and gather feedback
National (business) registry/ registrar	a public organization (registrar) that administers a data bank (registry) of legal entity records on behalf of an EU member state
Participant	any organization that is involved in the Early Adopters Program and that wants to pilot a use case
Qualified trust service provider (QTSP)	A certified organization that offers trust services
(Root-) TAO	Root Trusted Accreditation Organization - a public organization acting on behalf of an EU member state that sets up a trust environment in EBSI in a specific domain (business or social) under its authority.
Self-sovereign identity (SSI)	a concept and approach to digital identity management with the idea to give individuals more control over their own digital identities, allowing them to manage and share their personal information in a secure, private, and user-friendly manner
Trust environment	a Use Case specific concept that defines rules for technical transactions for invited participants promoting a secure and private issuing and verification process for Verifiable Credentials

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Trust Framework	a definition of roles and hierarchies provided by EBSI for Use Cases to design a specific trust environment
Trusted issuer	a legal entity issuing Verifiable Credentials within a certain Use Case declared as trustful by the root-TAO
Trusted verifier	a legal entity verifying Verifiable Credentials within a certain Use Case declared as trustful by the root-TAO
Verifiable Accreditation to accredit	a Verifiable Credential issued by a Root Trusted Accreditation Organisation (RTAO) to grant the Trusted Accreditation Organisation (TAO) the authority to accredit other entities to govern or issue domain-specific Verifiable Credentials. It serves as a foundational building block for the governance of the Trust Chain.[1]
Verifiable Accreditation to Attest	a Verifiable Credential issued by a Trusted Accreditation Organisation (TAO) to grant the Trusted Issuer (TI) the authority to issue domain-specific Verifiable Credentials.[2]
Verifiable Authorization	a Verifiable Credential issued by the root-TAO to a trusted issuer during the onboarding process that provides access to EBSI's infrastructure.[3]
Verifiable Presentation	The process of presenting a Verifiable Credential as holder to a Verifier.

[1] https://hub.ebsi.eu/vc-framework/trust-model/issuer-trust-model-v3
[2]https://hub.ebsi.eu/vc-framework/trust-model/issuer-trust-model-v3
[3] https://hub.ebsi.eu/vc-framework/trust-model/issuer-trust-model-v3

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

1 Executive Summary

This paper is a deliverable of the EU-funded consortium EBSI-VECTOR and describes specifications for an EBSI business registry. We explained how national business registries of EU member states can set up a trust environment as a Trusted Accreditation Organization and how they can issue and revoke digital Organizational Identities as short-lived Verifiable Credentials.

We made 8 proposals on how to improve the current EBSI documentation and wrote User Stories as functional requirements for Use Case designers in EBSI-VECTOR, for the EBSI development team and for developers of an Enterprise wallet. We recommend implementing a trusted verifier registry and a corresponding API to provide Use Case designers with a capability to control the number of verifiers for their Use Case. Moreover, we suggest to provide a solution for Trusted Issuers so that they get enabled to manage a status list for revocations.

We take our results as the basis for the subsequent piloting phase, in which we aim to pilot the business registry in several countries.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

2 Introduction

This document is an outcome of Task 3.3 conducted within the EU-funded consortium EBSI-VECTOR. Comprising 52 organizations from 20 countries, EBSI-VECTOR seeks to improve digital interactions of European citizens in both study and work domains, simplifying intricate and inefficient verification processes of non-machine-readable documents. The consortium is tasked with expanding the current capabilities of the European Blockchain Services Infrastructure (EBSI).

Task 3.3 specifically aims to define specifications for the EBSI implementation of business registries and to propose a procedure for digital organizational identities of legal entities being managed by using EBSI Registries and EBSI-conformant wallets. These specifications are a preparation for the subsequent piloting phase in which the recommended capabilities are implemented and tested with various national agencies in a cross-border context. The outlined functional requirements serve as a foundation for enhancing existing EBSI capabilities, including Enterprise wallets.

The participants within Task 3.3 comprise 12 identity experts representing 12 different EU member states. These experts bring diverse experiences to the table, with some possessing extensive familiarity with EBSI, while others have experimented with organizational identities at a national level. Additionally, some experts have already established communication channels with national commercial registries which improves chances for successful piloting.

This document begins by defining the scope of the business registry, identifying distinct types discussed in Chapter 3. Subsequently, an analysis of the current EBSI capabilities, as outlined in publicly available documentation, is presented in Chapter 4, also revealing opportunities for improving the documentation. Chapter 5 shifts focus to the onboarding procedure for legal entities within the EBSI trust framework, proposing an issuing process for legal PID (ODI) in Chapter 5. The necessary revocation mechanism for invalid legal PID (ODI) is introduced in Chapter 6. Building on those analyses, Chapter 7 outlines functional Requirements for Use Case Designers, EBSI developers, and Enterprise wallet providers, emphasizing EBSI use cases (Diploma and social security) and organizational identity issuance. User stories and context explanations are provided to enhance reader comprehension.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Chapter 8 presents 3 different versions of an EBSI architecture, considering Use Case adoption and the issuance of organizational identities. Lastly, chapter 9 engages with the legal environment and the pilot description.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3 Purpose and Scope

In this chapter, we will explore how we understand the term "business registry" in the underlying context. In general, business registries can be described as databases that record data about legal entities. Moreover, it is crucial to understand the specific purpose a business registry should serve to make proper design decisions. We identified relevant types of trusted sources that could be considered as business registries.

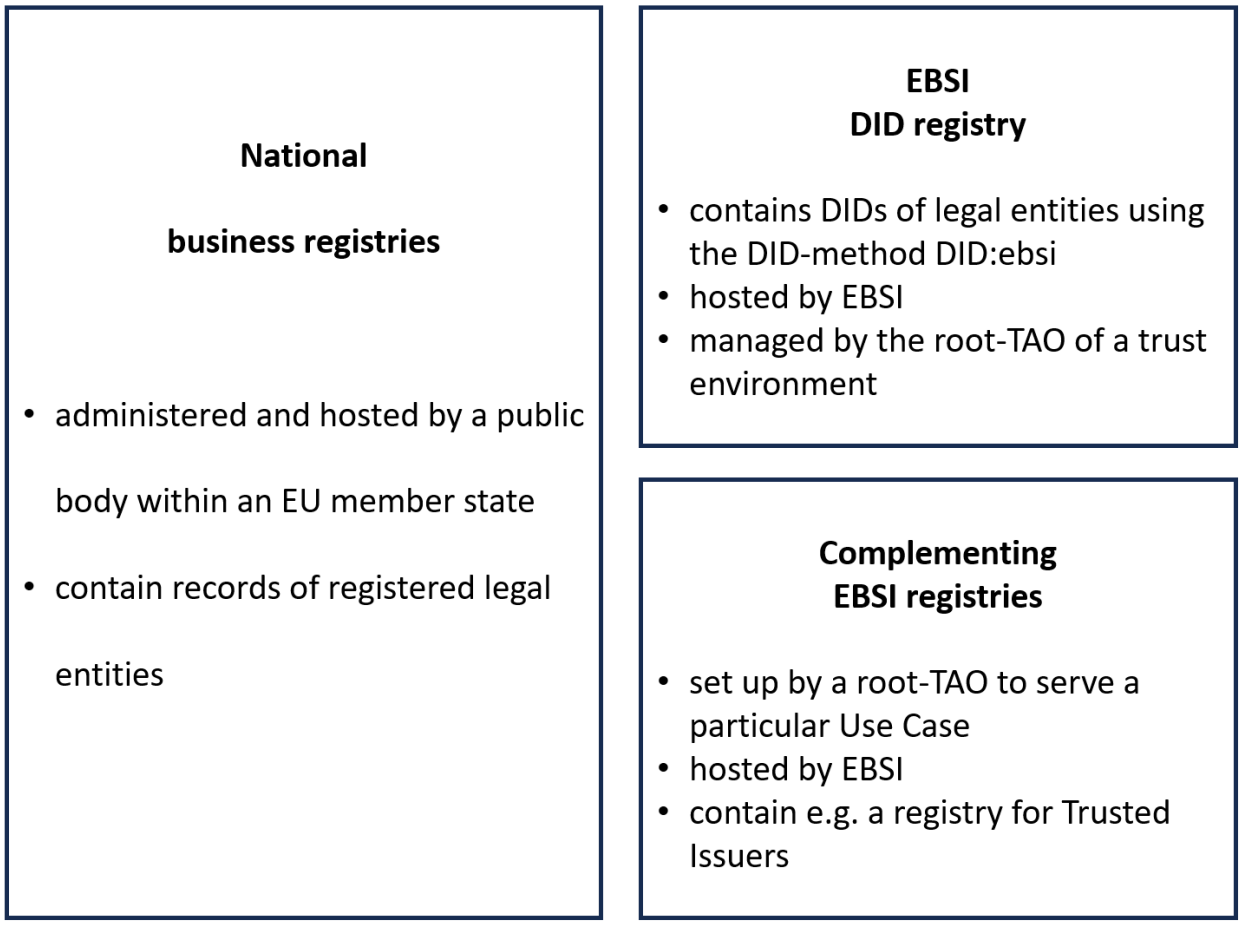


Figure 1: Types of trusted sources for business registries

3.1 National Business Registries in EU Member States

A national business registry refers to a centralized database maintained by a public institution of an EU member state. It records essential *primary* information about corporations (and for some

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

countries also about public authorities, associations, partnerships and sole proprietors) operating within their national jurisdiction. These registries play a crucial role in promoting transparency and legal compliance. They typically include details such as company names, registration dates, responsible director and financial statements. The purpose is to provide stakeholders, including investors and the public, with reliable information about the legal status and financial health of businesses. Generally, the recorded information is used to prove the existence of a legal entity including e.g. the place of business and the names of the directors. This information becomes very relevant in the case of liabilities that result from business transactions.

3.2 The EBSI DID Registry

The DID registry is a component of the European Blockchain Services Infrastructure (EBSI). The registry is operated on a distributed ledger and contains two essential information about legal entities:

- A DID[4] as a decentralized identifier referring to a legal entity as DID-subject using the DID-method DID:ebsi
- A DID document with DID-related information like the DID-controller and its associated public key

In this context, the EBSI DID registry owns the property of being a database for decentralized identifiers associated with legal entities regardless of their country of origin. Its purpose is to enhance trust, security and efficiency in digital cross-border transactions by enabling businesses to establish and manage their digital identities in a tamper-proof manner.

3.3 Complementing registries within the EBSI trust framework

The European Blockchain Service Infrastructure comes along with an integrated *trust framework*. This framework is applied so that each use case can set up a separate *trust environment*. A trust environment for a particular use case must be set up by a *Root Trusted Accreditation Organization* (root-TAO), which usually is a public institution within a European member state[5]. Once onboarded as root-TAO by the EBSI support office a root-TAO is enabled to assign sub-

[4] For details about DIDs, DID documents, DID-subjects and DID-controllers, please consult the DID specifications: https://www.w3.org/TR/did-core/
[5] https://hub.ebsi.eu/get-started/design/trust-chain

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

TAOs[6] (acting on behalf of the root-TAO) and create the following registry entries for their use case specific trust ecosystem:

- Trusted Schema Registry to define use case specific schemas[7]
- Trusted Issuer Registry to restrict the issuance of trusted schemas[8]
- Trusted Policies Registry to refer to use case specific policies[9]

The above-mentioned registries are already implemented. Moreover, we recommend extending that list by the following registry:

- Trusted verifier registry to enable TAOs to (optionally) whitelist legal entities that are authorized to conduct verifications within a certain trust environment (see chapter 7.2)

7.2Managed by TAOs, the Trusted Issuer registry and the trusted verifier registry are set up to serve a specific trust environment for a certain use case. Legal entities that are included in these registries gain predefined rights within a managed trust environment.

[6] Please note that we will continue using to term root-TAO in this document for the simplicity reasons.
[7] https://hub.ebsi.eu/apis/pilot/trusted-schemas-registry
[8] https://hub.ebsi.eu/apis/pilot/trusted-issuers-registry
[9] https://hub.ebsi.eu/apis/pilot/trusted-policies-registry

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4 Establishing a Use Case specific EBSI trust environment

The onboarding process for interested organizations that want to adopt the EBSI trust framework for a specific Use Case are well described[10]. As of early 2024, participants can apply for the new *Early Adopters Program* to pilot their Use Cases[11].

Setting up a Use Case for mass adoption requires extensive preparation. EBSI offers different levels of support based on a self-assessment conducted by the applying participants. This self-assessment is part of 15 questions[12] that participants need to answer before submitting their application for the *Early Adopters Program*. Once the application is reviewed by EBSI, qualified Use Cases for mass adoption will run through a three-stage process:

4.1 Discovery & Design stage

During the discovery stage, all belonging organizations that jointly want to set up a joint Use Case within the Early Adopters Program assemble for a kickoff-meeting in which at least the following aspects are agreed for the Use Case implementation:

1) Every organization participating in the kickoff-workshop is willing to get actively involved to pilot the underlying Use Case.
2) Every organization participating in the kickoff-workshop agrees how the trust environment should be set up and they agree on 1 root-TAO.
3) All open questions are collected and every organization is assigned to at least 1 working group to clarify these questions within the Design stage.

During the Design stage, the organizations will create a comprehensive solution design that describes detailed properties being necessary to implement the Use Case. EBSI offers guidelines for these descriptions[13].

[10] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Early+Adopters
[11] Please note, a public institution must be established as root-TAO for every Use Case. However, the root-TAO does not need to be the organization submitting the application for the Early Adopters program.
[12] https://ec.europa.eu/eusurvey/runner/EBSI-Application-Form
[13] https://hub.ebsi.eu/get-started/define

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4.2 Building stage

During the Building stage, the organizations are asked to build the solution they designed following the EBSI guidelines[14]. Doing so, they need to take the following steps.

