EBSI-VECTOR
Education and work reloaded

D3.1: Evaluation of the current ESSIF implementation and legal/governance framework with focus on the 1st implementation phase

Project title:	**EBSI-VECTOR** - EBSI enabled VErifiable Credentials & Trusted Organisations Registries
Grant Agreement No.	101102512 - DIGITAL-2022-DEPLOY-02-EBSI-SERVICES
Deliverable Title	D3.1: Evaluation of the current ESSIF implementation and legal/governance framework with focus on the 1st implementation phase.
Version:	1.1
Date:	05/07/2024
Responsible Partner:	DANUBETECH
Authors:	Markus Sabadello (DANUBETECH), Samuel Gomez (Gataca), Steffen Schwalm (MSG), Irene Hernandez (Gataca), Carlo Lentini (INAIL) Helmut Nehrenheim (GovPart)
Contributing Partners:	DANUBETECH, Gataca, MSG, DRV-BUND, INAIL, GovPart, IDunion SCE
Reviewers:	Irene Hernandez (Gataca), Helmut Nehrenheim (GovPart)
Dissemination Level:	PU – Public

Document Change History

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

Version	Date	Author (organisation)	Description
v0.0	11/09/2023	Multiple Authors	Work-in-progress
v0.1	12/09/2023	Multiple Authors	Ready for Internal Review
v0.2	27/09/2023	Multiple Authors	Work-in-progress
v1.0	29/09/2023	Multiple Authors	Final Release
v1.1	05/07/2024	Multiple Authors	Added mapping table (section 13) between capabilities and business requirements

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

1. EXECUTIVE SUMMARY 11

2. INTRODUCTION 13

3. INFRASTRUCTURE FEATURES 15

3.1. IDENTIFIER TYPES 15

3.1.1. As/Is 15

ToBe 15

3.2. OPERATIONS AND PERFORMANCE 15

3.2.1. As/Is 16

ToBe 16

4. ATTESTATION FEATURES 17

4.1. DATA MODELS OF VC CONTAINERS 17

4.1.1. As/Is 17

ToBe 17

4.2. DATA MODEL OF VC CONTENT (DIPLOMA AND SECONDARY SCHOOL CERTIFICATE) 18

4.2.1. As/Is 18

ToBe 18

4.3. DATA MODEL OF VC CONTENT (SOCIAL SECURITY PASS) 19

4.3.1. As/Is 19

ToBe 19

4.4. SELECTIVE DISCLOSURE 19

4.4.1. As/Is 19

ToBe 20

4.5. (QUALIFIED) SIGNATURE/SEAL OF CREDENTIALS BY ISSUER 20

4.5.1. As/Is 20

ToBe 20

5. PROTOCOL FEATURES 21

SUPPORTED PRESENTATION PROTOCOLS 21

5.1.1. As/Is 22

ToBe 22

SUPPORTED ISSUANCE PROTOCOLS 22

5.1.2. As/Is 22

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.

ToBe *22*

6. HOLDER WALLET FEATURES 23

6.1. MULTI-IDENTITY SUPPORT 23

6.1.1. As/Is 23

ToBe 23

6.2. MULTI-LANGUAGE SUPPORT 23

6.2.1. As/Is 23

ToBe 24

6.3. ACCESSIBILITY AND NON-DISCRIMINATION REQUIREMENTS 24

6.3.1. As/Is 24

ToBe 24

6.4. AUTHENTICATING WALLET INSTANCES 24

6.4.1. As/Is 24

ToBe 25

6.5. OPERATIONS AND PERFORMANCE 25

6.5.1. As/Is 25

ToBe 25

6.6. QUALIFIED SIGNATURE OF DOCUMENTS BY HOLDER 25

6.6.1. As/Is 25

ToBe 25

6.7. ADDITIONAL SOCIAL SECURITY REQUIREMENTS 26

6.7.1. Issuance flow 26

6.7.2. Wallet Functions 26

6.7.3. Interactions 27

6.7.4. Verification flow with Verifier 27

7. ENTERPRISE / LEGAL ENTITIES WALLET FEATURES 28

7.1. ENTERPRISE WALLET AND LEGAL ENTITY WALLET 28

Overall High Level Definitions 28

7.1.1. High Level Enterprise Wallet Features 30

7.1.2. As/Is 31

ToBe 31

7.1.3. Additional Considerations 31

ORGANISATIONAL IDENTITY 33

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.

7.1.4. As/Is 33
7.1.5. ToBe 33

8. DID LIFECYCLE MANAGEMENT 35

8.1. DID CREATION 35
8.1.1. As/Is 35
8.1.2. ToBe 35
8.2. DID DEACTIVATION/REVOCATION 35
8.2.1. As/Is 35
8.2.2. ToBe 35

9. CREDENTIAL LIFECYCLE MANAGEMENT 36

9.1. CREDENTIAL SHARING CONSENT APPROVAL (DATA AGREEMENTS) 36
9.1.1. As/Is 36
9.1.2. ToBe 36
CONSENT REVOCATION 36
9.1.3. As/Is 36
9.1.4. ToBe 37
CREDENTIAL STATUS CHANGE 37
9.1.5. As/Is 37
9.1.6. ToBe 37
CREDENTIAL EXPIRATION MANAGEMENT 38
9.1.7. As/Is 38
9.1.8. ToBe 38

10. INTEROPERABILITY 39

10.1. INTEROPERABILITY WITH OTHER TRUST FRAMEWORKS 39
10.1.1. As/Is 39
10.1.2. ToBe 39
10.2. VISUALIZATION OF CREDENTIALS 40
10.2.1. As/Is 40
10.2.2. ToBe 40

11. OTHER TECHNICAL TASKS 40

11.1. API DEFINITION & DOCUMENTATION 40
11.1.1. As/Is 40

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.

11.1.2. ToBe *41*
11.2. LONGEVITY OF CRYPTOGRAPHIC ALGORITHM 41
11.2.1. As/Is *41*
ToBe *42*
12. LEGAL/GOVERNANCE 45
12.1. COMPARISON EBSI GOVERNANCE ROLES EIDAS 2.0 GOVERNANCE ROLE 45
12.2. ISSUANCE AND CERTIFICATION OF WALLETS 49
12.2.1. As/Is *49*
12.2.2. ToBe *49*
12.3. ISSUANCE OF CREDENTIALS 51
12.3.1. As/Is *51*
12.3.2. ToBe *51*
IDENTIFICATION OF HOLDER, ISSUER AND VERIFIER 52
12.3.3. As/Is *52*
12.3.4. ToBe *52*
12.4. STATUS AND REVOCATION OF CREDENTIALS 53
12.4.1. As/Is *53*
12.4.2. ToBe *53*
12.5. TRUSTED ISSUER REGISTRY 54
12.5.1. As/Is *54*
12.5.2. ToBe *54*
12.6. VERIFICATION OF CREDENTIALS 54
12.6.1. As/Is *54*
12.6.2. ToBe *54*
12.7. TRUSTED VERIFIER REGISTRY 55
12.7.1. As/Is *55*
12.7.2. ToBe *55*
12.8. TRUSTED WALLET PROVIDERS REGISTRY 55
12.8.1. As/Is *55*
12.8.2. ToBe *56*
12.9. AUTHENTIC SOURCES 56
12.9.1. As/Is *56*
12.9.2. ToBe *56*
12.10. QUALIFIED SIGNING OF CREDENTIALS 56

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.

12.10.1. As/Is 56
12.10.2. ToBe 57
12.11. SECURITY AND CERTIFICATION OF EBSI LEDGER 57
12.11.1. As/IS 57
ToBe 57
13. CAPABILITIES AND BUSINESS REQUIREMENTS 58
14. **CONCLUSIONS 70**

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

FIGURE 1 – A SAMPLE OF A BLOCKCHAIN WITH ON-CHAIN AND OFF-CHAIN STORAGE – REHASHING ISSUE 42
FIGURE 2 – "LOGICAL" BLOCKCHAIN 43
FIGURE 3 – SOLUTION EXAMPLE 45
FIGURE 4 – EIDAS TRUST FRAMEWORK 48

List of Tables

TABLE 1 – ROLES WITHIN EIDAS 2.0 GOVERNANCE 45
TABLE 2 – EBSI/EIDAS2.0 COMPARISON 48

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

Abbreviation	Definition
API	Application Programming Interface
ARF	Architecture and Reference Framework
CAB	Conformity Assessment Bodies
CWT	Concise Binary Object Representation (CBOR) Web Token
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
EBSI	European Blockchain Service Infrastructure
EDIC	European Digital Infrastructure Consortium
eIDAS	electronic Identification, Authentication and Trust Services
ELM	European Learning Model
ETSI	European Telecommunications Standards Institute
EUDIW	EU Digital Wallet
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JSON-LD	JSON for Linking Data
JWT	JSON Web Token
MFA	Multi Factor Authentication
MS	Member State
OCSP	Online Certificate Status Protocol
OID4VC	OpenID for Verifiable Credentials
PID	Personal Identification
PKI	Public key infrastructure
QEAA	Qualified Electronic Attestation of Attributes
QES	Qualified Electronic Signature

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.

QTSP	Qualified Trust Service Provider
RFC	Request for Comments
TS	Technical Specification
VC	Verifiable Credential
W3C	World Wide Web Consortium
WG	Working Group
WP	Work Package

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

The EBSI-VECTOR project aims to provide the needed continued support of EBSI to provide improved services to citizens, simplify administrative processes for organizations, and provide opportunities for businesses. This document is part of a set of deliverables that attest to the three outcomes expected for the project, namely:

1. To reinforce the EBSI and progress the deployment and the extension of the EBP use cases
2. To provide recommendations for the further development of the EBSI ecosystem
3. To increase the engagement with stakeholders

Working Package 3 (WP3) was tasked, among other objectives, with further defining the specifications of the current European Self Sovereign Identity Framework (ESSIF) specification capabilities to be built in EBSI, so it can support use cases and business requirements in the education and social security domains (Task 3.1). T3.1 included the analysis of current capabilities and the definition of new required capabilities, including support of identities for legal entities, based on the business requirements identified in Working Packages 4 (education) and 5 (social security).

This document is the outcome of T3.1 and highlights both the as-is status of ESSIF capabilities and suggests improved and extended capabilities to-be implemented by the EBSI technical team to support the uptake of the verifiable credentials and decentralized registries by the targeted business domains.

During the work executed in T3.1 so far, a wide variety of topics in the technical, legal and governance areas were discussed and analyzed, which are reflected in the sections and sub-sections in this deliverable. Each major topic is reflected in a specific section of this document, containing a list of comments marked as "As/Is" and "ToBe" and reflecting the evaluation of the current capabilities, as well as ideas for future improvement. Subsequent deliverables of this T3.1 will further elaborate on the listed topics.

Among a comprehensive list of major topics, a few entailed long and recurrent discussions, highlighted below:

1. EBSI alignment with eIDAS 2 / ARF: Many task participants expressed a desire to align EBSI to the largest extent possible with eIDAS 2 and the Architecture Reference Framework (ARF). The main arguments revolved around the inconvenience for EU citizens and residents to hold an eIDAS 2 compliant wallet (e.g., for a mobile driver's license), and a separate EBSI compliant

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.

wallet for other domains (e.g., for a diploma credential), should EBSI not be in complete alignment with the ARF. While current ESSIF specifications comply with some aspects of the ARF v1.1.0 (link) (e.g., in the use of the OID4VC protocol suite), there seems to be less alignment in other areas (e.g., Verifiable Credential formats). Understanding that both the ARF and EBSI specifications are still moving targets and not finalized, efforts should be made to converge the two initiatives. This alignment does not only concern the technical specifications, but also topics such as governance and roles of participants in the ecosystem. In section 12.1, we therefore present a table which relates eIDAS 2 concepts (e.g., QTSP of Attestations of Attributes) with EBSI concepts (e.g., Trusted Issuer).

