



# EBSI-VECTOR

Education and work reloaded

## D4.1: Business Blueprint (BBP)

<b>Project title:</b>	<b>EBSI-VECTOR</b> - EBSI enabled VErifiable Credentials & Trusted Organisations Registries
<b>Grant Agreement No.</b>	101102512 - DIGITAL-2022-DEPLOY-02-EBSI-SERVICES
<b>Deliverable Title</b>	D4.1: Business Blueprint (BBP)
<b>Version:</b>	1.4
<b>Date:</b>	01/12/2023
<b>Responsible Partner:</b>	CIMEA
<b>Authors:</b>	Maria Oreshnikova - CIMEA
<b>Contributing Partners:</b>	ENG, Visions, BC diploma, Uni Lille, Uni Maribor, Nask, GovPart, Validated ID, Protokol, Logalty, UNIBO, Sikt, IZERTIS, GEANT, Gataca, UPT, KU Leuven, DUO, RI.SE.
<b>Reviewers:</b>	Markus Sabadello (DANUBETECH), Steffen Schwalm (MSG)
<b>Dissemination Level:</b>	PU – Public



Co-funded by  
the European Union

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

### Document Change History

Version	Date	Author (organisation)	Description
v1.0	12/10/2023	T4.1 partners	Draft and preliminary content
v1.1	20/10/2023	CIMEA	First Review
v1.2	30/10/2023	CIMEA	Final Review
V1.3	21/11/2023	MSG, Danube Tech	Peer Review
V1.4	01/12/2023	CIMEA	Final Review



## Table of Contents

<b>1</b>	<b>EXECUTIVE SUMMARY</b> .....	<b>9</b>
<b>2</b>	<b>INTRODUCTION</b> .....	<b>10</b>
<b>3</b>	<b>THE DIGITALIZATION OF EDUCATIONAL ECOSYSTEM</b> .....	<b>12</b>
3.1	CHANGING LANDSCAPE OF EDUCATION .....	12
3.2	THE NEEDS OF STUDENTS .....	13
3.3	THE NEEDS OF UNIVERSITIES AND QUALIFICATION ISSUING ORGANIZATIONS .....	14
3.4	THE NEEDS OF EMPLOYERS .....	15
<b>4</b>	<b>BUSINESS DESCRIPTION</b> .....	<b>15</b>
4.1	CORE VALUES .....	16
4.2	LEGAL FRAMEWORK .....	17
4.3	WHAT CAN SELF-SOVEREIGNTY AND EBSI TRUST MODEL BRING TO THE TABLE? .....	18
<b>5</b>	<b>MARKET ANALYSIS</b> .....	<b>19</b>
5.1	OPPORTUNITIES .....	19
5.2	CUSTOMER MIX.....	21
5.3	MARKET SEGMENTS .....	21
5.4	MARKET SIZE .....	23
5.5	MARKET PRESENCE.....	25
<b>6</b>	<b>INTEROPERABILITY</b> .....	<b>25</b>
6.1	INTEROPERABILITY DOMAINS .....	26
6.1.1	<i>Organizational Interoperability</i> .....	26
6.1.2	<i>Legal Interoperability</i> .....	27
6.1.3	<i>Technical Interoperability</i> .....	28
6.1.4	<i>Semantic Interoperability</i> .....	31
<b>7</b>	<b>CUSTOMER ANALYSIS</b> .....	<b>34</b>
7.1	HIGHER EDUCATION INSTITUTIONS .....	34
7.2	SECONDARY SCHOOLS .....	35

7.3	PROFESSIONAL CERTIFICATION ISSUERS.....	35
7.4	CONTINUING EDUCATION AND VOCATIONAL TRAINING PROVIDERS.....	36
7.5	STUDENTS (ACROSS DIFFERENT NATIONS AND LEVELS).....	37
7.6	PRIVATE AND PUBLIC ORGANIZATIONS .....	37
7.7	STRATEGY FOR SERVING TARGET CUSTOMER NEEDS.....	38
<b>8</b>	<b>SERVICE REQUIREMENTS &amp; DESCRIPTION.....</b>	<b>39</b>
8.1	SERVICE REQUIREMENTS.....	40
	<i>Journey 1. 8.1.1 Organizational Requirements.....</i>	<i>40</i>
	<i>Journey 2. 8.1.2 Technical Requirements .....</i>	<i>42</i>
	<i>Journey 3. 8.1.3 Semantic Requirements.....</i>	<i>44</i>
	<i>Journey 4. 8.1.4 Legal Requirements .....</i>	<i>47</i>
8.2	SERVICE FEATURES .....	47
8.2.1	ENTERPRISE WALLET GENERAL FEATURES.....	47
8.2.2	ENTERPRISE WALLET USER ONBOARDING & PROFILE MANAGEMENT.....	47
8.2.3	ENTERPRISE WALLET CREDENTIAL ISSUANCE & MANAGEMENT .....	48
	<i>Journey 5. 8.2.4 User Wallet &amp; Credential Access .....</i>	<i>49</i>
	<i>Journey 6. 8.2.5 Enterprise Wallet Credential Verification .....</i>	<i>49</i>
	<i>Journey 7. 8.2.6 User Wallet Privacy and Data Control.....</i>	<i>50</i>
	<i>Journey 8. 8.2.7 Enterprise Wallet Interoperability and Standards Compliance .....</i>	<i>50</i>
	<i>Journey 9. 8.2.8 Notification and Alerts .....</i>	<i>50</i>
	<i>Journey 10. 8.2.9 Multi-Language Support.....</i>	<i>50</i>
	<i>Journey 11. 8.2.10 Support and Help Center .....</i>	<i>51</i>
	<i>Journey 12. 8.2.11 Compliance and Security .....</i>	<i>51</i>
	<i>Journey 13. 8.2.12 Scalability .....</i>	<i>51</i>
	<i>Journey 14. 8.2.13 Legacy Document Management .....</i>	<i>51</i>
	<i>Journey 15. 8.2.14 User Feedback and Ratings .....</i>	<i>51</i>
	<i>Journey 16. 8.2.15 Accessibility Features .....</i>	<i>51</i>
8.3	BENEFITS .....	52
8.4	USER SCENARIOS & JOURNEYS.....	52
	<i>8.4.1 Overall Scenario requirements.....</i>	<i>53</i>
	<i>Journey 17. Prerequisites.....</i>	<i>53</i>



8.4.2	Process 1: Educational Credential Issuing.....	53
8.4.3	Process 2: Educational Credential Request & Verification.....	56
8.4.4	Process 3: Credential Revocation.....	58
8.5	POSSIBLE JOURNEYS.....	60
8.5.1	Transcript and Academic Record Management.....	60
8.5.2	Diploma issuance & Revocation scenarios.....	64
8.5.3	Employer verification scenarios.....	67
8.5.4	Student card verification & revocation scenarios.....	69
8.5.5	Publishing & Copyright Protection.....	72
8.6	CUSTOMER USER STORIES.....	74
<b>9</b>	<b>MARKETING AND DISSEMINATION STRATEGY.....</b>	<b>78</b>
9.1	INTRODUCTION.....	78
9.2	SERVICES OVERVIEW OF EBSI-VECTOR DIGITAL CREDENTIAL SERVICE.....	79
9.3	UNIQUE SELLING POINTS (USP) OF EBSI-VECTOR DIGITAL CREDENTIAL SERVICE.....	80
9.4	DISSEMINATION STRATEGY FOR THE EBSI-VECTOR DIGITAL CREDENTIAL SERVICE.....	80
9.4.1	Goals:.....	81
9.4.2	Channels and Platforms:.....	81
9.5	MARKETING CHANNELS FOR THE EBSI-VECTOR DIGITAL CREDENTIAL SERVICE.....	84
9.5.1	Digital Marketing Channels.....	84
9.5.2	Traditional Marketing Channels.....	85
9.5.3	Community Engagement.....	85
9.6	FEEDBACK & ITERATION FOR THE EBSI-VECTOR DIGITAL CREDENTIAL SERVICE MARKETING.....	86
9.6.1	Methods to Gather Feedback.....	86
9.6.2	Analytics Tools to Measure Performance.....	86
9.6.3	Strategies to Iterate and Refine based on Feedback and Data.....	87
9.7	CONCLUSIONS.....	87
<b>10</b>	<b>OPERATIONS AND MANAGEMENT.....</b>	<b>88</b>
10.1	DAILY OPERATIONS OF ISSUING ORGANIZATIONS.....	88
10.1.1	Operation Framework.....	88
10.1.2	Credential Issuance.....	89

10.1.3	<i>Credential Management</i> .....	89
10.2	TEAM PROFILES FOR ISSUING ORGANIZATIONS .....	89
10.2.1	<i>Operations Team</i> .....	89
10.2.2	<i>Technical Support Team</i> .....	89
10.2.3	<i>Compliance and Legal Team</i> .....	90
10.3	ORGANIZATIONAL STRUCTURE OF ISSUING ORGANIZATIONS.....	90
10.4	OPERATIONAL PROCESSES .....	90
10.4.1	<i>Issuance Process</i> .....	90
10.4.2	<i>Management Process</i> .....	90
10.4.3	<i>Verification Process</i> .....	90
10.4.4	<i>Continuous Improvement Process</i> .....	91
<b>11</b>	<b>SWOT ANALYSIS</b> .....	<b>91</b>
11.1	INTERNAL ANALYSIS.....	91
11.1.1	<i>Strengths</i> .....	91
11.1.2	<i>Weaknesses</i> .....	92
11.2	EXTERNAL ANALYSIS .....	92
11.2.1	<i>Opportunities</i> .....	92
11.2.2	THREATS .....	94
<b>12</b>	<b>LEGAL AND REGULATORY COMPLIANCE</b> .....	<b>95</b>
12.1	LEGAL REQUIREMENTS.....	97
<b>13</b>	<b>CONCLUSION</b> .....	<b>100</b>
<b>14</b>	<b>REFERENCES</b> .....	<b>101</b>

### List of Figures

FIGURE 1 - EDUCATIONAL MARKET USER SIZE .....24

FIGURE 2 – COUPLING CONCEPT .....33

FIGURE 3 - CREDENTIAL LIFECYCLE .....53



## List of Terms and Abbreviations

Abbreviation	Definition
EBSI	European Blockchain Service Infrastructure
EBSI-VECTOR	EBSI enabled Verifiable Credentials & Trusted Organisations Registries
ELM	European Learning Model
EUDIW	European Digital Identity Wallet
EUDI	European Digital Identity
DLT/Blockchain	Distributed Ledger Technology. Note that in this document the term 'blockchain' and DLT are used interchangeably even though blockchain is a subset of DLT technology-wise <sup>1</sup>
GDPR	General Data Protection Regulation
HEI	Higher Education Institution
SEO	Search Engine Optimization
TAO	Trusted Accreditation Organisation
VC	Verifiable Credential
VP	Verifiable Presentation
WPxx	Work Package number xx

<sup>1</sup> See ISO 22730 and ISO TC 307



# 1 Executive Summary

With a strong commitment to innovation, global collaboration, and personalized education, EBSI Vector aim to empower learners of all ages and backgrounds to achieve their full potential. Blockchain technology can bring positive and transformative changes, enhance various aspects in different fields, including education. We are dedicated to reshaping the educational environment by utilizing the blockchain technology made available through EBSI.

Our mission at EBSI Vector is to pioneer the integration of EBSI into the education sector, providing students and institutions with a secure, decentralized, and interoperable ecosystem for managing educational data. We aim to make educational processes more efficient, reduce administrative overhead, and provide students with greater control over their academic records. The mission extends to ensuring that learning, whether formal or non-formal, is recognized, validated, and portable across various educational and professional platforms.

The values of the educational ecosystem on EBSI align with principles such as transparency, security, decentralization, accessibility, and collaboration. These values would guide the development and implementation of blockchain-based solutions in education.

## *VISION*

Create a blockchain-powered education infrastructure that fosters global collaboration, innovation, and accessibility. Establish seamless pathways for learners and professionals, where their educational achievements are effortlessly recognized and transferred across international borders.

In this document, we will delve into the essential requirements and design considerations for cross-border user journeys in the educational sector. Creating an inclusive and user-centric

educational experience for learners across diverse countries and cultures, while simultaneously complying with international regulations, is a multifaceted challenge leading to a simple way for people to share any learning outcome in a wallet.

## 2 Introduction

A core objective of EBSI-VECTOR project is to develop the strategies in supporting the implementation of verifiable credential use cases (education and social security) interoperable with ESSIF and align it in a later stage with the emerging EUeID programme.

The various project WPs are strongly interconnected, to ensure a coherent strategy to develop the expected results and WP4 focuses on the implementation of EBSI capabilities in the educational domain.

In details, WP2 specifically focuses on developing the strategies for interoperability (D.2.2, D.2.3), strategies to take-up (D.2.4) and scale-up (D.2.5) use cases, as well as implementation strategies finetuned for country needs (D.2.1) and specific institutional conditions (D.2.6). The strategy documents contain technical, institutional, organizational, and legal recommendations and roadmaps to support early-adopters and future organizations to be part of the EBSI ecosystem.

WP3 focuses on the consolidation of these capabilities, to bring the EBSI capabilities on verifiable credentials and decentralised trusted registries towards a production stage.

The ESSIF specifications work (D3.1) redefine and stabilize the current specification and drive the adjustments and improvements on EBSI core service side to deliver a stable and production ready platform, based on the business requirement of the involved use cases in social security (D5.1) and education (D4.1).

WP4 education and WP5 social security develop, test and deploy user journeys (D4.2, D5.2) based on the requirement for new EBSI capabilities for education and social security (D4.1, D5.1 business blueprint).

With specific reference to D4.1, Business Blueprint education, it regards business requirements, scenarios and interoperability requirements and use-case governance model design. It is aimed to define the business requirements for production implementation.



## 3 The digitalization of educational ecosystem

In an increasingly interconnected world, the demand for quality education transcends geographical boundaries. Educational institutions and businesses are embracing the digital age to offer innovative learning solutions to a diverse global audience. However, with this global reach comes the challenge of designing seamless cross-border digital solutions based on user journeys that cater to the unique needs, preferences, and regulatory requirements of learners from various member states.

The main objective of the EBSI-VECTOR WP4 is to digitalize the entire document issuing and exchange process, supporting citizens in their educational journey, simplifying attestations of their achievements resulting in a diploma or any other qualification as for example the recognition of a personal skill or a professional competence, including ones awarded in different contexts (sport, association...).

### 3.1 Changing Landscape of Education

The landscape of education is rapidly evolving, advancements in technology, international mobility, and a growing demand for global education have created a dynamic environment in which students and educational institutions seek to navigate seamlessly. Whether it involves students pursuing degrees abroad, professionals seeking continuing education or institutions expanding their reach globally, the educational sector faces increasing demands for smooth, efficient, and transparent processes.

The increasing number of citizens studying outside of their home countries, combined with the sharp growth of online cross-border learning due to COVID-19 pandemic and diversifying lifelong learning pathways, has triggered the need for **portable, secure, and verifiable digital credentials**. The affordance of blockchain technologies carries unique potential to respond to this profound need.

From the digitization of educational records to the verification of credentials, blockchain is capable of:

- Facilitating **secure** and **tamper-proof** academic credential issuance and verification, making easier for students and institutions to share and verify educational achievements.

- Promoting **transparency** and **trust** in educational records, ensuring that students' qualifications are recognized and valued across borders.
- Enhancing data management and **privacy** in educational institutions by using blockchain's decentralized and encrypted nature.

This transformation of the educational landscape extends to smaller and specialized units of learning achievement known as *micro-credentials*.

### *Micro-credentials*

Micro-credentials, within the European educational context, are perceived as attestations of the acquisition of specific skills, knowledge, or know-how.

They are typically associated with smaller learning units than traditional qualifications, thereby allowing for enhanced flexibility and personalization in educational pathways. Micro-credentials can be accumulated and integrated into broader learning pathways, potentially leading to formal qualifications. They are often envisioned as tools for making lifelong learning visible and valuable, recognizing both formal and non-formal education.

Although their recognition and portability vary significantly across Europe, they are increasingly seen as means to facilitate student and worker mobility by validating and documenting skills in a transparent and verifiable manner. Micro-credentials are also tied to concepts such as "micro-learning," which refers to shorter, targeted learning pathways, often focused on developing specific skills in response to the changing needs of the labour market and society.

On 16th June 2022, a pivotal move was made by the Council of the European Union by adopting a Recommendation on a European approach to micro-credentials for lifelong learning and employability, signifying a robust commitment to integrating micro-credentials into the European educational and professional landscape. This recommendation underscores the imperative of micro-credentials in facilitating continuous learning and enhancing employability across the EU.

## 3.2 The needs of students

Students, navigating through the evolving educational and professional landscapes, seek mechanisms that can succinctly and effectively validate their diverse learning and skill

acquisition. Credentials and micro-credentials emerge as a pivotal tool in this context, addressing students' needs by providing a structured, recognized, and portable means of certifying their competencies, skills, and knowledge obtained through various formal and non-formal learning pathways<sup>2</sup>. Particularly, students express a keen interest in the 'micro' aspect of these credentials as they are less regulated than others, valuing short, effective, and updated courses that can be directly aligned with specific skill sets and employment opportunities<sup>3</sup>.

Digital-credentials facilitate a learner-centric approach, enabling students to curate their educational journey, accumulate, and stack credentials that are reflective of their unique learning trajectories and aspirations. This not only empowers them to navigate through their educational and professional pathways with autonomy but also ensures that their diverse and multifaceted learning experiences are validated and recognized across borders, thereby enhancing their mobility and employability within the European context.