1) **Onboarding an organization as root-TAO to start a new trust environment:** Due to the superior importance of the root-TAO for the to-be-established trust environment, the onboarding process involves close interactions with the EBSI Organization:
    a) Open a support-ticket at the EBSI Help Desk[15].
    b) Fill in a survey and send the e-signed document to EBSI Help Desk.
    c) Follow technical instructions provided by the EBSI Help Desk.
    d) Download an EBSI-conformant Enterprise wallet that can *Accredit & Authorize*[16]*.*
        - Alternatively, organizations can create own wallet solution and conduct a conformance test if the desired wallet is not listed[17].
    e) Create a DID and a DID document using the DID-scheme DID:ebsi[18].
    f) Submit a legal package for pilot as *Application Service Provider* to EBSI Help Desk[19].
    g) Request and obtain a *Verifiable Authorization* as Verifiable Credential from EBSI Help Desk.
    h) Present the *Verifiable Authorization* to the EBSI Authorization API[20] and request an access token to write DID and DID document on the DID Registry.
    i) Write DID and DID document to the EBSI DID registry.
2) **Onboarding Trusted Issuers within the trust environment**: Trusted Issuers are legal entities that are authorized to issue Verifiable Credentials following a Schema which was defined by a Trusted Accreditation Organization (TAO). Root-TAOs can build solutions that enable an efficient onboarding of Trusted Issuers (e.g. a Credential Issuer Service)[21]. In general, the following steps need to be conducted to onboard a trusted issuer:

[14] https://hub.ebsi.eu/get-started/build
[15] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Help+Desk
[16] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Conformant+wallets#find-your-wallet
[17] https://hub-test.ebsi.eu/wallet-conformance
[18] https://hub.ebsi.eu/tools/cli/register-trusted-issuer
[19] https://ec.europa.eu/eusurvey/runner/EBSI_Pilot_acceptance_form
[20] https://hub.ebsi.eu/apis/pilot/authorisation/v3
[21] https://hub.ebsi.eu/get-started/build/rtao

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

a) The trusted legal entity downloads and onboards to an EBSI-conformant Enterprise-Wallet with issuing capabilities[22].
b) The trusted legal entity creates a DID and a DID document.
c) The root-TAO issues a *Verifiable Authorization* as Verifiable Credential upon request to a trusted legal entity[23].
d) The Trusted legal entity
   - presents the *Verifiable Authorization* to the EBSI Authorization API[24] and requests an access token
   - to write DID and DID document into the EBSI DID Registry.
e) The root-TAO issues *Verifiable Accreditation to Attest* as Verifiable Credential upon request to a trusted legal entity.
f) The Trusted legal entity
   - presents the *Verifiable Accreditation to Attest to the* EBSI Authorization API and requests an access token
   - to write *Verifiable Accreditation* into the Trusted Issuers Registry
g) The Trusted legal entity has then become a trusted issuer within the trust environment that was set up by the root-TAO.

3) **Onboarding issuers outside a trust environment:** EBSI offers a self-registration option for issuers which are not part of an implemented trust environment[25]. Self-registered issuers underly certain technical constraints[26].
4) **Adding records to the Trusted Schema Registry:** EBSI offers a documentation for a *Trusted Schema Registry API v2*[27]*.* It is mentioned that the API enables developers to register and update existing schemas as well as read and validate them. However, we were not able to find an explanation on how to register a new schema. Nevertheless, the documentation provides information on how to contact the EBSI Support – Service Desk[28].

[22] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Conformant+wallets
[23] https://hub.ebsi.eu/tools/cli/register-trusted-issuer
[24] https://hub.ebsi.eu/apis/pilot/authorisation/v3
[25] https://ec.europa.eu/eusurvey/runner/Pilot_self-registered_TI_request?surveylanguage=EN#
[26] EBSI provides a link to access these constraints. When we tested it, we were asked to confirm them. However, we were not able to access the description behind the provided link: https://ec.europa.eu/eusurvey/runner/Pilot_self-registered_TI_request?surveylanguage=EN#
[27] https://hub.ebsi.eu/apis/pilot/trusted-schemas-registry/v2
[28] https://ec.europa.eu/digital-building-blocks/tracker/plugins/servlet/desk/portal/11

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

5) **Using a Trusted Policy Registry:** The available EBSI documentation provides details on how to interact with an existing Trusted Policy Registry[29]. It explains how to obtain policies and users. However, it is neither explained what a user is in this context nor how to register a new policy. Developers are asked to contact the EBSI support – Service Desk[30].

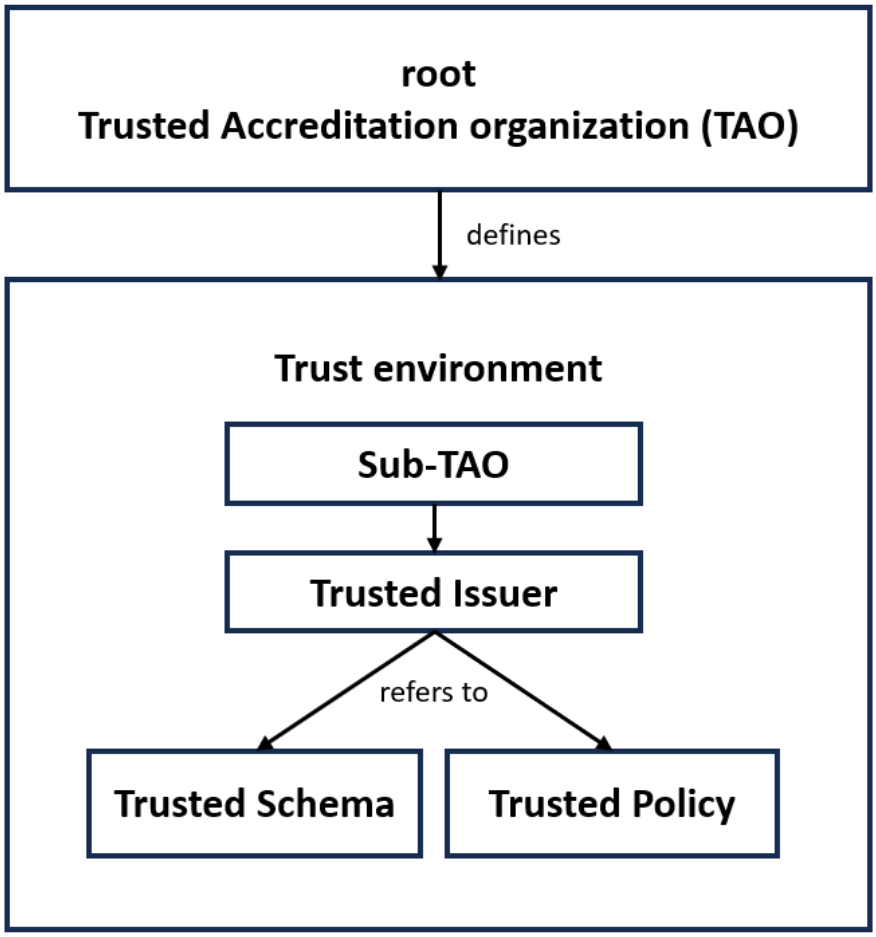


Figure 2: Definition of a trust environment

[29] https://hub.ebsi.eu/apis/pilot/trusted-policies-registry
[30] https://ec.europa.eu/digital-building-blocks/tracker/plugins/servlet/desk/portal/11

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4.3 Recommendations for improving the EBSI documentation

A comprehensive EBSI documentation plays a significant role in the adoption of the EBSI technology in various sectors. Domain-focused policymakers should find a well-defined process for building a new trust policy that is driven by legislation or sectorial needs. There should be clear definitions of used terms and processes. Implementers need to understand what must be developed and what EBSI API functions must be used. They need well-defined inputs and outputs and need to be educated on how to handle errors.

As this report aims to build functional requirements, this chapter will focus on developers' needs and will highlight our findings about drawbacks in the current EBSI documentation. There will be eight sub-chapters representing different problems and our recommendations on how to address them.

4.3.1 Improving root-TAO onboarding documentation

EBSI provides a well-structured and sophisticated documentation that helps to onboard a new trust environment with a root-TAO as the root of trust. It guides the user well through a step-by-step process to design an Identity Use Case. Nevertheless, we experienced difficulties understanding all the necessary actions and the correct sequential order implementing developers must undertake on behalf of the root-TAO to implement such a Use Case. Some important details are hidden within chapters that imply different explanations[31].

4.3.2 Explaining EBSI-specific terminology

Implementing developers need to learn EBSI-specific terms and their belonging context. E.g. issuers in a trust environment acquire rights about when they are able to present certain Verifiable Credentials to a certain EBSI API. These Verifiable Credentials are called *Verifiable Authorization, Verifiable Accreditation* and *Verifiable Attestation*. There is an EBSI glossary. However, due to the missing search function, it is not easy to find the glossary within the documentation. We recommend a learning module in which implementing developers can improve their knowledge of EBSI-terminology. This is crucial for the implementation since it avoids mistakes and improves communication among developers.

[31] E.g. The generation of a DID for Legal entities is hidden in the chapter Legal Entity DID resolver: https://hub.ebsi.eu/tools/libraries/ebsi-did-resolver

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4.3.3 Improving navigation

While each building block is well explained and there is an overall structure in place, we recommend guiding the implementing developers even more. This can be done e.g. by outlining an architecture showing all EBSI components on one graphic. Moreover, we recommend introducing a search function to better identify needed explanations by entering key words only. We also identified references to a confluence environment with restricted access[32] and recommend to either providing information to the implementing developers on how to access it or making the information publicly available.

4.3.4 Offering profound consulting

It is difficult to imagine that an implementing developer team will be able to harmonize the complexity of an identity Use Case with the complexity of the current EBSI documentation. We also realized that some essential onboarding information for root-TAOs is not publicly provided. This is for example the case for entering new records in the Trusted Policy or the Trusted Schema registry. While explanations about how to read information from the beforementioned registries are given, instructions about how to conduct entries are missing. Therefore, we conclude that profound consulting projects lead by knowledgeable EBSI experts will be needed for a successful Use Case onboarding with a new root-TAO.

4.3.5 Obtaining EBSI-conformant wallets

EBSI lists conformant digital Enterprise wallets that can be used by legal entities in the role of a root-TAO as well as for issuing and verifying Verifiable Credentials[33]. However, the provided URLs do not initiate a wallet onboarding process. Implementing developers will need to contact each listed wallet provider and initiate a rather sophisticated procurement process to obtain an acceptable solution for their Use Case. We recommend offering a better comparison between the listed Enterprise wallets and providing solutions for self-registration and automated onboarding.

[32]https://ec.europa.eu/digital-building-blocks/sites/display/BLOCKCHAININT/Issuers+trust+model+-+onboarding+and+accreditations
[33] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Conformant+wallets#find-your-wallet

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4.3.6 Offering Trusted Verifier Registry

To cover the business requirements of the Use Cases from Work Package 5 within EBSI-Vector, EBSI needs to introduce a Trusted Verifier Registry. Records within these registries need to be written by the root-TAO to allow only certain verifiers and wallet providers to verify and manage credentials that were created by using a Trusted Schema.

4.3.7 Including identity checks during the onboarding process

We envision a pan-European trust ecosystem where legal entities can hold and share their Organizational Digital Identity (ODI) with new business partners seamlessly. To realize this vision, a reliable and authoritative party must confirm the identity of the legal entity and issue the ODI. While it is likely that national business registries will serve as the authentic sources for the issuance process, the actual issuance may not necessarily be performed by these public authorities. Several configurations are conceivable, including:

- The national business registry directly issues the ODI
- A (qualified) Trust Service Provider (TSP) issues the ODI on behalf of a public authority
- A (qualified) Trust Service Provider issues the ODI independently as EAA using the national business registries in the European Members states as authentic source

With the establishment of the EDIC, there is now a governing body for decentralized ledger technology. Task 3.1 in the EBSI-VECTOR project analyzed the potential of EDIC becoming a Qualified Trust Service Provider (QTSP) for electronic ledgers as well. The analysis suggests that an electronic ledger offered by EDIC could serve as an alternative to or even replace the existing Trustlists according to Article 22 of eIDAS and ETSI TS 119 612, which is currently implemented in XML.

Besides maintaining the Trusted Issuer Registry, EDIC could also facilitate the registration for Relying Parties in accordance with Article 5b of eIDAS 2.0 by offering a trusted verifier registry. We assume that every relying party must provide a proof of existence to be included in that registry. Therefore, a new trust service for issuing ODI credentials is essential but currently not covered by (automated) trust services in Europe.

Given that nearly all use cases on EBSI will benefit from a confirmed identity of a legal person, and considering the importance of this for EBSI's scalability, we recommend that the EDIC:

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Provide these trust services directly
- Collaborate with partners who can offer this service on behalf of EDIC
- Advocate for the issuance of ODI at the EU membership level

To justify the investment required for the complex process of ODI issuance, it is critical to develop a sustainable business model. This model should outline the value proposition, revenue streams, and cost structure associated with the provision of ODI issuance services.

4.3.8 Reviewing the Section JSON Schemas Table

The Section JSON Schemas Table helps implementing developers to use pre-defined schemas and to adopt them into a Trusted Schema registry for a newly established trust environment. We recommend providing some context and guidelines to implementing developers how that table should be used. Moreover, we realized that some schemas share the same title and recommend a renaming for clarification.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

5 Onboarding Legal Entities for an established trust environment

Once a Trusted Issuer is set up for a specific trust environment, it can start issuing Verifiable Credentials for holders. This issuing process requires holders to own a digital wallet and to receive the Verifiable Credential properly. If the Verifiable Credential confirms attributes of a legal entity and it is supposed to be used in a productive business environment, then it is inevitable to conduct identity checks. An identity check is necessary e.g. to avoid that an issuer issues a legitimate Verifiable Credential to a wrong legal entity. To do so, the holder needs to confirm its identity to the issuer. For natural persons this will be the natural Person Identification Data (natural PID), consequently, for legal persons it will be the legal Person Identification Data (legal PID), or in other words, the Organizational Digital Identity (ODI).

We continue by assuming that a legal PID must be issued as Verifiable Credential so that digital identity Use Cases can scale to their full extent. As of 2024, different consortia in the European Union try to find a solution how a proper process can look like to issue a legal PID to a legal entity[34]. With reference to chapter 7.2. in deliverable D 3.1 from EBSI-VECTOR, we want to contribute to that work by providing the following proposal.

5.1 Proposal for an issuing process of a legal PID as a root-TAO

For this example, we imagine a natural person (legal entity representative) who applies for an Organizational Digital Identity (ODI) of a legal person. We assume that the EBSI Schema for legal entities[35] is used or that root-TAO successfully registered the schema for Legal-PID (ODI) in the Trusted Schema Registry.

The issuer of the legal PID MUST conduct the following identity checks:

- Assuring the identity of the company representative applying for the Legal PID (ODI)
- Assuring that the legal entity for the requested Legal PID (ODI) truly exists
- Assuring that the natural person is a legitimate representative of the legal entity

The three above-mentioned identity checks must be conducted to avoid misuse of the legal PID (ODI).

[34] https://eudiwalletconsortium.org/#
[35] https://hub.ebsi.eu/vc-framework/data-models/json-schemas

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

According to Article 45da of the current eIDAS 2.0 proposal[36], public bodies (or organizations that act on behalf of them) are legitimate issuers for legal PIDs. Hence, the application process for obtaining a legal PID is likely to be initiated at the beforementioned national commercial registries (see chapter 3.1).

5.2 Generation of an additional control anchor for a national business registry

National business registries act as authentic source to identify the legal representatives of an organization. They could initiate the onboarding procedure to the EBSI and register their DID and DID Document. However, they can neither control the lifecycle of provided permission to onboard nor can they suspend the enterprise wallet instance of an organization. Thus, we think that there is a need for an additional control mechanism which would allow to undertake certain legal actions, if necessary. This includes, i.e. disallowing the issuance of any VC due to the decision of a court while previously issued VCs should be left intact and the possibility to verify them using Trust model should remain. For this to achieve, national registries can host the enterprise wallet and control DID creation, access to it, etc. (see next chapter). While this solution could be desired for organisations not willing to handle Enterprise wallet software for others it could not be feasible due to the need to have deep integration between their backend systems and an Enterprise wallet software or due to legal limitations in case an issuer is handling sensitive natural persons data that must remain on premises of an organisation.