2. Revocation: As pointed out in ongoing discussions, revocation is a complex topic and hence different approaches can be observed in the market. Furthermore, revocation mechanisms seem to have strong dependencies with the specific Verifiable Credential data formats. For example, the well-known and widely adopted "StatusList2021" specification is based on the JSON-LD W3C Verifiable Credential Data Model, while the JWT community is working on their own "JWT and CWT Status List" approach. The team suggests using existing revocations mechanisms such as RFC 6960 that ensure no dependency on data formats. We also note that EBSI already defines a framework for various strategies of credential status change.

3. Organizational Identity, Legal Entity Wallets, Enterprise Wallets: We explored the importance of wallets for enterprises and legal entities, noting that they may not necessarily be the same. **R**equired functionalities were discussed, including custody of private keys, issuance/verification of Verifiable Credentials, storing/requesting/presenting Verifiable Credentials, providing API/GUI to admin/operate, and identification and anchoring of DIDs. One conclusion is the need to define a modular service called "EBSI 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.

2. Introduction

This document is the outcome of activities conducted in Task 3.1 (Define ESSIF Specifications) within WP3 from the EBSI-VECTOR project inception until the end of month 3.

The main scope of task T3.1, that will continue over the following 15 months, is to act as a bridge on one hand between the technical work package WP3 and the use case work packages WP4 and WP5, and on the other hand between EBSI-VECTOR and the EBSI core team. The objective is ultimately to ensure that the requirements of the use cases can be successfully implemented given the capabilities provided by EBSI.

This document constitutes Deliverable D3.1 and includes an evaluation of the current ESSIF capabilities and a list of recommendations for improved and new capabilities.

For the elaboration of this document, T3.1 responsible organizations and individual participants held a liaison meeting on 28th June 2023 with participants from both WP4 and WP5, with the intention of learning more about the use case requirements. We subsequently invited WP4 and WP5 leaders to our weekly T3.1 meetings. We also requested additional input from WP4 and WP5 via email on 17th August 2023. We hope to be able to intensify exchange with those work packages and obtain clear use case requirements as the project progresses, to ensure successful implementation.

Individual participants of T3.1 also interacted with the EBSI core team in various ways, e.g., through regular calls, email threads, personal meetings (e.g., in Ljubljana in June 2023), and via the new EBIP (EBSI Improvement Proposal) mechanism.

A meeting was also held between T3.1 and T2.2 leads, in order to understand the overlap and dependencies between the two tasks. The common understanding was that D3.1 would serve as input for later T2.2 deliverables, and that later in the project the T2.2 deliverables in turn would inform work in T3.1.

Additionally, several topic-focused discussions were conducted based on presentation delivered by individual partners:

- Ideas on revocation within EBSI, 14th August 2023, by MSG
- Enterprise Wallets and Legal Entity Wallets, 21st August 2023, by INAIL
- Data Agreements, 28th August 2023, by Gataca
- Organisational Identities, 4th September 2023, by GovPart

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.

As a result, this deliverable D3.1 includes major sections that address the needs of these internal and external stakeholders to the EBSI-VECTOR project. First, the document focuses on defining feature requirements for the core infrastructure (**section 2**) and Verifiable Credentials (**section 3**), including considerations for data models in the two target domains. Next, the document focuses on how these attestations shall be exchanged and dives into the different exchange protocol features for issuance and verification (**section 4**). Once the basic building blocks are analyzed, the document dives into wallets and necessary functional requirements for both natural persons (**section 5**) and legal entities (**section 6**).

Following the definition of technical features for the infrastructure, data and application layers, the document dives into the lifecycle aspects of these features, defining requirements for the lifecycle management of DIDs (**section 8**) and VCs (**section 9**). The technical sections of the document are further completed with requirements related to interoperability (**section 10**) and other miscellaneous topics (**section 11**).

The document includes also with a comprehensive analysis of the requirements needed from a legal/governance perspective (**section 12**).

Last, the document includes (**section 13**) a map between the technical capabilities evaluated in this deliverable, and business requirements related to 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.

3. Infrastructure Features

3.1. Identifier types

This section describes requirements related to identifiers for issuers, holders, verifiers.

3.1.1. As/Is

- EBSI uses W3C Decentralized Identifiers (DIDs)
- EBSI uses two different DID Methods for legal and natural persons.
- DIDs for natural persons:
    - EBSI uses did:key method (off-ledger) for natural persons (link)
    - EBSI uses only one form of did:key based on the “jwk_jcs-pub" multicodec value.
    - Previously, EBSI also defined a did:ebsi v2 method for natural persons, but that seems to be deprecated (link)
- DIDs for legal entities:
    - EBSI defines did:ebsi method (on-ledger) for legal entities (link)
    - DIDs for legal entities are considered public identifiers, and their uniqueness is enforced through the DID Registry.

ToBe

- Many other communities are also using did:key, but there are many types of did:key, and EBSI’s use of did:key (the “jwk_jcs-pub" multicodec value) is not what most other projects use. Perhaps EBSI should also support more common types of did:key.
- If EBSI favors the “jwk_jcs-pub" multicodec value of did:key, then perhaps EBSI should also consider the did:jwk method instead.
- There is a recommendation to analyze the need for EBSI to support other DID methods like did:indy, did:ion etc., and what does “support” shall mean in this context.
- An issue was raised into the did:key repository to add the EBSI implementation into the official repository. https://github.com/w3c-ccg/did-method-key/issues/63.

3.2. Operations and Performance

This section describes requirements about performance, real-time protocols, etc. of the EBSI ledger and APIs

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.

3.2.1. As/Is

- EBSI is a blockchain with nodes hosted in each member state, which provides resilience against failure of individual nodes.
- EBSI Network Operators can be "any organisation in one of the European Blockchain Partnership countries (EU 27 + Norway and Liechtenstein)". However, today, EBSI nodes are mostly operated by government entities, e.g., Italian Ministry of Business.
- There is an EBSI Support Desk available to answer requests about EBSI node operations, API usage, etc. This Support Desk service is provided by the European Commission.
- EBSI is currently built with Hyperledger Besu and therefore "inherits" various properties (such as performance) from this blockchain technology.

ToBe

- There should be further clarity about roles and responsibilities for the operation of the EBSI network. E.g. In cases where bugs are found, performance is low, a node is down, an attack happens, etc., who is authorized to report the issue and who is responsible for addressing the issue, in particular when it attains different nodes, which channels shall be used and what protocols shall be implemented in case of disaster. In particular, further clarifications are needed regarding the roles and responsibilities of:
    - Qualified Trust Service Provider (QTSP) of Electronic Ledger (see eIDAS section 11)
    - European Digital Infrastructure Consortium (EDIC)
- There should be a clear plan for business continuity of EBSI after projects like EBSI-VECTOR end.
- There should be a clear governance model for EBSI-related support, e.g. what are the responsibilities of the EBSI Service Desk, who can request what type of support, what are the processes for service management. This should be implemented according to ISO 20000.
- Furthermore, Service levels need to be defined for both the infrastructure and EBSI Service Desk, e.g. network availability and response times
- A disaster plan, including backup and recovery procedures, should be defined, in case of major infrastructure failures or attacks.

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.

- There should be clearer guidelines regarding who should be EBSI node operators. E.g. should EBSI nodes only be operated by member state public authorities, or by universities, or by QTSPs, or any mix of these.
- It should be clarified if in the future there will be only active validator nodes, or also read-only "observer" nodes.
- In the case the current EBSI blockchain technology (based on Hyperledger Besu) gets replaced by an "EBSI-next" infrastructure, it should be clarified how any necessary transition/migration steps will be carried out. Any major breaking change shall carefully consider the operational and economic impact on the larger ecosystem, in particular efforts needed by stakeholders with existing technology/deployments.

4. Attestation Features

4.1. Data Models of VC Containers

This section describes what data models are supported for exchange of data.

4.1.1. As/Is

- The data model for Verifiable Credentials in EBSI is the W3C Verifiable Credential Data Model (link) and also JWT Data Model (link). The format depends on the use case requirements.
- In the last few years, many EBSI-based projects (including Diploma use case) have been using the W3C VC Data Model based on JSON-LD.
- Other data models, including the JWT and ISO 18013-5 data models, are also being used in other relevant communities.
- EBSI defines various schemas of VCs, including Verifiable Accreditation, Verifiable Attestation, and Verifiable ID (link).
- EBSI defines various JSON schemas (link).

ToBe

- If the objective is to align EBSI with ARF / eIDAS 2, then EBSI should align/map its classification of VCs with Type 1 and Type 2 credentials, as defined in the ARF.
- EBSI's Verifiable ID should be aligned with ARF PID.
- Signatures on VCs shall be compatible with TS 119 182-1 (JAdES).

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.

- EBSI data formats shall be aligned with data formats specified by the EUDI Architecture Reference Framework (ISO mDL, SD-JWT, optional JSON-LD).
- Decision shall consider long-time community conversations and disagreements about JSON-based and JSON-LD-based data models, and various mixed forms.
- EBSI should be up to date with recent developments in the W3C VC WG, such as:
    - Support for proof expiration dates, separate from credential expiration date
    - Poison graph mitigation
    - MultiKey, JsonWebKey

4.2. Data Model of VC Content (Diploma and Secondary School Certificate)

This section describes requirements related to data models and schemas for Diplomas and Secondary School Certificates.

4.2.1. As/Is

- EBSI already has a schema specification related to diplomas (link), based on EuroPass.
- The current diploma description in EBSI is based on ELM V2 (linklink).
- EBSI uses JSON data format related to diplomas (link).
- The EBSI Verifiable Diploma Schema mentions the JSON-LD context https://base.uri.europass/contexts/v1, but the content of this JSON-LD context doesn't seem to be defined anywhere.
- Current available schemas seem to be focused on the needs of higher education institutions.

ToBe

- EBSI needs to make sure that its VC diploma specification is aligned with a European Standard for certificates in the education domain.
- https://europa.eu/europass/en/node/2128Efforts shall be made to:
    - Adapt EBSI to ELM V3
    - To define ELM V3 in JSON format
    - To define the corresponding proof formats.
    - Alternatively, another format (e.g. ELMO) may have to be considered. The work of DC4EU WP 5 should also be taken into account.

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.

- Other relevant standards that should be considered are the European Qualifications Framework (EQF), ESCO (European Skills, Competences, Qualifications and Occupations), the International Standard Classification of Education (ISCED), and Open Badges.
- Further analysis shall be conducted to determine if current EBSI specifications and schemas for diplomas are sufficient to cover the EBSI-VECTOR (and other) use cases, or if more is needed.
- Schemas shall also consider the needs of secondary education institutions. In particular, a Secondary School Certificate schemas shall be defined.

4.3. Data Model of VC Content (Social Security Pass)

This section describes requirements related to data models and schemas for Social Security Passes.

4.3.1. As/Is

- EBSI has a JSON schema related to PDA-1 (link).

ToBe

- EBSI shall consider existing EHIC (payload), PDA-1 data models.
- Further analysis shall be conducted to determine if current EBSI specifications and schemas for PDA-1 are sufficient to cover the EBSI-VECTOR (and other) use cases, or if more is needed. The current EBSI specifications and schemas for PD A1 have to be adapted (coordination with WP 5).

4.4. Selective disclosure

This section describes EBSI's support for selective disclosure of claims in Verifiable Credentials and Verifiable Presentations.

4.4.1. As/Is

- Selective Disclosure for JWTs (SD-JWT) (link) is gaining a lot of attention in various communities and is also mentioned by EBSI (link).
- Support for SD-JWT is also a requirement in the ARF.
- And alternative proposal by EBSI has been made called SD-JWS (link)
- A specification for SD-JWT-based Verifiable Credentials (SD-JWT VC) also exists (link).

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.

- Having JSON-LD payloads inside SD-JWT could potentially be problematic, since that mixes different data models and could lead to problems with verifying proofs.
- Selective Disclosure is also possible with the W3C VCDM and Data Integrity, not using SD-JWT (link).