### 3.3 The Needs of universities and qualification issuing organizations

Universities, as pivotal entities in the educational domain, are navigating through the transformative wave brought about by digital credentials, seeking to align their offerings with the evolving needs of students and the labour market. The integration of digital-credentials and micro-credentials into the higher education (HE) sector necessitates universities to adapt their curricular structures, ensuring they are modular, flexible, and reflective of both academic and industry standards. Furthermore, universities and qualification issuing organizations are grappling with the challenge of ensuring that digital credentials are not only recognized within the institutional context but also are portable and recognized across various educational and professional contexts within the European Union.

The need to ensure that digital & micro-credentials are quality-assured, validated, and aligned with the European Qualifications Framework (EQF) and other relevant frameworks is paramount, ensuring their credibility and value in the eyes of both students and employers.

---

<sup>2</sup>[EBSI's success stories. A PhD student applies for specific courses in a foreign country](#)

<sup>3</sup>[Challenges and Opportunities of Micro-Credentials in Europe](#)

Within this context, universities are exploring mechanisms to facilitate the smooth integration of micro-credentials into existing academic structures, ensuring they complement and enhance traditional degree offerings, and provide students with additional avenues to showcase their skills and competencies<sup>4</sup>.

### 3.4 The Needs of employers

Employers, as key stakeholders in the digital-credential's ecosystem, exhibit a diverse range of needs and perspectives. While there's awareness in digital credentials, and their use is well accepted, there is also a discernible lack of a unified understanding of micro-credentials among employers, with many associating them merely with certificates of attendance at professional courses rather than recognizing them as attestations of specific skills and competencies. Employers often value certifications that indicate proficiency in soft and social skills, although the time and resources to verify such credentials are frequently lacking. In certain instances, technical certifications might be overlooked unless they pertain to professions where continuous professional development is mandated, such as in legal or medical fields. Employers acknowledge the potential of micro-credentials to transparently represent specific skills and facilitate linguistic and professional homogeneity in CVs, thereby simplifying recruitment processes.

## 4 Business description

The educational ecosystem encompasses the entire network of stakeholders involved in the educational process, including students, educational institutions, government bodies, employers, and service providers. EBSI is a part of this ecosystem, with the objective to facilitate secure, decentralized data management and interoperability.

To put these actors together we can enhance the educational ecosystem by ensuring the security and integrity of educational data. Academic records, certificates, and other sensitive information are linked on a blockchain, making them tamper-proof and resistant to fraud with a level of data security that gives trust among all stakeholders. Establishing a cross-border educational network

---

<sup>4</sup>[Recommendation on a European approach to micro-credentials for lifelong learning and employability](#)

where academic institutions and employers worldwide can trust the authenticity of educational credentials and achievements is a significant and transformative goal.

## 4.1 Core Values

Embracing the European Blockchain Services Infrastructure (EBSI), we're introducing a solution that embodies core values essential for the future of education: decentralization, authenticity, transparency, and security. EBSI-VECTOR aims to ensure that educational credentials are verifiable, tamper-proof, and universally recognized across the European Union, elevating trust and simplifying cross-border academic pursuits.

This marks a pivotal step in harmonizing and modernizing European education in alignment with the digital era, following our core values as detailed below:

### Transparency

Blockchain's transparent nature enables EBSI-VECTOR to enhance transparency in various processes, reducing the risk of fraud and corruption. Ensuring that all educational records and credentials are securely referenced on the blockchain, providing a transparent tamper-evident history of achievements.

### Security

Security and data protection are paramount in EBSI-VECTOR. EBSI infrastructure is designed to ensure the integrity and confidentiality of data while leveraging the immutability of blockchain. Prioritizing the security and privacy of student and institutional data through blockchain's encryption and decentralized architecture guarantees an unprecedented level of data security instilling trust among all involved stakeholders.

### Decentralization

Embracing the decentralized nature of EBSI blockchain to reduce reliance on centralized authorities for verification and validation of educational credentials. Students can securely manage their data and share it with potential employers and other institutions, reducing bureaucracy and administrative overhead.

### Accessibility



EBSI-VECTOR aims to ensure that blockchain-based educational services are accessible to all learners, regardless of their geographic location, socioeconomic status or physical capability.

### Collaboration

While primarily focused on EU member states, EBSI-VECTOR believes that collaboration with international partners and organizations is a key element for qualification ecosystem as students do not mind crossing borders of EU to non-EU learning centres and viceversa. Encouraging collaboration between educational institutions, governments, and technology providers to create a standardized and interoperable blockchain infrastructure for education is mandatory to make possible that cross-border education and recognition of qualifications become more accessible, enhancing global mobility for students and the exchange of knowledge and skills.

The integration of blockchain technology is revolutionizing how we manage, verify, and utilize educational credentials. EBSI-VECTOR will focus not only on traditional academic credentials but also on micro-credentials. This approach empowers individuals to showcase their specific skills and competencies, thereby enhancing their career opportunities and personal growth. Micro-credentials have emerged as a pivotal element in contemporary education, offering a nuanced, modular approach to learning and skill acquisition. Integrated with technologies like the European Blockchain Services Infrastructure (EBSI), they present a robust framework for enhancing educational achievements ecosystem.

## 4.2 Legal framework

Having established our core values as the guiding principles of our educational ecosystem, we now turn our attention to the necessary legal framework that underpins our commitment to these values.

The legal foundation of our operations is vital to ensure compliance, protect the rights and data privacy of all actors involved in the process, provide a secure environment for learning and credential management, as well as for students.

The legal framework for EBSI-VECTOR educational ecosystem must follow existing laws and regulations related to education and data privacy while also consider emerging blockchain-specific regulations.

Legal framework will be extensively discussed in Chapter 11, nevertheless we highlight here some key aspects that constitute the baseline of the next chapters:

- **Data Protection:** Compliance with data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, to ensure the privacy and security of educational linked data on the blockchain.
- **Interoperability Standards:** Collaboration with relevant authorities and educational bodies to establish interoperability standards for blockchain-based educational records and credentials.
- **Recognition and Accreditation:** Working with regulatory bodies to ensure that blockchain-verified educational credentials are recognized and accepted by academic institutions, employers, and government agencies.
- **Smart Contracts:** Legal considerations for the use of smart contracts in educational agreements, such as automated transcript requests, student enrolment, and certification issuance.

### 4.3 What can self-sovereignty and EBSI trust model bring to the table?

Authentication and Verification:

Digital credentials need to be authentic and verifiable to ensure their value and credibility. The European Blockchain Services Infrastructure (EBSI) is an ecosystem based on blockchain technology that is utilized to issue verifiable credentials to assure the authenticity and verifiability of digital credentials.

Personal Data Management

Students, as the owners of their digital credentials, should have full control over their data and be able to share it selectively with employers or educational institutions. Self-sovereignty allows individuals to own and control their information without the intervention of a central authority, which is pivotal for the mobility and portability of digital credentials.

Interoperability and Standardization

Digital credentials need to be recognized and accepted uniformly across different institutions and countries. Self-sovereignty and EBSI trust model can facilitate interoperability by ensuring

credentials are issued and verified in a consistent manner, using common standards. The recommendations from the European Commission and various initiatives and projects highlight the need for a standardized and interoperable approach.

#### Recognition and Portability

Recognition of digital credentials across borders and among different institutions is essential for their utility and efficacy. Self-sovereignty and EBSI trust model will enable broader recognition by providing a reliable verification mechanism and eliminating the need to trust a central authority for certification management.

#### Privacy and Security

Self-sovereignty can enhance privacy and data security by allowing individuals to share only the necessary information, without revealing their entire data. This is particularly pertinent in the context of digital credentials, where sensitive information about students' skills and achievements needs to be managed with strict security and privacy.

In summary, self-sovereignty and EBSI trust model can play a pivotal role in managing digital credentials in Europe, addressing key issues related to authentication, data management, interoperability, recognition, and data security.

## 5 Market analysis

### 5.1 Opportunities

The VECTOR project aims to guarantee that verifiable credentials linked to educational and professional history are interoperable and usable within an official EU Wallet, making them easy to issue for the authorized entities, to share for the citizen and to verify by any legal entity or institutions.

For public and private bodies, this means developing certified education and training programs that are accessible in quality, attractive in design, affordable and effective. Open education resources and paths, in initial and vocational education will lead to micro and macro certifications that will greatly help any people to further access to resources that can improve the skills and

training they need to succeed in their working environment but also offer a range of new curricula and training possibilities.

Digital credentials can be used in an array of different ways. For example, a private or public education institution can issue different types of documents and certificates to their students. Example of documents that can be issued are:

- graduation diplomas,
- yearly school reports,
- separate course completion certificates,
- summer school participation,
- professional certification,
- different competition awards,
- etc.

Due to the nature of the type of information held inside such credential wallets there is a need for ***different supporting solutions (technology enablers)***.

Such solutions can be divided in two major technology enablers:

*Tech Enabler 1.* **Enterprise wallet** used by legal entities when **issuing or verifying** credentials to/of their users, enabling secure storage of data and private keys used to sign, verify and issue credentials;

*Tech Enabler 2.* **User wallet** used by citizens to receive, share and store achievements, accreditations and any type of digital certifications.

**Market development opportunities** that descend from such enablers can be shortly described below:

- Creation of standards and technology framework for an enterprise wallet to become a **product** for legal entities as issuers and verifiers
- Provisioning of an open and widely accessible online **issuance & verification service** for non-professional (e.g., educational) issuers and verifiers
- Extending the **user wallet** capabilities to match a specific market (e.g., tailoring functions for the educational ecosystem) to become a bespoke product for the holders (students)
- Provisioning of a web-based public **custodian wallet** AsAService for students.

EBSI-VECTOR doesn't aim to become a business-oriented project and the scope of this paragraph is merely to be an input for external stakeholders that would be interested in further developing the EBSI-based educational area.

## 5.2 Customer Mix

Our customer mix is focused on three customer profiles:

**Employers/Public Organizations:** Credential validation is necessary to ensure potential candidates possess the skills and qualifications they claim they have. Relying on trusted credentials, employers can make educated decisions during their hiring process or public bodies can include such digital verification process within their internal processes.

**Educational Institutions:** During enrolment processes the educational institutions must ensure that students meet the necessary academic standards and qualifications required. Institutions can also use credentials when showcasing the academic achievements of their students and professors, increasing their credibility.

**Individuals:** Individuals can use their verifiable credentials and accreditations for pursuing a career in specific fields with set educational requirements. They can also be used for showcasing their skills, expertise and achievements. Freelancers can use it to demonstrate their capabilities, securing more work opportunities.

## 5.3 Market segments

The market segments of education and competences can be divided into several different categories. If the need for certification in early childhood and primary education is sometimes not required, the employees of such sector are certified, and their skills could also be subject to verification.

From the standpoint of an **ISSUER**, we can define the following market segments:

- **Higher Education Institutions:** any type of higher education institution which, in accordance with national law or practice, offers recognised degrees or other recognised

tertiary level qualifications, whatever such establishment may be called, or any institution which, in accordance with national law or practice, offers vocational education or training at tertiary level (*Reference: Glossary in the Erasmus+ Programme Guide 2023, <https://erasmus-plus.ec.europa.eu/programme-guide/part-d>*).

- **Vocational education and training institutions:** in education and training, bodies issuing qualifications (certificates, diplomas or titles) formally recognising the learning outcomes (knowledge, know-how, information, values, skills and competences) of an individual, following an assessment procedure for initial and continuing vocational education and training (IVET and CVET). (*Reference Cedefop: Terminology of European education and training policy: <https://www.cedefop.europa.eu/en/tools/vet-glossary/glossary>*)
- **Schools:** institutions providing general, vocational or technical education, on any level from pre-school to upper secondary education (*Reference: Glossary in the Erasmus+ Programme Guide 2023, <https://erasmus-plus.ec.europa.eu/programme-guide/part-d>*).
- **Early childhood education and care schools:** Early childhood education and care refers to any regulated arrangement that provides education and care for children from birth to compulsory primary school age (*Reference: European Education Area, Education levels: <https://education.ec.europa.eu/education-levels/early-childhood-education-and-care>*).

All the stakeholders (i.e., citizens) of the above-mentioned market segments are by themselves part of a market segment, i.e., being a **HOLDER** of a user wallet.

There are also some market segments to look at, from the standpoint of a **VERIFIER**. These would mainly be businesses or institutions looking to provide verification services to their clients or for themselves.

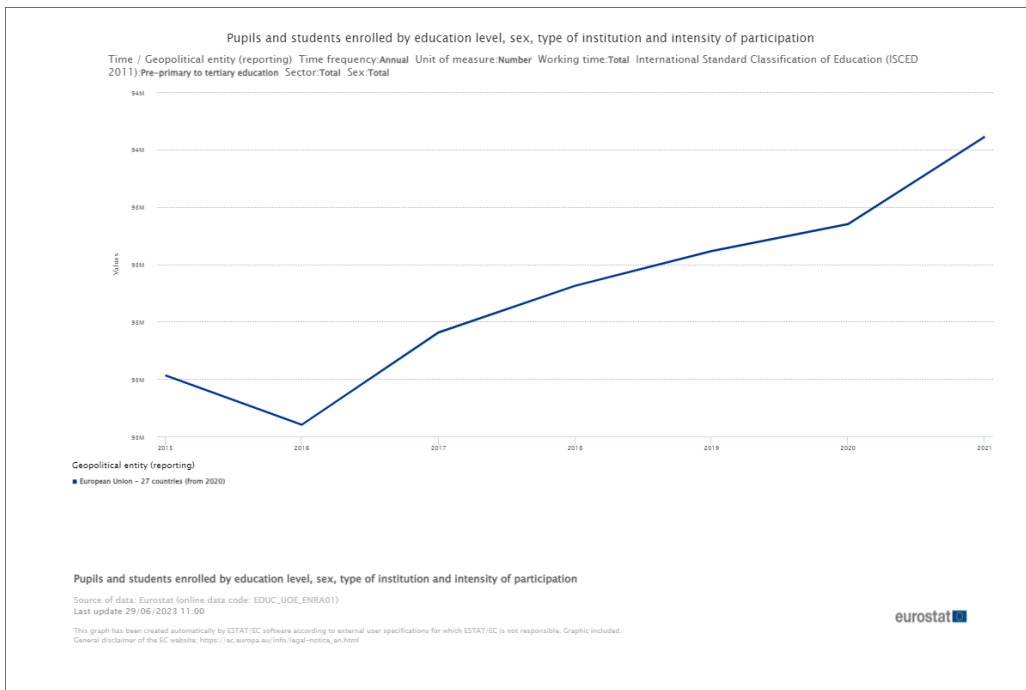
- **Service providers:** Providing a trusted verification service to all businesses or end users who require a confirmation on the truthfulness of an attestation.
- **Educational institutions:** providing verification services to their student and working partners.
- **Employers/Public bodies:** Using their own infrastructure and products to fulfil the verification process for their internal usage, in the case that no external service provider is used.

The market for education and competences is large and diverse. It is expected to grow significantly in the coming years due to the increasing demand for lifelong learning and the need for new ways to validate and recognize skills and competences.

In addition to the market segments listed above, there are a number of other factors that can be used to segment the education and competences market. For example, the market can be segmented by geographic region, by industry, or by the type of organization that provides the education or training.

## 5.4 Market size

The EU has over 4,000 higher education institutions with millions of graduates each year, making the need for digital transformation of issuers highly significant and in growth. The overall EU internal market is estimated in the hundreds of millions of euros, considering the various verification services in the human resources sectors of any companies, public institutions and tech platforms using data. It is also due to the changing nature of work as new skills are constantly emerging. Accompanying their formal and informal recognition through digital tools has become a crucial factor within this market.



**Figure 1 - Educational market user size**

Expanding on the trend in the rising number of enrolled pupils and students, we can assume some theoretical numbers, valuing the available market for issuers and verifiers. For example, looking at the higher education institutions in the EU, according to the Eurostat statistics, there are 17 million students enrolled in higher education programs from a bachelor’s to doctoral level studies. Making some assumptions we can calculate the projected potential yearly valuation of issuing credentials in higher education institutions.

**Assumptions:**

- Market size: 17 million students
- Courses per Year: 10
- Certificates per finished course: 1

Total certificates for all students = Market size × (certificates per finished course × courses per year)

- $17,000,000 \times (1 \times 10) = 170,000,000$  certificates



### Statements

- **Digital Transformation:** Digital solutions are becoming increasingly popular for ease of use and instant verification.
- **Regulatory Hurdles:** Different countries have different requirements, making standardization a challenge.
- **Rise of Soft Skills:** There's a growing interest in verifying "soft skills" like leadership, communication, etc., not just formal education.

## 5.5 Market Presence

Public stakeholders:

- ENIC-NARIC centres: Responsible for recognizing qualifications and periods of study.
- Europass: Provides a portfolio of documents to make skills and qualifications easily understandable across Europe.

Enablers:

- Diplome
- TrueLayer
- Accredible
- Verifdiploma
- Prosoon
- Talao
- CV Trust
- BCdiploma
- Telau
- Gataca

This market is ripe for digital solutions that can handle verification in a secure, efficient, and universally accepted manner.

## 6 Interoperability

*Interoperability* describes the ability of different systems, software, components to interact seamlessly with each other such as when they exchange data, provide services, etc.

*Interoperability requirements* refer to the specifications, standards, and conditions that must be met for different systems, software, or components, libraries to work together effectively and seamlessly.

Interoperability is a crucial factor especially in the field of digital services where many different projects, standards, visions, use cases, etc., are in place. These requirements ensure that separate systems can communicate, exchange data, and function together.