Here is a possible solution that we think would provide an additional control to national registries and yet keep the self-sovereignty nature of EBSI ecosystem for the issuer. It should be noted that enterprise wallet software can be tailor-made by an issuer (if it is complying with the EBSI rules), thus it would be unreasonable to impose rules where wallet software must check legal status with national registry before issuance of VC. Developers might not respect those or build a conditional override to pass compliance tests and keep the possibility of issuance bypassing the national registry enforcement. Such control anchor should be implemented within EBSI Trust framework and be kept outside of Enterprise wallet functionality. To achieve this EBSI team must implement a new check point before allowing to anchor issued VC DID to the registry. So, if the national registry revokes an organization either through DID revocation method or some sort of

[36] https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

smart contract, issuers should not get access to write to a DID registry thus prohibiting to issue VC as it won't be valid.

5.3 Generation of DID and DID document at a national business registry

We assume that a legal entity representative is not able to self-create a DID without further guidance. While tools for DID generations are publicly available and an integral part of a regular onboarding process for (most) digital wallets, we recommend incorporating that feature at websites hosted by national business registries. This way, national business registries can log the generation of DID and DID document and can define themselves as (additional) DID controller.

This approach offers the distinct advantage of a joined management of DID documents that refer to legal entities. By designating national registrars as DID controllers, it allows them to undertake certain legal binding initiatives if necessary. This control reflects reality as the existence of a legal entity is intrinsically tied to the legal framework of the specific jurisdiction in which they are established. In contrast to Use Cases for natural persons, where external control of a DID document may not be desirable, for legal entities, it may ensure alignment with regulatory requirements and foster a more transparent and compliant integration within a trust environment. The generated DID gains a nature of being issued by the national registry to the legal entity while both, national registry and legal entity, are entitled to control it. Technically, the national registry remains in control to conduct changes in the DID document. This is e.g. relevant during a key recovery process[37]. Hence, integrating national registries as DID controllers do not only enhance the security and authenticity of identities but also strengthen the link between legal entities and their governing jurisdictions.

The following aspects of DID creation and control should be considered:

- DID documents and control over them can be updated without having to create a new DID. This can enable a legal entity to "take full control" of their DID, even if it was originally created via a business registry with the "joint management" approach described above. The inverse scenario is also possible: A DID that has been created independently by a legal entity can be updated to "share control" and begin "join management" with the business registry.

[37] https://www.w3.org/TR/did-core/#example-did-document-with-a-controller-property

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- DID creation supports an architecture called "client-managed secret mode"[38]. This means that the business registry could expose a DID create/update/deactivate API that simplifies and abstracts away all details of DID operations, but cryptographic key operations (signing) happen in a different component, such as an Enterprise wallet hosted by the legal entity. This makes management of the DIDs easy without sacrificing sovereign control of the keys.
- In order to express a binding between a DID and a legal entity, such information could potentially be included directly in the DID document (the "alsoKnownAs" property), or perhaps as a service endpoint that contains a Linked Verifiable Presentation[39] with additional information about the legal entity.
- In the interest of interoperability, multiple DID methods should be supported via a single consistent API, such as the one exposed by the Universal Registrar[40] or comparable tool.

Nevertheless, we must admit that we have not identified volunteering business registries to test our above-mentioned proposal. We recommend profound testing before implementation.

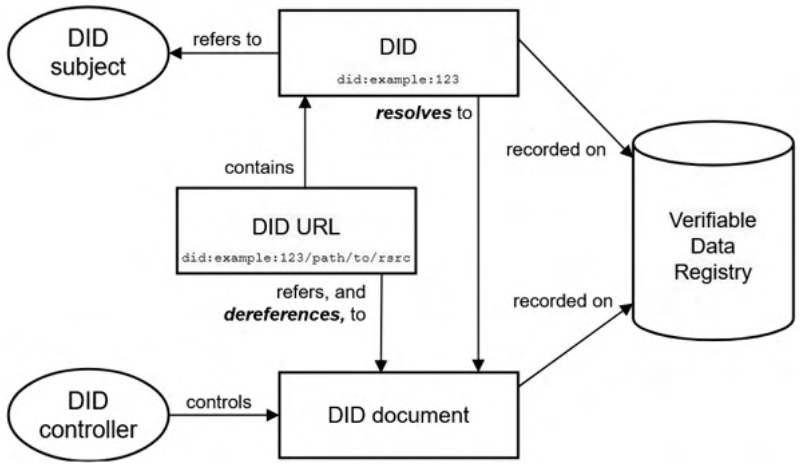


Figure 3: Overview of DID architecture and the relationship of the basic components

[38] https://identity.foundation/did-registration/#client-managed-secret-mode
[39] https://identity.foundation/linked-vp/
[40] https://uniregistrar.io/

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

5.4 Onboarding a legal entity for an existing trust environment

We continue by assuming that a national registrar is successfully onboarded as root-TAO and a legal entity has successfully generated a DID and a DID document within a digital wallet. For the sake of simplification, we assume that a legal entity wants to onboard to an established trust environment, e.g. for one of the following reasons:

- Proving its identity to other onboarded legal entities within the given trust environment to facilitate business processes.
- Issuing Product Passports as Verifiable Credentials for products the legal entity produces.
- Verifying certificates or social security documents as employer[41]

The following process describes the issuance process of a legal PID:

1) **Onboarding a legal entity to an Enterprise wallet**: The legal entity representative configures the wallet settings according to her specific needs.
2) **Identifying the identity of the legal entity representative:** The digital wallet guides the new user[42] through a qualified identity check with Level of Assurance high[43]. A Verifiable Credential is issued that confirms the identity of the new user.
3) **Requesting access to a trust environment:** Using the digital wallet, the natural person initiates the onboarding process on behalf of the legal entity. The natural person identity is proven by providing a natural PID as Verifiable Credential to the national registry.
4) **Matching natural PID with legal entity record:** The national registry accepts the proven identity of the natural person, queries the data record of the legal entity and validates that the natural person is a legitimate representative of the legal entity.
5) **Providing access to trust ecosystem**: The national registry issues *Verifiable Authorization* as Verifiable Credential to the digital wallet.
6) **Entering the trust ecosystem**: The legitimate entity representative uses the Verifiable Authorization to write DID and DID document into the EBSI DID Registry.

[41] Please note, as EBSI is currently designed as of early 2024, legal entities do not need to onboard to EBSI to be able to verify Verifiable Credentials. However, later on in this document we will recommend to introduce a Trusted Verifier Registry.
[42] In this case the new user is the legal entity representative of the legal entity obtaining a legal PID
[43] Level of Assurance high reduces the risk taken by a relying party / verifier to a minimum: https://id4d.worldbank.org/guide/levels-assurance-loas

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

The legal entity is now able to participate in the trust environment that was set up by the national registry as root-TAO. Following the process mentioned in chapter 4.2 the legal entity can be entered into the Trusted Issuer Registry and start issuing Verifiable Credentials.

Moreover, we assume that legal entities will need a Verifiable Credential to digitally proof their existence to their new business partners. This makes it necessary to issue a legal PID (ODI).

Following the above-mentioned procedure, the national registry has verified

- the identity of the natural person,
- the existence of the legal entity and
- the legitimate representation of the natural person to act on behalf of the legal entity.

Hence, it can now issue the legal PID (ODI) as Verifiable Credential into the Enterprise wallet. Please note, EBSI uses the terminology *Verifiable Attestation* for Verifiable Credentials that assert claims about a legal entity[44].

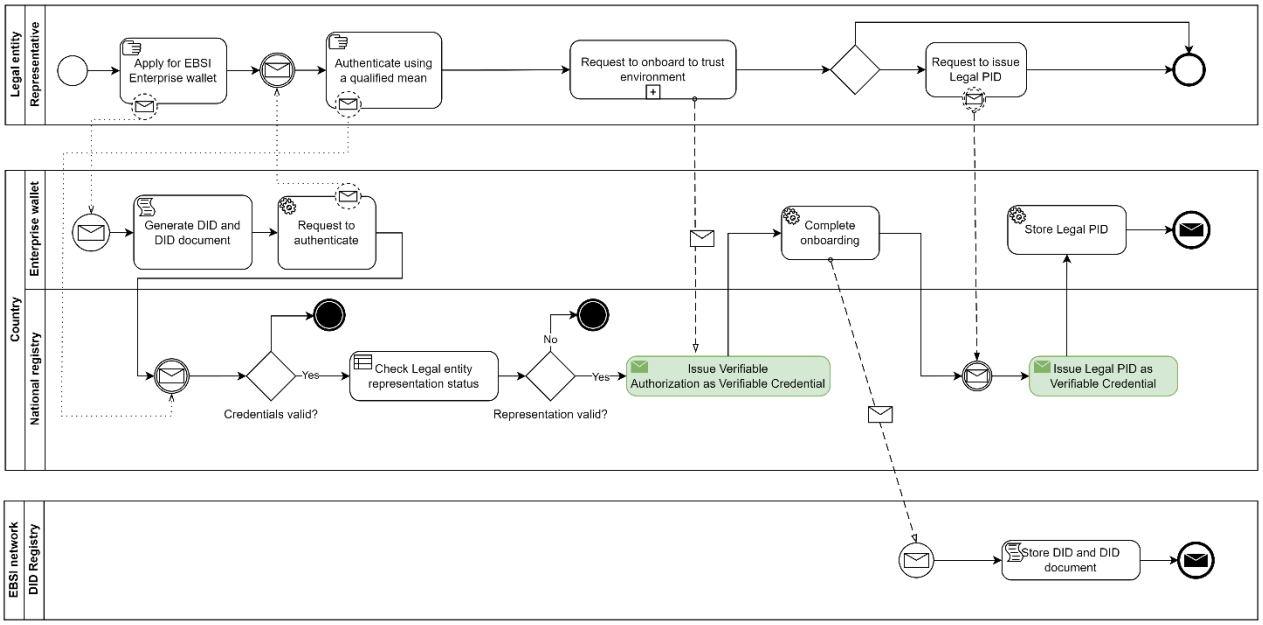


Figure 4: Process for issuing a legal PID (ODI)

[44] https://hub.ebsi.eu/vc-framework/credential-status-framework/revocation-methods

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

6 Removing legal entity rights within a trust environment

6.1 Relevance and context

Revocations play a critical role in an identity environment, being an integral part of verifying the status of a Verifiable Credential´s validity[45]. This control over the credential's lifetime is particularly vital for legal entities facing organizational changes, such as restructuring, policy updates, or termination. Unlike natural persons, privacy concerns for legal entities are less significant in the underlying context. National registries which issue legal PIDs within an EBSI trust environment can become enabled to trace which verifier request revocations.

Our analysis of EBSI's revocation methods[46] revealed distinctions in the setup of revocation methods, depending on the level of privacy demanded for holders of Verifiable Credentials. For legal entities, we recommend implementing a revocation method for legal PIDs at the national registry, being the root-TAO for the trust environment for issued Organizational Identities.

6.2 Excluding a legal entity from a trust environment

A root-TAO has full control over the existence of a legal entity within a trust environment. If a legal entity needs to be excluded from a trust environment, the root-TAO needs to change the respective accreditation status. To reduce complexity for the root-TAO we recommend using the accreditation status within the Trusted Issuers Registry hosted by EBSI[47]. Verifiable Credentials issued by the excluded legal entity may become invalid because verifiers will not receive the expected information about the issuer when sending requests to the DID Registry during a verification process.

6.3 Disabling Peer-to-peer verification between legal entities

For simplicity reasons, we propose employing short-lived Verifiable Credentials as legal PID (ODI). This requires legal entities holding a legal PID (ODI) to contact the national registry and refresh it for each verification process. Using the Verifiable Credential immediately after issuance makes a revocation registry in the traditional sense obsolete. If security needs to be optimized, we

[45] Please see chapter 8 of deliverable 3.1 in EBSI-VECTOR for DID Lifecycle Management.
[46] https://hub.ebsi.eu/vc-framework/credential-status-framework
[47] https://hub.ebsi.eu/vc-framework/credential-status-framework/revocation-methods

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

recommend setting the validity of the Verifiable Credential to 1 minute after issuance and observe user interactions assuring that there is no negative impact on the user experience during the verification of the issued legal PID[48].

6.4 Revoking Verifiable Credentials issued by a Trusted Issuer

Considering that legal entities who were onboarded as Trusted Issuers in a trust environment want to issue Product Passports as Verifiable Credentials, we recommend implementing Status lists[49]. These status lists must be updated by a trusted issuer. We recommend outsourcing the hosting of a status list to EBSI or another specialized service provider to facilitate the onboarding process.

A status list defines the status of each issued credential and is updated whenever a Verifiable Credential is revoked. Besides being valid or revoked, Verifiable Credentials can also have the status of being suspended which makes it possible to re-gain its validity to a later point in time. Following this procedure creates fundamental value for legal entities since they are now able to track their products forward along their supply chain. This might pave the way for a circular economy making it possible to re-gain control over sold products and recycle them.

[48] Please note, pdf-based company records that are handed in to proof the identity of a legal entity an EU tender ask for an issuing date not older than 3 months.

[49] Please note, the specifications of status lists are currently a working draft only: https://www.w3.org/TR/vc-bitstring-status-list/

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

7 Functional requirements and User Stories

7.1 Functional requirements for Use Case Designers in EBSI-Vector

We analyzed the drafted business requirements from Work Package 5 as of January 2024. The following functional requirements are written to support the Use Case Designers of the digital European Health Insurance Card (EHIC) and the digital Portable Document A1 (PD A1) to successfully onboard their Use Cases on EBSI.

#1 - Use Case designers MUST define a root-TAO for the EHIC/ PD A1.

User Story: As a root-TAO, I want to assign trusted issuers, so that they can issue a digital EHIC/PD A1 as Verifiable Credential.

Remarks: Use Case designers must define which public institution takes over the role as root-TAO. Having that role defined, the necessity for sub-TAO can be derived. Furthermore, implementing developers will understand whether 1 European trust environment or several national trust environments should be designed.

#2 - The root-TAO SHOULD be a public institution registered within an EU member state.

User story: As European Commission, I want all trust environments set up with the EBSI technology to be set up by a public body, so that I can guarantee that all Verifiable Credentials issued in a given trust environment are somehow tied to a jurisdiction of an EU member state.

Remark: This requirement is derived from a strategic position. On one hand the requirement reflects the reality since legal entities only exist in accordance with a belonging jurisdiction. On the other hand it slows down adoption of the EBSI technology since a rather sophisticated onboarding procedure with a public body is needed before legal entities adopt a trust environment.

#3 - Root-TAOs SHOULD define trusted issuers for the EHIC/ PD A1.

User Story: As a root-TAO, I want to assign trusted issuers, so that they can issue a digital EHIC/ PD A1 as Verifiable Credential.

Remarks**:** The root-TAO plays a crucial role on how well a newly established trust environment is adopted. Therefore, the root-TAO should list all trusted issuers that will need to be onboarded

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

for the trusted issuer registry. The list should contain at least these three attributes about each trusted issuer:

- Name and legal form of the trusted issuer: This attribute defines the legal entity.
- Schema for issuance of Verifiable Credentials: This attribute refers to a Schema within the trusted Schema registry and defines which Verifiable Credentials the issuer is allowed to issue.
- Need for Verifiable Accreditation: This attribute highlights that Verifiable Accreditation is necessary to be included in the trusted issuer registry. If Verifiable Accreditation is not needed for some reason, the legal entity CAN NOT be part of the trusted issuers registry.