ToBe

- If the objective is to align EBSI with eIDAS 2, then EBSI shall support disclosure mechanisms defined in the ARF, instead of defining its own approaches.
- There should be clear guidelines whether unlinkability between multiple presentations to different Verifiers is a concern, and how it will be addressed. The processes should be designed according to the relevant requirements in eIDAS 2.0 (non-traceability etc.).

4.5. (Qualified) signature/seal of credentials by Issuer

This section describes how an issuer should sign any kind of credential to release a valid VC (QEAA). This must be compliant with the new eIDAS regulation.

4.5.1. As/Is

- EBSI provides JWT VC format
- EBSI provides JWS (ES256) and JAdES (compact serialization Baseline-B) signatures
- EBSI supports optionally ES384, ES521 RSA
- EBSI provides a specification for the VCs https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/E-signing+and+e-sealing+Verifiable+Credentials+and+Verifiable+Presentations

ToBe

- EBSI should be aligned with eIDASv2 to comply with the requirements about using different signatures. There is a discussion about signatures a data model that must be resolved to be aligned.
- EBSI should be combined with qualified trust services acc. EIDASv2:
    - Creation of qualified certificates for QES, QSeal,
    - Qualified timestamps
    - Validation of qualified signatures, seals, timestamps

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.

  - Preservation of qualified signatures, seals, timestamps especially to ensure crypto stability within EBSI
  - Remote signing
- EBSI should be used as decentralized PKI for QTSP for QES, QSeal, qualified timestamps which requires the integration and compatibility with ETSI:
  - ETSI EN 319 411, 412
  - ETSI EN 319 401
  - ETSI EN 319 421

As well as interaction with HSM acc. CEN EN 419 241 and the relevant signature formats:

ETSI EN 319 122, 132, 142, 162 as well as signature validation ETSI EN 319 102 and recognition of cryptographic requirements under ETSI TS 119 312 so the correlation of EBSI with ETSI ESI: https://portal.etsi.org/TB-SiteMap/ESI/Trust-Service-Providers

- Possibly development new standards on signatures using EBSI as decentralized PKI
- All signature profiles of AdES should be possible:
  - Baseline
  - LT
  - LTA

Also in combination with timestamps

- QES or QSeal have to be provided by QTSP for QES/QSeal or the issuer of VC has to be such a QTSP
- Issuer shall be QEAA Provider under eiDAS 2.0
- Issuer shall validate the identification and authentication of the holder before issuance VC
  - Identification has to fufill certain LoA acc. EiDAS 2.0 (see Art. 24 for details)

5. Protocol Features

Supported presentation protocols

Description: Supported protocols for presenting a VC to a 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.

5.1.1. As/Is

- EBSI has considered OpenID for Verifiable Credentials, ISO 18013-5 (mDL), DIDComm, WACI. From these protocols, EBSI has selected OpenID for Verifiable Credentials (OID) (link).
- [Samuel] Version implemented by EBSI is not aligned with the last one from OIDC / ISO.

ToBe

- EBSI should continue to ensure that its use of the OID suite of protocols is consistent with how the same protocol is used by the EUDI ARF.
- As EBSI-VECTOR progresses, we need to consider if the functionality offered by OID is sufficient for the EBSI-VECTOR use cases, or if additional features are needed for credential presentation (e.g. DIDComm, VC API, etc.).
- Need to consider the addition of MFA in those protocols.

Supported issuance protocols

This section describes supported protocols for issuing a VC to a holder.

5.1.2. As/Is

- EBSI has considered OpenID for Verifiable Credentials, ISO 18013-5 (mDL), DIDComm, WACI. From these protocols, EBSI has selected OpenID for Verifiable Credentials (OID4VC) (link).
- [Samuel] Version implemented by EBSI is not aligned with the last one from OIDC / ISO.

ToBe

- EBSI should continue to ensure that its use of the OID4VC suite of protocols is consistent with how the same protocol is used by the EUDI ARF.
- Need to consider if the functionality offered by OID4VC is sufficient for the EBSI-VECTOR use cases, or if additional features are needed for credential issuance (e.g. DIDComm, VC API, etc.).
- Need to consider the way of notifying a user the VC is ready to be downloaded in an asynchronous way (Push notifications, email, ...)
- Need to consider the addition of MFA in those protocols.

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. Holder Wallet Features

6.1. Multi-identity support

This section describes support for multiple identities/personas/profiles in a wallet instance. In order to keep the privacy of the user, he/she can use different "profiles" (DIDs) in the same wallet.

6.1.1. As/Is

- EBSI is not providing any kind of mechanism to do this.

ToBe

- A mechanism to create a new profile into the wallet
- A mechanism to select a concrete profile to be used in the next processes.
- A mechanism to issue PID for natural and legal entities in different LoA in the wallet
- Follow ARF regarding Key Management, Protocols and Formats
- The PID should be bound to a DID, but there should also be the possibility to have additional DIDs which are not bound to the PID.
- There should be a mechanism for proving that different DIDs identify the same subject, if required by a use case.
- A mechanism to present PID for natural and legal entities in different LoA with the wallet.

6.2. Multi-language support

This section describes support for multiple language in the User Wallet / Enterprise Wallet for all the languages used in EU.

6.2.1. As/Is

- The actual EBSI-conformant wallets (https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Conformant+wallets) could not be checked regarding multi-language support (not found in the Apple-AppStore)

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.

ToBe

- In order to achieve broad acceptance among citizens, wallets should adapt to the standards of the major manufacturers. This includes ease of use without great technical knowledge, but also support for the languages of the users.
- It's necessary a property translation to work with all the schemas provided by EBSI. The way represent a VC (QEAA or PID) is a key-value tree (JSON) so, it's necessary to have a translation in all the languages of the member states. (I think to delegate the translations into the Wallet provided is not good enough as the Schemas are dynamic)

6.3. Accessibility and Non-Discrimination Requirements

This section describes the accessibility requirements by a user wallet / enterprise wallet

6.3.1. As/Is

- None

ToBe

- Requirements for the necessary HW to use a User Wallet
- Requirements for the necessary SW to use a User Wallet
- Alignment with ARF – Not defined yet
- Necessary to include security constraints. HSM, TTE, external signing service, ...
- Holder wallets need to be compliant with relevant national laws related to accessibility
- Holder wallets should follow relevant guidelines from standardization bodies such as W3C, ISO, e.g. https://www.iso.org/news/ref2612.html
- Holder wallets should be usable with affordable hardware, to avoid economic discrimination

6.4. Authenticating Wallet Instances

This section describes mechanisms to authenticate a user into a User Wallet or Enterprise Wallet.

6.4.1. As/Is

- None

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.

ToBe

- Mechanism to authenticate a user in a concrete wallet instance. (Requirements)
- Mechanism to authenticate a user in a concrete enterprise wallet. As the enterprise wallet can be accessed by many people.
- Alignment with ARF
- Very related with Sync and Backup mechanism on the User Wallet / Enterprise Wallet, also with open question of possible migration of full wallet instance (including all credentials) to a different device.

6.5. Operations and Performance

This section describes requirements about security, performance, real-time protocols, etc.

6.5.1. As/Is

- None

ToBe

- Holder wallets should require minimum versions of the operating system, e.g. prevent use of outdated Android OS version.

6.6. Qualified signature of documents by Holder

This section describes the term qualified digital signature, including QES and QSeal.

6.6.1. As/Is

- Currently EBSI provides no solution to issue qualified electronic signature using EBSI as decentralized PKI or issuer QES into EBSI or signing resp. Validate a QES or Qseal with a wallet.

ToBe

- Ensure that remote signing will be possible with the wallet acc. To ARF with any signature format acc. to ETSI ESI standards: https://portal.etsi.org/TB-SiteMap/ESI/Trust-Service-Providers
- Ensure that validation of QES/QSeal and qualified time stamps will be possible with the 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.

- Ensure that creation of qualified certificates using EBSI as decentralized PKI by QTSP will be possible.
- Ensure that validation and preservation of QES/QSeal and timestamps created based on qualified certificates using EBSI as decentralized PKI by QTSP will be possible.
- Definition of exchange or export formats for verification reports, revocation and status information on QES/QSeal or timestamps created using EBSI as decentralized PKI by QTSP will be possible in order to ensure their preservation acc. ETSI TS 119 511/512.

6.7. Additional Social Security Requirements

6.7.1. Issuance flow

- Authentication
    - Confirm sharing Identity Credential with issuer
    - Display result of credential issuer verification
- Storing
    - User can confirm (or decline) the storage of a new credential
    - Import multiple credentials in same transaction (batch transaction)

6.7.2. Wallet Functions

- Visualization/UX
    - Show list of all credentials and its basic information including status (e.g. revoked)
    - On selection, display detailed credential information (business content)
    - Show history of verifications (or rather activity log)
    - Delete credential(s)
        - this does not affect the business decision
- Status handling/checks
    - Validate credentials periodically against registries (issuer, revocation, schema)
    - Additional manual validation by holder
    - Allow push by issuer (e.g. permanent after provisional credential; register wallet at issuer system)
    - Process updates by credential issuers automatically
        - Handled as revocation and reissuance of a specific credential using the best configured flow (e.g. use push if available, else manual)

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.

- Transfers
    - Migrate content to new EUDI wallet
        - Full switch, so that wallet binding stays valid
    - Backup/restorage of credentials via "export button"
        - In case of data loss
    - Transfer credential(s) to other (EUDI) wallet
        - E.g. Parents want to hold childs EHIC – desired credential status is that the attestation stays valid, while only identity check is failing

6.7.3. Interactions

- Accept proof requests as deep links within the issuance flow or/and identification
    - Same device flow
- Integrate a QR code reader for Proof Requests (PR) (Cases Issuance and Verification)
    - Issuance starts like verification with a PR to share (wallet) identity credential and directly follows the issuance
- Provide proximity protocols to share presentations, e.g., QR-code, NFC or Bluetooth (PDA1-SD-JWT will most likely be too big for QR code)
- Provide remote protocols to share presentations
    - A: Verify a verifier endpoint provided in PR and display result to wallet user to afterwards send credential to endpoint (push)
    - B: Offer holder wallet endpoint to share presentation (pull)

6.7.4. Verification flow with Verifier

- Process proof requests of unregistered verifiers
    - Security concerns are high so special data handling is required (to be decided)
- Display result of relying party verification
    - holder checks verifier signature of PR against registries regarding authorization and approved schemas.
- Enable the user to select the right VC to share if several VCs of same type are available
- Enable the user to share the same identity credential (already used in the issuance process) additional to requested credential to facilitate automatic identity check
- Allow user to partially answer a Proof Request if not all requested information is stored in 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.

- Enable the user to select the PDA1 presentation schema (e.g. “min”, “half”, “full”) for presentation – Selective Disclosure
- Enable User to select method of data transmission himself?
- Holder should always be able to decline/abort and needs to confirm his choices in the verification flow

7. Enterprise / Legal Entities Wallet Features

7.1. Enterprise Wallet and Legal Entity Wallet

Overall High Level Definitions

Business Registries are official organizations authorized by government or relevant regulatory bodies. These entities offer services aimed at identifying, documenting, and certifying enterprises during their onboarding or registration phase. The primary purpose of Business Registries is to maintain accurate and up-to-date records of businesses, companies, and other legal entities operating within a jurisdiction. These records often include essential information such as enterprise names, ownership details, registration numbers, business structures, and more. By providing reliable and accessible information about entities, Business Registries play a crucial role in promoting transparency, accountability, and legal compliance within the business environment.

Legal Entities refer to both public and private organizations, that actively participate as issuers and verifiers of Verifiable Credentials (VCs) within specific business contexts. In these roles, legal entities serve to provide the necessary Verifiable Credentials required by enterprises and holders' wallets for seamless interaction with services offered within the European Blockchain Services Infrastructure (EBSI) network. These Verifiable Credentials act as digital attestations, allowing for secure and trusted exchange of information, transactions, and interactions in the digital realm. Legal Entities play a fundamental role in ensuring the authenticity, validity, and reliability of these credentials, thereby contributing to the effectiveness and credibility of the EBSI network's operations.