To address the interoperability aspect in this deliverable properly, we are following the “divide and conquer” approach by splitting up the interoperability aspect into different domains such as organizational, legal, technical and semantic domain. Each of these domains addresses the interoperability and its requirements from their specific point of view and details their interoperability requirements. This could be, for example, a data exchange protocol for the technical domain. The full study is presented in section 5.1 Interoperability Domains.

## 6.1 Interoperability Domains

Interoperability should take in consideration the standardization frameworks it should rely on, the European Standards for Interoperability are based on various standards set by European standardization bodies, primarily:

- CEN (European Committee for Standardization)
- CENELEC (European Committee for Electrotechnical Standardization)
- ETSI (European Telecommunications Standards Institute)

Regarding Open Standards, there isn't a single legislation that mandates open standards, but initiatives like the **Digital Single Market Strategy** emphasize their importance.

### 6.1.1 Organizational Interoperability

**Identified organizations:** All the entities related to being part of the platform must be previously identified, to provide information about the entity issuing a credential or is receiving a credential. Identification metadata provides security and trust to other parties (avoiding impersonations and

fraud). Related information must be anchored in an “official and neutral” trust layer as the EBSI infrastructure.

**Hierarchy:** It’s necessary to have an organizational structure to ensure all the information anchored there is reliable. In this way, the responsibility is delegated in regional organizations to improve trust and processes relating to the onboarding of such entities (each member state has its own procedures).

E.g., In Spain, the ministry of education could onboard any Spanish university. (In EBSI, this structure is defined with RootTAOs, TAOs and Issuers).

**Required Metadata:** Each organization must provide information to be identified:

- **OID/DID (Organization Identity):** Legal Name, National registration number (e.g., VAT code), etc.
- **Accreditations:** Unique identifiers of the schemes the organization can issue.
- **Display information:** Type of organization (private, public, NGO, etc), display name, EU member state of incorporation,
- **Open Services:** Each entity (in case of issuers) could define a list of services to verify issued credentials or other services they provide.

### 6.1.2 Legal Interoperability

**Standard contract and governance framework for data networks:** there is a need a standard way to describe participants, data sets, term of use, governance framework, accession rules and business elements of a data sharing network.

The following elements set the framework to take in consideration to guarantee legal interoperability:

**GDPR's Data Portability Requirement:** Services must be capable of providing users with their data in a standardized, commonly used, and machine-readable format. This allows users to easily move their data between different services.

**eIDAS Regulation Identification, Signature Requirements:** The legal foundation is Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (to be noted that this regulation is in progress to be updated).

**Open Data and Public Sector Information Directive:** Directive (EU) 2019/1024 on open data and the re-use of public sector information as some of the involved data falls within this area.

**Directive 2005/36/EC on the recognition of professional qualifications:** This directive provides a modernized framework for the recognition of professional qualifications between EU member states. It establishes the rules under which EU citizens can have their professional qualifications recognized in another EU country, either for the purpose of pursuing regulated professions on a permanent basis or providing temporary services. The directive has been amended by **Directive 2013/55/EU** to simplify and streamline the recognition procedures.

**European Qualifications Framework (EQF):** The EQF is a common European reference framework which acts as a translation device to make national qualifications more readable across Europe. It promotes workers' and learners' mobility between countries and facilitates lifelong learning. The Recommendation of the European Parliament and of the Council of 23 April 2008 established the EQF. It was further reviewed and updated by the Council Recommendation of 22 May 2017 on the European Qualifications Framework for lifelong learning. **Any qualification issued within EBSI-VECTOR must include EQF-compliant information.**

**Bologna Process (for higher education):** The Bologna Process aims to create a European Higher Education Area (EHEA) and promote the European system of higher education worldwide. It seeks to ensure more comparable, compatible, and coherent higher education systems in Europe. While the Bologna Process is an intergovernmental initiative and not a legislation, the principles and agreements established by its participating countries impact the recognition and interoperability of higher education qualifications across Europe

**Europass Framework:** The Europass Framework ensures transparency of qualification and competencies by providing documents that help to showcase skills and qualifications in a manner easily understood throughout Europe. While it doesn't provide recognition itself, it aids in making qualifications and credentials more readable. Regulation (EU) 2018/1723 of the European Parliament and of the Council of 14 November 2018 established the new Europass Decision.

### 6.1.3 Technical Interoperability

**Technical interoperability** primarily involves standard protocols to exchange information between the holder and third parties (issuer, verifier). Currently, the most extended one is

[OpenID Connect for Verifiable Presentations](#) (OIDC4VP) defined and maintained by the [OpenID Foundation](#) (OIDF) used also within the future eIDAS2 [Architecture and Reference Framework \(ARF\)](#). On the other hand, regarding the ARF is necessary to define a new protocol for proximity scenarios. The ARF defines for this scenario the use of the [ISO/IEC 18013-5:2021 Mobile driving license \(mDL\)](#) protocol standard.

- **Standard protocol to request/issue credentials:** Currently, the most extended protocol in this area is [OpenID Connect for Verifiable Credential Issuance \(OIDC4VCI\)](#) also defined and maintained by OIDF.
- **Standard crypto-suites (serialization + cryptographic algorithm):** a standard cryptographic algorithm is needed to sign the structures exchanged between the parties. To sign credentials, the choice lays within eIDAS approved JAdES<sup>5</sup> and for signing presentations ed25519 (JCS, context, ...).
- **Standard data models:** The data models are defined for SSI. There are Credentials and Presentations.
  - **Diploma Data Model:** The data model for diplomas themselves is already defined as Verifiable Diploma Schema. This data structure contains all the necessary elements needed to describe a diploma. This can serve as the basis for storing the diploma data and generation of the documents or presentations needed later in the user journey as needed<sup>6</sup>. Regarding different data formats please see chapter "Semantics".
  - **Micro-credential data model** would include :
    - **Issuer:** The organization or entity granting the micro-credential.
    - **Recipient:** The individual or entity awarded the micro-credential.
    - **Issue Date:** The date the micro-credential was awarded.
    - **Expiration Date:** The date the micro-credential may expire.
    - **Criteria:** Requirements the recipient met to earn the micro-credential.
    - **Evidence:** Supporting materials validating the recipient's achievement.

---

<sup>5</sup> [Jades ETSI Standard](#)

<sup>6</sup> [EBSI VC Schema](#)

- **DID:** A URI that supports verifying the micro-credential's authenticity through related DID document signature<sup>7</sup>.
- **Status:** The current standing of the micro-credential (e.g., active, expired).
- **Credentials format:** The credential data model is used to store information. Currently, there are some structures (JSON-LD, JWS, SD-JWT, mDoc). Also is applicable for Presentations. (EBSI is providing SD-JWT and JWS specs. SD-JWT is being discussed, please refer to WP3 for more details on this subject)
- **Data agreement:** (New) From the GDPR side, it's necessary to have a consent agreement which sets the information requested and the purpose for that requested information.
- **Trusted Schema Registry:** Registry with all the schemas in the Trust Framework (EBSI). Supporting operations for registering new schema, updating registered schema, reading and validating registered schemas. Supporting different data formats (JSON, JSON-LD, XML, etc...).
- **Trusted Issuer Registry:** Registry containing signatures related to all the Identities and Accreditations belonging to the issuers.
- **DID Registry:** Registry with all the DIDs related to the Trust Framework (EBSI). Supporting operations: Insertion of DID and DID Document; Update of DID Document; Revoking DID and DID Controlling key; Resolve and obtain DID Document.
- **Trusted Verifier Registry:** Registry with all signatures related to the Identities for the authorized verifiers. Other verifiers do not need signatures within this registry
- **Revocation mechanism:** To allow credential revocation is first necessary **to identify which entity is allowed to revoke credentials** as in some legislation issuer and revocation entity may not be the same. From implementation side not every EU member state allows revocation of certificates as not all types of educational certificates can be revoked and in other member states the revocation must happen within a reasonable time limit (e.g., Italian legislation normally 12months). Revocation technical interoperability therefore would require a '**mere functional feature**' that can be placed within different workflows based on different use-cases or applicable legislations. 'Fully fledged' revocation solutions as for example 'revocation lists' furthermore pose a lot of concerns from privacy (GDPR) side as they collide with two main aspects of the regulation:

---

<sup>7</sup> [W3C DID Specifications](#)

- Even in case a revocation list only contains non-personal data, such as cryptographic hashes without directly identifiable information, at the first verification case when the original certificate and the entry within this list is performed, such 'linkage' can be traced/reproduced/published/made public, thus posing great concerns from GDPR point of view.
- Under GDPR, individuals have the right to request the deletion of their data and there could be cases when, due to mistakes or other reasons, the revocation itself needs to be 'revoked'. Implementation of this process and identification of authorized actors involved is a great challenge.

#### 6.1.4 Semantic Interoperability

There are different schemas for transport of educational data and semantics that exists in Europe, the main are detailed below.

##### ELMO

- Based on XML
- Mainly used for [EMREX](#), and [EWP](#)
- The current version is ELMO 1.7

The ELMO specification was produced by the CEN Workshop for learner technology (CEN WSLT) to drive the implementation of the two new CEN standards:

- EN-15981 European learner mobility - performance information [EuroLMAI].
- EN-15982 Metadata for learning opportunities - Advertising [MLO-AD].

These two standards describe data models. EN-15982 is a data model for learning opportunities, such as program, course, module, etc. EN-15981 is a data model for assessments, modelling the information found on diplomas, transcripts and diploma supplements. These specifications were developed by CEN WSLT and the standards were developed by CEN/TC 353 Information and Communication Technologies for Learning, Education and Training.

The ELMO format is an XML format that supports assessment information in diplomas, transcripts of records and diploma supplements. It also includes descriptions of qualifications, programs,

courses and modules for these assessments. This information is required in admission and recognition procedures.

### **ELM (European Learning Model)**

- Currently based on XML, planned to support JSON-LD.
- Currently only Europass uses this standard.
- The current version is ELM Version 3.

Other schemas are:

[Open Badges](#). Open Badges are digital symbols of achievements, skills, or competencies. They're based on an open standard, enabling verification and sharing across various platforms and digital portfolios. Issuers can provide badges, while earners can showcase them, facilitating recognition and credential transparency.

[Micro-Credentials](#) Micro-credentials are digital proof of specific skills or knowledge areas, smaller than traditional qualifications. They focus on granular competencies, allowing learners to showcase niche expertise. These credentials are easily shareable across digital platforms and recognized by various institutions or employers.

ELMO 1.7 and ELM V3 are semantically 100% equivalent (a mapping list already exists), even ELM V3 has a broader scope than ELMO 1.7 currently (so ELM V3 supports enrolment, a use case ELMO 1.7 does not support currently).

EBSI is based on ELM Version 2 supporting JSON. The schema converters that will be developed in DC4EU are based on ELM Version 3 supporting JSON-LD. The semantic scope of the different schemas varies in place thus, a semantic 1:1 conversion will be difficult in some places.

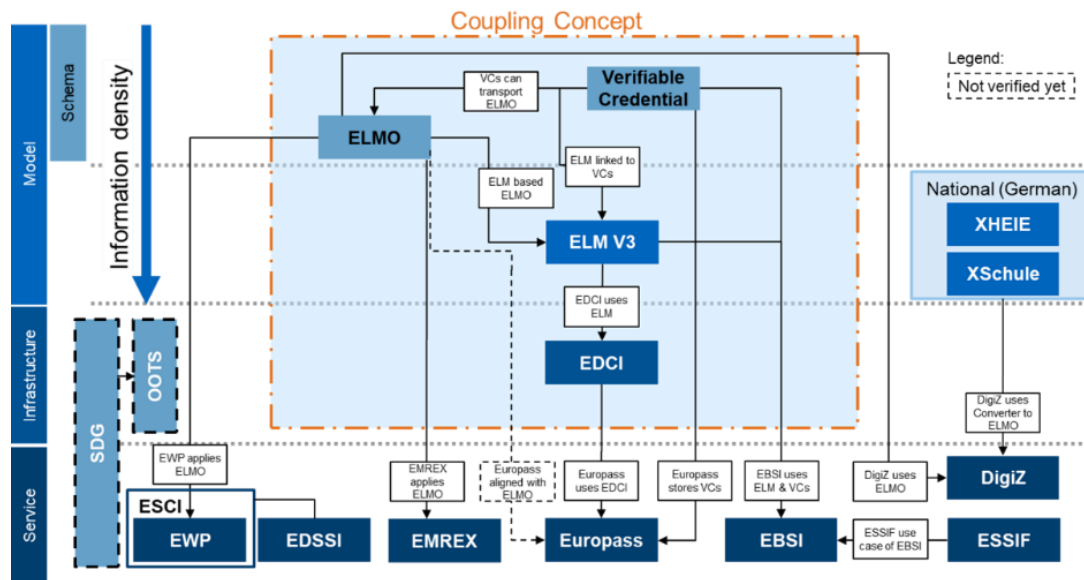
Schema and interoperability “To be”

- The vision is to allow interoperability even of different schemas by technical and semantical conversion



- It should be possible to create educational semantic data in one semantic standard (ELMO, ELM, ...) and to use it for different applications by converting it to another semantic standard if needed.

The following Figure 2 illustrates it:



Quelle: Cleaning Up: Interplay Between European Standards and Verifiable Credentials for Higher Education Institutions, Springer 2023

Figure 2 – Coupling concept

The usage of skill standards like European Qualifications Framework (EQF), ESCO (European Skills, Competences, Qualifications and Occupations), the International Standard Classification of Education (ISCED), and the usage of common value lists based on international standards should be used for all standards in future. Currently that is not the case (some standards use strings to support arbitrary content in the values, possibly also outside European standard value lists).

National data standards also should be converted from and to one of the international standards (most likely ELM V3 or ELMO) to enable an international data exchange in such an interoperable ecosystem. In some countries (like NL) that is already done, in other countries (like Germany with the national data standard for educational data XBildung) that is at least planned.

The DEP project DC4EU is already realizing a future expansion of that interoperable ecosystem e.g., by creating an EMREX gateway to an eIDAS wallet. In parallel a bridge between EMREX and

SDG/OOTS was developed and is currently tested. The development of converters from and to ELM V3 in the DC4EU project will allow to have direct and indirect interoperability between the data standards ELMO, ELM V3, SDG/OOTS evidence, Open Badges and Micro credentials (with the using systems like EMREX, EWP, Europass, SDG/OOTS etc.).

## 7 Customer Analysis

Developing a Self-Sovereign Identity (SSI)-based digital credential service leveraging EBSI requires a nuanced understanding of the diverse clientele it aims to serve. Below is a detailed profile of the service's target customers, categorizing their distinct needs, preferences, and behaviours.

The main identified actors' typologies are:

1. Students (citizens)
2. Education Institutions
  - a. Higher Education Institutions
  - b. Secondary Schools
  - c. Professional certification issuers
  - d. Vocational Training
3. Private organizations (legal entities)
4. Public bodies (legal entities)

For each of these actors we'll define needs, preferences, behaviours, taking in consideration that for all such actors the need of compliance with actual legislation is intrinsic.

### 7.1 Higher Education Institutions

#### *Needs:*

- Secure, verifiable, and cost-effective ways to issue, manage, and revoke credentials.
- Compliance with international education standards and data privacy laws.
- Systems that are interoperable with other institutions and industry credentials.

#### *Preferences:*

- Platforms that are easy to integrate with current student information systems.
- Customizability to align with the institution's branding and credentialing standards.
- Scalability to accommodate a growing number of digital credentials.

#### *Behaviour:*

- Conservative towards adopting new technologies but open to innovation that reduces administrative burden.
- Collaborative initiatives to maintain relevancy and improve institutional offerings.

## 7.2 Secondary Schools

#### *Needs:*

- Digital solutions to issue verifiable academic records like diplomas and certificates.
- Secure and efficient transfer of student records for college admissions.
- Platforms that are easily navigable by both staff and students.

#### *Preferences:*

- Intuitive systems that require minimal training for educators and administrators.
- Engagement tools to keep students informed about their credential status.
- Cost-effective solutions due to often limited school budgets.

#### *Behaviour:*

- Cautious in adopting new technologies, with a focus on reliability and support.
- Look for solutions that align with educational standards and regulations.
- May require more guidance and support to transition from paper-based systems.

## 7.3 Professional Certification Issuers

#### *Needs:*



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.

- Robust, cost-effective systems to manage the lifecycle of a professional certification, from issuance to expiration and renewal.
- Ways to prevent fraudulent representation and misuse of certifications.
- Integration with professional development platforms and HR systems.

#### *Preferences:*

- High-level security to protect the reputation of their certifications.
- Real-time verification services for employers and other verifying parties.
- Reporting features to track the usage and status of issued certifications.

#### *Behaviour:*

- Proactive in utilizing technology to maintain the value and integrity of their certifications.
- Focus on long-term tracking and validation to support career progression.
- Engage in continuous improvement to ensure their certifications meet industry needs.

## 7.4 Continuing Education and Vocational Training Providers

#### *Needs:*

- Issue credentials that reflect specialized skills and competencies in various trades and professions.
- Create stackable credentials that professionals can accumulate over time.
- Maintain a dynamic credentialing system that adapts to changing industry demands.

#### *Preferences:*

- Agile systems that can issue credentials soon after course completion.
- Solutions that cater to a diverse range of industries and professional standards.
- Flexibility to update and revise credentials as industry requirements evolve.

#### *Behaviour:*

- Quick to adopt innovative solutions that provide them a competitive edge.

- Collaborative, often seeking to integrate their offerings with other education providers and industry partners.
- Heavily focused on outcomes and practical applications of skills.

## 7.5 Students (across different nations and levels)

### *Needs:*

- A secure digital wallet for lifelong credential storage and access.
- Assurance that credentials will be recognized by educators and employers globally.
- Control over who gets access to their educational data.