#4 - Root-TAOs SHOULD define trusted verifiers for the EHIC/ PD A1.

User Story: As a root-TAO, I want to assign trusted verifiers, so that only legitimate organizations are able to verify a digital EHIC/ PD A1.

Remarks: Within an established trust environment, the root-TAO might want to limit the number of verifiers that are able to read and verify data the digital EHIC/ PD A1. Therefore, the root-TAO should list all trusted verifies that will need to be onboarded to a trusted verifier registry. The list should contain at least these three attributes about each trusted verifier:

- Name and legal form of the trusted verifier: This attribute defines the legal entity.
- Schema for Verification: This attribute refers to a Schema within the trusted Schema registry and defines which Verifiable Credentials the verifier is allowed to verify.
- Need for Verifiable Accreditation: This attribute highlights that Verifiable Accreditation is necessary to be included in the trusted verifier registry. If Verifiable Accreditation is not needed for some reason, the legal entity CAN NOT be part of the trusted verifier registry.

#5 - The root-TAO SHOULD provide a policy defining rules and regulation on how to use the digital EHIC/ PD A1

User Story I: As issuer, I want to consult a policy on how to use the digital EHIC /PD A1 so that I learn how to comply with the rules and regulations.

User Story II: As verifier, I want to consult a policy on how to use the digital EHIC /PD A1 so that I learn how to comply with the rules and regulations.

User Story III: As holder of a digital EHIC/ PD A1, I want to consult a policy on how to use the digital EHIC /PD A1, so that learn which rules and regulations need to be complied with.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

#6 - If a policy is present, the root-TAO MUST register it in the Trusted Policy Registry.

User Story: As an issuer, I want to include a reference to my issued Verifiable Credentials, so that holders and verifiers know which rules and regulations they need to comply with.

Remark: We recommend to use EBSIs Trusted policies registry[50] to register an EHIC/ PD A1 policy.

#7 - The root-TAO MUST register the EHIC/ PD A1 schema in the Trusted Schema registry.

User Story: As an issuer, I want to make a reference to the EHIC/ PD A1 schema in every Verifiable Credential I issue, so that holders and verifiers have proof that the Verifiable Credential they hold/ verify complies with the schema that was set up by the root-TAO.

#8 - Trusted issuers for EHIC/ PD A1 MAY obtain a legal PID (ODI)

User Story: As a root-TAO, I want to assure that only registered legal entities within the jurisdiction of an EU member state can issue a digital EHIC/ PD A1.

Remark: Root-TAOs for EHIC/ PDA have an interest that only publicly registered legal entities issue digital EHIC/ PD A1. We recommend linking this privilege to the ownership of a non-revoked legal PID (ODI). If, for any reason, the legal PID (ODI) is revoked, the issuer loses the right to issue digital EHIC/ PD A1 automatically. However, the root-TAO is also able to manage that self-sufficiently by changing the status of the Verifiable Accreditation (see chapter 6 for details).

#9 - Trusted verifiers for EHIC/ PD A1 MAY obtain a legal PID (ODI)

User Story: As a root-TAO, I want to assure that only registered legal entities within the jurisdiction of an EU member state can verify a digital EHIC/ PD A1.

Remark: Root-TAOs for EHIC/ PDA have an interest that only publicly registered legal entities verify digital EHIC/ PD A1. We recommend linking this privilege to the ownership of a non-revoked legal PID (ODI). If, for any reason, the legal PID (ODI) is revoked, the verifier loses the right to verify digital EHIC/ PD A1 automatically. However, the root-TAO is also able to manage that self-sufficiently by changing the status of the Verifiable Accreditation (see chapter 6 for details).

#10 - EBSI SHOULD host a revocation registry for PD A1/ EHIC issuers

[50] https://hub.ebsi.eu/apis/pilot/trusted-policies-registry/v2

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

User Story: As a root-TAO, I want a central revocation registry for PD A1 / EHIC hosted by EBSI, so that I avoid that issuers can track verification transactions.

Remark: The Use Case designers for the digital PD A1/ EHIC plan to onboard more than 3.000 social security institutions. Each of these institutions must be provided with a simple solution to revoke credentials they issued. However, it must be avoided that these issuers track verification transactions. We recommend EBSI to provide a revocation registry and collaborate with all EBSI conformant (enterprise) wallet providers to establish a revocation mechanism that can be used right after a social security institution is properly onboarded.

7.2 Functional requirements for EBSI developing team

#11 - EBSI MUST provide a Trusted Verifier Register

User Story: As a holder, I want to make sure that a verifier is authorized to request a certain verifiable presentation, so that I achieve mutual trust, enhance security and that I am protected from misuse.

Remarks**:** Article 6b of the current eIDAS 2.0[51] draft will affect most Use Cases implemented with EBSI. It requires EU member states and wallet providers to register all relying parties that want to verify a natural PID. Moreover, the Use Case designers of the digital EHIC and the digital PD A1 will use a defined list of verifiers.

#12 - EBSI conformant wallets SHOULD be eIDAS compliant

User Story: As an issuer, I want to ensure that the wallet in which I issue my credentials was audited according to the eIDAS 2.0 policy private, so that I fulfil my legal obligations, assure a high degree of interoperability, avoid misuse and assure that that private keys of holders are protected.

Remarks: Article 6c of the current eIDAS 2.0[52] draft will affect most Use Cases implemented with EBSI. It requires EU member states to certify and register all wallet providers for identity use cases. We recommend EBSI to audit the eIDAS 2.0 compliance in their wallet conformance tests. For example, audited wallets should not transfer data to unauthorized instances.

[51] https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf
[52] https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

#13 - An enterprise wallet MUST enable users to onboard to the PD A1 / EHIC trust environment.

User Story: As a social security institution, I want to onboard to the PD A1 / EHIC trust environment as fast as possible, so that I can start issuing digital PD A1 / digital EHIC.

Remark: While the onboarding process for trusted issuers is well explained[53], we recommend providing a simplified onboarding process for social security institution that are going to issue digital PD A1 / EHIC. This is necessary for all trust environments with a potentially significant number of trusted issuers.

#14 - EBSI MUST enable issuers of the digital PD A1 / EHIC to revoke it

User Story: As issuer, I want to be able to revoke a digital EHIC, so that misuse of outdated EHICs can be avoided.

Remarks: Revoking EHICs as they are currently used in Europe is not possible. It is appreciated to include the revocation feature when implementing the digital EHIC. We recommend EBSI to provide an EHIC revocation registry to facilitate onboarding for trusted issuers.

#15 - EBSI SHOULD offer service levels and consulting for root-TAO onboarding

User Story: As root-TAO, I want to be supported during the design and implementation of my trust environment, so that I can compensate missing competencies.

Remarks: Onboarding root-TAOs in EBSI requires a high level of expertise and an interdisciplinary team. It cannot be expected that each root-TAO provides the needed expertise during the onboarding process. Therefore, EBSI should have the availability of a profound consulting team combining at least the expertise of business consultants, IT architects and implementing developers.

#16 - EBSI SHOULD provide documentation about adding a new schema and a new policy

User Story: As a root-TAO, I want to add a Trusted Schema/ a Policy to my trust environment, so that Trusted issues can include references to the Trusted Schema and the Policy within Verifiable Credentials.

[53] https://hub.ebsi.eu/get-started/build/ti

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Remarks: As explained in chapter 4.3.4, we were not able to find documentation about how to add Trusted Schemas or new policies. We recommend, adding this information.

#17 - EBSI MAY improve the documentation

User Story: As an implementing developer, I quickly want to find to learn how to build a trust environment in EBSI, so that I can efficiently finish my project.

Remarks: As explained in chapter 4.3.1, we experienced difficulties to identify information needed for our analysis in EBSIs documentation. While almost all information we searched for, was eventually being found, we recommend to improve the educational journey for implementing developers e.g. by offering a (standardized) architecture model and a search function for key words.

#18 - EBSI SHOULD facilitate the onboarding for digital wallets

User Story: As an implementing developer, I quickly want to identify the digital wallet(s) I need for my trust environment, so that I assist issuers, verifiers and holders to enter my trust environment.

Remarks: Efficient onboarding to a digital wallet for issuers, verifiers and holders is a crucial step for adoption in a trust environment set up with EBSI. While EBSI currently lists all conformant wallets making issuing, verifying, accrediting and authorizing capabilities transparent, a more comprehensive comparison is recommended. This requires a profound analysis and evaluation of all available EBSI conformant digital wallets. Criteria for evaluation should include User Experience, Security, Fees, Interoperability, Simplicity of development, Compliance and available interfaces. Links to demo versions should be provided.

#19 - EBSI SHOULD provide a mechanism how legal entities can obtain a legal PID

User Story: As a root-TAO, I want all legal entities to obtain their legal PID (ODI), so that existence of the legal entity and controllership of a legal entity representative can be proven and that changes in status of the legal entity has a direct impact within my trust environment.

Remarks: Rights of legal entities within a trust environment in EBSI should be reviewed and, if necessary, being adopted if the status of a legal entity changes. The root-TAO has the technical ability to conduct these changes if onboarded to a wallet with accreditation and authorization capabilities. Moreover, we recommend EBSI to offer a mechanism that enables legal entities to obtain a legal PID. Doing so will ideally automate the legal entity status management. The

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

mechanism can be implemented in different manners. We recommend introducing a policy created by EBSI that requires root-TAOs to use a predefined Trusted Schema for legal PID (ODI) and to include national business registries as Trusted Issuers in each trust environment.

#20 - EBSI SHOULD offer self-registration for trusted issuers

User Story: As a root-TAO, I want to offer my Trusted Issuers a solution for self-registration, so that onboarding them can be done efficiently.

Remarks: Adoption and scaling of an EBSI trust environment currently depends on the initiative of a root-TAO going through a comprehensive onboarding process. It is assumed that the root-TAO also takes initiatives to attract issuers and verifiers for their trust environment. This is a rather high threshold for adoption. We recommend EBSI to offer self-subscription[54] for issuers in which they can select a trust environment and receive guiding for the onboarding process. We believe that this building block is needed as a low threshold entry barrier for Use Case adoption.

7.3 Functional Requirements for Enterprise wallet providers

#21 - An enterprise wallet MUST enable users to onboard to the PD A1 / EHIC trust environment.

User Story: As a social security institution, I want to onboard to the PD A1 / EHIC trust environment as fast as possible, so that I can start issuing digital PD A1 / digital EHIC.

Remark: While the onboarding process for trusted issuers is well explained[55], we recommend providing a simplified onboarding process for social security institution that are going to issue digital PD A1 / EHIC. This is necessary for all trust environments with a potentially significant number of trusted issuers.

#22 - An Enterprise wallet MUST support a mechanism of verifying the identity of a natural person

User Story: As a legal entity representative, I want to proof my personal identity to a national registry, so that I can apply for a legal PID (ODI) for my company.

[54] A self-subscription feature for piloting Use Cases can be found here: https://ec.europa.eu/eusurvey/runner/Pilot_self-registered_TI_request?surveylanguage=EN
[55] https://hub.ebsi.eu/get-started/build/ti

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Remarks: To avoid media discontinuity and provide a decent User Experience for legal entity representatives, we recommend offering an extensive set of capabilities within an Enterprise wallet. This includes a verification mechanism to prove the identity of the natural person claiming it is a legal entity representative. This requires adoption of the different national identification schemes that are currently in place in EU member states while knowing that these different processes are harmonized under the renewal of the eIDAS regulation. Wallet providers find themselves in a difficult situation, not knowing whether to set up a large roadmap to implement existing solutions or waiting for the new one. For the upcoming piloting phase, we recommend starting to implement an identity check for Swedish Citizens in the Enterprise wallet MVP since the Swedish commercial registry Bolagsverket is already activated to issue legal PID (ODI) as root-TAO for a pilot scenario.

#23 - An Enterprise wallet MUST enable issuers of legal PID (ODI) to issue short-lived Verifiable Credentials

User Story: As an issuer, I want to issue legal PID (ODI) with a short validity, so that I don´t need to manage a revocation registry.

Remarks: While different revocation methods can be implemented, we recommend short-lived Verifiable Credentials for legal PID (ODI) due to the ease of implementation. This means that short-lived legal PID (ODI) are issued whenever a legitimate holder requests it. For production environments this results in non-functional requirements for issuer-controlled wallet instances so that the requests can be responded quickly whenever they occur.

Hence, Enterprise wallet providers must support the above-mentioned capability by offering issuers

- to define the validity period for short-lived legal PIDs (ODI) and
- to automatically check and respond issuing requests from holders.

Following that proposal will result in a query between the Enterprise wallet and the national commercial registry which contains up-to-date information about the legal entity record.

#24 - Enterprise wallets MAY limit the functionalities for legal entities that did not obtain a legal PID (ODI)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

User Story: As a root-TAO, I want to prevent legal entities that did not obtain a legal PID (ODI) to issue and verify Verifiable Credentials in my trust environment, so that I increase the overall security.

Remarks: Root-TAOs that set up a trust environment want to avoid any misuse about the data shared as part of a Verifiable Credential. This includes keeping out legal entities for which the legal status is not proven. Besides managing the Trusted Issuer and the Trusted Verifier registry this can be done via functionalities within an Enterprise wallet. It is recommended that Enterprise wallet providers introduce two different statuses a wallet can have, depending on whether a legal PID (ODI) is present or not. Missing legal PIDs (ODI) may prevent issuers and verifiers to issue and verify Trusted Schemas. Having that functionality implemented, Enterprise wallet providers can make themselves attractive for root-TAOs to put them in a Trusted wallet provider registry.

#25 - Digital PD A1 MUST be transferable to another wallet

User Story: As legal entity representative of a construction company, I want to collect all the digital PD A1 from my team, so that I can present them as a bulk to customs upon request.

Remarks: Digital PD A1 is issued to the natural person who applied for it. When customs audit a construction site, they usually request all documents from a responsible person. In this case, this could be a construction manager. Hence, the construction manager must be enabled to hold all the digital PD A1 from his entire team inside the enterprise wallet of his company.

#26 - Enterprise wallets SHOULD be accessed via a browser extension

User Story: As a legal entity representative controlling an Enterprise wallet, I want to access it via a browser extension, so that I reduce media discontinuities while I obtain data from and deliver it to a web-page.

Remarks: We assume that Enterprise wallets need intersections to a wide range of existing systems. This includes web interfaces as well. We imagine that a legal entity that was successfully onboarded to a digital wallet will request a legal PID at the issuer's website. Hence, it is recommended to use a browser extension that the legal entity representative uses to enter the issuing process.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

8 System architecture

In this chapter, our focus is on mapping the EBSI infrastructure, providing an overview of its documented components and shortly explaining them. Additionally, we present recommendations for incorporating new building blocks, aiming to enhance the functionality as described earlier in this document. Furthermore, we address the needed adjustments to the standardized architecture, specifically in the context of issuing legal PIDs (ODI), by tailoring the architecture to align with requirements from National Commercial Registries.