An Holder Wallet refers to a digital repository or container specifically designed for storing and managing Verifiable Credentials (VCs) of a natural person. These credentials serve as digital attestations of various attributes, qualifications, or certifications possessed by the individual. The Holder Wallet is certified by a Decentralized Identifier (DID) registry, which 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.

a decentralized and secure system for creating, managing, and verifying unique identifiers associated with entities in the digital space. The certification from the DID registry adds an extra layer of trust and authenticity to the Holder Wallet, ensuring that the stored credentials are tamper-resistant, secure, and verifiable. This setup enables individuals to control and share their digital credentials in a privacy-preserving and controlled manner, enhancing their ability to participate in various digital interactions and transactions while maintaining their data sovereignty.

An Enterprise Wallet is a digital platform or repository used by both public and private organizations to manage and facilitate interactions, both external and internal, within a digital ecosystem. This wallet is certified by Business Registries, which are official organizations authorized by government or regulatory bodies. The certification from Business Registries adds an element of legitimacy and trust to the wallet's capabilities.

The Enterprise Wallet serves as a secure and controlled environment where the organization can store, manage, and exchange Verifiable Credentials (VCs), tokens, or other forms of digital representations. This asset may pertain to the organization's identity, qualifications, certifications, ownership, or other relevant attributes.

Externally, the Enterprise Wallet enables the organization to interact with other entities, such as citizens, partners, suppliers, or regulatory bodies, in a seamless and secure manner. It facilitates the sharing of verified information and credentials, streamlining processes like compliance checks, contract negotiations, and transactions.

Internally, the Enterprise Wallet aids in managing interactions and data sharing among different departments or divisions within the organization. It can provide a secure and controlled platform for employee authentication, access management, and the exchange of sensitive data.

Overall, the Enterprise Wallet, with its certification from Business Registries, ensures that the organization's digital interactions are trustworthy, compliant, and efficient, contributing to enhanced operational processes and establishing a higher level of credibility in the digital business landscape.

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.

7.1.1. High Level Enterprise Wallet Features

- **Advanced Security:** An Enterprise Wallet is designed to ensure maximum security for business information and resources. It employs robust encryption protocols, multi-factor authentication, and other technologies to safeguard sensitive data.
- **Certification from Business Registries:** The Enterprise Wallet is certified by Business Registries or authorized entities, ensuring that the enterprise's identity and credentials are verified and authentic.
- **Management of Verifiable Credentials (VC):** The Enterprise Wallet allows the enterprise to store, manage, and share Verifiable Credentials (VC) that attest to business attributes such as the legal name, registration data, certifications, ownership, and more (compliance EIDAS annex par. The minimum data set for a legal perso**n)**.
- **Access Rights Management:** The enterprise can control who has access to which information within the Enterprise Wallet. This is particularly important for maintaining the privacy and security of business data.
- **Secure Information Sharing:** The Enterprise Wallet enables the enterprise to securely share verified information with business partners, suppliers, customers, and other stakeholders.
- **Regulatory Compliance Interactions:** The Enterprise Wallet can assist the enterprise in meeting regulatory and compliance requirements by controlled sharing of verifiable information with regulatory or oversight entities.
- **Transaction Traceability:** Leveraging blockchain technology or distributed ledger, the Enterprise Wallet provides the capability to trace business transactions, enhancing transparency and auditability.
- **Digital Identity Management:** The Enterprise Wallet can serve as a hub for employees' digital identities, enabling secure and seamless access to internal systems.
- **Interoperability:** The Enterprise Wallet is designed to seamlessly interact with other systems and platforms, fostering compatibility and data exchange across diverse digital environments. This promotes efficient collaboration and data flow between the enterprise and its partners.

Those macro-areas listed, can be verged into the following more technical functionalities that will be better describe in 3.2 deliverable:

- New identity creation

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.

- Multi profile management
- Hard wallet connection
- 2 factor authentication
- Qrcode scan functionality
- Multi-sign: Implement a multi-signature feature for transactions that require approval from multiple users.
- Delegate: Temporarily delegate authority to other users
- Activity: list transactions and details
- Public address sharing
- Delete Wallet
- Key Management (view & export)

7.1.2. As/Is

- None

ToBe

- Legal Entity wallet and Enterprise wallet competence area definitions. Points of contact between them definitions.
    - Business Requirements for creating and managing an enterprise wallet. Also, requirements for internal (within the enterprise) and external (outside the enterprise) interaction are required
- Alignment with ARF is mandatory
- Technical (SW – HW) requirements for developing the business requirements defined
- EBSI should define the difference between legal entity wallet and enterprise wallet. A first definition is given in this paragraph and, in order to understand the logic applied for the enterprise multi-profile wallet, following both specifications – holder & enterprise – is reported.

7.1.3. Additional Considerations

Holder Wallet

Spport for multiple identities/personas/profiles in a wallet instance. In order to keep the privacy of the user, he/she can use different “profiles” (DIDs) in the same wallet.

Natural 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.

> educational (degree, master)

> social security (EHIC, PDA1)

Legal Person

> employment (workplace)

> bank reference (IBAN)

Enterprise (organization) Wallet provides and supports multi-profiles wallets (defined by its own dedicated private key) in one single wallet instance.

Profiles related to public & private organizations are:

-> Enterprise Identity (automatically created when the enterprise ask for the wallet creation)

> enterprise legal profile (DID and company sensible data)

-> Business/DID Registries

> Official organizations authorized by government or relevant regulatory bodies. These entities offer services aimed at identifying, documenting, and certifying enterprises during their onboarding or registration phase

-> Legal Entity

> Issuers and verifiers of Verifiable Credentials (VCs) within specific business contexts. To be defined if legal entity just identify an issuer role or both issuer and verifiers because the latter can be identified by a generic third role (that it will have its own different and dedicated wallet that of course it's supported and can be contained into the enterprise wallet as another profile)

-> Third party or Legal entity Verifier

> VC interaction as verifier vs legal person wallet, enterprise wallet, legal entity wallet

Internal Organization Services:
Enterprise wallet's owner can access services, sharing its data, authorize data consultation within the enterprise for enterprising purpose.
Enterprise : Legal Person

External Organization Services:

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.

Enterprise wallet's owner can access services, sharing its data and act based on its authorized profile (business registries, legal entity, third party) outside the enterprise context

Enterprise : Natural Personal

Enterprise : Enterprise

Additional requirements from Social Security for the Issuer System:

- Basic technical checks of approaching holder wallet
- Validate Identity Credential of approaching User (need "strong" identity for our use cases - at least DID derived from PID)
- Offer capability for Identity Mapping on Issuer Side

Additional requirements from Social Security for the Verifier App/System:

- Create Proof Requests via proximity protocol
- Allow only Proof Requests for which the Verifier is authorized (defined in registry)
- Automatic Check of User's Identity (holder binding?) if submitted by holder
- Offer interfaces to further process data (…)

Organisational Identity

This section describes how Organisational Identity is handled by EBSI.

7.1.4. As/Is

- EBSI specifies that the DID method did:ebsi is specifically for legal entities, not natural persons. This DID could be considered the basis (or first step) for an organisational identity in EBSI. This is a prerequisite for an organisation becoming an Issuer of VCs.
- To create such a DID, an onboarding token is required that allows access to the EBSI APIs. At the moment, such an onboarding token can be obtained from an EBSI website. It is not clear yet how this onboarding process will work in the future in a production setting, i.e., what an organisation needs to do before it can create an EBSI DID.

7.1.5. ToBe

- Sometimes a distinction is made between "enterprise wallets" and "organisational wallets". EBSI should clarify if it is going to make such a distinction, and if the onboarding process will be the same or different for "enterprises" and "other organisations".

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.

- EBSI should clarify what information (if any) will be available via EBSI about participating organisations. Perhaps anyone will be able to create DIDs without any kind of vetting process of the organisation, or perhaps EBSI will collect detailed data about participating organisations before they can create DIDs. Or something in between.
- The Global Legal Entity Identifier Foundation (GLEIF) is prominently engaged in various current digital identity projects, with a concept called “vLEI” that uniquely proves the identity of organisations and their officers. EBSI should consider how (if at all) vLEIs fit in with EBSI's own concept of organisational identity. EBSI should clarify interoperability to KERI approach of vLEI
- In addition to GLEIF, several other authentic sources for ODI exist, e.g., commercial registries, association registries, registries for public authorities (like the EESSI Institution Repository for Social Security) etc., which are not covered by GLEIF. EBSI shall consider which authentic sources have to be taken into account in cooperation with relevant LSP.
- Technically, organisational identity can be expressed in various ways. One approach would be to associate organisational identity data directly with a DID, e.g., by adding information to a DID document, or by linking a DID to some external identifier or record. Another approach would be to issue VCs to an organisation’s DID, i.e., the “organisation equivalent” of a Verifiable ID or PID.
- Another option is to express the organisational identity by a QEAA issued in a cloud wallet of the organization. The acting people can now be linked to the wallet with their PID stored in the cloud wallet as well as linking their DID to the DID of the organization.
- EWC is the only Large-Scale Pilot mainly focusing also on the topic of organisational identity. EBSI should explore synergies and alignment with EWC which also included e.g., ID Union with well-grounded experience in ODI.
- Various ecosystems and communities may already have their own mechanisms related to organisational identity, e.g., universities are already getting accredited and verified by governmental authorities. EBSI should clarify how such existing structures should be used if they exist.

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. DID Lifecycle Management

8.1. DID Creation

This section describes how DIDs can be created in EBSI.

8.1.1. As/Is

- EBSI distinguishes between a DID method for legal entities (did:ebsi) and natural persons (did:key) (link).
- Creation of DIDs using the did:key method involves only generating a private/public key pair.
- Creation of DIDs using the did:ebsi method involves an Onboarding Service.

8.1.2. ToBe

- More details on how the Onboarding Service will be operated in the future would be desirable.
- EBSI should keep track of potential new developments in a future W3C DID WG.

8.2. DID Deactivation/Revocation

This section describes how DIDs can be deactivated/revoked, so that they can't be used anymore for signatures. This is the equivalent to revocation of eIDAS 1.0 certificates. Also, how such revocation of identifiers can be modeled and shared in a provable way, e.g. if a ledger goes away.

8.2.1. As/Is

- In did:ebsi, a DID can be deactivated on the ledger, and the resolver will return metadata about its deactivation status.

8.2.2. ToBe

- It should be possible to use traditional OCSP responders (RFC 6960) or e.g. the revocation mechanism of EBSI for revoking DID, QEAA (Verifiable Credentials) etc. But to ensure that the revocation information will be issued to wallet without packing them into a credential format in order to be independent a) from credential format and its data model and b) from the EBSI ledger and other ledgers)?

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.

- Potentially an extension for DID documents can be defined that makes it possible to have revocation or status lists for DIDs in a DID method independent way, similar to how it is already done today with Verifiable Credentials (“credentialStatus”).

9. Credential Lifecycle Management

9.1. Credential sharing consent approval (data agreements)

This section describes a mechanism to build a data agreement between a data holder and third parties for sharing personal information. This agreement should be use to control (legally) how the third parties are using that personal information, based on the scope, purpose, ...

9.1.1. As/Is

- Current flows are not GDPR-compliant, e.g. the “purpose” of data sharing is not communicated to the Holder.

9.1.2. ToBe

- Some existing work by Gataca iGrant.io, and others, e.g. see DIF Verifier Universal Interface
- Consider consent record information structure https://www.iso.org/standard/80392.html
- This should be included e.g., in Presentation Exchange, which is used by OID4VP
- Define a protocol to build a consent agreement

Consent revocation

This section describes that the holder needs a mechanism to revoke the use of his/her personal information by a third party. Currently, once the holder shares the information with a third party, there is no way to control what is happening with that data. Although, technically is very complex, it can be done by the legal perspective.

9.1.3. As/Is

- Current flows don’t provide a mechanism for consent revocation
- Not standardized in OID protocol stack

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.