### *Preferences:*

- User-friendly interfaces with minimal learning curves.
- Mobile access to credentials for ease of sharing and verification.
- Services that enhance their employability and educational opportunities.

### *Behaviour:*

- Digitally native and expect seamless online experiences.
- Value the autonomy and privacy of their data.
- Socially active, sharing milestones and credentials online.

## 7.6 Private and Public Organizations

### *Needs:*

- Streamlined processes for verifying the educational background of potential hires.
- Assurance of the authenticity of credentials presented by job applicants.
- Reduction of fraud and misrepresentation in recruitment processes.

### *Preferences:*

- Rapid verification processes to minimize time-to-hire.
- Integration with HR systems for easy retrieval and auditing of credentials.
- Continuous updates to stay aligned with compliance and legal requirements.

**Behaviour:**

- Proactive in adopting solutions that promise improved operational efficiency.
- Value partnerships with educational institutions for talent acquisition and development.
- Cautious about data handling to ensure regulatory compliance.

## 7.7 Strategy for Serving Target Customer Needs

### Customization and Integration:

Offer services that are adaptable to the specific systems and processes of each target group. Integrate seamlessly with existing platforms to avoid any friction in adoption.

### User-Centric Design:

Ensure that the system is intuitive for students while also being robust enough for the more complex needs of institutions and organizations.

### Education and Support:

Provide comprehensive support and resources to educate stakeholders on the benefits and operation of SSI-based credentials.

### Data Privacy and Security:

Design the service with a strong focus on data security, ensuring that all user data is protected and that users retain control over their information.

#### Global Standards Compliance:

Ensure the platform adheres to international credentialing standards to facilitate widespread acceptance and portability.

#### Cross-Sector Collaboration:

Foster partnerships with both educational and corporate entities to ensure the service is well-tailored to the job market's needs.

#### Marketing and Communication:

Clearly communicate the value proposition to each target segment, focusing on the unique benefits that SSI-based credentials provide to each.

By thoroughly understanding and strategically addressing the varying needs, preferences, and behaviours of these target customers, an SSI-based digital credential service can position itself as an indispensable tool for secure, portable, and verifiable academic and professional qualifications.

## 8 Service Requirements & Description

Today's methods of issuing, storing and verifying educational credentials and diplomas have long been plagued by challenges such as fraud, cumbersome paper-based processes, inefficiencies in the creation and verification of credentials and the lack of a unified and universally accepted verification system.

These limitations have significant implications for individuals, educational institutions, and employers, leading to delays in cross-border movement of students, recruitment, increased administrative burdens, unnecessary costs, and a lack of trust and credibility in academic qualifications.

EBSI-VECTOR Digital Credential seeks to address these challenges by introducing a secure, efficient, and Self-Sovereign solution for credential management that puts students (citizens) at the centre of an integrated and interoperable ecosystem.

The EBSI-VECTOR Digital Credential Service will demonstrate how EBSI blockchain can revolutionize the way educational credentials are managed, accessed, verified, and shared. By enhancing trust, reducing fraud, and streamlining processes, it paves the way for a future where educational records are secure, easily accessible, easily verifiable, and universally recognized. This benefits not only individuals, but educational institutions, and employers across the European Union and beyond.

## 8.1 Service Requirements

In this paragraph, we will outline the fundamental business requirements that serve as the foundation for our educational business vision. These requirements encompass various aspects such as organizational, legal, technical, and semantic considerations, ensuring a comprehensive understanding of our business needs.

A list of main requirements divided to the following strategic areas:

1. Organizational Requirements
2. Technology Requirements
3. Semantic Requirements
4. Legal Requirements

### Journey 1.

#### .1.1 Organizational Requirements

##### ReqOrg.1. Governance Structure

The need of a service-wide cross-border governance structure would be necessary to clarify decision-making processes within our educational ecosystem for each EU member state while at the same time identify key stakeholders and their roles, responsibilities, and supervisory authorities.



#### ReqOrg.2. Resource Allocation

It would be a key element to assess the financial resources required for sustaining and expanding this innovative educational services system, defining high-level human resources allocation to effectively support the growth of the new market.

#### ReqOrg.3. Strategic Planning

Develop a clear and actionable strategic plan that outlines our educational goals, objectives, and growth strategies, while establishing a timeline for achieving key milestones and objectives.

#### ReqOrg.4. Policy Development and Enforcement

There is a need of establishing policies and procedures governing the use of EBSI blockchain technology within the educational system, to address data privacy, security, smart contract management, in compliance with relevant regulations.

#### ReqOrg.5. Smart Contract Governance

There is a need of establishing a framework for the creation, management, and auditing of smart contracts, define the roles & responsibilities for reviewing and approving smart contract code changes.

#### ReqOrg.6. Change Management

To evolve from the actual ecosystem to an EBSI-based we need to develop a structured change management process to assess and implement process changes, upgrades, and improvements while ensuring that such changes do not disrupt the existing educational services.

#### ReqOrg.7. Dispute Resolution

We need to establish a mechanism for resolving disputes related to data ownership, credential verification, or other blockchain-related matters.

#### ReqOrg.8. Language Requirements

Services, certifications, courses are conducted in different languages sometimes different than the official language(s) of the country they are issued; therefore EBSI-VECTOR should be able to run in different languages while handling multi-language certifications.

## Journey 2.

### .1.2 Technical Requirements

#### ReqTech.1. User Onboarding and Profile Management

User onboarding and profile management involve the process of identifying and registering individuals into an EBSI-VECTOR service. It typically includes guiding users through the initial setup, providing access to features, and collecting essential information. Once onboarded, profile management allows users to maintain and update their personal information, preferences, and settings within the platform. This seamless process ensures a positive user experience, fosters engagement, and enables tailored interactions, ultimately enhancing user satisfaction and the platform's effectiveness.

#### ReqTech.2. Credential Issuance and Management

Educational credential issuance and management involve the processes related to creating, distributing, and overseeing educational/academic credentials, micro-credentials and other types of educational certificates such as diplomas, degrees, and transcripts. This includes verifying students' academic achievements, generating official documents, and ensuring their secure and authorized delivery. It also encompasses ongoing tasks like handling requests for reissuance or updates.

#### ReqTech.3. User Wallet and Credential Access

A user e-wallet for educational purposes is a digital wallet designed for students to securely store, manage digital certificates (Verifiable Credentials) for various educational-related activities.

#### ReqTech.4. Credential Verification

Educational credential verification is the process of confirming the authenticity and validity of academic qualifications, certifications, or degrees earned by an individual from an educational institution. This verification is typically conducted by employers, educational institutions, government agencies, or other relevant entities to ensure that the presented educational credentials are accurate and obtained from a legitimate source. Educational credential verification is crucial for making informed decisions in areas such as employment, admissions, or professional licensing.

#### ReqTech.5. Credential Revocation:

Credential revocation is a critical aspect of digital credential management systems. It ensures that once a credential is no longer valid or has been compromised, it can no longer be used.

Credential revocation requires a **non-business-driven revocation** system but **agnostic revocation** capability that can be plugged in different business processes to match different MS requirements.

#### ReqTech.6. Privacy and Data Control

Privacy under the General Data Protection Regulation (GDPR) is a fundamental right that grants individuals control over their personal data. It requires educational organizations to ensure transparent data collection, processing, and protection practices. The regulation aims to safeguard individuals' privacy by imposing strict rules and accountability on organizations handling personal information, promoting data minimization, and emphasizing the principles of purpose limitation and data accuracy.

#### ReqTech.7. Interoperability and Standards Compliance

Interoperability will be key element to activate the ability of EBSI-VECTOR systems, technologies, & software applications to work together seamlessly and exchange data with legacy systems without encountering compatibility issues.

Standard compliance will ensure that systems, products, and processes meet recognized standards, facilitating consistency, compatibility, and quality. Compliance with standards enhances interoperability by providing a common framework for interaction and data exchange among diverse systems.

Please refer to the details present in the related chapters of this document.

#### ReqTech.8. Notification and Alerts

Notifications and alerts, managed by automated messages will be used to inform users, issuers or verifiers about specific events, updates, or actions that require attention. They serve to keep individuals informed, engaged, and aware of important information or changes in real-time.

#### ReqTech.9. User Feedback and Ratings

User feedback and ratings provided by users of products, services, or experiences to express their opinions, experiences, and satisfaction levels will help organizations gauge customer satisfaction, identify areas for improvement, and make informed decisions to enhance the quality and user-friendliness of their services.

#### ReqTech.10. Legacy Document Management

Offer citizens alternative methods for sharing and verifying their credentials, such as providing the possibility to print/use physical copies or paper certificates, is a key element to ensure inclusion for non-digitalized citizens.

#### ReqTech.11. Compliance and Security

To effectively ensure compliance and security for a new education credential management system, a holistic approach is essential, from one side implementation of robust data encryption and access control measures to safeguard sensitive credential information and from the other side enablement of regular security risk management processes to identify and address potential risks promptly.

#### ReqTech.12. Scalability

In case of high load of transactions EBSI-VECTOR can from one side rely on EBSI blockchain, that may be required to employ techniques such as sharding, layer-2 solutions, and optimized consensus algorithms to increase transaction throughput and reduce latency.

### Journey 3.

#### .1.3 Semantic Requirements

Semantic requirements for EBSI-VECTOR service leveraging W3C Verifiable Credentials focus on the representation and exchange of verifiable educational data in a standardized and interoperable manner. These requirements help ensure the accurate and secure sharing of credentials among educational institutions and other stakeholders.

#### ReqSem.1. Curriculum Design

Develop a curriculum that aligns with the institution's educational objectives and meets industry standards. Ensure that the curriculum is adaptable to changing educational needs and trends.

ReqSem.2. Language and Accessibility

Provide educational content in multiple languages to accommodate diverse student populations. Ensure that educational materials are accessible to individuals with disabilities.

ReqSem.3. Verifiable Credential Schema

Use of W3C Verifiable Credentials Data Model to define a standardized schema for representing educational credentials, including degrees, certificates, transcripts, and badges. This schema should capture essential attributes, such as issuer, recipient, credential type, and credential status.

ReqSem.4. Linked Data:

Implement Linked Data principles to enable the creation of globally unique and resolvable Uniform Resource Identifiers (URIs) through DIDs (Decentralized Identifiers) for educational institutions, courses, and individuals. This supports the creation of verifiable credentials with contextual links.

ReqSem.5. Educational Ontologies:

Use established educational ontologies, such as Schema.org Education Extension or the Credential Transparency Description Language (CTDL), to define vocabulary and terms specific to educational data. This ensures semantic consistency and alignment with existing educational standards.

ReqSem.6. Credential Verification:

Incorporate mechanisms for credential verification and validation, enabling third parties to verify the authenticity and integrity of a verifiable credential by checking against the issuer's public key and relying on decentralized identifiers (DIDs) for verification.

ReqSem.7. Contextual Information:

Include contextual information in verifiable credentials, such as course descriptions, competencies achieved, and relevant metadata, to provide a comprehensive understanding of the credential's significance.

**ReqSem.8. Consent and Privacy:**

Implement consent management mechanisms that allow individuals to control the sharing of their verifiable credentials, ensuring compliance with data privacy regulations like GDPR. Provide transparency on how data is used and shared.

**ReqSem.9. Revocation and Expiry:**

Specify semantic requirements for handling credential revocation and expiry, enabling authorized entities to revoke or update credentials as necessary while maintaining the integrity of historical data.

**ReqSem.10. Interoperability Standards:**

Align with interoperability standards, such as JSON-LD and JSON Web Tokens (JWT), to ensure that verifiable credentials can be easily exchanged and interpreted by different systems and services.

**ReqSem.11. Access Control and Permissions:**

Define access control policies that determine who can issue, verify, and request verifiable credentials. Ensure that permissions are consistent with privacy and security requirements.

**ReqSem.12. Semantic Validation:**

Implement semantic validation checks to verify that verifiable credentials conform to the defined schema and vocabulary, reducing the risk of data errors and inconsistencies.

**ReqSem.13. User-Friendly Display & Print:**

Develop user interfaces that present verifiable credentials in a user-friendly format, ensuring that individuals can easily understand and manage their digital credentials and allowing export in printable version.

By incorporating these semantic requirements, an educational management service leveraging W3C Verifiable Credentials can facilitate the secure and interoperable exchange of educational credentials while enhancing data integrity, privacy, and user control.

## Journey 4.

### .1.4 Legal Requirements

Legal requirements for education domain on EBSI typically revolve around ensuring data privacy, security, and compliance with relevant laws and regulations. In the *Chapter 11* of this document about *Legal and Regulatory Compliance*, we'll carefully explain legal requirements and considerations that educational businesses should be aware of to ensure cross-border compliance with relevant regulations and standards. From the chapter you will understand all about the rules that we have to apply, how to stay within the law and avoid legal issues.

## 8.2 Service Features

EBSI-VECTOR is looking for a range of service features in the educational domain to enhance the management of educational records, credentials, and processes. Here are key service features that we ensure to provide in the educational sector:

### 8.2.1 Enterprise wallet General features

- Wallet encryption and two-factor authentication for added security.
- Hardware wallet integration for eIDAS L3 compliance
- Web app integration for non-mobile access.

### 8.2.2 Enterprise wallet User Onboarding & Profile Management

- User identification based on eIDAS regulation (L3)
- Secure authentication with minimum eIDAS L3 level of assurance.
- User self-sovereign profile creation with multiple contact channels (email, notifications, phone, social, etc).
- User-friendly UI both mobile and web based.
- Multiple digital identities capability
- OneTime Identity creation capability
- Pin protection

## 8.2.3 Enterprise wallet Credential Issuance & Management

- Digital Credential Issuance:
  - Ability for educational institutions to issue digital credentials, including diplomas, certificates, transcripts and micro-credentials
  - Full compliance with EBSI W3C Verifiable Credential and Verifiable Presentation standards
  - Customizable credential templates.
  - Support for various credential types, including academic, vocational, and professional.
  - Multi-format for credential signature (eIDAS) that can be upgraded on need.
  - Full portability of credentials with different e-wallets.
  - Capability to issue credentials in bulk e.g., for graduating classes.
  - Multi-signature and multi-issuer credential management
  - Issue credentials in bulk
- Issued Credential Management:
  - Ability to list issued credentials.
  - Ability to view in detail an issued credential
- Secure Credential Management & SSI Storage:
  - Blockchain integration for verification and immutability.
  - Credential encryption for enhanced security
  - Automatic timestamping eIDAS compliant through blockchain
  - Full integration with TAO/TAR for issuer verification and trust management.
- Credential Revocation:
  - Non-business-driven revocation system but agnostic revocation capability that can be plugged in different business processes to match different MS requirements.



## Journey 5.

### .2.4 User Wallet & Credential Access

- eUID-compliant Digital User Wallet:
  - Secure eIDAS compliant e-wallet for users to manage their credentials.
  - Wallet encryption and two-factor authentication for added security.
  - Hardware wallet integration for eIDAS L3 compliance
  - Web app integration for non-mobile access.
- Credential Management:
  - Capability to request, store and share digital credentials
  - Selective Disclosure, e.g., capability to share a subset of data present in the credential without disclosing all data
  - Verifier Limitation: ability for users to choose who can access their credentials and how long they can be accessed for, including one-time access sharing for one-shot verification.
  - Multiple sharing methods including full machine2machine methods
  - Shareable credential links for ease of access for employers or institutions & request credentials from users to be shared directly with the enterprise wallet.

## Journey 6.

### .2.5 Enterprise Wallet Credential Verification

- Machine-based real-time Verification:
  - Employers and educational institutions can automatically verify received credentials in real time without human intervention.
  - Monitored access to blockchain-based credential anonymized references for authenticity verification.
- Verification Reports:
  - Generate GDPR-compliant verification reports and verification history.
  - Timestamped verification records for audit trails.
- Verification Revocation: capability for user to stop/deny verification from selected parties.

## Journey 7.

### .2.6 User Wallet Privacy and Data Control

- User Data Privacy:
  - Compliance with data protection regulations (GDPR).
- Auditable user consent management for data sharing.
- Permanent data export and deletion options.

## Journey 8.

### .2.7 Enterprise Wallet Interoperability and Standards Compliance

- Interoperability:
  - Support for widely accepted standards like EBSI W3C Verifiable Credentials.
  - Compatibility with other digital credential systems.
  - Open format
- Integration APIs:
  - APIs for seamless integration with educational institutions' systems and HR platforms.
  - Single sign-on (SSO) capable login management.
- Full compliance with all EU digital-based regulations

## Journey 9.

### .2.8 Notification and Alerts

- Credential Updates notifications
- Credential issuing process status notifications.
- Expiry alerts for time-sensitive credentials.
- Warning alerts for unsuccessful access to verification process

## Journey 10.

### .2.9 Multi-Language Support

- Support for multiple languages in:
  - Credential data (W3C Verifiable Credential multi-lang support)

- Mobile and Web front end
- Data formats
- Support for UTF16 charset.

## **Journey 11.**

### **.2.10 Support and Help Center**

- Comprehensive help centre with FAQs, tutorials, and multi-language user support options.

## **Journey 12.**

### **.2.11 Compliance and Security**

- Regular security audits and updates to ensure data protection.
- Compliance with relevant educational and privacy regulations.
- Full compliance with NIS directive requirements.

## **Journey 13.**

### **.2.12 Scalability**

- Scalable infrastructure to accommodate growing user and credential volumes.

## **Journey 14.**

### **.2.13 Legacy Document Management**

- Capability to export digital credential in PDF format to be able to be printed by holder.