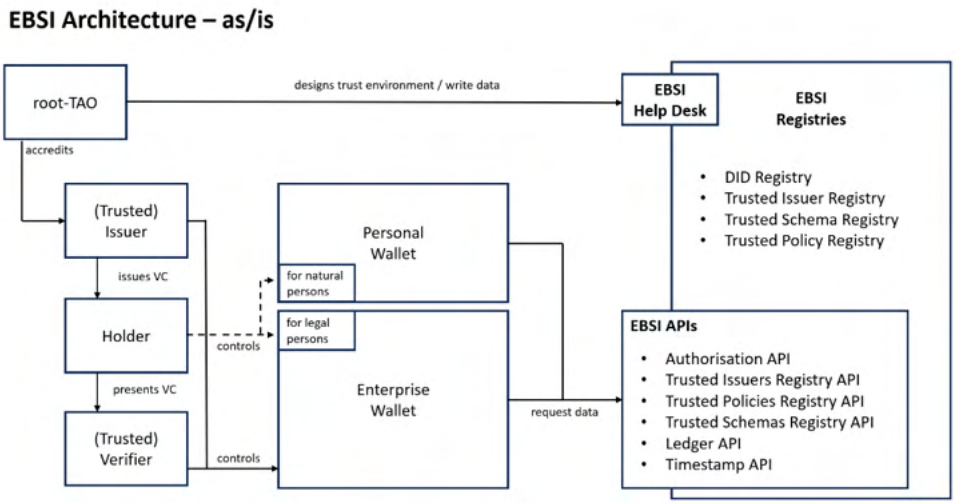


Figure 5: EBSI Architecture components as publicly documented

The architecture of the European Blockchain Service Infrastructure at its core consists of 4 Registries: DID Registry, Trusted Issuer Registry, Trusted Schema Registry and Trusted Policy Registry. Information can be gathered and written by sending requests to APIs.

Each trust environment is designed by the root-TAO. Under the guidance of the EBSI Help Desk, a trusted schema and a trusted policy can be written into the respective registry. Subsequently, the Root-TAO accredits issuers and verifiers to actively participate in this environment. Entities seeking accreditation must possess the relevant verifiable credentials issued by the root-TAO, allowing them to apply for registration within the DID registry and the trusted issuer registry. This accreditation process ensures that only trusted parties are authorized to engage in transactions within the defined trust environment.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Integral to the EBSI architecture is the requirement for every participant to possess a digital wallet tailored to their status. Legal entities utilize Enterprise wallets, while individuals are equipped with natural person wallets. These EBSI-conformant wallets serve as the primary interface through which actors can interact with the system. Specifically, they facilitate communication with the APIs, enabling the gathering and recording of data from the registries.

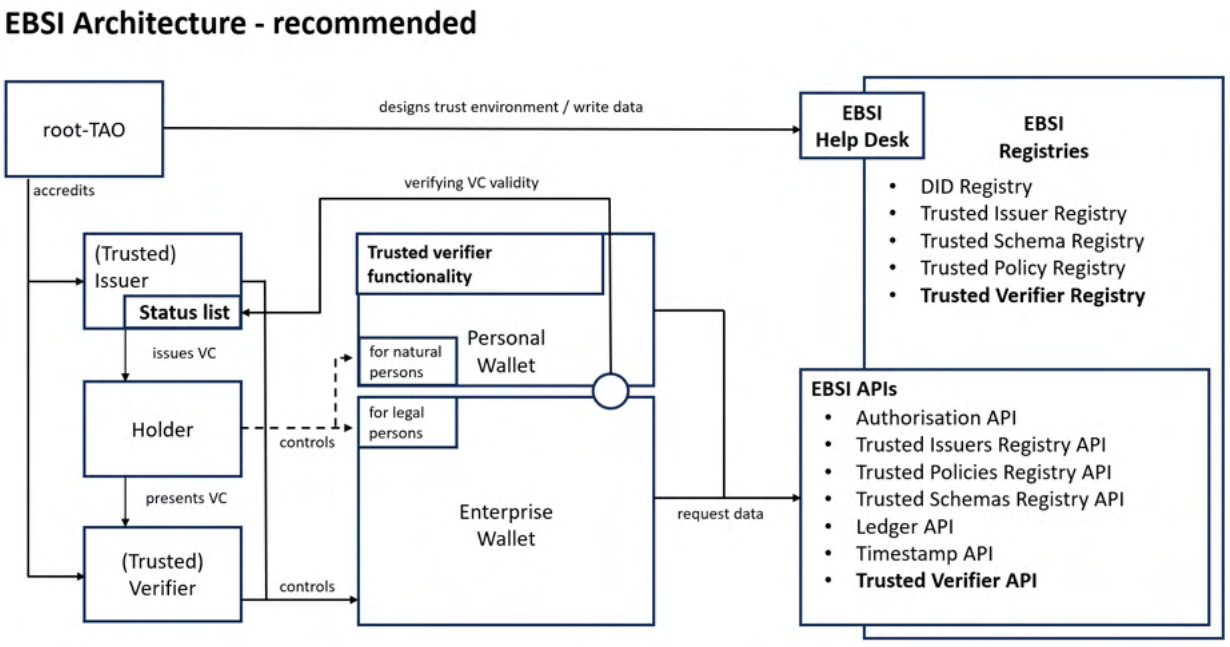


Figure 6: Recommended components to be added to EBSI Architecture

In addition to the existing architecture, we recommend incorporating the following components into the EBSI framework to enhance its functionality and security and to meet upcoming requirements by Use Cases that want to adopt the technology. Firstly, the inclusion of a Trusted Verifier registry and the corresponding API will empower the root-TAO to register companies permitted to verify Verifiable Credentials within the trust environment. This ensures that only authorized entities participate in the verification process, reinforcing the integrity of the trust environment the root-TAO set up.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Furthermore, we propose the introduction of a functionality within digital wallets for natural persons to call the aforementioned APIs. This feature empowers users to interact exclusively with trusted verifiers and trusted wallets, fostering a more secure trust environment. Additionally, we advocate for the provision of a Software Development Kit (SDK) by EBSI. This SDK should enable issuers to establish and manage their own status lists, that indicate whether a formerly issued Verifiable Credential is still valid. SDK is quite important as it could ease the technology integration and adoption, therefore it should be available in most used programming languages (e.g. TypeScript, JavaScript...) in Europe. Consequently, both Enterprise wallet and personal wallet providers must integrate a functionality to access the status of a Verifiable Credential against these lists, adding the urgently needed capability to conduct revocations within the entire EBSI architecture.

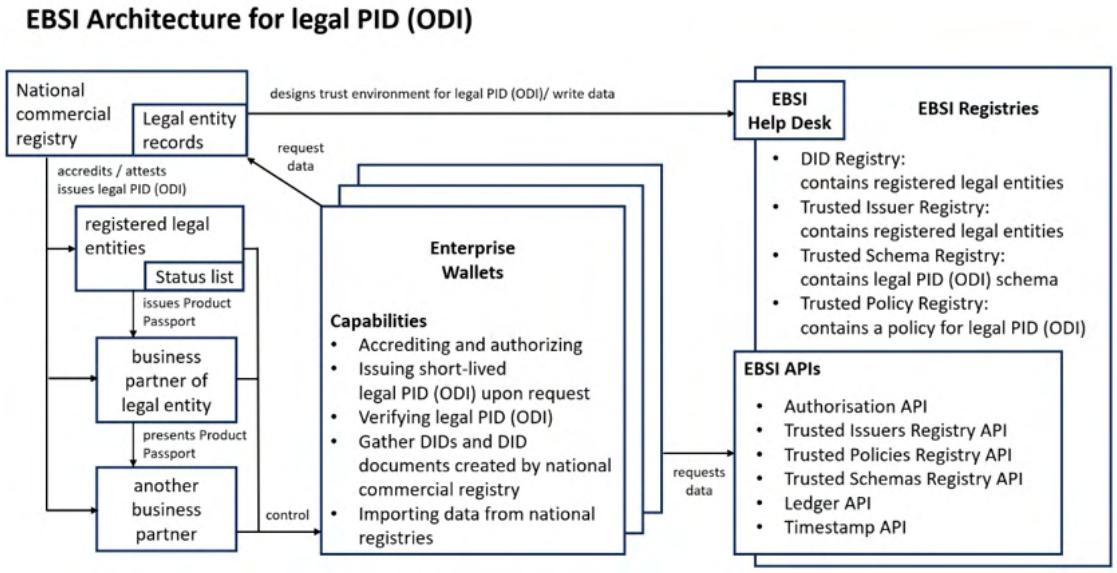


Figure 7: Proposal for an EBSI Architecture for Legal PID (ODI)

To enable the issuance of legal PIDs (ODI) for legal entities, we propose a procedure wherein each national commercial registry that maintains records of legal entities establishes a dedicated trust environment. This entails the registration of a schema tailored for the legal PID (ODI) and the formulation of a policy within the EBSI registries specific to these legal identities. The commercial registry, acting as the accreditor, grants legal entities access to the trust environment, permitting them to register their respective Decentralized Identifiers in the DID

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

registry. As a result, each legal entity is qualified to receive a unique legal PID (ODI) issued by the national commercial registry, ensuring a secure identity verification process within the EBSI infrastructure.

We strongly advocate for the integration of a value proposition wherever the legal PID (ODI) is introduced so that legal entities are incentivized to adopt it. One such proposition could involve empowering legal entities with the capability to issue product passports as digital twins for their products. Additionally, compliance with regulatory frameworks such as the supply chain act could be tied to obtaining and utilizing legal PIDs (ODI). To facilitate these functionalities, wallets may establish and maintain a continuously open and secure communication channel with the national commercial registry. This communication serves a dual purpose — supporting the onboarding process of legal entities for Enterprise wallets and facilitating the automatic response to requests for short-lived Verifiable Credentials as revocation method for legal PID (ODI).

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

9 Pilot Scenarios

9.1 Legal Considerations

The European Blockchain Services Infrastructure (EBSI) utilizes trust registries as a fundamental component to ensure that its operations adhere to legal, regulatory, and security standards. Trust registries in the context of EBSI play a critical role in managing the identities of entities (organizations, services) that interact within the EBSI ecosystem. They ensure that only identified and authorized entities can issue valid and verifiable attestations, enhancing trustworthiness and compliance across EU. EBSI is part of the European Union's digital strategy, which aims to foster digital transformation across the EU. The legal context for EBSI, including its trust registries, is influenced by various EU regulations and directives aimed at digital identity, data protection, cybersecurity, and electronic transactions.

9.1.1 EU Digital Services Act

The Digital Services Act (DSA) represents a cornerstone of the European Union's digital strategy, aiming to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. While EBSI primarily focuses on enabling secure, cross-border digital services through blockchain technology, its operations and trust registries must also consider the implications of the DSA to ensure legal compliance.

Transparency Requirements: The DSA mandates high levels of transparency from digital services, particularly concerning how they moderate content, advertise, and manage algorithms. For EBSI, this translates into ensuring transparent operations of its blockchain services, including how data is handled and how decisions are made within its infrastructure.

Regarding Trusted Registries (Business Registries) it will be important to guarantee open and free public access to the information contained within together with proof/track of the approval process for any entry added to them.

Protection of Fundamental Rights: EBSI must ensure that its services do not infringe on users' fundamental rights, including privacy, freedom of expression, and data protection. This

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

alignment is crucial as EBSI handles identity and transaction data across EU borders, necessitating strict adherence to principles that protect personal data and ensure the right to privacy.

Regarding Trusted Registries (Business Registries) it will be important to avoid any personal data to be included in such registries.

Legal Accountability: Under the DSA, digital services must be legally accountable for their compliance with the regulation. EBSI, while being an infrastructure rather than a digital service provider in the conventional sense, must ensure that its trust registries component, comply with DSA requirements where applicable, especially in aspects related to data management and protection.

Cooperation with Regulatory Authorities: The DSA emphasizes the importance of cooperation between digital services and regulatory authorities. EBSI, as a project initiated by the EU and involving member states, is inherently aligned with regulatory frameworks but must maintain proactive engagement with relevant authorities to ensure ongoing compliance and address emerging legal and regulatory challenges.

Risk Management: The DSA requires digital services to assess and mitigate risks associated with their operations, including risks to users' rights and societal harms. EBSI trust registries must implement robust risk management processes, especially concerning data integrity, security, and privacy, leveraging blockchain's inherent features for security and transparency while addressing potential risks associated with data management.

Facilitating a Digital Single Market: The DSA aims to foster innovation and competitiveness in the EU's digital single market. EBSI trust registries supports this goal by promoting interoperability and the use of open standards for blockchain services, facilitating seamless digital interactions across member states. Compliance with the DSA also means ensuring that EBSI services are accessible and equitable, supporting the EU’s broader digital inclusion goals.

9.1.2 EU Data Act

The EU Data Act is a regulation aimed at ensuring fairness in the digital environment, facilitating access to and use of data, and fostering a competitive data market. While its primary focus isn’t

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

specifically on blockchain infrastructures like the European Blockchain Services Infrastructure (EBSI), the principles and regulations it introduces are relevant for EBSI, especially considering its role in managing and facilitating access to a wide range of data across the EU.

Facilitating Data Sharing: The Data Act aims to make it easier for individuals and businesses to access and share data generated by their activities, including data in the hands of public sector bodies or generated by IoT devices. EBSI, thanks to its Trust Registries model by facilitating secure and trustworthy data transactions across borders, can support the objectives of the Data Act by providing the infrastructure needed for secure data sharing and access within the EU.

Data Governance: EBSI will need to implement governance mechanisms that comply with the Data Act's requirements for data sharing and access. This includes ensuring that data sharing practices respect the rights of data holders and adhere to principles of transparency and fairness.

Data Intermediaries: EBSI's role as a facilitator of data transactions may align with the Data Act's provisions on data intermediaries. The infrastructure will need to ensure that it operates transparently and fairly, without abusing its position to access or use data beyond what is necessary for the provision of its services.

Free Flow of Non-Personal Data: The Data Act emphasizes the free flow of non-personal data within the Single Market. EBSI can play a crucial role in facilitating cross-border data transactions, ensuring that data localization requirements do not hinder the availability of data across the EU. Compliance with the Data Act means ensuring that EBSI does not impose unjustified restrictions on where data can be stored or processed within the EU.

Interoperability and Standards: Compliance with the Data Act also involves adhering to EU standards for data interoperability and openness. EBSI will need to ensure that its protocols and standards facilitate interoperability with other data spaces and digital services, supporting the creation of a competitive and innovative data ecosystem in the EU.

9.1.3 NIS/NIS2 Directive

The Directive on Security of Network and Information Systems (NIS Directive) and its subsequent update, the NIS2 Directive, are key components of the European Union's cybersecurity strategy.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

They aim to enhance the security of network and information systems across the EU, with a particular focus on essential and important entities that provide critical services.

As the European Blockchain Services Infrastructure (EBSI) plays a crucial role in facilitating secure and efficient digital services across EU borders, compliance with the NIS and NIS2 Directives is fundamental to its operation.