9.1.4. ToBe

- Based on the credential sharing consent approval entry, we should define a protocol to build a consent agreement.
- Using that protocol, it could be possible to implement a mechanism to revoke the access / store of that personal information in the third-party side.
- Although technical specifications should be necessary, the current scope I think should be from the legal point of view. Technical limitations make this very complex.

Credential status change

This section describes approaches to revoking or otherwise changing the status of credentials

9.1.5. As/Is

- EBSI defines a framework for various strategies of credential status change, including OneTimeStatus2023, StatusList2021, CRLBloomFilter2023, CRLPlain2023, DynamicSLBloomFilter2023. (link).
- S-Pass (based on EBSI) defines revocation, but need to check if that is S-Pass specific, or if there is any information in the "core" EBSI documentation itself.

9.1.6. ToBe

- We have to find out if "revoked" is the only status change mechanism we need, or if other status (such as "suspended" or "provisional") are needed. See RevocationList2020Status and StatusList2021Entry.
- It should be possible to issue the flat lists which EBSI specification provides for revocation https://api-pilot.ebsi.eu/docs/specs/credential-status-framework/credential-status-vcs to the wallet in case the revocation information is requested and to avoid putting revocation and/or status information into credential format in order to ensure independence from credential format and data model. This would mean:
- Use the flat lists mentioned https://api-pilot.ebsi.eu/docs/specs/credential-status-framework/credential-status-vcsIssue those lists directly into the wallet without packing them into a credential and so credential format Wallet only needs to be able to receive and interpret those status lists, but as EUDIW has to be able anyway to sign but also to handle with signature validation means verification reports acc. OASIS DSS specification and OCSP/CRL responses reg. ETSI EN 319 102Design and

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.

implementation of revocation mechanism including Governance: When has to be revoked what by whom? Technology: Issuance and verification of revocation information: Revocation responder similar to OCSP/CRL Responder acc. EN319 411/412 and RFC 6960 resp. RFC 5280 Revocation information should be signed by issuer of related credential In WP4, there may be a requirement that the entity which issues a VC (e.g. university) may not be the same entity that can revoke a VC (e.g. a judge). The Social Security's position is that only the issuer can revoke a VC.

- We are aware of three approaches to revocation: EBSI, S-Pass 2020, S-Pass 2022. Only the Issuer can revoke, but the revocation data should NOT be at the Issuer system (the issuer should not be asked by the verifier if the VC is valid – this information should be provided through the registries). Using the ledger for revocation registries has the advantage that less infrastructure is required on the Issuer side, therefore EBSI should define a way of doing this. In S-Pass, the registry can contain a member state identifier, issuer identifier, a document type and reference identifier.
- The mechanism for status change should not be just binary (not revoked / revoked) but support additional statuses (suspended, etc.). Inside the credential could be defined, what status the binary means. Therefore no information is exposed. This implies, that there can be multiple revocation list references inside the credentials for e.g. revocation (1) and suspension (2).

Credential expiration management

This section describes how credentials expire.

9.1.7. As/Is

- Not defined the journey to renew a VC, and its implications.
- Currently there`s no revocation

9.1.8. ToBe

- If a credential expires, this doesn't mean that the "business decision behind it" has expired ("harsh revocation"), only that the credential itself has expired. You could get a new one re-issued. Re-issuing could happen automatically.
- Revocation should be independent from the credential format as it`s done in existing PKI. Possibility would be that as CRL is already used to use CRL and OCSP for revocation

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.

status information for any credential and to avoid packaging revocation into VC acc. W3C Data Model.

- It has to be possible to validate all Credentials as long as they are needed so for whole retention period to make evident, that a valid credential existed at a certain point of time.
- EBSI must be enabled to export all validation information (Revocation, status, verification reports, information on VC etc.)needed for validation of VC to an external system in standardized formats and structure.

10. Interoperability

10.1. Interoperability with other Trust Frameworks

This section describes that the protocol / structures defined in EBSI must resolve the European requirements as the main purpose, but it would be great to have a interoperable Trust framework. This means, European wallets could interact with LATAM, US, Asia, Private .... Trust Frameworks.

10.1.1. As/Is

- EBSI is based on W3C standards

10.1.2. ToBe

- It's necessary to define a common standard for all the regions.
- We must avoid multiple protocols / specifications for the same purpose.
- Very complex to achieve a common understanding between different regions. Depends on the wallet provider to provide a mechanism to talk different "languages"
- EBSI shall achieve compliance to eIDAS 2.0 trustframework. Based on this the interoperability with other frameworks should be designed and tested on certain pilots. Close collaboration with DC4EU might be meaningful
- Assessment of certain trust frameworks and their legal and technical frameworks should be done alongside the use cases of EBSI-VECTOR project ISO TR 23635:2022 and ISO TR 23644:2023 should be taken into account
- The ETSI TR 103 684 should be taken into account https://www.etsi.org/newsroom/news/1701-2020-02-etsi-releases-a-technical-report-on-global-acceptance-of-eu-trust-services

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.

10.2. Visualization of credentials

This section describes how credentials can be visualized inside a wallet.

10.2.1. As/Is

- EBSI does not currently provide much guidance on how credentials should be visualized. This may however be helpful for better user experience and consistency across EBSI-compliant wallets.

10.2.2. ToBe

- EBSI should consider the following community developments intended for visualization of credentials:
- At the Rebooting-the-Web-of-Trust#11 workshop, a "render" property was introduced for the W3C VCDM: https://github.com/WebOfTrustInfo/rwot11-the-hague/blob/master/advance-readings/rendering-verifiable-credentials.md
- The W3C VCDM 2.0 currently (as of 21 Aug 2023) lists a "renderMethod" property as a reserved extension point: https://w3c.github.io/vc-data-model/#reserved-extension-points
- The W3C VCDM 2.0 currently (as of 21 Aug 2023) has an open Pull Request (probably will be merged soon) to add "name" and "description" properties for Verifiable Credentials, which are intended to help with visualization: https://github.com/w3c/vc-data-model/pull/1252
- Depending on the VC domain, the way to display information is different so it's necessary a common way to display information.

11. Other Technical Tasks

11.1. API definition & documentation

This section evaluates available EBSI documentation materials.

11.1.1. As/Is

- Documentation can be found in the following places:
    - https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/
    - https://api-pilot.ebsi.eu/docs

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.

- Currently, not all the EBSI documentation is publicly available, e.g. EBSI Early Adopter Starter Kit
- Sometimes EBSI documentation is outdated or inconsistent with implementations, e.g. the following two resources are inconsistent regarding the format of EBSI DIDs for Natural Persons (NPs):
    - https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+DID+Method#EBSIDIDMethod-method-specific-identifier-structure
    - https://www.npmjs.com/package/@cef-ebsi/ebsi-did-resolver

11.1.2. ToBe

- Consider releasing all the EBSI documentation to the public
- Maybe introduce a changelog, to better understand which part of the documentation applies to which release version of the EBSI APIs.

11.2. Longevity of cryptographic algorithm

11.2.1. As/Is

- Currently, one challenge in the utilization of EBSI is the longevity of the strength of the cryptographic algorithms. This means A typical DLT application like EBSI implies the storage of the relevant data (at minimum transaction records) in a dedicated transaction object (e.g. Tx01 on Figure 1) directly on the chain, possibly linked to off-chain records. The transaction records are protected by a Merkle-tree (by using the hash algorithm H), which's root (e.g. HR1) is placed in the block header (e.g. B1H) and together with the tree constitutes a single block (e.g. B1) on the chain [NA08]. On the other hand, the block header together with the tree constitutes a single block (e.g. B1) on the 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.

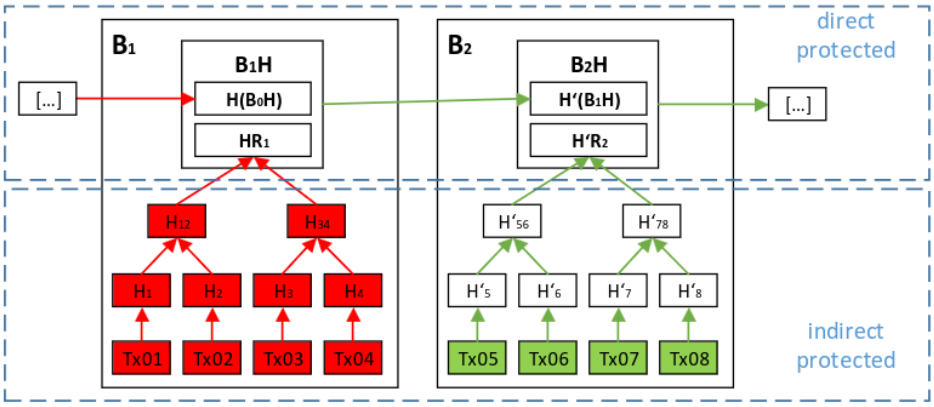

Figure 1 – A sample of a blockchain with on-chain and off-chain storage – rehashing issue

- In case the used hash algorithm H (see block B1) is about to become weak, a hash algorithm change has taken place and the new block B2 is using the new stronger hash algorithm H', which means sufficient protection (because directly hashed with H') for B2 and the header of B1 (pointed at with green arrows), but not for the Merkle-tree of B1 (because only indirectly hashed with H' – actually only root of the tree) and all blocks before B1 (red marked parts). It means, it is not definitely excluded, that possible manipulation of those transaction data remains undetected, which means, that the integrity protection and further the evidence preservation of those data is irrevocable lost.

ToBe

- Ensure longevity of cryptographic protection of EBSI including Proof of Existence and by combination of preservation service acc. EIDAS and EBSI. Possible solution described below [ISO CD TR24332], [DINTS31648]
- Due to the weakness of the hash algorithm H, which has been used in the block B1 and before the next block, B2 is using a stronger hash algorithm H'(typical blockchain rehashing approach). In such a case all the information hashed directly with H' is still sufficiently protected (marked green), but the parts of the chain, which have not been directly hashed with H', became weak (marked red) – the evidence would be lost [eIDAS], [VDG]. In order to keep the evidence on the whole chain, the approach of a "logical blockchain", which based on the evidence record method described in RFC4998 [GBP07], has been developed. The RFC4998-method of the evidence preservation is purely based on the Merkle-trees and does in particular support the rehashing mechanisms. By using this approach, the whole blockchain data will be

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.

protected by a dedicated RFC4998-enabled tree. Following Figure 2 depicts the approach of "logical blockchain" by using the example of the blockchain illustrated in Figure 3.

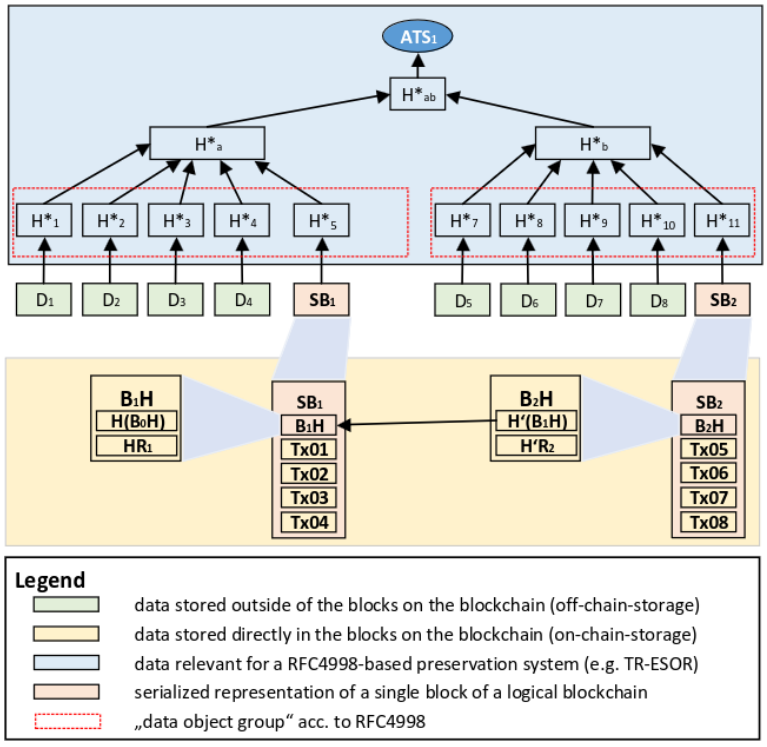

Figure 2 – "Logical" blockchain

Every single block from the chain (here B1 and B2) has to be slightly prepared in advance and suitably submitted to the RFC4998-based system. The following steps have to be performed:

1. A serialized replication of a block on the chain (serialized block, e.g. SB1 on Figure 2) has to be created by the DLT for every single block to be protected on the RFC4998-based system. The serialized block does contain the data of the single block (especially the transaction data with the hash references on the external documents, but also the header and the hash tree) stored in a well-defined manner. The hash from the referenced off-chain records are renewed in this step.
2. For every block the serialized block (e.g. SB1) and (optional) a collection of the referenced documents (e.g. D1, D2, D3, D4 and D5) build so called data object groups acc. to RFC4998.
3. Depending on the implemented approach by the preservation service to be used, it is possible either to submit the whole data object group built in step 2, or only 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.

suitable hash value list, containing a hash of every single object in the group to the preservation service [TR-ESOR], [ET20a].