## **Journey 15.**

### **.2.14 User Feedback and Ratings**

- Feedback mechanism for users to rate and provide feedback on credential issuers.

## **Journey 16.**

### **.2.15 Accessibility Features**

- Accessibility options for users with disabilities, ensuring inclusive access to digital credentials.

## 8.3 Benefits

### Enhanced Trust:

Employers and educational institutions can trust the authenticity of educational credentials, streamlining the hiring and application process and reducing the risk of credential fraud. Students who hold verifiable become more attractive to recruiters, training organizations or employers than applicants with non-verifiable credentials, due to the ability to efficiently present and share trusted, verified credentials.

### Efficiency:

The service reduces administrative burdens on educational institutions and verification agencies, making credential issuance and verification faster and more cost-effective. Students can quickly and efficiently access, retrieve, and share their credentials rather than relying on inefficient paper-based processes. The administrative burden of re-issuing lost certificates is significantly reduced.

### Global Recognition:

EBSI credentials are internationally recognized, facilitating the mobility of students and professionals across borders.

### Privacy Control:

Students have better oversight and control over their personal data, deciding who can access their credentials and for what purpose.

## 8.4 User Scenarios & Journeys

Implementing blockchain in the educational domain isn't just about the technology; it's also about understanding the user journeys. It ensures that technology solutions are designed to meet the needs and expectations of the students, educators, and administrators who interact with the system. By understanding 'pain points' in educational experience and by addressing these issues

through blockchain technology, institutions can elevate the quality of interactions and services provided to students and staff; can reduce administrative burden, minimize errors, resulting in time and resource savings. As a result, institutions can foster trust among users, stakeholders, and regulatory bodies.

### 8.4.1 Overall Scenario requirements

By enabling portable and verifiable digital credentials, EBSI allows individuals to easily share their credentials with multiple parties while maintaining privacy. The overall schema by such scenarios is represented below (Figure 3).

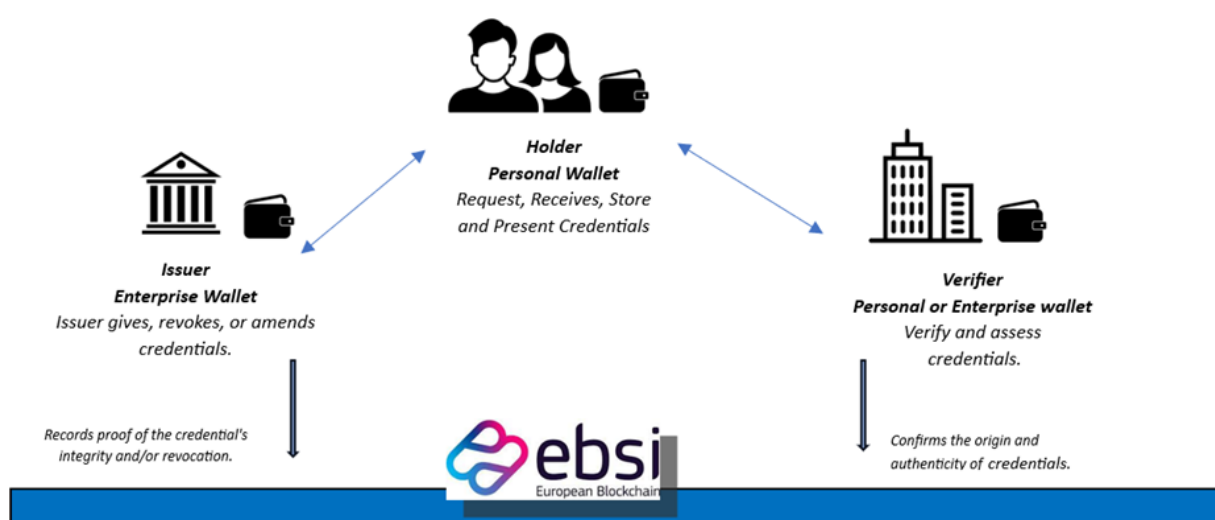


Figure 3 - Credential lifecycle

## Journey 17.

### Prerequisites

- Institution (Issuer) already onboarded in EBSI
- Institution (Issuer) has specific schemas, already registered on EBSI, linked to a particular kind of VC, e.g., a university degree, micro-credential or a course participation.

### 8.4.2 Process 1: Educational Credential Issuing

Objective:

- Securely register students on the EBSI network.
- Issue educational credentials, such as diplomas, degrees, and certificates, with enhanced security and authenticity.
- Streamline administrative tasks related to user registration and credential issuance.

→ Step 1 Student Registration

Student logs into the EU educational institution portal (EBSI Enterprise Wallet Service integrated with institution portal)

**Case 1:** User already onboarded on EBSI (e.g., from previous institution or else)

- Student authenticates using their pre-existing DID and Proof of Identity, proving his/her identity on the system without the need to enter personal details.
- The enterprise wallet verifies provided student data securely, based on the DID/signature.

**Case 2:** User not already onboarded on EBSI

- User through his/her already verified personal information (at educational institution) onboarded on EBSI and receives a unique blockchain identifier (e.g., a DID - Decentralized Identifier) is generated for the student.
- User may use his/her EUDI wallet to store this information.

→ Step 2 Credential Preparation

Upon course completion, the institution prepares a W3C EBSI-compliant Verifiable Credential version of the educational credential (see steps below)

- The educational institution (issuer) gathers the required data for the credential, ensuring it adheres to the format and attributes defined in the corresponding/matching schema

already registered on EBSI. (By adhering to the schema, the issuer ensures that the VC will be universally recognizable and verifiable by any party).

- As the VC is prepared, a reference to the schema (an identifier or a URI) is embedded within the credential itself. This tells any verifier which schema the VC adheres to.
- The issuer signs the VC using its private key associated with its DID. The resulting signature is embedded within the VC.

→ Step 3 Credential Issuance

**Case 1:** Credential is automatically issued to the user on course completion

- The student is notified about the availability of the credential (by available means such as mail, mobile notification, SMS, etc.).
- The student authenticates into EU educational institution portal/enterprise wallet and accesses the credential for approval.

**Pathway 1.1:** User request data modification due to errors/mistakes. In this case internal review from educational institution will be activated

**Pathway 1.2:** User successfully verifies credential data and approves its delivery to his/her EUID wallet (if available)

**Case 2:** Credential is issued on user request.

- The student authenticates into EU educational institution portal/enterprise wallet and requests the credential issuance
- The Educational institution provides a preview of the credential for user approval.

**Pathway 2.1:** User request data modification due to errors/mistakes. In this case internal review from educational institution will be activated

**Pathway 2.2:** User successfully verifies credential data and approves its issuance & delivery to his/her EUID wallet (if available)

- The signed VC is sent to the user through a secure channel. This could be an application interface, a secure email, or a EUID wallet that the user employs. In case of EUID usage, credential is self-verified on reception.

#### Benefits:

- Secure and tamper-proof storage of educational credentials.
- Transparent and efficient credential verification.
- Reduced risk of fraud and misrepresentation of qualifications.
- Streamlined administrative processes for user registration and credential issuance.

### 8.4.3 Process 2: Educational Credential Request & Verification

**Objective:** To enable employers and institutions to verify the authenticity of educational credentials.

→ Step 1 Organization Requesting certification

1. A verifier organization (e.g. employer or another institution) requests a credential to a user specifying the means of receiving this credential. This request may happen in different ways, for example:
  - A web portal where the user logs in and gets prompted to share their VC (EUID-enabled student receives a verification request notification).
  - An enterprise wallet (EUID-enabled student receives a verification request notification).
  - A QR code mechanism where the user scans the code with his/her EUID wallet to initiate the VC sharing.
2. Note: Steps from here are only related to user with EUID wallet.
3. In case of user with EUID wallet, the wallet requests consent from user to share the credential
4. There are 2 possible options:

**Option 1:** requesting organization *is NOT an Authorised verifier*. The EUID wallet notifies the user that this organization isn't pre-authorized and provides comprehensive details about which specific data the requester seeks. The EUID wallet seeks the user's consent to share the Verifiable



Credential (VC) using a Selective Disclosure feature, which restricts the amount of data that will be disclosed.

**Option 2:** requesting organization *is an Authorised verifier*. EUID wallet informs user that organization is a pre-authorized entity and requests permission to share VC.

5. After reviewing the request, the student gives consent (ensuring GDPR compliance) and issues a Verifiable Presentation (VP) containing the set of data as specified by the request and sign the request with his/her private key linked to personal DID  
*Note: user may own more DIDs connected to his identity.*
6. EUID wallet asks user confirmation if he/she wants to limit verification process to a specific timeframe or a specific number of verifications.
7. EUID wallet shares VP with requesting institution (using alternative sharing means as specified in the request.)
8. Upon successful completion, the EUID informs the user that the Verifiable Presentation (VP) has been delivered successfully.

→ Step 2 Verification Process

1. Verifier's enterprise wallet receives VP shared by the user
2. Verifier's enterprise wallet verifies the holder's signature on the VP using the holder's DID Document from the EBSI ledger (which contains the public key).
3. There are 2 different options:

**Option 1:** If constraints set by user are matched (e.g., timeframe allowed for verification or number of verifications), Verifier's enterprise wallet unpacks the VP to access the embedded VC(s) and verify the original issuer's signature on the VC(s). This is done using the issuer's public key, which can also be retrieved from their DID Document on the EBSI Trust Registry.

- Once verification is complete, the verifier will provide feedback or an acknowledgment to the holder, depending on the context (e.g., granting access to a service or confirming the authenticity of the shared data).

- A verification report is generated and stored on EBSI for transparency and traceability and user gets notified accordingly.

**Option 2:** If constraints set by user are NOT matched, user gets notification of verification tentative failed due to constraints. VC cannot be verified.

#### 8.4.4 Process 3: Credential Revocation

In cases of fraud or other exceptional circumstances, the institution (Issuer) can revoke a credential. The revocation status is updated on the blockchain, marking the revoked credential as no longer valid. The verifier may need the information if a credentials has been revoked.

In cases of fraud or other exceptional circumstances, it could be necessary can revoke a credential. In different legislations and for different certification types the revocation may be performed by the same institution (Issuer) or other authorized entities. A simple example would be revocation of a student card where the issuer institution may be the only one authorized to revoke it or a diploma where in some legislations (e.g. Italy) revocation may be performed only by a judicial authority and can be performed by the issuer **only in case** the holder requires it because of mistakes (see GDPR rights); furthermore the issuer may revoke it within a specific timeframe (12 months).

This complex situation requires a revocation process that is not ‘business driven’, i.e., performed with a pre-defined business workflow (where for example the issuer can always revoke a certification). The revocation process should therefore be ‘atomic’ i.e., developed as a mere function where the specific implementing entity is bound to use it within a business workflow conformant with applicable legal framework.

The revocation updated on the blockchain may be furthermore prone to issues related to GDPR rights, as some questions arise:

1. Who is authorized to access this information?
2. How is this information accessed? Is there a limitation (number of accesses, number of days that can be accessed, etc.)
3. Is this access traced? Who can therefore see this trace log?
4. Can an authorized entity who accessed this information share it with a third party?

5. How a revocation can itself be revoked? E.g., in case the holder gets such right from judicial entity?

There are several strategies for this can be developed:

**Strategy A:** Holder obtains a fresh VC: When using short-lived VCs, the holder obtains a fresh VC each time it is needed. As a result, a short-lived VC does not require additional revocation. This strategy may be applicable in some contexts (see student card) but surely not in case of diplomas as it would 'break' the SSI concept, driving the user to be dependent on the issuer.

**Strategy B:** The VC status is retrieved through an external trusted entity (EBSI) that has the duty to enforce all applicable legal framework: This approach would bring the load of the legal analysis and enforcement for any type of certification and any MS legal framework on EBSI.

**Strategy C:** Holder wallet is built in a way that certifications include revocation rules, therefore revocation is performed at wallet level, with approval of the user or without depending on the applicable legislation. In this way the user will not be able to share anymore his certificate and any further verification will fail.

### *Challenges and Considerations:*

When exploring overall scenarios, we encounter a series of significant challenges and factors that require careful consideration.

- Data privacy and access control for sensitive educational records.
- Integration with existing educational systems and processes.
- Adoption and acceptance of digital credentials by employers and other institutions.
- Ensuring the ongoing security and integrity of the blockchain platform.

## 8.5 Possible Journeys

Based on the comprehensive scenario details for three main processes: Educational Credential Issuing and Educational Credential Request & Verification, Credential Revocation which include student enrolment, registration, issuance, verification and revocation of digital credentials by both institutions and third-party organizations, we can explore the following potential user journeys. It's important to consider that not all students may have a European digital ID (EUID), and some verifiers may possess blockchain wallets while others may not.

### 8.5.1 Transcript and Academic Record Management

Across multiple places in the world, the most labour-intensive and time-consuming task in academic institutions is producing Transcripts.

The verification of transcripts, whether for high school or university, continues to rely on a labour-intensive process that entails individual examination and the management of extensive paper records.

EBSI Distributed ledger technology and its solutions could easily streamline these procedures as well as minimize fraudulent claims of unearned educational credits.

Journey 1. Educational to educational Student Journey

Objectives:

- Seamlessly transition from one educational institution to another.
- Maintain access to educational records and achievements.
- Begin studies at the new institution without significant delays or duplicative coursework.

**Scenario:** Maria, from Spain, applies to a master's program in Germany. Maria (Holder) owns a EUID wallet. German university (Verifier) owns an enterprise wallet.

Journey:

Step 1: Applying to the New Institution

Maria applies to German university and indicates their intention to transfer credits.

### Step 2: Credential Verification

1. The German university requests Maria's undergraduate credentials.
2. Maria shares her VC (Verifiable Credential) from her Spanish university using her EUID wallet & EBSI infrastructure.
3. German university enterprise wallet verifies the VC against the Spanish university's DID on EBSI, confirming its authenticity.

### Step 3: Notification and Acceptance

1. Maria's application proceeds based on verified credentials and notification is sent to her EUID wallet.
2. German University notifies Maria about the outcome of the credit evaluation.

### Step 4: Enrolment and Registration

1. Maria enrolls in courses at the new institution, using the exemptions where applicable.
2. Maria completes the registration process and receive access to course materials.

### Step 5: Maintaining Access to Credentials

Maria continues to access her digital credentials through EUID wallet.

## Journey 2. Erasmus Program Participation

### Objectives:

- Seamlessly apply, participate, and manage the Erasmus Program with the benefits of EBSI Network.
- Ensure the secure storage and transfer of academic records and credentials.
- Resume academic studies in home university, with blockchain-verified credentials and academic history.

**Scenario:** Luca, an Italian student, participates in the Erasmus exchange program to study in France.

Luca (Holder) doesn't own a EUID wallet.

Italian Institution (Issuer) owns enterprise wallet.

French Institution (Verifier) owns enterprise wallet.

Journey:

#### Step 1: Application Submission

Luca submits the application to the French institution.

#### Step 2: Credential Verification

1. Luca's French host institution enterprise wallet requests his academic history.
2. Luca provides his VCs from his Italian home institution enterprise wallet via EBSI.
3. The French institution enterprise wallet verifies these credentials and automatically enrolls Luca into the right courses.

#### Step 3: Notification

Luca's Italian home institution enterprise wallet receives notification and forward it to Luca via email.

#### Step 4: Program Participation

Luca engages in academic and cultural experiences while his academic progress is recorded on the blockchain.

#### Step 5: Course Completion and Return

1. After the program, Luca decides to get a EUID wallet and receives new VCs from the French institution, which he adds to his digital portfolio.
2. Luca returns to home institution and resume his academic studies, with blockchain-verified credentials and academic history on his EUID wallet
3. Luca's EUID wallet additionally requests Italian home institution enterprise wallet to provide his academic history. Whole academic history is stored in Luca's EUID wallet.

### Journey 3. PhD Research Collaboration

Objectives:

Page 62



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.

- Collaborate on research projects securely and transparently.
- Ensure the authenticity and integrity of research data and findings.
- Streamline communication and data sharing among collaborators.

**Scenario:** Sofia, a PhD student in Greece, collaborates with researchers in Belgium and Italy.

Sofia (Holder) owns EUID. Collaborating institutions (Verifiers) own enterprise wallets.

Journey:

#### Step 1: Project Initiation

Researchers from different institutions decide to collaborate on a research project.

#### Step 2: Credential Verification

1. The collaborating institutions require verification of Sofia's prior research credentials.
2. Sofia shares VCs indicating her past research projects and qualifications.
3. The institutions enterprise wallet verifies these VCs, establishing trust and facilitating the joint research initiative.

#### Step 3: Data Sharing and Management

1. Research data, findings, and documents are securely stored on the blockchain.
2. Access to data is controlled via encryption and access keys, ensuring data privacy and security.

#### Step 4: Data Preservation

1. Research data, findings, and outcomes are permanently stored on the blockchain.
2. They remain accessible for future reference and further research.

### Step 5: Project Conclusion

The research project concludes, and collaborators have a secure and transparent record of their contributions and rewards.

## 8.5.2 Diploma issuance & Revocation scenarios

### Journey 4. Higher Education Diploma Issuance

Objectives:

- Securely apply for Master course or job opportunities after graduating.
- Streamline the application process and improve efficiency.

**Scenario:** Daniele, Italian student who studied in France, applies for a job in Hungary.

Daniele (Holder) owns a EUID wallet.

Employer (Verifier) does not own an enterprise wallet.

### Step 1: Graduation Eligibility Confirmation

Daniele completed his HE programs.

**Action by French Institution:** French institution's academic board verifies that the student has fulfilled all the program requirements and is eligible for graduation.