Here below we evaluate the main elements of the directive that have impact on EBSI Trust Business Registries:

Risk Identification and Mitigation: Both the NIS and NIS2 Directives require entities to identify, assess, and mitigate risks to their network and information systems. For EBSI, this means implementing a continuous risk management cycle, using EU standards (e.g. ITSRM2) and applying the consequent security measures to protect the Trust Registries against potential cyber threats, vulnerabilities, and incidents.

System Security: EBSI must ensure the security of its technology stack, including hardware, software, and networks. This involves adopting state-of-the-art cybersecurity technologies and practices to detect, prevent, and respond to cyber threats effectively.

Timely Incident Reporting: The directives mandate that entities report significant cybersecurity incidents to the relevant national authorities. EBSI must establish mechanisms for early detection of incidents and timely reporting for any cyber event involving Trusted business registries. This ensures that appropriate measures can be taken to mitigate the impact of incidents and prevent their recurrence.

Transparency and Accountability: By adhering to the incident reporting requirements of the NIS and NIS2 Directives, EBSI will need to demonstrate transparency and accountability in its operations. This builds trust among users, member states, and stakeholders in the reliability and security of the infrastructure.

Business Continuity Planning: The directives require entities to have business continuity and disaster recovery plans in place. EBSI must ensure it can maintain or quickly restore the availability and access to its Trusted Registries in the event of a physical or cyber incident.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Testing and Auditing: Regular testing and auditing of the EBSI infrastructure are essential to ensure compliance with the NIS and NIS2 Directives. This includes conducting penetration tests, vulnerability assessments, and compliance audits to evaluate the effectiveness of cybersecurity measures and identify areas for improvement.

9.1.4 GDPR

The General Data Protection Regulation (GDPR) is a cornerstone of privacy and data protection in the European Union, setting stringent requirements for the processing of personal data. As the European Blockchain Services Infrastructure (EBSI) is an initiative designed to enable secure and efficient digital services across the EU, including services that may involve the processing of personal data, compliance with GDPR is essential.

Trusted business registries are supposedly focusing on legal entities therefore GDPR regulation applies to it indirectly.

Consent and Legal Basis for Processing: Trusted registries must ensure that in case any personal data is present (e.g. in case of a single person legal entity) processed has a clear legal basis, such as consent from the data subject or the necessity for the performance of a contract or compliance with legal obligations.

Transparency in Data Processing: Clear information must be provided about the collection, storage, and potential use of personal data within trusted registries. This includes the purpose of data processing, the retention period, and the rights of data subjects.

Facilitating Rights of Data Subjects: Trusted registries must provide mechanisms for individuals, if personal data is present) to exercise their rights under GDPR, such as accessing their data, rectifying inaccuracies, erasing data, and data portability.

Automated Decision-Making and Profiling: If trusted registries use automated decision-making or profiling in regards of potential presence of personal data, individuals have the right to be informed, to obtain human intervention, to express their point of view, and to contest the decision.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Data Protection Impact Assessment (DPIA): Trusted registries should conduct DPIAs for processing activities likely to result in a high risk to the rights and freedoms of individuals, particularly concerning large-scale processing of sensitive data or systematic monitoring.

Documentation and Compliance: Trusted registries must maintain detailed records of data processing activities and implement policies and procedures to demonstrate GDPR compliance. This may involve appointing a Data Protection Officer (DPO) to oversee compliance efforts.

Safeguarding Data Transfers: If trusted registries involve transferring personal data outside the EU, they must ensure such transfers are carried out in compliance with GDPR, using mechanisms like adequacy decisions, Binding Corporate Rules (BCRs), or Standard Contractual Clauses (SCCs) to provide adequate protection.

9.1.5 eIDAS/eIDAS2.0 Regulation

Interoperability with eID/PID Systems: EBSI would need to ensure interoperability with national eID schemes certified under eIDAS, and with the new EUDIW facilitating seamless and secure cross-border transactions and interactions within the EU. This involves adhering to standards, including PID processes and recognition together with protocols that enable mutual recognition of digital identities.

Trust Services Integration: For EBSI to comply with eIDAS1 and eIDAS2 framework, it would need to support trust services such as electronic signatures, electronic seals, time stamps, electronic delivery services, and electronic attestations. EBSI would have to ensure that these services are provided in a secure manner that complies with the regulatory standards set out by eIDAS.

Legal Recognition of Electronic Transactions: EBSI would need to ensure that electronic transactions facilitated by its infrastructure are legally recognized across EU member states. This includes usage of electronic signatures and records in accordance with eIDAS standards, mostly setting EBSI as a Trust Service.

Facilitation of Cross-border Services (EBSI as a Trust Service): One of the core objectives of eIDAS is to facilitate cross-border electronic transactions. EBSI would play a crucial role in this context

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

by providing a blockchain-based infrastructure that supports secure, cross-border digital services, aligning with the goals of eIDAS to remove barriers to digital transactions across the EU.

This means that EBSI shall guarantee "the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger", thus each Trust Registry transaction must be recorded into EBSI guaranteeing such factors.

9.1.6 Business Registries Governance legal aspects

Within eidas context we have 3 governing bodies:

- **National Supervisory Body**: an authority designated by an EU Member State to oversee and ensure that Trust Service Providers (TSPs) within its jurisdiction comply with the eIDAS regulation. This body is responsible for the accreditation, supervision, and enforcement actions related to the provision of electronic identification and trust services,
- **National Accreditation Bodies:** entity recognized by a government to assess and accredit organizations that provide certification, testing, inspection, and calibration services. In the context of eIDAS, NABs may play a role in accrediting Conformity Assessment Bodies (CABs) that evaluate Trust Service Providers (TSPs) against the standards set forth by eIDAS
- **Conformity Assessment Body**: organization accredited by the national supervisory body to evaluate the conformity of Trust Service Providers (TSPs) with the requirements set out in the eIDAS regulation.

These 3 bodies need to oversee the activities related to trusted registries in order to guarantee conformance with eidas2 regulation.

In particular taking in consideration a multi-layered model where each Member State will run his own tree of Registry (within EBSI or partially outside EBSI maybe leveraging different technologies) there will be a need of 'decentralized' governance.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Here below an high-level schema of the multi-layered registry approach:

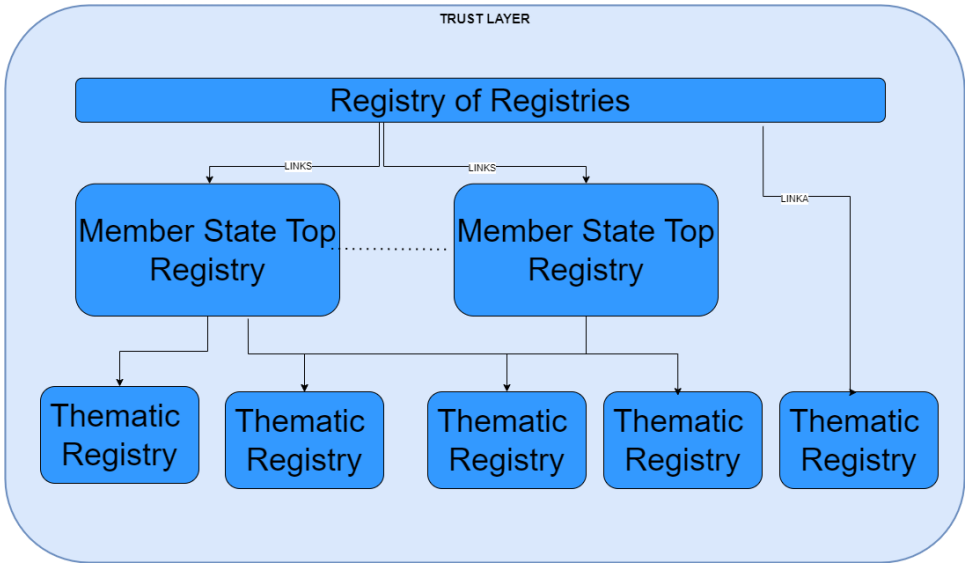


Figure 8: Multi-layer approach for EU Trust Registries

Within this model/architecture, there will be a unique registry of registries, managed directly by European Commission/EBSI where there will be a unique reference to each MS- root level Top Registry.

Each embers state Top level registry will have references to thematic registries (registries and related schemas registries) that will be authoritative for that Member State and Theme (e.g. Health Care, University, Secondary Education, etc). Each Thematic Registry could be managed within EBSI ecosystem with the existing governance model.

In any case, each MS National Supervisory body will have responsibility to appoint the appropriate entity both at MS level (Top Registry) and at Thematic level. Each appointed entity, whether directly or using a QTSP to operationally perform this task would need to be accredited by the MS NAB.

9.2 Scope

Our piloting phase is grounded in the concept of empowering each national business registry within the EU member states to become a root Trust Anchor Organization (TAO) within EBSIs Trust Model. Central to our pilot are two indispensable schemas: Organizational ID and the Power of Attorney. The Organizational ID uniquely confirms the identity of legal entities, while the Power of Attorney grants designated individuals the authority to represent their respective

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

organizations. We assume that a unified schema can effectively encompass legal entities across all jurisdictions within the European member states.

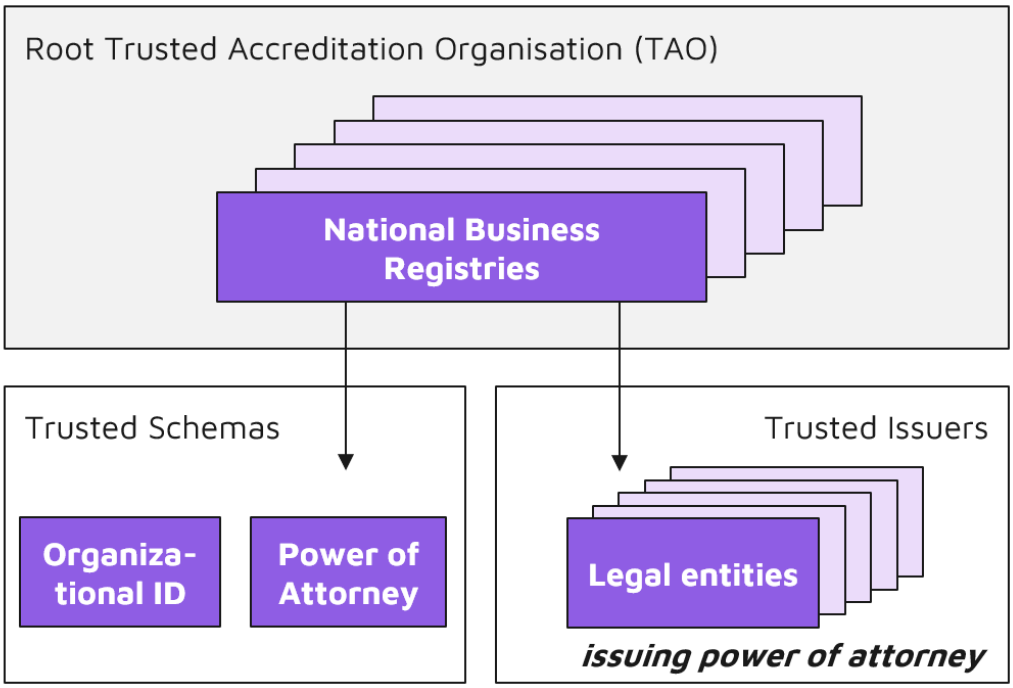


Figure 9: Piloting concept

The participating legal entities are supposed to become trusted issuers and, hence, become enabled to issue Power of Attorney to their belonging company representatives. Therefore, three critical processes must be implemented, ideally through fully automated means:

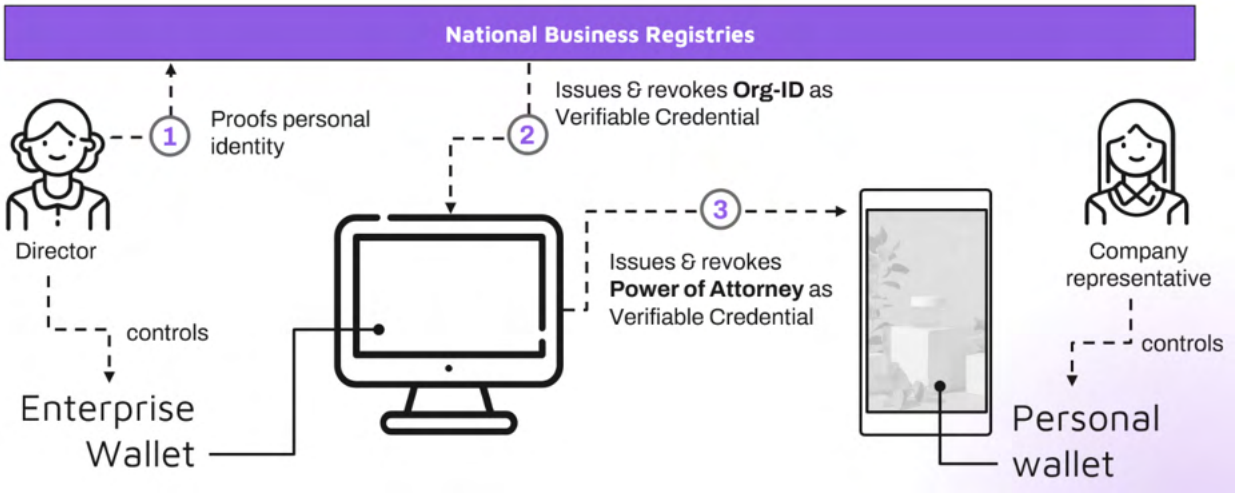
1) **Director Controls Enterprise Wallet and Proofs Identity**: In this step, the director of a legal entity assumes control of the enterprise wallet and verifies their identity with the National Business Registry (or with an intermediary). This ensures that only authorized individuals can access and manage the organization's digital identity.

2) **Issuance and Revocation of Org-ID**: The National Business Registry, or an intermediary acting on its behalf, is responsible for issuing and revoking Organizational IDs. These unique identifiers serve as the cornerstone of the digital identity framework, enabling seamless interactions within the ecosystem.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3) **Activation of Enterprise Wallet and Power of Attorney Issuance**: Once the Organizational ID is issued, the enterprise wallet is activated, granting the legal entity access to more services. For example, the enterprise wallet facilitates the issuance of a Power of Attorney to a personal wallet



belonging to the company representative, further empowering them to conduct business transactions securely.

Figure 10: Obtaining an LPID (ODI) during the Pilot phase

After careful consideration of available resources, we deliberated on various approaches for setting up the pilot and ultimately determined that IDunion SCE would serve as the root Trust Accreditation Organization (TAO). IDunion, being a European Cooperative, assumes this interim role on behalf of public bodies. This decision is rooted in the fact that IDunion operates as a neutral, non-profit organization governed by its members, ensuring impartiality and trustworthiness.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

The pilot encompasses four participating countries: Lithuania, Cyprus, Poland, and Slovenia. Each country aims to onboard 10 legal entities, which will receive an Organizational ID issued by IDunion SCE. Our goal is to orchestrate a test scenario wherein these previously unfamiliar legal entities engage in the exchange of their Organizational IDs. This exchange serves as a crucial step in fostering trust and confidence in cross-border interactions within the digital identity ecosystem.