4. The preservation service internally builds the Merkle-tree and seals it with an archive-timestamp (e.g. ATS1).
5. The preservation service provides a unique id (AOID[1]) for every submitted data object group, which has to be stored for further purposes.
6. By using the received AOID it is possible to obtain the corresponding evidence record for the protected block incl. referenced off-chain records (e.g. ER1*={<[{(H*1, H*2, H*3, H*4, H*5, H*6),(H*b)}, ATS1]>}[2]).

In case the hash algorithm of the preservation service (here H*) is about to lose its security suitability, the rehashing operation acc. to RFC4998 (see [GBP07], chapter 5.2) shall be applied in advance (by using a new hash algorithm e.g. H**) including the replicated block and sends notification to the DLT to rehash the off-chain-records referenced from the transaction records. This means it is an interaction of preservation service, DLT and off-chain storage. The resulted rehashed hash tree will preserve the evidence of the whole block data (on- and off-chain records). In order to perform the rehashing operation, the preservation service has to have access either to every corresponding data or its new hash value (see step 3 above). The renewed (rehashed) evidence record for a particular block, can be obtained by providing the corresponding AOID (see step 5 above) directly from the preservation service (e.g. ER1**={<[{(H*1, H*2, H*3, H*4, H*5, H*6),(H*b)}, ATS1]>, <[{(H**1, H**2, H**3, H**4, H**5, H**6),(H**b)}, ATS2]>}[3]). Even if the data of B1 is protected by a weak algorithm H, the possible manipulation of it could be easily detected by verifying the corresponding evidence record, respectively ER1* or ER1**. The provided solution makes use of 3 components, the preservation service, the DLT and the data storage with the off-chain records. The preservation service ensures the preservation of evidence acc. to [ET20a], [ET19b], [TR-ESOR] and the crypto-stability of the DLT as transaction- and or anchoring layer itself. The DLT represents the distributed application and contains the transaction records, the storage contains the off-chain records. To make a transaction evident the authenticity and integrity of on-chain transaction records as well as the linked off-chain records are needed [Ve16], [Ve17], [IS20], [IS21]. Picture below (Figure 3) shows the interaction.

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.

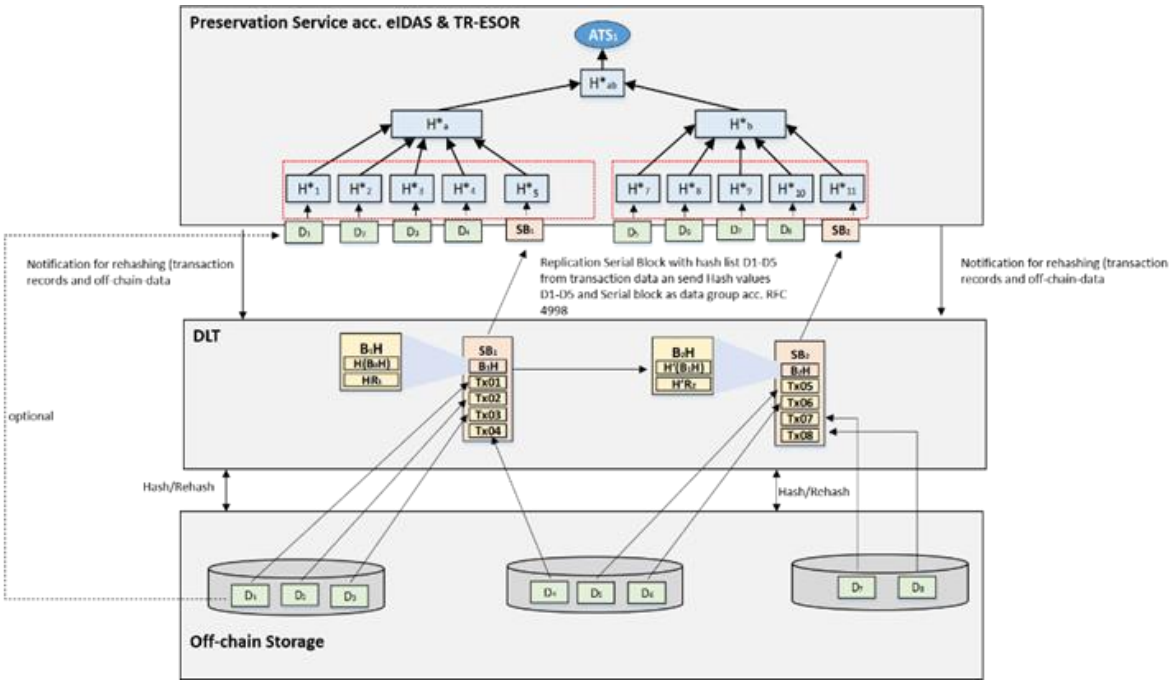

Figure 3 – Solution example

12. Legal/Governance

12.1. Comparison EBSI Governance roles eIDAS 2.0 governance role

Table 1 – Roles within eIDAS 2.0 Governance

Role	Explanation
Wallet Provider	Member State authority of private company which issues an EUDIW to citizen or legal entity Private company only on behalf of member state or in case of certified private wallet Depends on which option of EUDIW issuance member state chosen
EUDIW	Wallet instance of and EUDIW issued by MS Will be certified by CAB against conformity assessment requirements

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.

	Must fulfill Type 1 configuration
PID Provider	Authority issuing the PID for natural and/or legal entities into the EUDIW Must meet Type 1 Must be based on notified eID Scheme (at least 1 eID Scheme has to be notified by MS)
(qualified) trust service provider for Attestation of attributes	QTSP certified by National Supervisory Body based on conformity assessment of accredited CAB Must meet Type 1
Other (qualified) trust service provider	QTSP certified by National Supervisory Body based on conformity assessment of accredited CAB for: - Issuance of qualified certificates for QES, QSeal, QWAC - Issuance of qualified timestamps - Electronic mail and delivery services - Preservation of (qualified) signatures, seals and timestamps - Validation of (qualified) signatures, seals and timestamps - Archiving - Remote signatures - Electronic Ledger See e.g.: https://portal.etsi.org/TB-SiteMap/ESI/Trust-Service-Providers Any QTSP will be listed in national trust list of member state and List of the Lists (LOTL) by EC https://webgate.ec.europa.eu/tl-browser/#/

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.

National Supervisory Body	National Authority supervising QTSP and Wallet providers and CABs Supervised by EC
Conformity Assessment Body	Authority executing conformity assessment on QTSP (Trust services) and Wallet Providers (EUDIW) Accredited by national accreditation bodies Supervised by National Supervisory Body
Authentic Source (Provider)	Registry provided by Member State for QEAA Provider as Data Source for (Q)EAA
Relying Party	Public or private organization accepting the EUDIW (or with obligation for acceptation) and verifying PID and/or (Q)EAA from the wallet (Verifier)
TrustList Provider	Authorities providing the TrustList in which any certified EUDIW and QTSP will be listed (typically: National Supervisory Bodies and EC)
Wallet Supplier	Authority which produces the EUDIW

The picture below (Figure 4) shows the eIDAS trust framework in overview.

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.

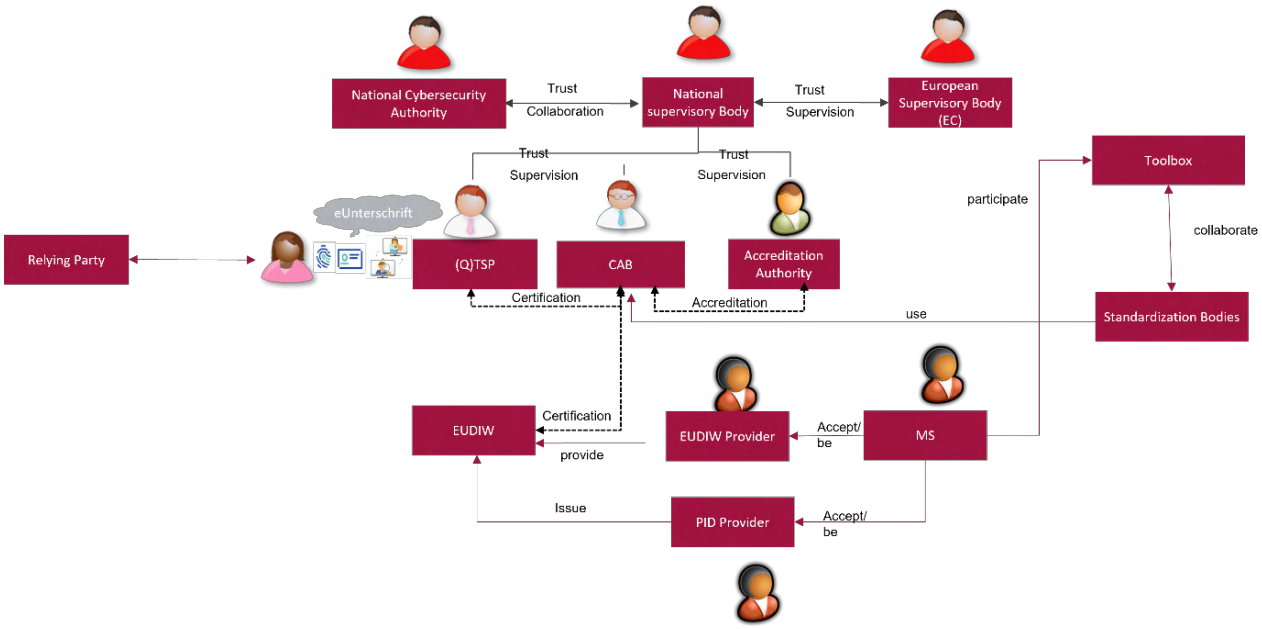

Figure 4 – eIDAS trust framework

Table 2 – EBSI/EIDAS2.0 comparison

EBSI	EIDAS 2.0
Trusted Issuer	(qualified trust service provider for - Attestations of Attributes - Signatures - Seals - Timestamps - QWAC PID Provider
Trusted Accreditation Organization	National Supervisory Body
	Conformity Assessment Body
none	Authentic source
None (certified Wallet)	EUDIW
None	Other QTSP
Trusted Wallet Provider Registry	Wallet Provider
Trusted Issuer Registry	Trust List Provider

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.

	Wallet Supplier

The EBSI Governance shall be aligned with eIDAS Governance.

12.2. Issuance and Certification of Wallets

This section evaluates how EBSI-compliant wallets are issued and certified. What does “EBSI-compliant” mean in relation to eIDAS 2.0 wallet issuance?