### Step 2: Digital Diploma Creation

**Action by French Institution:** The registrar's office gathers the necessary information and creates a digital diploma in the form of a Verifiable Credential, which includes claims about the student's achievements and the institution's digital signature. A time-limited temporary VC can be prepared and issued to the student for his verification and confirmation of included data.

### Step 3: Issuance of Verifiable Credential



#### Action by Credentialing System:

- The digital diploma is packaged as a VC, incorporating the necessary metadata such as issuer, issuance date, and credential subject.
- The credential is then signed using the institution's private keys to ensure authenticity and integrity.

#### Step 4: Notification to Student

**Action by Institution:** Daniele is informed that his digital diploma is available and is provided with instructions on how to retrieve and store it securely.

#### Step 5: Diploma Retrieval

**Action by Student:** Daniele accesses his EUID wallet, which could be a secure app or online service, to retrieve the digital diploma VC.

#### Step 6: Sharing the Digital Diploma

**Action by Student:** When applying for jobs or further education, Daniele shares his VC/VP directly with potential employers or institutions.

#### Step 7: Verification of the Diploma

##### Action by Employers/Other Institutions:

- Employers in Hungary or academic institutions verify the digital diploma by checking its cryptographic proofs against the public keys recorded in EBSI.

#### Journey 5. Diploma replacement (revocation & re-issuance)

#### Objectives:

- Securely replace a student's diploma guaranteeing GDPR rights and following national legislative framework.

**Scenario:** Mateo, Spanish student who studied in Italy found error in his issued diploma. Mateo (Holder) owns an EUID wallet.  
Italian University (Issuer) owns an enterprise wallet.

#### Journey:

##### Step 1: Trigger for Revocation

**Scenario:** Mateo found a misspelling in his surname within issued Diploma.

##### Step 2: Initiation of Revocation Process

**Action by User:** Mateo records this request through issuance of a replacement request VC in EBSI. Mateo reports the issue through the institution's enterprise wallet portal or contacts the administration sharing the created VC with the institution's wallet.

##### Step 3: Verification and Confirmation

**Action by Institution:** The institution receives in its enterprise wallet the replacement VC, verifies the reason for replacement and confirms the need of replacing existing Diploma.

##### Step 4: Replacement Execution

**Action by Institution:** Institution use its enterprise wallet and calls EBSI-VECTOR revocation service to revoke diploma, e.g., the DID Document is updated to indicate the credential is revoked and creates a new digital diploma in the form of a Verifiable Credential, which includes corrected metadata and claims about the student's achievements and the institution's digital signature.

##### Step 5: Notification

**Action by Institution:** Notifies the student that his diploma card has been replaced

## Step 6: Diploma Retrieval

**Action by Student:** Daniele accesses his EUID wallet, which could be a secure app or online service, to retrieve the digital diploma VC.

### 8.5.3 Employer verification scenarios

Students and learners can get fast and convenient access to their records and share it securely with potential employers. It also eases the burden on employers as they don't have to go through the background verification processes to confirm the student/applicant's accomplishments.

#### Journey 6. Job Application Post-Graduation

##### Objectives:

- Securely apply for job opportunities after graduating.
- Ensure the authenticity and integrity of application materials.
- Streamline the application process and improve transparency.

**Scenario:** Elise, who studied in the Netherlands, applies for a job in Sweden.

Elise (Holder) owns a EUID wallet.

Swedish employer (Verifier) does not own an enterprise wallet.

##### Journey:

1. The Swedish employer requests proof of Elise's degree.
2. Elise shares her VC from the Dutch university via her EUID wallet using standard means (e.g., email).
3. The employer, using EBSI open verification portal, verifies the degree's authenticity and proceeds with the hiring process.

#### Journey 7. Professional Course Certification

Objectives:

- Securely obtain a professional certification for a specific course.
- Verify the authenticity and validity of the certification.
- Streamline the certification process and improve transparency.

**Scenario:** Dmitri, from Estonia, completes a professional course in Portugal and wants to use this certification to enhance his job prospects in several EU countries.

Dmitri (Holder) doesn't own a EUID wallet.

Portuguese institution (Issuer) does not own enterprise wallet.

Employers (Verifiers) do not own enterprise wallets.

Journey:

1. The Portuguese institution issues a VC to Dmitri upon course completion via email.
2. Dmitri applies for jobs in France, Italy, and Greece, sharing his VC with potential employers via mail or other means.
3. Employers across these countries verify his VC seamlessly using EBSI open verification portal, recognizing the value of his professional course.

Journey 8. Recognition of Informal Education

Objectives:

- Securely obtain recognition for informal education.
- Verify the authenticity and validity of the recognition.
- Enhance the professional or educational opportunities with recognized informal education.

**Scenario:** Mikael from Finland has taken several online courses from institutions across Europe and wants to consolidate these for a job application in Austria.

Mikael (Holder) owns EUID

Institutions across Europe (Issuers) own enterprise wallets.

Employer (Verifier) does not own enterprise wallet.

Journey:

1. Each course provider enterprise wallet issues a VC to Mikael upon completion.
2. Mikael EUID wallet presents a consolidated VP (Verifiable Presentation) containing all his VCs to the Austrian employer.
3. The employer verifies each VC in the VP through EBSI open verification portal, appreciating Mikael's diverse learning journey.

#### 8.5.4 Student card verification & revocation scenarios

EBSI technology provides a secure and efficient way to manage student discounts by reducing fraud and simplifying the verification process. It also enhances user privacy as sensitive personal information is not shared with individual online services, reducing the risk of data breaches.

Journey 9. Special discounts from online services

Objectives:

- Secure student discounts and special offers from online services.
- Verify student status to qualify for discounts.
- Simplify the process and ensure transparency and data security.

**Scenario:** Luigi is a second-year student in Italian university. He wants to activate Spotify paying the discounted price reserved for active students. Spotify accepts electronic studentship attestation issued by European High Education institutions.

Luigi (Holder) owns a EUID. Italian University (Issuer) owns an enterprise wallet. Spotify (Verifier) owns an enterprise wallet.

Journey:

1. Luigi logs into the University student portal and asks for an electronic studentship attestation.
2. Italian University verifies Luigi's studentship status and issues the verifiable student identity that is stored in Luigi's credential wallet.
3. Luigi shares its verifiable student identity with Spotify and pays the reduced annual fee for the service.
4. The Verifier system may periodically re-verify the user's student status to ensure ongoing eligibility.

Journey 10. Student card revocation

Objectives:

- Securely revoke a student's access or student card in a transparent and traceable manner.
- Maintain records of the revocation for future reference.

**Scenario:** After one year, Luigi decides to retire from the UNIBO bachelor's degree program before graduating. UNIBO closes the student career and revokes the electronic studentship attestation issued to Luigi.

The electronic studentship attestation held by Luigi in its user wallet, is marked as revoked and cannot be used anymore to obtain student discount.

Journey:

#### Step 1: Trigger for Revocation

**Scenario:** A student graduates, transfers, or withdraws from the institution, or card is reported lost or stolen.

#### Step 2: Initiation of Revocation Process

**Action by User:** The student or a representative from the institution initiates the revocation process. In case of loss or theft, the student reports the incident through the institution's digital portal or contacts the administration.

#### Step 3: Verification and Confirmation

**Action by Institution:** The institution verifies the reason for revocation. For instance, checking the student's graduation status or confirming the report of a lost card.

#### Step 4: Revocation Execution

**Action by Institution:** Institution uses EBSI-VECTOR revocation service to revoke cards, e.g. the DID Document is updated to indicate the credential is revoked.

#### Step 5: Notification

**Action by Institution:** Notifies the student that their digital student card has been revoked and updates any relevant parties (e.g., campus security, library services,..).

#### Step 6: Verification of Revocation

**Action by Verifiers:** When the card is presented, verifiers (e.g., campus services, online resources) check the credential status using the appropriate EBSI service.

#### Step 7: Replacement (if applicable)

**Action by User:** The student applies for a replacement card if necessary, following the institution's procedures for issuing new credentials.

#### Step 8: Confirmation of New Credential Validity

**Action by Institution:** The institution ensures that the new credential is added to the system and all services that require student identification are updated with the new card details.

### 8.5.5 Publishing & Copyright Protection

Many students, professors, teachers and researchers constantly generate quality material. However, the publication of this material is often very hard. Publishing on a blockchain could help new writers, researchers and many others get a break into the industry without risking theft of their research work.

In the academic world, plagiarism is a serious problem. EBSI network can be used to control the copyrighted material across the Internet.

EBSI technology discourages plagiarism by making unauthorized use easily detectable while enabling authors to share their work with confidence. It opens a transparent pathway for new writers, researchers, and educators to establish their presence in the academic world. EBSI thus stands as a guardian of academic integrity in the digital age, fostering trust and innovation in scholarly communication.

#### Journey 11. Publishing & Copyright Protection

Objectives:

- Publish creative work securely and transparently.
- Protect copyright and intellectual property.
- Prove ownership and manage distribution using blockchain.

Scenario:

This user journey highlights the streamlined process of securely publishing academic work using blockchain technology through EBSI, addressing common pain points such as plagiarism and copyright theft, while also enabling broader collaboration and visibility within the academic community.

Journey:

Step 1: Creation of Work



- **User:** An academic (student, professor, teacher, or researcher).
- **Action:** Completes a piece of quality academic material ready for publication.

#### Step 2: Initial Engagement with EBSI

- **User:** Searches for secure academic publishing platforms and discovers EBSI Copyright protection service.
- **Action:** Visits the EBSI platform and reads about its anti-plagiarism capabilities and secure publishing process.
- **Goal:** To understand how EBSI can protect their intellectual property.

#### Step 3: Account Setup and Verification

- **User:** Decides to use EBSI for publishing their work.
- **Action:** Creates an account on EBSI, verifies identity as an academic, and sets up a digital wallet.
- **Goal:** To establish a verified presence on the platform and prepare for publication.

#### Step 4: Pre-Publishing Material Preparation

- **User:** Prepares the material for blockchain publication.
- **Action:** Formats the document according to EBSI's guidelines and attaches metadata (authorship, date, abstract).
- **Goal:** To ensure the material is blockchain-ready for traceability and authenticity.

#### Step 5: Uploading and Hashing

- **User:** Ready to upload the material to EBSI.
- **Action:** Submits the document to EBSI, where the platform generates a unique hash of the work and records it on the blockchain. EBSI creates a certification of publishing based on the copyright protection features (not detailed here).
- **Goal:** To create an immutable record of the document's originality.

#### Step 6: Publication and Issuance of Certificate

- **User:** Waits for the confirmation of publication.

- **Action:** Receives a EBSI certificate confirming the work's registration and copyright details.
- **Goal:** To obtain proof of publication and copyright ownership.

#### Step 7: Monitoring and Alerts

- **User:** Wants to ensure ongoing protection of their work.
- **Action:** Activates monitoring services on EBSI that alert them to potential unauthorized use or plagiarism.
- **Goal:** To proactively protect their work from misuse.

#### Step 8: Sharing and Dissemination

- **User:** Seeks to share their published work with peers and the academic community.
- **Action:** Uses EBSI's secure sharing tools to distribute the work, ensuring receivers can verify its authenticity.
- **Goal:** To gain visibility and credibility within the academic community while safeguarding their intellectual property.

#### Step 9: Receiving Feedback and Collaborating

- **User:** Engages with other academics on the platform.
- **Action:** Utilizes EBSI's collaboration tools to receive feedback, discuss research, and co-author future works.
- **Goal:** To foster academic collaboration and improvement of their work.

#### Step 10: Expansion and Recognition

- **User:** Aspires to grow their academic reputation.
- **Action:** Leverages the security and traceability of their blockchain-published works to apply for grants, positions, and speaking opportunities.
- **Goal:** To utilize their secure, verifiable portfolio of work as a foundation for professional growth.

## 8.6 Customer user stories

Young citizen who wants to apply to a Bachelor Course

Luigi is 19 years old; he holds a diploma. Max, a German student, is also 19 years old. He has a German Abitur (upper secondary school certificate). They both want to study and apply for the bachelor's in computer science (e.g.) at the University of Bologna (UNIBO). Luigi lives far from Bologna and prefers to avoid moving to Bologna until the lessons start. Luigi and Max must complete some administrative procedures to become a UNIBO student. They know that UNIBO offers an online registration service which easily allows citizens to be securely identified and to provide all the necessary information to be enrolled. The UNIBO online registration service asks Luigi and Max to provide its electronic Identity attestation to be securely authenticated. Luigi and Max ask its local Registry Office to issue an eIDAS compliant electronic Identity attestation in the form of a verifiable identity. Luigi and Max easily share their verifiable identities and Diploma attestations with the UNIBO online registration service to allow UNIBO to verify they hold the required education title. Luigi and Max complete online all the enrolment procedures and become UNIBO students.

Student who wants to obtain student's special discounts from online services

Luigi is 21 years old. He is a student of the second year of the UNIBO Computer Science course. He wants to activate Spotify paying the discounted price reserved for active students. Spotify accepts electronic studentship attestation issued by European High Education institutions Luigi logs into the UNIBO student portal and asks for an electronic studentship attestation. UNIBO verifies Luigi's studentship status and issues the verifiable student identity that is stored in Luigi's credential wallet. Luigi shares its verifiable student identity with Spotify and pays the reduced annual fee for the service.

Student who retires from a bachelor's degree program

After one year, Luigi decides to retire from the UNIBO bachelor's degree program before graduating. UNIBO closes the student career and revokes the electronic studentship attestation issued to Luigi. The electronic studentship attestation held by Luigi in its user wallet, is marked as revoked and cannot be used anymore to obtain student discount.

Foreign bachelor student applies for a master in a university in another European country

Eva has a UNIBO bachelor's degree in computer science and want to apply for a master at KU Leuven in Belgium. Eva visits the KU Leuven online registration service to share her verifiable

bachelor diploma obtained at UNIBO and her Italian verifiable identity. After all the information is verified, Eva is enrolled at KU Leuven.

#### *A student wants to easily access educational environments*

Eva, a student of KU Leuven, can obtain a verifiable student identity from her university. She can use this verifiable student identity to authenticate and access all educational environments like the e-learning platform and the student information system. Verifiable student identity becomes an alternative to log in and a (additional) MFA app is no longer needed to authenticate.

#### *Foreign student wants to apply for student residence and study allowance*

Eva wants to come to Belgium to study and wants to apply for a student residence. An online apply form exists where Eva can share her verifiable identity and verifiable student identity. She wants to do the same for applying for a study allowance.

#### *Eva goes on an exchange program to UNIBO*

In the context of Eva's master study, Eva goes on Erasmus for a period of 6 months at the University of Bologna in Italy. She onboards at Unibo, using her verifiable student identity, issued by KU Leuven. During the onboarding, Unibo will verify that Eva's academic id is present in a pre-existing list of Erasmus students. Since Eva is present in Unibo's list of exchange students, Eva is successfully signed into the virtual campus of Unibo and becomes an active Unibo student.

#### *Student at university A easily access educational services at university B*

During her Erasmus program, Eva wants to follow an online course, organized by Uniwersytet Jagiellonski w Krakowie in Poland. Eva authenticates herself at Uniwersytet Jagiellonski w Krakowie using her Verifiable student id, issued by KU Leuven. After sharing her student id, Eva is automatically logged into the online course.

#### *Student receives a verifiable transcript of records after successfully completing online courses*

After successful completion of the course, Eva asks for a Verifiable Transcript of Record, including the credits for the course she followed at Uniwersytet Jagiellonski w Krakowie. She authenticates herself, based on her Verifiable Student ID, and receives a V-TOR, issued by Uniwersytet Jagiellonski w Krakowie.

### *Automatic recognition of learning achievements*

Eva shares the V-TOR with KU Leuven, her home university, since the obtained credits are part of her master study. KU Leuven automatically includes learning achievements in the student career without any human intervention.

### *John is an alumnus who wants to obtain his verifiable diploma*

John graduated years ago from KU Leuven and wants to obtain his verifiable diploma to share with a possible future employer. John visits the self-service portal of KU Leuven and requests a verifiable educational ID by presenting his verifiable ID. KU Leuven verifies the provided info and consults the database to see if John graduated. KU Leuven issues an educational ID with affiliation alumnus. John can now request his verifiable diplomas in the self-service portal by presenting his verifiable educational ID.

### *Staff members want to use verifiable credential to access environments in the university*

Philip is a staff member of KU Leuven and uses MFA to authenticate to get access to environments in KU Leuven. He must use his MFA app. Philip wants to use his wallet instead. This way Philip has less apps to use for accessing different services. Philip accesses the account self-service portal of KU Leuven and can request a verifiable educational ID with the affiliation of being staff. From now on Philip can use his verifiable educational ID to authenticate to the Central KU Leuven Login and get access to the different environments of the university.

### *A person pays a fee to attend conference*

Luigi uses his verifiable identity or verifiable student identity to log into a conference portal. He pays the conference fee and receives a verifiable conference ticket which allows him to access the conference material website and to physically access the conference centre through a physical access control system.

### *Student or staff loses his wallet*

Students or staff lose their phones with all their user credentials. They go to their local registration agency to obtain a verifiable identity. University provides a recovery procedure which allows them to obtain again their verifiable student identity by presenting their verifiable identity.

### *Services restricted to members of a university alliance*

The Una Europa university alliance provides many online services to students and staff members of the participants university/higher education institutions. These Una Europa services can be easily accessed using the verifiable alliance id stating the alliance membership. Leonardo, a staff member of UNIBO, which is a Una Europa member, wants to access the Una Europa online learning portal. He logs into the UNIBO portal and requests his verifiable alliance id, then he uses this credential to log into the Una Europa learning portal.