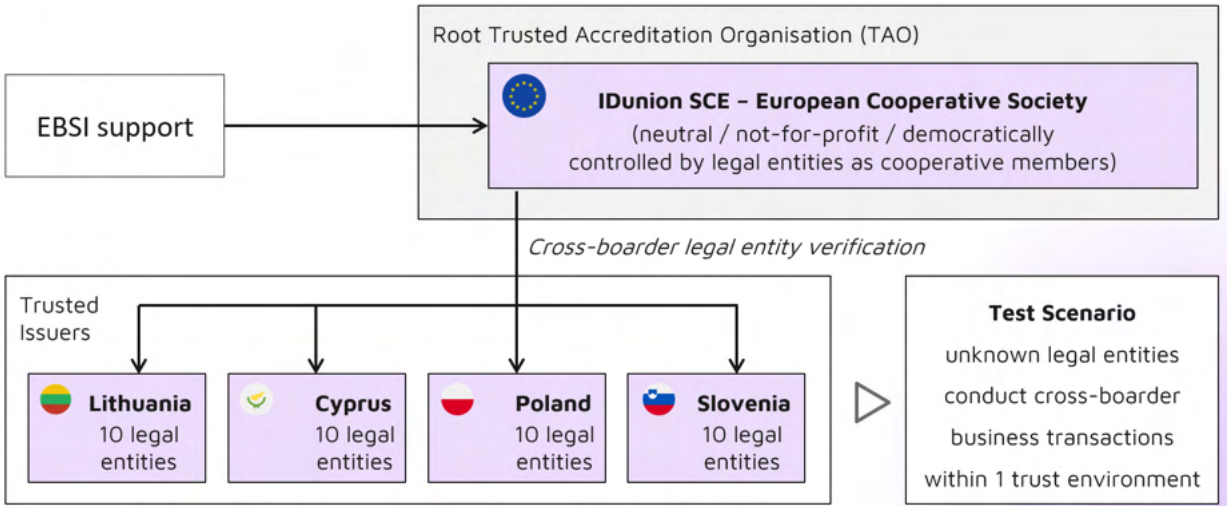


Figure 11: Pilot Participants

We've mapped out our next steps. Firstly, we'll establish IDunion as the primary authority to trust and finalize the definition of the two key components of our system. Additionally, we'll wrap up the development of the enterprise wallet, ensuring it's ready for basic testing.

During the testing phase, spanning six months, all participating legal entities will be onboarded onto the enterprise wallet. They'll obtain their unique IDs and authorize specific employees to act on their behalf. Furthermore, they'll exchange these authorizations among themselves to assess the functionality of our system.

Following this phase, we'll analyze our findings and compile them into a comprehensive report. We aim to complete this report by mid-2025, and it will serve as a valuable resource for determining our next steps and refining our approach.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

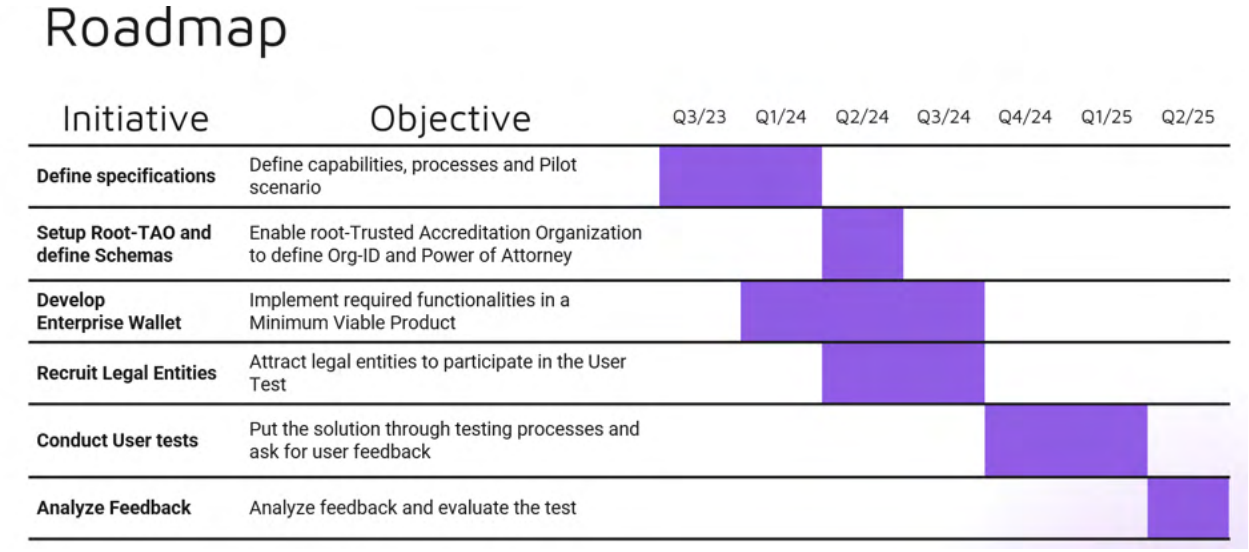


Figure 12: Roadmap for Piloting Phase

9.3 National specifics

9.3.1 Pilot in Italy

Pilot lead: INAIL

Scope

- INAIL becomes a TAO for companies that issue social security documents (WP5)
- INAIL will activate the Italian business registries to participate in the pilot
- INAIL will conduct the pilot with a 3-5 legal entities
- INAIL will test its new building Enterprise wallet to perform organizations onboarding to the EBSI network

Expected outcome

- Spreading knowledge on the EBSI network and new identity management protocols to other stakeholders in Italy
- Testing new Enterprise Wallet capabilities and checking its compliance with new EBSI-Vector specifications.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Helping organizations to join the EBSI network

Risks & Mitigation

- If Italian business registries are unable to participate in the pilot, INAIL may evaluate to emulate this role on its own by using data contained in its internal business registries (probably INAIL could work as Sub-TAO)
- If the new Enterprise Wallet implementation is not available for the pilot start date, INAIL may decide to conduct experiments using one of the open source and EBSI compliant Enterprise wallets available on the EBSI website

9.3.2 Pilot in Poland

Pilot lead: NASK

Scope

- NASK will activate the national commercial registry to participate in the pilot
- NASK will conduct the pilot with 5 collaborating universities and will include 10-15 legal entities
- NASK will develop a solution design for the Polish TAO

The goal of the VECTOR pilot in PL is to:

1. implementation in PL a pilot environment for EBSI Chain of trust by onboarding Root TAO, TAO, TI, Verifier, Holder wallets
2. implementation the use cases for the issuance and revocation for VC and VP for digital higher education diplomas, PDA1, EHIC and micro credentials in the area of professional qualification certification in cross-border communication between PL and EU Member State
3. testing the process of granting and revoking a VC for a power of attorney for an individual to represent a company through the OGR-ID mapping service
4. use of an EBSI-compliant open-source Enterprise Wallet in the pilot by TAO, TI, Verifier
5. use of an EBSI-compliant Holder wallet in the pilot by individuals (users) involved in the VECTOR pilots

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

6. implementation and integration with the national EID node on the test environment of the online PoC Service Provider ID-mapping service to binding/mapping of the DID holder wallet EBSI with the Minimal Data Set (eIDAS 1) of the user's personal data from the means of electronic identification at LoA substantial

Tasks to be undertaken to implement the Pilot

Tasks of the coordinator (NASK)

1. NASK performs Root TAO/TAO tasks by implementing a pilot EBSI Trust chain ecosystem.
2. Establishment of one test Polish EBSI blockchain trust chain under the supervision of the Minister of Digital Affairs as Root TAO via National Supervisory Body for Trust Services for the domain of education, social security PDA 1 and European Health Insurance Card EHIC. NASK defines Trusted Issuer Registry, Trusted Policy Registry, Trusted Schema Registry, Trusted Verifier Registry for the pilot.
3. support in onboarding TAO/TI, Verifier for EBSI compliant Enterprise Wallet + development integration component
4. NASK will coordinate and lead the implementation in the VECTOR pilot in Poland by involving identified public bodies as TAO, Trusted Issuer, Trusted Verifier and selected users (individuals) as holders of EBSI compliant digital wallets.
5. the NASK will onboard the involved Stakeholders at TAO/TI level in the implementation of Enterprise Wallet (OPI/ NFZ/ZUS)
6. for the implementation of the pilot in PL, NASK will use the EBSI holder wallet for an individual user from iGant.io/walt.id/ Altme/Gataca.io and the open-source digital Enterprise wallet from WP 3 as product D3.6 Reference open-source implementation of the issuer wallet and verifier for EBSI.
7. NASK will prepare the test data of individuals' users and coordinate the transfer to the LSP participants in PL. In the pilot, after functional and integration testing of the environments, the use of real personal data will be allowed only with formal consent as part of the parties' data processing (ensuring GDPR compliance).
8. implementation and integration with the PoC Service Provider test environment to carry out the ID-mapping process with the DID Holder wallet to bind the decentralized identifier with the data from the electronic identification medium at the LoA substantial.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

9. Integration with the PoC Service Provider ID mapping function (NASK builds/adopts) to assign and revoke a VC for a proxy to an individual to represent a company via the OGR-ID mapping service.
10. revocation of VC issued DID Legal Person TAO/TI and VC DID Holder wallet from PoC SP ID-mapping process
11. NASK is the operator of an EBSI node in Poland
12. NASK will prepare a summary report of the LSP VECTOR pilot conducted in PL.

Holder Wallet User tasks (list of participants)

1. download and install EBSI-compliant Holder Wallet (Altme/iGrant.io/Wallt.id/Gataca.io)
2. downloading VC DID Holder. Carry out the process of binding DID Holder wallet with Minimal Data Set - the physical user wallet will be used to communicate with PoC SP ID-mapping integrated with the national EID scheme test environment (cross-border node and national node) to map/bind DID Holder wallet with public registry data. The PoC Service Provider ID-mapping issues in response to VC requests the PID EBSI Holder wallet by mapping the DID with user data based on data from the electronic identification measure LoA substantial (eIDAS 1)
3. download VC - run test scenarios for downloading to Holder Wallet the TI issued verifiable credentials for WP4 (education) and WP 5 (PDA1, EHIC)
4. transfer of VPs - Carry out the process of transferring VPs to Verifier
5. collection of VC micro credentials - conduct test scenarios for collection of VCs to the holder wallet for micro credentials in the area of professional credentials
6. cancellation of VCs - conduct VC cancellation process for diplomas, PDA1, EHIC, micro credentials
7. transfer of VP to another Holder Wallet holder + verification of VP compliance

Tasks TAO/TI (OPI, NFZ, ZUS, University) + VC micro credentials

1. Enterprise Wallet EBSI - download and install EBSI-compliant Enterprise Wallet on open-source test environment
2. DID Legal Person - generate DID for TAO/TI (ORG-ID)
3. VC Attorney - perform VC process for a power of attorney for an individual to represent a company via OGR-ID mapping service (download on Holder Wallet)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4. import of test data into the test environment to synchronize EBSI Holder Wallet data with the data in the source registry to issue VC for [Diploma, PDA1, EHIC, Micro Credentials].
5. release of VC Perform VC release process and VP verification for use cases in pilot processes for their domain
6. issuance of VC micro credentials for professional credentials (Universities)
7. VP - verify personal data in their registers upon receipt of VCs
8. revocation of VCs - carry out revocation of VCs of issued credentials

Verifier tasks (University, OPI, Universities + VC micro credentials)

1. Enterprise Wallet EBSI - download and install EBSI compliant Enterprise Wallet on open-source test environment
2. DID Legal Person - generate DID for TAO/TI (ORG-ID)
3. perform VP verification process provided by Holder wallet for use cases in pilot processes for their domain
4. import test data into the test environment to synchronize EBSI wallet holder data with the data in the source registry to issue VCs for [Diploma, PDA1, EHIC, Micro Credentials].

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

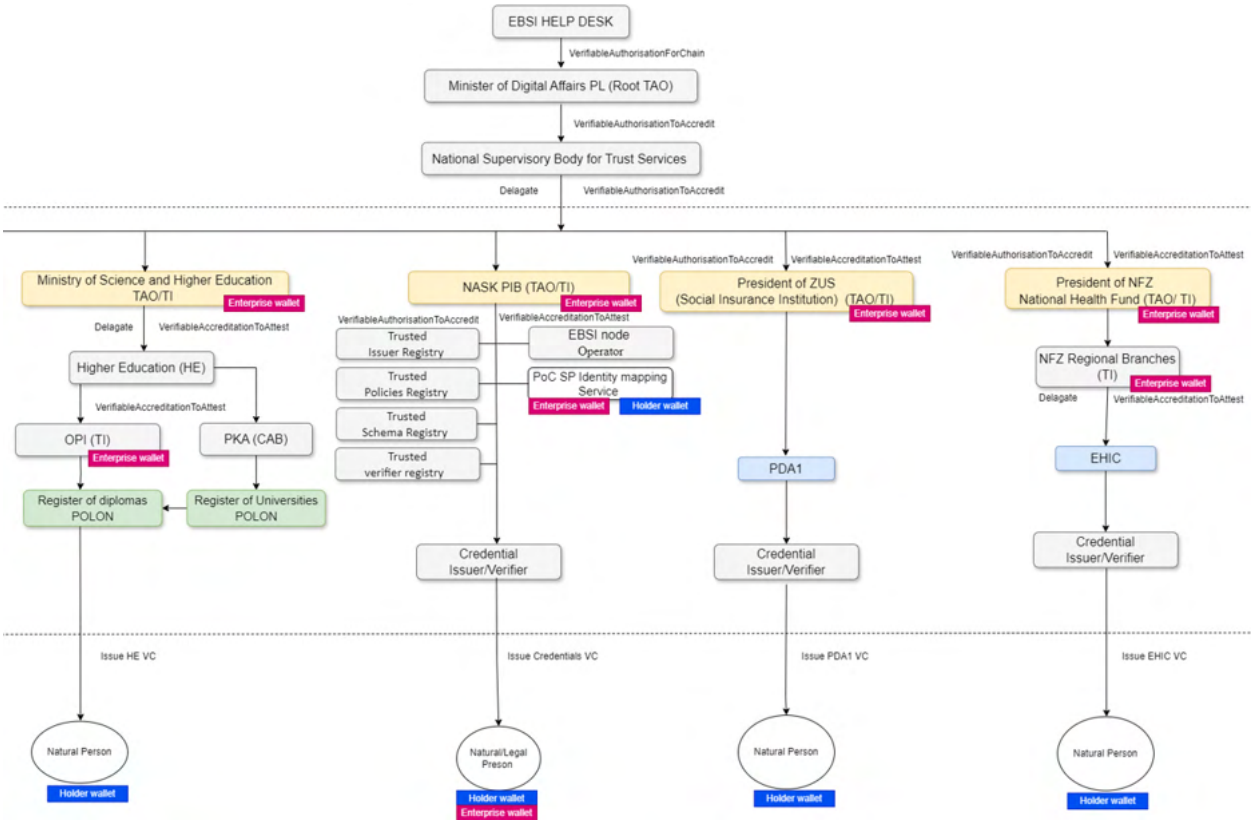


Figure 13: Piloting concept for Poland

Expected roadmap

- Pilot Month 1: Construction and implementation in PL of the EBSI test ecosystem completed with (confirmation of) role setting for Root TAO, TAO, TI, Verifier, Holder Wallet + onboarding wallets for each participant
- Pilot Month 2: Implementation and functional testing of EBSI digital wallets for use cases in Poland
- Pilot Month 2&3: Implementation and functional testing of EBSI digital wallets for use cases in Poland Implementation and functional testing of EBSI digital wallets for use cases between PL and other EU countries
- Pilot Month 4: Preparation of a summary and draft report of the VECTOR pilot in PL
- Pilot Mont 5: Development of a final report on the pilot in PL with recommendations

Risks & Mitigation

- Delay in delivery of Enterprise Wallet

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Lack of involvement or non-participation of the required public institutions in the pilot phase - mitigation of risk by political support from Ministry of Digitalization.