12.2.1. As/Is

- Today anybody can issue a wallet and use EBSI as decentralized infrastructure. The certification is not necessary or mandatory.
- Today, EBSI has its own wallet conformance testing process, and any wallet providers can become “EBSI-compliant”.
- The EBSI certification requirements are not based on international standards and it`s currently unclear how they were developed and reviewed. Requirements currently focused on interoperability but not security like key management etc.
- The tools used for testing are currently not published like e.g. done by several National Cybersecurity Authorities
- The certification process as well as certification authority is not accredited by accreditation body such as DAKKS or similar. It`s also not integrated in legal framework by any Member State nor European Commission.

12.2.2. ToBe

- Certification shouldn’t be a one-time action that puts a wallet on a website, but should be ongoing and require regular renewals or similar processes.
- Certification should be repeated every 2 years, equivalent to QTSP.
- Wallet should be issued in accordance with eIDAS 2.0.
- The certification scheme and governance of EBSI shall be correlated with eIDAS 2.0.
- Ensure alignment with eIDAS 2.0 wallet issuance process, three options:
    - member states issue wallets, or
    - issued by public authority on behalf of member state government, or
    - private vendors can get their wallets certified

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.

- EBSI might be the step to private wallets certified by CAB. The responsibility might have to be shifted as CAB works under supervision of National Supervisory Body which is typically not the EC as current lead in EBSI governance. Alignment EBSI government and eIDAS Governance
- It should be clarified who is wallet issuer using EBSI. Typically EBSI is the shared infrastructure but not an issuer. This could mean that member state could issue EUDIW using the issuance possibilities of eIDAS 2.0 and using EBSI as decentralized PKI. In this case it should also be clarified what`s the scope of assessment of infrastructure for the wallets will look like:
    - Only the node operated by member state
    - The whole EBSI infrastructure
    - Only those parts of the network used as decentralized PKI for certain EUDIW

same applies for any (qualified) trust service provider using EBSI as decentralized PKI for

Issuance qualified certificates (QES/QSeal/QWAC), timestamps and/or QEAA

- Segregation from QTSP for Electronic Ledger should be clarified.
- Discuss issuance of Edge wallet for natural entities and cloud wallet for legal entities
- Discuss wallets able to fulfill Type 1 and Type 2
- Certification requirements are developed in eIDAS Toolbox in close collaboration with European Standardization Bodies (ETSI, CEN). The certification will be done by accredited Conformity Assessment Bodies, the EBSI certification process shall be integrated in this eIDAS governance. This would mean to have several member states accepting EUDIW based on EBSI and using an EBSI certification process accepted by EBP.
- Discuss role of EC and EBP in conformity assessment including the relationship to National supervisory bodies which are not necessarily member of EBP.
- EBSI shall at least fulfill Type 1 and Type 2 for Wallets
- Discuss issuance of PID for natural and legal entities into the wallet.
- Discuss role of trust list where certified wallets will be listed
- EBSI shall be ARF compliant. EBSI certification process shall be integrated in Wallet
- Close collaboration with European standardization bodies should be taken into account.

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.

12.3. Issuance of Credentials

This section evaluates legal/governance related topics about issuance of Personal identification credentials (PIDs), and other types of credentials (attestations of attributes)

12.3.1. As/Is

- Currently any issuer can issue credentials in wallet as long as it uses EBSI as infrastructure.
- There are no security requirements on key management, authentication, authorization for issuers
- A standardized process for issuance of PID into EBSI wallets does not exist.

12.3.2. ToBe

- Wallets shall be able to receive PID acc. ARF incl.:
    - Key Management
        - External HSM
        - Trusted Execution Environment
    - Formats
        - SD-JWT
        - ISO mDL
- (Q)EAA
    - (Q)EAA shall be issued in formats and protocols acc. Type 1 and Type 2 ARF
- Only QEAA provider shall be able to issue QEAA using EBSI as decentralized PKI and also in Wallets which are not using EBSI
- Differentiate between PID and (Q)EAA
- Only accredited PID Provider should be able to issue PID using EBSI as decentralized PKI
- Issuance of (Q)EAA basically:
    - QTSP access the authentic source provided by MS, identifies the possible holder verifying PID of the EUDIW (QEAA could be issued by Non-Qualified Trusted Issuers on behalf of Authentic Sources supported by the Seal of a QTSP)
    - Issuance QEAA acc. Type 1 ARF
    - 2FA of EUDIW (SCA on LoA high) of user

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.

Means integration authentic source and verification & interaction with EUDIW needed

Identification of Holder, issuer and verifier

This section describes personal identification credentials, and other credentials (attestations of attributes).

12.3.3. As/Is

- Currently there are some identification credentials (https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Data+Models+and+Schemas)
  - Verifiable ID (Natural Person) – Wiki, TSR
  - Student ID – Wiki, TSR
  - PDA1 – Wiki, TSR
- Other credentials as Diplomas, Transcript of records, Microcredentials, PDA1 and EHIC are attestations about personal information but they are not identification credentials
- In addition, EBSI also manage some credentials as VID for Legal Entities and accreditations.

12.3.4. ToBe

- The new ARF based on new eIDAS regulation includes the PID, that is comparable with the VID previously remarked.
- This PID also includes the following claims:
  - Current Family Name (Mandatory)
  - Current First Name(s) (Mandatory)
  - Date of Birth (Mandatory)
  - Unique Identifier (Mandatory)
  - Family Name at Birth (Optional)
  - First Names at Birth (Optional)
  - Place of Birth (Optional)
  - Gender (Optional)
  - Nationality (Optional)
  - National level claims (Optional)
- It should be possible to identify holder with EUDIW acc. ARF.

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.

- It should be possible to issue PID for natural an legal entities into EUDIW by certain PID Providers acc. ARF. And PID on different LoA.
- Identification of Holder has to be done:
    - Issuance wallet: using eID mean (e.g. eID card) on needed LoA
    - Issuance (Q)EAA/access Relying: using EUDIW and 2FA acc. ARF
- Identification QEAA Provider
    - During conformity assessment resp. Registration for it
    - Authenticity of QEAA via e.g. QSeal from the QTSP (signed QEAA). Otherwise possible through DID linked to proven identity from QEAA
- Identification Relying Party
    - And Relying Party has to be listed in public list acc. EIDAS
    - Authentication e.g. via QWAC possible

12.4. Status and Revocation of Credentials

This section describe the necessity for a mechanism to get / revoke any credential. This revocation process will disable the validity of the credential forever.

12.4.1. As/Is

- EBSI specifies Status List 2021 as revocation mechanism.
- Reference: https://www.w3.org/TR/vc-status-list/

12.4.2. ToBe

- In WP4, there may be a requirement that the entity which issues a VC (e.g. university) may not be the same entity as the one that can revoke a VC. In addition, there may be a requirement that the entity with the technical ability to revoke a VC (e.g. the issuer) may not be the same entity as the one that has the legal authority (e.g. a court). This distinction may have to be recorded somewhere.
- I would add a mechanism to be used by the owner, the creator (Issuer) or a third party with “super powers” (court). There are some ideas in the ecosystem, but I think my preference is the Issuer has the permission to do that, and the rest of the actors must do it through the Issuer (Social Security agrees).
- For technical subjects see Section 9.3.
- Revocation shall be possible for (Q)EAA providers/issuers (if needed based on decision by public authority like court) only.

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.

12.5. Trusted Issuer Registry

This section describes a registry to store all the information about the entities which can issue some kind of credential.

12.5.1. As/Is

- EBSI defines Trusted Accreditation Organisation (TAO), Trusted Issuer (TI), Trusted Issuer Registry (TIR), Trusted Schema Registry (TSR) (link)
- I would change the description and the registry name for Trusted Entity Registry. This means, all the entities will be included here also if they are issuers or verifiers. The problem comes when an entity is verificating users but they are not issuing VCs. The user has no way to verify the identity of the company is trying to request his information so that could be a security problem.
- Currently, EBSI is not validating the information entered into the TIR. It's necessary a validator to confirm the information attached is valid and comes from a valid entity with enough permissions.

12.5.2. ToBe

- A registry to store any entity which want to "play" in the EBSI ecosystem. This registry must have a validation function to avoid "dirty" data. The registry should include:
    - Verifiable IDs of the entities
    - Verifiable Accreditations to include the capabilities of the entity.
- Any EUDIW, QTSP has to be listed in National Trust list and LOTL. Both might be provided within EBSI.
- Trusted Issuer Registry of EBSI shall be correlated with developments on TrustLists and LOTL acc. eIDAS 2.0

12.6. Verification of Credentials

12.6.1. As/Is

- None

12.6.2. ToBe

- The Credential verification must comply with some validation steps
    - Presentation signature is OK (so data model is OK and DID is correct)

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.

- Credential type is the type requested (if necessary)
- Credential signature is OK (so data model is OK and DID is correct)
- Credential creator is valid
  - Credential creator is available in the TIR
  - Credential creator Verifiable ID is OK
    - Validate all the signature chain until an “official” TAO is found
      - VID signature and VID status (this is a very hard process in terms of performance)
  - Credential creator accreditation to issue that kind of credential is OK
    - Validate all the signature chain until an “official” TAO is found
      - Accreditation signature and Accreditation status (this is a very hard process in terms of performance)
- Credential status is Valid (Not revoked)

12.7. Trusted Verifier Registry

12.7.1. As/Is

- None

12.7.2. ToBe

- The Relying Parties allowed to validate PID/QEAA from EUDIW will be listed in public list
- EBSI shall be able to handle this
- In Case of QTSP the TrustList/LOTL will be the Trusted Verifier Registry. EBSI could contain the TrustList/LOTL which will combine Trusted Issuer and Verifier (QTSP will act as Verifier in identification of holder and issuer in case issuing (Q)EAA into the EUDIW.

12.8. Trusted Wallet Providers Registry

This section describes – based on the ARF – the necessity for a registry to include all the Wallet providers, ensure the security of the Identity Wallets is OK.

12.8.1. As/Is

- None

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.

12.8.2. ToBe

- It's necessary a registry to include all the Wallet Providers (DID) available to offer a wallet to their users.
- It can be used as an Accreditation in the TIR.
- It could be revoked
- The registry must be checked each X event, or each X hours to verify the conformity of the provider.
- Regarding EUDIW: Any certified EUDIW will be listed in national trust list and LOTL. EBSI shall correlate its governance to eIDAS 2.0 to use TrustList/LOTL for verification of EUDIW.
- Revocation will be done if
    - e.g. mobile phone of EUDIW stolen
    - EUDIW is withdraw by MS e.g. due to technical changes, security breaches etc. EBSI governance shall be correlated.
- Revocation done by EUDIW issuer acc. EIDAS 2.0 and ARF

12.9. Authentic Sources

12.9.1. As/Is

- Currently does not exist within EBSI

12.9.2. ToBe

- EBSI should comply with eIDAS 2.0 so issuance of (Q)EAA using EBSI as decentralized PKI shall be done by QTSP using authentic sources provided by MS and mentioned by EC only.
- Interfaces between QTSP and authentic sources as well as protocols and formats shall be defined in accordance with ARF.

12.10. Qualified signing of Credentials

12.10.1. As/Is

- QES/QSeal used for eiDAS Bridge https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about

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.

12.10.2. ToBe

- It shall be possible to sign and/or timestamp QEAA shall with QSeal and/or QES according to what`s required by eIDAS and user.
- The QES/QSeal or timestamp should follow formats acc. ARF resp. ETSI ESI so it should be possible to use JAdES acc. ETSI TS 119 182 or alternatively CAdES (ETSI EN 319 122) or ASiC S/E (ETSI EN 319 162) in order to ensure easy issuance by existing QTSP

12.11. Security and Certification of EBSI Ledger

12.11.1. As/IS

- Currently there is no scheme for certification of security, operations etc. of any provide of EBSI node or network.