### *An alumni want to apply for a job in which only the graduation title is required*

Carlo is an alumnus of the University of Bologna. He wants to apply online for a job which requires a specific set of bachelor's degree types, but he prefers to not share the bachelor grade. When he shares his verifiable diploma with the job application web site, he uses selective disclosure to share only the bachelor's degree type.

### *Cross border use and verification of micro-credentials*

Fatima moved to Sweden from another EU country and seeking jobs related to her expertise. She secured welding micro-credentials from her home country. She applied for job, and they asked to proof her skill in welding. Based on this use case following scenarios may occur:

- Share verifiable credentials to ensure that Fatima possess required skills.
- On request, she may share verifiable identity (name and home address) and verifiable micro credentials without revealing her personal information.

Based on the above scenarios, she will create a verifiable presentation and then share verifiable presentation with the employer.

## 9 Marketing and Dissemination strategy

### 9.1 Introduction

The modern educational landscape is undergoing a transformation, driven by digital evolution and a globalized student populace. At the heart of this shift is the EBSI-VECTOR Digital Credential Service—a groundbreaking solution designed to address the challenges of today's fragmented

credential management systems. But a solution, no matter how revolutionary, only realizes its full potential when it reaches its intended audience and garners their trust.

This chapter delves into our comprehensive marketing and dissemination strategy crafted to spotlight the unique advantages of the EBSI-VECTOR Digital Credential Service. From harnessing the decentralized trust of blockchain to ensuring unparalleled transparency and accessibility, our strategy is tailored to resonate with students, educational institutions, employers, and other stakeholders.

With a cross-border perspective, our plan not only aims to inform and educate the European community but also reaches out to potential users from across the globe. By highlighting the service's commitment to self-sovereignty, interoperability, and rigorous compliance standards, we aim to build a narrative that not just informs but also inspires confidence.

The Marketing and Dissemination strategy intrinsically aligns with the EBSI-VECTOR project Communication and Dissemination Strategy and the Dissemination and Communication Plan. These foundational documents provide general guidance regarding the target audience, channels, and tools essential for effective communication and promotion, ensuring a harmonized approach to boost the uptake of the educational use case.

## 9.2 Services Overview of EBSI-VECTOR Digital Credential Service

The EBSI-VECTOR Digital Credential Service is a cutting-edge platform designed to revolutionize the management and verification of educational credentials. Rooted in blockchain technology, it offers a seamless user onboarding experience, facilitating self-sovereign profile creation, multi-faceted digital identity management, and secure credential issuance. The platform integrates various features ranging from user-friendly UIs, robust wallet management systems, real-time credential verification mechanisms, to comprehensive support and help centres. Catering to diverse stakeholders, from students to institutions, its comprehensive toolkit ensures streamlined operations in the ever-evolving educational landscape.

The service's core strength lies in its **interoperability** and **stringent compliance standards**. It supports a broad spectrum of educational segments, from early childhood education to lifelong learning. With an emphasis on **data privacy**, the platform adheres to the GDPR and other pivotal EU digital regulations, ensuring users' personal data remains protected while facilitating efficient

credential management. Moreover, its multi-language support, scalability, and legacy document management features make it a truly global solution for the modern educational realm.

### 9.3 Unique Selling Points (USP) of EBSI-VECTOR Digital Credential Service

- **Blockchain Integration:** Offers unmatched trust and immutability, ensuring every credential remains tamper-proof.
- **Self-Sovereignty:** Empowers users with full control over their educational records, fostering trust and autonomy.
- **Real-time Verification:** Streamlines the verification process, allowing instant authentication of credentials without human intervention.
- **Interoperability:** Designed for global applicability, ensuring compatibility with various educational systems and standards worldwide.
- **Data Privacy:** Prioritizes user data protection, with strict adherence to GDPR and other data protection regulations.
- **Scalability:** Built to accommodate growing user volumes, ensuring efficient performance regardless of scale.
- **Multi-Language Support:** Caters to a global audience, offering a range of language options for accessibility.
- **Legacy Document Management:** Bridges the digital and physical realms, allowing users to export and print their credentials when needed.

### 9.4 Dissemination Strategy for the EBSI-VECTOR Digital Credential Service

By leveraging this dissemination strategy, the EBSI-VECTOR Digital Credential Service aims to penetrate diverse markets, resonating with its target audience's unique needs and preferences. The emphasis is on creating an informed, engaged, and empowered user base that recognizes the platform's transformative potential in the educational sector.



### 9.4.1 Goals:

- **Educate:** Raise awareness about the features and benefits of the EBSI-VECTOR Digital Credential Service, ensuring that potential users understand its value proposition.
- **Engage:** Foster active participation and interest among educational institutions, students, and other stakeholders.
- **Drive Adoption:** Encourage a transition from traditional credential systems to the EBSI-VECTOR platform, emphasizing its security, efficiency, and global applicability.
- **Maintain Trust:** Continually emphasize the service's commitment to data privacy, blockchain-backed security, and regulatory compliance.

### 9.4.2 Channels and Platforms:

#### 9.4.2.1 Digital Channels

**Social Media:** Engage users on platforms popular among students and institutions, such as LinkedIn for professionals and academic forums, and Instagram for a younger audience.

**Email Marketing:** Send out informative newsletters, updates, and success stories.

**Webinars & Online Workshops:** Host sessions to introduce features, benefits, and conduct live demonstrations.

**SEO & PPC:** Optimize online content for search engines and run paid campaigns targeting keywords related to digital credentials and education.

#### 9.4.2.2 Traditional Channels

**Educational Magazines & Newspapers:** Feature articles, case studies, and interviews.

**Conferences & Symposiums:** Attend and sponsor events, ensuring a presence where educational decisions are made.

**Community Building:** Engage with student communities, educational forums, and institutional networks to foster organic discussions and endorsements.

#### 9.4.2.3 Content Strategy

**Educational Content:** Produce articles, infographics, and videos that explain the EBSI-VECTOR system's intricacies, its blockchain foundation, and its benefits.

**Testimonials & Case Studies:** Showcase success stories from early adopters, emphasizing the platform's real-world advantages.

**How-to Guides:** Provide step-by-step guides on using the service, from onboarding to credential issuance and verification.

**Explainer Videos:** Visual content to simplify complex topics, making them easily digestible for all audience segments.

#### **9.4.2.4 Localization Strategy:**

**National Adaptation:** Customize content to resonate with national educational systems in different EU countries.

**Language Translation:** Offer content in multiple languages of EBSI-VECTOR partners, ensuring that the service's benefits are communicated effectively across these countries.

**Regional Partnerships:** Collaborate with local educational institutions, government bodies, and influencers to gain trust and establish credibility in different regions.

**Feedback & Iteration:** Continually gather feedback from different stakeholders at national level to refine and adapt the strategy, ensuring maximum relevance and resonance.

#### **9.4.2.5 Target audience**

The educational landscape, with its diverse market segments, presents a multifaceted arena where the need for secure, verifiable credentials transcends various levels and types of educational engagement. While early childhood education may not necessitate student certification, the professionals operating within this sector certainly require verifiable credentials, underlining the universal applicability of the EBSI-VECTOR Digital Credential Service across educational and professional spectra.

#### **9.4.2.6 Issuers:**

From the standpoint of credential issuers, market segments span a broad range:

- **Early Childhood Education:** Comprising childcare centres, preschools, and kindergartens, this segment, while not demanding student certification, necessitates verified credentials for its workforce.

- **K-12 Education:** Encompassing public and private institutions, this foundational segment molds future citizens and professionals, necessitating a secure framework for issuing credentials.
- **Higher Education:** Colleges and universities fall into this category, marking a critical juncture where verifiable academic credentials become paramount in both academic pursuits and career progression.
- **Vocational Education:** This practical segment demands a high degree of credential verification to ensure skill competency for specific trades and occupations.
- **Professional Development:** Often overlooked, this segment plays a crucial role in continual skill enhancement, requiring updated and verifiable records of professional growth.
- **Lifelong Learning:** Perhaps the most dynamic segment, it includes diverse educational activities undertaken throughout an individual's life, emphasizing the need for a cohesive, lifelong credential management system.

All stakeholders within these segments, especially students, represent a distinct market segment themselves, acting as **Holders** of user wallets, a digital repository of their verifiable credentials.

#### 9.4.2.7 Verifiers

Parallely, from a verifier's perspective, several critical market segments emerge:

- **Service Providers:** Entities dedicated to offering trusted verification services to businesses or end users, ensuring the authenticity of attestations.
- **Educational Institutions:** These not only issues but also often need to verify credentials, particularly for incoming students or professional collaborations, especially in the Human Resources departments.
- **Employers:** Whether leveraging external services or utilizing their own infrastructure, employers consistently engage in the verification process, affirming the qualifications of potential or current employees.
- **Public institutions at national and regional level:** Ministries of Education and regional entities that define policy in the educational sector, including ENIC-NARIC.

## 9.5 Marketing Channels for the EBSI-VECTOR Digital Credential Service

By employing a diverse mix of digital, traditional, and community engagement channels, the EBSI-VECTOR Digital Credential Service aims to reach its varied target audience effectively. The strategy is to blend broad-reaching campaigns with targeted engagements, ensuring widespread awareness while also addressing the unique needs and interests of specific user groups.

### 9.5.1 Digital Marketing Channels

- **Website and SEO (Search Engine Optimization):** The primary platform to introduce and detail the EBSI-VECTOR Digital Credential Service, optimized to rank high in search results.
  - **Implementation:** Regularly update with fresh content, optimize for relevant keywords, and ensure mobile responsiveness. Utilize on-page and off-page SEO tactics to increase organic reach.
- **Social Media:** Engage with a diverse audience, share updates, success stories, and foster community discussions.
  - **Implementation:** Create tailored content for platforms like LinkedIn (targeting professionals and institutions), X-Twitter (for real-time updates), and Instagram (utilizing visual content for younger demographics). Run ad campaigns, host live sessions, and engage with followers through Q&A sessions.
- **Newsletter:** Provide targeted information to subscribers, stakeholders, and potential users.
  - **Implementation:** Segment email lists based on user type (students, institutions, employers). Send regular newsletters, feature updates, success stories, and exclusive offers.
- **Content Marketing & Blogging:** Educate the audience, establish thought leadership, and improve organic search rankings.
  - **Implementation:** Regularly publish informative articles, infographics, and research studies on the benefits, features, and use-cases of the EBSI-VECTOR system.

## 9.5.2 Traditional Marketing Channels

- **Educational Magazines & Newspapers:** Reach a broader audience, especially those less engaged with digital channels.
  - **Implementation:** Feature articles, op-eds, interviews, and advertorials showcasing the advantages and success stories of the EBSI-VECTOR system.
- **Conferences, Workshops, & Symposiums:** Direct engagement with educational stakeholders, policymakers, and potential partners.
  - **Implementation:** Attend key educational events, sponsor sessions, and host workshops or booths to demonstrate the system's capabilities including events organized by each country ENIC-NARIC and EBSI.

## 9.5.3 Community Engagement

- **Educational Forums & Communities:** To Foster organic discussions, gain insights, and address queries or concerns.
  - **Implementation:** Engage actively in for a to share content, participate in discussions, and gather feedback.
  - Relevant fora are: EdSurge, Chronicle of Higher Education, eLearning Industry, International Society for Technology in Education, European Education and Training Forum (EETF), EPAL (Electronic Platform for Adult Learning in Europe).
- **Affiliate & Partnership Marketing:** Leverage the reach and credibility of established entities in the educational sector at national level as well as the EBS partnership.
  - **Implementation:** Collaborate with educational institutions, eLearning platforms, and industry influencers for co-marketing opportunities and mutual promotions.
  - **Relevant National networks:**
- **Webinars & Online Workshops:** Engage with a targeted audience, demonstrating the system's capabilities and benefits in real-time.
  - **Implementation:** Host sessions addressing different user groups, from students to institutional decision-makers, providing hands-on demonstrations and Q&A sessions. These webinars should be in the language of each country of the EBSI-VECTOR project.

## 9.6 Feedback & Iteration for the EBSI-VECTOR Digital Credential Service Marketing

Incorporating feedback and iterating based on data ensures that the marketing and dissemination efforts of the EBSI-VECTOR Digital Credential Service remain relevant, effective, and aligned with the target audience's needs and preferences. It fosters a culture of continuous improvement, ensuring that the service's value proposition is communicated effectively and resonates with its diverse user base.

### 9.6.1 Methods to Gather Feedback

- **Surveys and Questionnaires:** Deploy regular online surveys targeting end-users to gather insights on the effectiveness of marketing campaigns and to understand areas for improvement.
- **Feedback Forms on Website:** Incorporate an easily accessible form on the website for visitors to provide feedback on their experience, queries, or concerns.
- **Community Engagement:** Actively participate in online forums, social media platforms, and community chats to gather organic feedback and address concerns in real-time.

### 9.6.2 Analytics Tools to Measure Performance

- **Website Analytics:** Utilize tools like Google Analytics or Matomo to monitor website traffic, user behaviour, bounce rates, and conversion rates, assessing the effectiveness of digital campaigns.
- **Social Media Management Tools:** Platforms like Facebook Insights, Twitter Analytics, and LinkedIn Analytics provide detailed data on post reach, engagement rates, follower demographics, and more.
- **Email Campaign Metrics:** Monitor open rates, click-through rates, and conversion rates of email campaigns to gauge their effectiveness and areas of improvement.
- **Customer Relationship Management (CRM) System:** To track interactions with various stakeholders and to schedule follow-ups.
- **Webinar Software:** For hosting and archiving online events.

### 9.6.3 Strategies to Iterate and Refine based on Feedback and Data

- **Data-Driven Decisions:** Use the metrics from analytics tools to identify high-performing campaigns and channels, reallocating resources and efforts accordingly.
- **A/B Testing:** For digital campaigns, use A/B tests to compare different marketing strategies, designs, or messages. This helps in understanding what resonates best with the audience.
- **Feedback Implementation:** Actively incorporate the feedback received from users and stakeholders into marketing strategies. This could mean refining the messaging, redesigning certain campaign elements, or introducing new channels based on demand.
- **Regular Review Meetings:** Organize monthly or quarterly review meetings with the marketing team to discuss feedback, analytics data, and to brainstorm new strategies.
- **Training and Upgradation:** Based on feedback and evolving marketing trends, ensure that the marketing team undergoes regular training and upgradation sessions to stay updated and effective.

## 9.7 Conclusions

The EBSI-VECTOR Digital Credential Service emerges as a beacon of innovation, addressing the pressing challenges of credential management with a solution grounded in blockchain technology. As we've mapped out in this chapter, a multi-pronged marketing and dissemination strategy is paramount to its success, ensuring the service's groundbreaking features are effectively communicated and resonate with its diverse target audience.

Our strategy is not static but is designed to evolve. By leveraging both digital and traditional marketing channels, we aim to cast a wide net, reaching stakeholders from students to policymakers across the European Union. The emphasis on feedback and iteration underscores our commitment to continuous improvement, ensuring that our efforts remain aligned with the ever-changing needs and preferences of our audience.

Furthermore, our active engagement in key European educational forums and communities amplifies our reach, fostering organic discussions and ensuring the service's value proposition is understood at all levels of the educational sector.

By enhancing trust, reducing fraud, and streamlining processes, the EBSI-VECTOR Digital Credential Service stands poised to pave the way for a future where educational records are secure, universally recognized, and easily accessible, benefiting individuals, educational institutions, and employers across the European Union and beyond.

## 10 Operations and Management

### Introduction

In Chapter 9, we provide an overview of the operations and management structures for the organizations involved in issuing Verifiable Credentials (VCs). We shed light on the daily operations, team profiles required, the intricate organizational structure, and the step-by-step operational processes.

By understanding the daily operations, required team profiles, organizational structure, and necessary operational processes, these organizations can efficiently issue, manage, and verify credentials while ensuring compliance, security, and service excellence. This chapter serves as a guide for establishing a well-organized, competent, and compliant issuing organization within the EBSI framework.

### 10.1 Daily Operations of Issuing Organizations

#### 10.1.1 Operation Framework

Organizations issuing VCs (Trusted Issuers) will be engaged in credential issuance, management, and verification processes daily. These organizations should establish and adhere to standard operating procedures to ensure the accuracy, authenticity, and confidentiality of the credentials issued.



### 10.1.2 Credential Issuance

This involves user onboarding and profile management for identifying and registering individuals into an EBSI-VECTOR service. It typically includes guiding users through the initial setup, providing access to features, and collecting essential information. Once onboarded, profile management allows users to maintain and update their personal information, preferences, and settings within the platform. This seamless process ensures a positive user experience, fosters engagement, and enables tailored interactions, ultimately enhancing user satisfaction and the platform's effectiveness. VCs could be issued for educational/academic credentials, micro-credentials and other types of educational certificates such as diplomas, degrees, and transcripts.

### 10.1.3 Credential Management

Daily tasks include monitoring issued credentials and providing support to holders of VCs. This includes verifying students' academic achievements, generating official documents, and ensuring their secure and authorized delivery. It also encompasses ongoing tasks like handling requests for re-issuance or updates.

## 10.2 Team Profiles for Issuing Organizations

### 10.2.1 Operations Team

The Operations Team handles the day-to-day tasks related to VC issuance and management. This team will need individuals with skills in data management, cryptography, customer support, and a deep understanding of the EBSI platform.

### 10.2.2 Technical Support Team

Responsible for addressing technical challenges and ensuring the system's seamless functionality. They should possess a strong background in blockchain technology, troubleshooting, and system maintenance.