9.3.3 Pilot in Slovenia

Pilot lead: Hashnet

Scope

- Hashnet will contact and try to activate the Ajpes (i.e. national commercial registry) to participate in the pilot.
- Waiting for meeting with Ajpes/Slovenian business registry.
- Observing the progress development of enterprise wallet by other partners.
- Knowledge and technology transfer from other partners to Hashnet.
- Testing new Enterprise Wallet capabilities.

Expected outcome

- Ajpes will not want to collaborate, due to a lack of resources and budget.
- Spreading knowledge on the EBSI network and to other stakeholders in Slovenia.

Expected roadmap

- Pilot Month 1: Work on the project scope
- Pilot Month 2: Work on the project scope or risk and mitigation proposal

Risks & Mitigation

If Slovenian business registries are unable to participate in the pilot and other conditions in the project scope are not met:

- Hashnet will conduct the pilot with 10 legal entities and universities using Hashnet Mainnet, Wallet and Diploma on blockchain application;
- Hashnet will work on a solution design for the Slovenian TAO;
- Hashnet will use SI-Chain (i.e. Slovenian National Blockchain Infrastructure) to act as Slovenian TAO.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

10 Conclusions

In this document we conducted an in-depth analysis upon specifications for an EBSI business registry. While we initially felt it challenging to define a scope for this registry, the team of 12 identity experts from 12 different EU-member states could agree on a common approach: The implementation of an EBSI business registry means onboarding national commercial registries as Trusted Accreditation Organizations for a specific trust environment that is set up using the EBSI technology.

We explained a generic onboarding procedure for national commercial registries as basis for our piloting phase. Doing so, we translated EBSI´s publicly available documentation for our context and developed the following recommendations:

- The onboarding procedure for TAOs should be simplified
- EBSI-specific terminology should be explained an a glossary
- The documentation´s navigation should be improved
- EBSI should offer a set of consulting services for the onboarding process
- EBSI should provide links to download EBSI-conformant wallets
- EBSI should provide a trusted verifier registry
- Identity checks should be included during the onboarding process
- JSON Schemas table should be reviewed

Moreover, we described how Organizational Identities can be issued and revoked as Verifiable Credential. Since the procedure might differ depending on the underlying context, we imagined a specific scenario from which we were able to derive clear recommendations. In this scenario we assume that legal entities want to become a trusted issuer in a trust environment to be able to issue digital passports of the products they produce. In this case, we recommend national commercial registrars to include legal entities they know in the trusted issuer registry and provide them with short-lived Verifiable Credentials that confirm their organizational identity.

Considering the needs from Work Package 5 within EBSI-VECTOR as well, our analysis resulted in functional requirements for Use Case designers, the EBSI development team and Enterprise wallet providers. Eventually, we set the identified new building blocks in context by providing an overview of a proposed system architecture.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Last but not least, we scoped the piloting phases for the participating countries in Lithuania, Cyprus, Poland and Slovenia.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

11 Annex I: Fundamental differences between natural persons and legal persons

	Natural Person (NP)	Legal person (LP)
Nature of existence	Natural persons are individual human beings. Each person has a unique identity, consciousness, and the capacity for personal experiences and decision-making.	Legal persons are entities created and recognized by the law. They don't possess consciousness, emotions, or personal experiences. Legal persons exist as a ***legal fiction***, allowing them to have rights and responsibilities similar to natural persons.
Formation	Individuals are born and acquire legal personality automatically by virtue of being human. Legal recognition is not a result of any formal process.	Entities such as corporations are ***created through legal processes*** such as registration, incorporation, or establishment in accordance with specific legal frameworks.
Rights and Responsibilities	Individuals have a broad range of rights and responsibilities, including the right to live, liberty, and property. They can enter into contracts, sue or be sued, and are subject to legal obligations.	Legal entities are granted certain rights and responsibilities by law. They can own property, enter into contracts, sue or be sued, and engage in legal activities. The scope of rights and responsibilities may vary based on the type of legal person.
Decision making	Individuals have the capacity for personal judgment and decision-making. They can act on their own behalf and make choices in various aspects of life.	Legal entities act through agents, officers, or representatives. While these representatives can make decisions and engage in legal transactions, it is done ***on behalf of the entity*** rather than as a result of personal judgment.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Duration of existence	Human life has a finite duration, and the legal personality of an individual ceases upon death.	Entities recognized by the law can have perpetual existence, regardless of changes in ownership or leadership. They can continue to exist even if the individuals associated with them change.

Table 1: Fundamental differences between natural person and legal person

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

12 Annex II: Improving the EBSI Documentation

This Annex specifies our recommendations for improving the EBSI documentation available in the "EBSI Hub", which contains valuable content for different stakeholder groups. Our analysis and recommendations aim to enhance the usability, clarity, and accessibility of the documentation.

Overview

1. Analysis of Current Documentation Structure: We examined each page of the current documentation, providing remarks and specific recommendations for improvement.
2. New Approach for User Groups (Personas): We propose a new approach to address the needs of different user groups who require information from the EBSI documentation.
3. Core Needs for Trust Ecosystem Builders and Natural Persons: We identified and addressed the core needs of these two key user groups.

Main Menu					
#	**Topic**	**#**	**Subtopic**	**Leads to**	**Remarks**
1	About us	a)	What is EBSI	Three pillars of EBSI	Combine with “About us” to avoid redundancy
		b)	About us	• A Menu: i) about us, ii) EU Expert Group on Blockchain Ehtics, iii) European Blockchain Sandbox • Subchapter: Governance and Coordination, Community and Participants, EBSI figures, history & context	• Not Mutually exclusive to “What is EBSI” • Avoid naming subtopic equally to topic • Consider merging Topic 1a) and 1b)
		c)	Legal	A menu with all legal documents	Create a dedicated area for legal experts
		d)	News	A series of blog posts	Merge and relocate these sections to the footer to minimize distractions
		e)	Events	Shows 3 past events	

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

2	Learn	a)	Explained Series	Learning modules	Include interactive learning modules to engage users and test their knowledge
		b)	Success Stories	• Piloted Use Cases • Explanations about the ecosystem • EBSI Demo Day 2022 • Requirements to join Early Adoptes Programme	• Clarify purpose of this Subtopic and ensure relevance • See remark 1d) if this is a marketing initiative • Include a call-to-action if you want website visitors to onboard to the Use Cases
		c)	EBSI Projects	• A concept of the challenge for digital verification • The Vision • Links to past on ongoing projects	• Consider renaming the subtopic, e.g. “challenge of verification” • Consider excluding the Project links from the subchapters since they do not clearly address the learner
		d)	EBSI Verifiable Credentials	• A history of web3 • An explanation of the EBSI ecosystem • Introduction of 2 VC domains • A link to success stories	Leave as is
		e)	Experience Center	• An explanation what the Experience Center is • Pictures showing the center	• Website seems incomplete: physical address and opening hours are missing

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

				• Announcement for interactive demos and talks	• Don´t promote activities if the experience center does not exists anymore
3	Use EBSI	a)	Choose a wallet	• An explanation about EBSI conformant wallets • A menu to select the wallets	Make sure all displayed wallet provider can onboard a natural person as holder
		b)	Pilot with EBSI	A detailed description of the Early Adopters programme	Change the description for subtitle from "EBSI incubator" to "Early Adopters programme"
		c)	Apply for grants	Shows outdated open calls	Keep content updated and relevant
4	Deve-lopers	a)	Start a project	EBSI Hub: Overview about how process how to develop a project	Change topic to "Develop" to remain consistent with other topics (Learn – Use – Develop)
		b)	VC Framework	EBSI Hub – Ba)	Consolidate developer-specific content in the EBSI Hub men
		c)	Technical Specifications	EBSI Hub – Bb)	
		d)	Tools	An overview of tools for developers	
		e)	Tests	Conformance guidelines and a subchapter: i) learn ii) build solutions, iii) Standard versions, iv) changelog	
5	Node opera-tors	a)	Become a node operator	Instructions on how to become a node operator	Move sections related to node operation to the footer to reduce distractions

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

		b)	Network map	Figures and a map showing the location of nodes	
		c)	Node operators community	An authentication gateway to log in	

EBSI Hub					
#	**Topic**	**#**	**Subtopic**	**Leads to**	**Remarks**
A	Start a project	a)	Get started	EBSI Onboarding Kit, Overview of essential ressources, brand guidelines	Move brand guidelines to a separate area for legal experts (see Main Menu 1c)
		b)	Define	Process on how to set up User Journeys for a Use Case	Leave as is
		c)	Design	Technical design for implementation	Leave as is
		d)	Build	Details description on implementation	Leave as is
B	Specifica-tions	a)	VC Framework	Technical guidelines on defining, issuing, and revoking Verifiable Credentials	Move this section to the learning chapter (see Main Menu 2)
		b)	APIs	An overview of APIs for Pilot and Conformance environment	Provide context for API descriptions to ease understanding
		c)	Improvement Proposals (EBIPs)	Links to current development activities	Remove as it addresses a different audience
		d)	EBSIs Blockchain Ecosystem	Explains the blockchain technology, taxonomy and	Move to learning section (see Main menu 2)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

				how EBSI configured Hyperledger Besu for their purposes	
C	Tools	a)	Libraries	Manuals to four different libraries	Leave as is
		b)	CLI	Comprehensive technical documentation about the EBSI Command Line Interface	Highlight the need for profound knowledge about the EBSI trust model and a defined Use Case.
		c)	DID Resolver	Demonstration on how a DID is resolved	Provide recommendations for implementing the DID Resolver.
		d)	DID Generator	Demonstration on how a DID is generated	Offer guidance for wallet providers and natural persons on the next steps after generating a DID
		e)	Multiformat Converter	Demonstrations on how different input parameters can be transformed to different output formats	Provide context for implementers on the purpose of the demonstration
		f)	VC Validator	Demonstrates how a VC is validated	
D	Confor-mance	a)	Guidelines	Contains comprehensive procedure for wallet providers to become EBSI conformant, provides current API versions and a changelog	Leave as is
		b)	Testing	Guidance for wallet providers to proof EBSI conformancy	Leave as is

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Overall, we believe that the content can be overwhelming for some users since it requires to have gained a lot of knowledge before people can comprehend certain aspects of the documentation. The order in which information is supposed to be read is not obvious. User with previous knowledge will also find it to identify a starting point for their skill level.

In a first step, we recommend improving the usability of the documentation by implementing a robust search feature to allow users to quickly find relevant information. This should include keyword search, filters for the below mentioned personas, knowledge areas and types of information as well as an autocomplete function to improve the search efficiency.

In a second step, we recommend defining different user groups and addressing them with tasks they can directly start working on.

We foresee these user groups to be addressed with these specific tasks:

#	Persona	Task
1	Wallet provider	Build an EBSI conformant wallet
2	Trust Ecosystem builder	Define a Trust Environment with the EBSI Trust Model Become a root-TAO Define a Schema
3	Implementing developer	Test EBSI Get an EBSI conformant wallet
4	Legal expert	Check legal documents and compliance
5	Natural person	Get an EBSI conformant wallet Request your Digital Diploma Request your Digital Social Security Document
6	Trusted Issuer	Get an EBSI conformant wallet Onboard to a Trust Environment Issue your first Verifiable Credential
7	Verifier	Get an EBSI conformant wallet Test EBSI
8	EBSI developer	See latest EBSI developments
9	Node operator	Become a node operator

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

We realize that the current documentation primarily addresses Wallet providers. The fact that quite a few EBSI conformant wallets already exist, confirms that the documentation fulfills their needs.

However, other Personas might not find the EBSI documentation suitable for their purposes and for their previous knowledge. We highlight this aspect and recommend the following.

Addressing Trust Ecosystem Builders

A Trust Ecosystem Builder is an individual or organization responsible for establishing and maintaining trust environments using the EBSI framework. These builders act on behalf of (public) organizations that seek to leverage EBSI's capabilities to set up a trust infrastructure.

Currently, the process for onboarding a root-TAO is managed via a ticketing system and requires an EU-Login. This process can be cumbersome and may not scale effectively as the demand for EBSI services grows.

Recommendations (if Trust Ecosystem Builders are considered as target audience)

Streamline Onboarding Process

- Automate Onboarding: Develop an automated onboarding system for root-TAOs to enhance the current manual ticketing system. This system should include clear, step-by-step instructions to guide users through the process.
- Parallel Onboarding Capability: Design the system to handle multiple onboarding requests simultaneously, ensuring that many organizations can be onboarded without delays.

Enhance User Experience

- Clear Entry Points: Create a dedicated and prominent section on the EBSI website for Trust Ecosystem Builders. This section should provide an overview of the onboarding process, necessary requirements, and resources.
- User-Friendly Interface: Ensure that the interface is intuitive and accessible, catering to both technical and non-technical users.

Provide guided Tutorials: Ideally, develop video guides that explain the onboarding process, the roles and responsibilities of a root-TAO, and how to utilize EBSI tools.

Addressing End Users

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

End Users are individuals who use EBSI-conformant wallets to manage their digital identities and credentials. They need clear guidance on how to generate, manage, and use their digital identities securely.

End Users may find the existing documentation overwhelming, particularly when it comes to self-generating Decentralized Identifiers (DIDs) and managing their private keys.

Recommendations (if Natural Person are considered as target audience)

Support Self-Generation of DIDs

- Step-by-Step Guides: Provide clear, step-by-step instructions on how to self-generate DIDs and DID documents. This should include an explanation of the importance of self-sovereign identity and how to keep private keys secure.
- Context and Next Steps: Ensure that the DID Generator tool on the EBSI Hub (https://hub.ebsi.eu/tools/did-generator) includes context on how to use the generated DID and what the next steps are, such as importing the private key into a password manager or other secure storage.

Enhance Security Education: Ideally, educate users on best practices for securing their private keys and managing their digital identities. This could include guidelines on creating strong passwords, using two-factor authentication, and safely storing recovery phrases.

Conclusion

Overall, the content can be overwhelming for some users, requiring substantial prior knowledge. To mitigate this, we recommend defining different user groups and addressing them with actionable tasks. By refining the structure and providing clear guidance, EBSI documentation can become more accessible and useful to all stakeholders.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.