ToBe

- Development of requirements catalogue and possible standards which defines concrete security, privacy, operations and maintenance, governance, business and technical requirements for conformity assessment of qualified trust service providers for electronic ledger acc. Section 11 of eIDAS 2.0
- DIN TS 31648 and ISO CD TR 24332 should be considered which already contain useable criteria catalogues on this subject
- ISO 23257:2022 should be considered acc. Architecture of EBSI

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. Capabilities and Business Requirements

Since this Deliverable D3.1 was created in the beginning of the EBSI-VECTOR project, specific business requirements from the use case work packages WP4 (Education), WP5 (Social Security) and Business Registries (Wp3) were still under development. Nevertheless, as update, the following table includes a mapping between the technical capabilities evaluated in this deliverable, and business requirements related to them, also with the related short term priority expectation:

Capability	**Business Requirement**	**Short Term Priority (High, Medium, Low)**
Identifier Types	This is needed as a foundational feature for all use cases. WP4 business requirements do not require any specific format for Identifiers WP5 doesn't see the need of further did: key methods and the sentence "is not what most other projects use" should bring proofs and references to be accepted This is needed as a foundational feature for all use cases from a Business Registries perspective. Business registries: The issuance of Organizational Digital Identity (ODI) Credentials will be piloted with an DID:ebsi identitier. Other optional identifiers (e.g. EUID) are included in the ODI-Schema.	High (Social Security) Low (Education) High (Business Registries
Operations and Performance	WP4 agrees with provided suggestions	High (Education, Social Security)

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.

	WP5 agrees to the toBe requirements which are also required by the business. High availability and trust are of great importance to avert financial damage. Business registries: No specific requirements during the piloting phase within EBSI-VECTOR. For a potential EU-wide adoption beyond 2026 we foresee the following business requirements. Business Goal: • Reduce the time to acquire an ODI • Remain responsive during ODI promotion campaigns • Enable ODI issuance for thousands of legal entities in parallel • Issue an ODI for 24 mio EU-companies within a period of 5 years • Requirements for a scaling scenario: • Issue ODI for 24 mio EU-companies • Keep performance and operations stable during peak times • Handle up to 50.000 requests in parallel	Low (Business Registries)
Data Models of VC Containers	WP4 agrees on suggested toBe, however we would like to have EuDi that is open to any standard data model now used in any Eu Country	High (Social Security/Education)

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.

	Required by WP5. Interoperability towards eIDASis required. T3.3: Business registries There is a need to define a minimum set of attributes that all Data Model (Schema) for an ODI in Europe should contain. Business goal: • Relying parties across Europe can rely on similar issuing processes for ODI in an every EU-member state • Every ODI issued in an EU-member state shares at least a minimum set of attributes • The minimum set of attributes include at least the company name, the legal form, the country of issuance and the issuer name	Medium (Business Registries)
Data Model of VC Content (Diploma and Secondary School Certificate)	Required by WP4	High
Data Model of VC Content (Social Security)	WP4 agrees on suggested toBe, however we would like to have EuDi that is open to any standard data model now used in any Eu Country WP5agrees with ToBe requirements	High (Social Security, Education) High
Selective Disclosure	Both work packages WP4 and WP5 have privacy requirements that benefit from	Medium (Social Security, Education)

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.

	selective disclosure functionality.WP4 agrees with provided suggestions. WP5 agrees with provided suggestions	
(Qualified) signature/seal of credentials by Issuer	WP4 requires eIDAS compliance without additional requirement. Long-term validity and verifiability are necessary. WP5 agrees with provided suggestions. Long-term validity and verifiability are necessary. Business registries Context • Relying parties want to verify who issued the ODI Business registries Business goal: • The issuer who signed/ sealed an ODI must be identifiable for the relying party	High
Supported Presentation Protocols	WP4 agrees with the use of OID4VC Interop between EBSI based and eIDAS based wallets is highly desired. WP5. Agrees to toBe requirements. Interop between EBSI based and eIDAS based wallets is highly desired. Business registries Business goal: • Protocol must be interoperable with existing ERP-system • An cost-efficient integration is desirable	High

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.

Supported Issuance Protocols	WP4 agrees with the use of OID4VC WP5 agrees with the use of OID4VC Business registries Business goal: • Protocol must be interoperable with existing ERP-system • A cost-efficient integration is desirable	High (Social Security, Education) Low (Business Registries)
Multi-identity Support	WP4 agrees with ToBe requirement. WP5 agrees with ToBe requirement.	Medium
Multi-language Support	WP4 agrees with ToBe requirements. WP5 agrees with ToBe requirements Business registries Business goal • ODI is issued in countries with non-Latin letters (e.g. Greece) • Global standards should be used to assure that there are no barriers in the international context	Medium
Accessibility and Non-Discrimination Requirements	WP4 agrees with ToBe requirements WP5 agrees with ToBe requirements Business registries Business goal	Medium Low (Business Registries)

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.

	• An ODI should be accessible for people with handicap in the role of an applicant (holder) or verifier	
Authenticating Wallet Instances	WP4 agrees with ToBe requirements. WP5 agrees with ToBe requirements	Medium
Operations and Performance	WP4 agrees with ToBe requirements. WP5 agrees with ToBe requirements s.	Medium
Qualified Signature of Documents by Holder	WP4 agrees with ToBe requirements. WP5 agrees with ToBe requirements	Medium
Additional Social Security Requirements	WP4 agrees with some ToBe requirements, pls refer to WP4.1 for details. WP5 requires that this paragraph directly refers to WP5.1 document without additional details	Medium
Enterprise Wallet and Legal Entity Wallet	Required by WP5.	High
Organisational Identity	WP4 does not see ToBe requirements as part of its business needs. Required by WP5. t. Business registries Business goal • Every company self-manages their Organizational Digital Identity (ODI)	Medium (Social Security, Education) High (Business Registries)

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 ODI is used for identification and to issue digital product passports	
DID Creation	WP4 has no business requirements related to this. Requred by WP5. Business registries Business goal • Companies should be able to create and manage their own DID(s)	High (Social Security) Low (Business Registries)
DID Deactivation/Rev	WP4 has no business requirements related to this. WP4 does not agree with requirements as DID revocation would imply revocation of all VCs related to this DID and this brings complex legal consequences. WP5 aligns with WP4 in this suggestion, provided details are not enough to guarantee end-user protection from potential revocation side-effects. Further details would be needed. Business registries: A need in which a DID is de-activated or revoked could not be identified. If a DID is outdated, it is not used anymore.	Medium (Education Social Security) Low (Business Registries)
Credential Sharing Consent Approval (Data Agreements)	Required by WP5 – WP5 disagree with ToBe section referencing to private implementations as this may lead to private entities conflict of interest. We suggest changing this with detailed requirements without such references.	Low (Social Security)
Consent Revocation	WP5 agrees with provided suggestions	Low (Social Security)

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.

Credential Status Change	WP5 partially agrees with provided suggestions as Status Attestation/Assertion is not mentioned while clearly indicated in WP5 and also WP4. Business registries Business goal: • If an attribute within the ODI is outdated, the ODI should be revoked immediately and it should be replaced by a new one	Medium (Social Security, Education) High (Business Registries)
Credential Expiration Management	WP5 partially agrees. Expired credential must be anyway available to holder to proof its validity within provided date range. E.g. a residency certificate, while expired, should be available to holder for any request related to its validity. I'ts verifier's role to decide if this credential fulfills its requirements Business Registries Business goal • There is no need that an ODI expires. • Status changes should trigger an ODI revocation Security considerations • It may be reasonable to include an expiration date to confront unforeseen missuse	High (Social Security) Low (Business Registries)
Interoperability with other Trust Frameworks	WP5 agrees as this would improve acceptance and distribution of use. Business Registries Business goal • The ODI should be interoperable and accepted in all Trust Frameworks	Low (Social Security) High (Business Registries)

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.

Visualization of Credentials	WP5 agrees as this would improve acceptance and distribution of use. Business registries Business goal • The credential must be displayed in a way that a human verifier understands the purpose of the ODI	Low (Social Security) Medium (Business Registries)
API Definition & Documentation	WP5 agrees with ToBe requirements Business registries Business goal • Verifiers and Holders must be able to integrate the ODI in their ERP-systems, e.g. via an API • Documentation must be provided to integrate it cost-efficiently	High (Social Security) Low (Business Registries)
Longevity of Cryptographic Algorithm	WP5 agrees With requirement while suggested solutions should consider pluggable cryptographic capability (e.g. capability to update cryptographic algorithms on need) Business Registry Business goal • Longevity must be given according to existing know-how • Fall-back scenario must be developed if cryptographic algorithm must be changed	Low
Comparison EBSI Governance Roles and eIDAS 2.0 Governance Role	WP5 agrees, but suggests to avoid providing fixed governance schemes as each member state has a wide range of flexibility in its implementation and such schema may not be always applicable Business registries Context: It is assumed that public authorities issue ODI-credentials. They	Medium

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.

	represent the root-TAO in EBSIs Trust Model or the authentic source in the ARF	
Issuance and Certification of Wallets	WP5 agrees with provided suggestions Business registries Business goals • We see a certification of wallets as competitive advantage for some wallet providers • Certification may need to play an important role when wallet providers proof their interoperability	Low
Issuance of Credentials	WP5 while agreeing with the overall approach suggests simply requiring EBSI to be compliant with eIDAS2 model without providing specifics as such model is not yet fully defined. Business registries Business goals • The ODI must be issued by a trustful source. • The issuance of the ODI must be cost efficient	High
Identification of Holder, Issuer, and Verifier	WP5 suggests simply requiring EBSI to be compliant with eIDAS2 model without providing specifics as such model is not yet fully defined. We remind here that ARF is not part of the regulation and as stated "...holds **no legal value"** Business registries Context: • The ODI identifies the Holder	Medium

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.

	• Issuer and Verifier should hold an ODI as well	
Status and Revocation of Credentials	WP5. To align with what stated into D5.1. Status Attestations must be mentioned as well. Business registries Business goal • There must be a solution to revoke ODIs	High
Trusted Issuer Registry	WP5 agrees with provided suggestions Business registries Business goal • It is expected that legal entities use the ODI to issue digital product passport • Hence, all legal entities that hold a ODI and that want to issue a digital product passport must be included in the Trusted Issuer Registry	High
Verification of Credentials	Required by WP5	High
Trusted Verifier Registry	Required by WP5 only for a subset of verifiers (Trusted) without limitation in other verifiers	High
Trusted Wallet Providers Registry	WP5 agrees with provided suggestions	Medium
Authentic Sources	WP5 agrees with provided suggestions Business Registries Business goal • It must be assured that attributes within the ODI originate from a source verifiers can trust	Low (Social Security) High (Business Registries)
Qualified Signing of Credentials	WP5 agrees with provided suggestions	Medium

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.

Security and Certification of EBSI Ledger	WP5 agrees with provided suggestions Business Registries Business goal • A fully performant and secure service to obtain ODIs and verify them is expected.	Medium (Social Security) Low (Business Registries)

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.

14. Conclusions

Through this document we have been able to evaluate and compile all the functionalities and processes that should be included in an infrastructure and trust framework such as EBSI. All the existing functionalities have been evaluated, indicating the necessary changes and new ones have been added to complete the necessary functionality.

We have explored all the necessary mechanisms that a framework of this type has to provide to the different actors that are going to participate in its processes. The use cases based on the Self-Sovereign Identity (SSI) paradigm are infinite, since this new technology is transversal to all sectors and industries (Identity, Education, Social Security, Travel, ...). That is why this document does not deal with specific use cases, but the objective has been to compile the general functionalities to be able to fulfill all the processes related to the generic processes.

Although the user journeys are totally dependent on the domain and region where they are executed (Member States, Europe, ...), as they are strongly controlled by their regulations, the trust framework must include all those aspects that allow to execute all the processes from a neutral point of view. These aspects provided by the framework will be duly adapted by the integrations of the different actors and based on their corresponding regulations.

Regarding the next steps, we intend this Deliverable to become either a living document, or at least the basis for future deliverables D3.2 and D3.9 (“ESSIF specification for the new capabilities in EBSI”). We also contribute this deliverable as input for ongoing work in T3.2 (“Develop an enterprise wallet and legal entities service) and T2.2 (“Interoperability”).

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.