### 10.2.3 Compliance and Legal Team

Ensuring that the VCs issued comply with the legal standards and policies of each jurisdiction involved. They are also responsible for addressing any legal concerns or disputes related to the issued VCs.

## 10.3 Organizational Structure of Issuing Organizations

Each issuing organization should have a clear hierarchical structure with defined roles and responsibilities. The Operations Team will be at the core of the issuance process, supported by the Technical and Compliance teams. There should be efficient coordination mechanisms among these units to ensure smooth operations.

## 10.4 Operational Processes

### 10.4.1 Issuance Process

VC issuance involves the processes related to creating, distributing, and overseeing educational/academic credentials, micro-credentials, and other types of educational certificates such as diplomas, degrees, and transcripts. This includes verifying students' academic achievements, generating official documents, and ensuring their secure and authorized delivery.

### 10.4.2 Management Process

This involves routine updates, revocation, suspension, or reissuance of credentials based on the holders' or issuers' requests and the data received from educational institutions.

### 10.4.3 Verification Process

For any organization or employer seeking to verify the credentials of an individual, the issuing organizations should facilitate a seamless and secure verification process that protects the privacy of the credential holder while providing accurate information. This verification is typically conducted by employers, educational institutions, government agencies, or other relevant entities to ensure that the presented educational credentials are accurate and obtained from a legitimate source. Educational credential verification is crucial for making informed decisions in areas such as employment, admissions, or professional licensing.

#### 10.4.4 Continuous Improvement Process

Issuing organizations should regularly evaluate and optimize their processes, adopt best practices, and stay compliant with the legal and technical standards that evolve over time.

## 11 SWOT Analysis

### 11.1 Internal analysis

#### 11.1.1 Strengths

The Strengths category includes internal factors that are likely to have a positive effect on achieving the objectives of the institutions and other stakeholders in the ecosystem. They capture the positive aspects internal to each institution that add value or offer a competitive advantage. Strengths include the positive attributes of the people involved in the institution, including their knowledge, research, backgrounds, education, credentials, contacts, reputations, or the skills they bring to the organization. Strengths also include tangible assets such as available infrastructure, equipment, funds, established academic and administrative staff, students, and other valuable resources within the institution. Strengths describe the positive attributes, values, tangible, and intangible attributes, internal to each institution.

- Institutions recognised internationally, offering high-quality academic programmes accredited throughout Europe. This experience can be easily extended to other types of credentials, such as academic micro credentials.
- Partnerships with other European institutions (alliances) in a cross-border environment. This can facilitate the development of a sectorial trust model complementing the eIDAS 2 Regulation.
- A lot of sustainability initiatives and practices within the institutions exist, that can be applied to the SSI ecosystem.
- An environment that encourages innovation and is more open to adopt new technological paradigms such as SSI based in DLT.
- Mature technological infrastructure for student services, easily pluggable to the EBSI SSI approach.
- Dedicated and highly skilled staff, with an agile way of working.

- Many use cases for the use of verifiable credentials within student and staff services.
- EBSI is a well-tested and proven technological approach for SSI.

### 11.1.2 Weaknesses

The Weaknesses category covers those factors that are within the institution's control and detract from its ability to obtain or maintain a competitive edge. These factors are most likely to have a negative effect on achieving the institution's objective.

- Different technologies used at the different partner institutions.
- Different legislation within the different countries.
- Legal and organizational structures are not in place and this process takes a lot of time.
- Slow agreements between organizations and governments for the trust chain (authorization model): will take time.
- Lack of financial resources / funding.
- Limited resources for professional development.
- Insufficient collaboration and communication across the institution (competitive).
- Weaknesses in current digital credential framework: no standard data model to represent credentials, often manual verification step needed, not user centric, full data disclosure.

## 11.2 External analysis

### 11.2.1 Opportunities

The Opportunities category entails those external to the institution factors that most probably will bring a positive effect on achieving or exceeding the objective(s), or goal(s). Opportunities may be amongst others technological advances, resolution of problems associated with current situations, or the ability to offer greater value that will create a demand for the institution's services.

- Offer **digital credentials** to students, not just in pdf format but **in a universal standardized tamper free data format**. In this way, shared credentials can be processed automatically and faster compared to their paper version. For educational credentials, the European learning model provides a **single format** to describe certificates of credits, degrees, diplomas, diploma supplements and any other kind of claims that are related to learning. This European learning model is the enabler of educational credentials.

- secure digital documents that can be easily shared and automatically verified
- based on standards (W3C Verifiable Credentials Data Model, OpenID Connect, ...)
- robust protection against any potential breaches or tampering
- cryptographically secure, verifiable through machines, and that guarantee privacy
- organizations can seamlessly and automatically verify user information without worrying over the legal validity of their credentials
- standardization: converging of use case specific solutions
- efficiency
- Empower students with digital trustworthy certificates. Especially in the context of lifelong learning but also to promote mobility, it becomes important that **students gain verifiable, shareable, and portable records of achievement** that enable them to take their valuable credentials on-the-go for presentation to third parties.
  - allowing users to control their data and hold pre-verified identity documents and other data in a digital wallet
  - user centric
  - one app to access all (government, education, online services, ...)
  - manage credentials in one place
- These digital credentials should **facilitate the relationship between the student and our universities**. We aspire to have happier students through simpler processes and less paperwork. By integrating verifiable credentials into the admission and registration processes, these processes are greatly simplified.
  - faster and simpler verification and administration processes
  - online services without user/passwords and faster onboarding
  - happier people (e.g., students, administrations, ...) due to faster and more secure processes
  - reduce costs
  - simplifying the process of proving their identity and sharing information in online interactions
- Information sharing with respect to privacy of students. Especially in the European context of GDPR, privacy must be guaranteed at all times, with the **student able to choose**

**what information is shared with whom**, based on the concept of selective data disclosure.

- possibility of selective disclosure when sharing information
- improvement of data ownership
- alignment with data protection regulations
- no need to store a lot of personal data
- better compliance
- Others
  - based on current delegation of organizations: issuers remain
  - usable not only for identity information, but any kind of data (e.g. tickets, tracking, ...)
  - independent of big current providers of personal data

### 11.2.2 Threats

Threats category covers external factors and conditions that are expected to have a negative effect on achieving the institution's' objective(s) or making the objective redundant or unachievable.

- Vendor lock-in through standardisation activities conveyed to the ARF process (e.g., SD-JWT)
- Technologically complexities for the implementation, and the need to mature some functionalities (e.g. functionality of revocation).
- The risk of not being able to restore credentials in case of losing wallet, including the need to redo process like losing your physical wallet or, when using backups, security issues and access to backup.
- Existing solutions for sharing data for specific purpose (cf. education), which are not based in the SSI approach or in DLT supported approaches (EBSI).
- Intuitive user wallets: Simplify presentation of complex data to end user in wallet. Difficulty for end users if a lot of VC's are in wallet: structuring VC's in wallet.
- Resistance of current TAO's and TI's to participate and onboard.
- Adaptation of service providers (e.g. secondary schools).

- Gathering information by service providers (DID's).
- Adaptation
  - End users: mass of people
  - Internationally: outside Europa
- Integration with other decentralized infrastructures

## 12 Legal and Regulatory Compliance

Although there are many credential wallets under development and several companies are looking forward this prominent paradigm, the reality is that the legal framework is still not fully mature. Currently we have the eIDAS regulation, mostly focused on traditional PKIs and Certificates. In the next months will be approved the new eIDAS regulation that states that the new identities of the European citizens will be based in the SSI principles and backed by identity wallets.

eIDAS regulation has a direct impact on this project. The core of the current draft is completely aligned with the SSI and the scope of this project. There are however some relevant issues to be defined, such as the identity wallets provider or the possibility for a university to act as a provider of attestations of attributes without the need to formally establish itself as a trust and confidence service provider.

### *Privacy aspects*

The Decentralised Identity paradigm empowers users to "collect" and manage their identity attributes securely through their digital identity wallets, so that they are in control of their own information and can consciously share it with third parties when appropriate and desired, thus ensuring compliance by default with the principles of privacy, confidentiality and the protection of personal data required by the GDPR.

In this way, a secure, digital peer-to-peer channel is established between all participants. It allows attributes to be exchanged privately, as they are encrypted and therefore not even the self-sovereign identity system provider knows what is being exchanged. The credential issuing process becomes more efficient and respectful of user privacy.

In addition, fundamental issues of the proportionality principle and especially data minimisation are addressed by taking advantage of the properties offered by new technology capabilities, as selective disclosure, or under the concept of Zero-Knowledge Proof, e.g. to prove the possession of an academic degree without the need to provide further information.

The university, in its role as issuer, already has a set of personal data about the student (language level, whether the student belongs to the university ...) as well as mechanisms for electronic identification of the student. What the project will allow is that this personal data can be generated in the form of a verifiable credential so that the student can manage it and present it to verifiers.

In any case, in order to share his or her personal information with a verifier, the data subject must give explicit consent to this sharing process, as well as to what kind of data will be shared.

#### *Aspects associated with issuer trustworthiness*

One of the important aspects in the verification process is to ensure that the source of the data, i.e., the issuer of the electronic attestation of the attribute, is an authentic source of the data. The entire EBSI Trusted List scheme is used for this purpose.

EBSI has a distributed registry called TIR (Trusted Issuer Registry) that contains a list of valid issuers for a credential type. Therefore, the verifier, once it receives a credential and validates that the signature is correct, must also validate that the issuer's DID is in the list of registered issuers for the type of credential provided in the submission process.

#### *Aspects relating to the traceability of the actions carried out by the interested party*

It is important to point out that, as it is a distributed system, the issuer has no record of this consultation, thus preventing traceability of where and when a specific attestation issued by a university is used. Therefore, by default the verifier should not share any personal information about a holder with any third party.

In very specific circumstances, there may be exceptions to this rule, e.g., when the verifier requires additional information about the holder. In this case, the user must give explicit consent to share personal information.



In order to guarantee this confidentiality of the use of credentials, it is also necessary to have a revocation mechanism that allows to know the validity of a credential without having to ask the issuer directly. This functionality is also one of the requirements established by the ARF produced by the Toolbox for the reference implementation of identity wallets.

## 12.1 Legal Requirements

### Regulatory Compliance

Legal requirements for educational businesses in Europe vary by country but in accordance with the European Union's strategic framework for the European Education Area [Strategic Framework | European Education Area \(europa.eu\)](#) in particular in the synergies with other relevant initiatives, including the European Research Area and the Bologna Process. However, there are some common legal requirements and considerations that educational businesses should be aware of to ensure cross-border compliance with relevant regulations and standards.

### Intellectual Property Rights

Any deliverables of the project to address issues related to intellectual property rights, including copyright for educational content and materials.

### Accessibility

The EBSI-VECTOR service will need to ensure that educational materials and services are accessible to students with disabilities in accordance with European accessibility laws.

### Equal Treatment

The EBSI-VECTOR service will need to comply with anti-discrimination laws. European countries have strong laws against discrimination based on race, gender, religion, disability, and other factors.

### Recognition of Non-EU Qualifications

The EBSI-VECTOR service will need to be able to handle qualifications that are recognized internationally, ensuring that they are properly transferred in/out Europe to guarantee that students can use them for further studies or employment.

#### Accreditation and Recognition:

The EBSI-VECTOR service will need to ensure that all involved educational institutions and issuers are accredited or recognized by the relevant national or regional authorities. This ensures that issued degrees and certificates have legal value.

#### Data Protection (GDPR)

Europe has strict data protection laws, most notably the General Data Protection Regulation (GDPR). Educational institutions must handle student data in compliance with GDPR, including obtaining informed consent and ensuring data security.

#### Work and Study Visas:

If an educational business admits international students, there's a need to link processes to visa requirements. Students may need student visas to study in Europe legally and sometimes visa issuance is linked to approval for a course participation.

#### Accessibility:

The EBSI-VECTOR service will need to ensure that educational digital certifications and tools are accessible to students with disabilities in accordance with European accessibility laws.

#### Equal Treatment:

The EBSI-VECTOR service will need to ensure compliance with anti-discrimination laws. European countries have strong laws against discrimination based on race, gender, religion, disability, and other factors.

**Recognition of Foreign Qualifications:** If your institution offers qualifications that are recognized internationally, ensure that they are properly recognized within Europe and that students can use them for further studies or employment.

**Consumer Protection:** Be aware of consumer protection laws that apply to educational services. Students have rights as consumers, including the right to clear information about courses and fees.

**Copyright and Intellectual Property:** Respect copyright laws when using and distributing educational materials and ensure that intellectual property rights are upheld.

**Employment and Labor Laws:** Comply with employment and labour laws if you hire staff. This includes contracts, working conditions, and employee rights.

**Health and Safety:** Ensure that your educational facilities meet health and safety standards to protect students and staff.

**Tuition Fees and Financial Transparency:** Be transparent about tuition fees and any additional costs associated with education. Some European countries have regulations on tuition fee levels and financial transparency.

**Language Requirements:** If your courses are conducted in a language other than the official language(s) of the country you are operating in, be aware of language requirements for students and instructors.

**Taxation:** Comply with tax regulations related to educational services and income generated from tuition fees.

It's important to note that legal requirements can vary significantly from one European country to another. Therefore, it's crucial to conduct thorough research and seek legal counsel to ensure compliance with the specific laws and regulations that apply to your educational business in the European region where you operate. Additionally, staying informed about any legislative changes and updates is essential to maintaining legal compliance.

## 13 Conclusion

In conclusion, the integration of blockchain technology within the educational domain represents a groundbreaking step towards a more transparent, secure, and accessible learning environment. It's not just about storing records; it's about creating an unchangeable and trustworthy system that ensures the credibility of each student's achievements.

Moreover, this document shows a shift towards a more connected and inclusive learning ecosystem. With EBSI VECTOR, we're not only safeguarding data; we're fostering a global network where educators and learners can easily connect and collaborate, going beyond geographical barriers. Blockchain technology doesn't just make learning more secure—it opens doors for a future where education is available to everyone, no matter where they are.

Ultimately, this document isn't just a guide; it's a vision for a new way of education. We try to step toward a world where learning is fair, reliable, and for everyone. Through the EBSI we believe we can improve education where every student has an equal chance to learn, grow, and thrive.

## 14 References

- [1] Council of the European Union, «Proposal for a Council Recommendation on a European approach to micro-credentials for lifelong learning and employability - Adoption» 22 May 2022. [Online]. Available: <https://data.consilium.europa.eu/doc/document/ST-9237-2022-INIT/en/pdf>.
- [2] European Commission «Erasmus+ EU programme for education, training, youth and sport. Part D Glossary of terms». Available: <https://erasmus-plus.ec.europa.eu/programme-guide/part-d>.
- [3] CEDEFOP, «Terminology of European education and training policy. Glossary». Available: <https://www.cedefop.europa.eu/en/tools/vet-glossary/glossary>.
- [4] European Commission, «European Education Area. Quality education and training for all». Available: <https://education.ec.europa.eu/education-levels/early-childhood-education-and-care>.
- [5] EBSI – European Blockchain, «EBSI’s success stories». [Online]. Available: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Micro-credentials>.
- [6] MicroHe, «Challenges and Opportunities of Micro-Credentials in Europe» 20 May 2021. Available: <https://microcredentials.eu/wp-content/uploads/sites/20/2021/05/D3.1-Interviews-with-Key-Stakeholders-Decision-Makers-Overall-Summary-Report.pdf>.
- [7] European Parliament and the Council of the European Union, «Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)» 27 April 2016. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.
- [8] European Parliament and the Council of the European Union, «Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC» 23 July 2014. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910>.

[9] European Parliament and the Council of the European Union, «Regulation (EU) 2019/1024 on open data and the re-use of public sector information (recast)» 20 June 2019. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024>.

[10] European Parliament and the Council of the European Union, «Directive 2005/36/EC on the recognition of professional qualifications» 7 September 2005. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0036>.

[11] European Parliament and the Council of the European Union, «Directive 2015/36/EC on the recognition of professional qualifications and Regulation (EU) No 1024/2012 on administrative cooperation through the Internal Market Information System (“the IMI Regulation”) » 20 November 2013. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0055>.

[12] Council of the European Union, «Council Recommendation on the European Qualifications Framework for lifelong learning and repealing the recommendation of the European Parliament and of the Council of 23 April 2008 on the establishment of the European Qualifications Framework for lifelong learning. 2017/C 189/03» 22 May 2017. Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H0615\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H0615(01)).

[13] European Parliament and the Council of the European Union, «Decision (EU) 2018/646 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC» 18 April 2018. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018D0646>.

[14] OpenID, «OpenID Connect For Verifiable Presentations» 17 December 2021. Available: [https://openid.net/specs/openid-connect-4-verifiable-presentations-1\\_0-07.html](https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0-07.html).

[15] European Commission, «The European Digital Identity Wallet Architecture and Reference Framework» 10 February 2023. Available: <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework>.

[16] ISO «ISO-compliant driving licence. Part 5: Mobile driving licence (mDL) application» September 2021. Available: <https://www.iso.org/standard/69084.html>.

- [17] OpenID « OpenID for Verifiable Credential Issuance» 3 February 2023. Available: <https://openid.net/specs/openid-4-verifiable-credential-issuance-1.0.html#name-introduction>.
- [18] European Commission. European Blockchain, «Verifiable Diploma Schema». Available: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+Diploma+Schema>.
- [19] Open Badges, «Elevate your learning with Open Badges» 2022. Available: <https://openbadges.org/>.
- [20] European Commission «A European approach to micro-credentials» June 2022. Available: <https://education.ec.europa.eu/education-levels/higher-education/micro-credentials>.
- [21] European Commission « Strategic Framework». Available: <https://education.ec.europa.eu/about-eea/strategic-framework>.