EBSILUX

Co-funded by the European Union

uni.lu | SnT | LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST | THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry for Digitalisation | Infrachain

Issuing and verifying digital diplomas with the European Blockchain Services Infrastructure

Insight from the EBSILUX project

Interdisciplinary Centre for Security, Reliability and Trust | 29, Avenue John F. Kennedy, L-1855 Luxembourg, Kirchberg | **snt.uni.lu**

uni.lu UNIVERSITÉ DU LUXEMBOURG

Disclaimer

This whitepaper is made by the EBSILUX consortium members for information purposes and for the benefit of the public only.

The authors do not make or purport to make, and hereby disclaim, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the accuracy, adequacy, reliability and completeness of any of the information set out in this whitepaper. The use of this whitepaper is solely at the user's own risk.

In no event shall the authors be liable for any damages, whether direct or indirect, resulting from the use of this whitepaper.

It is not intended to be nor should it be relied upon on as a substitute for legal or other professional advice. Users are solely responsible to obtain any appropriate professional advice relevant to their particular circumstances.

The contents of this publication are the sole responsibility of its authors and the Innovation and Networks Executive Agency of the European Commission is not responsible for any use that may be made of the information it contains.

The EBSILUX project is co-financed by the Connecting Europe Facility of the European Union (Grant Agreement no 2287601) and Luxembourg’s Ministry for Digitalisation.

Issuing and verifying digital diplomas with the European Blockchain Services Infrastructure

Insight from the EBSILUX project

Whitepaper

Management Summary

Although digital has become the new normal in many areas of our daily lives, Europe's educational sector still lags behind when it comes to digitalising administrative processes. European universities heavily rely on manual processes for issuing and verifying university diplomas – often in the form of paper-based documents.

On the side of issuers, paper-based documents often need to be passed around various internal administration units to collect approvals and physical signatures, causing significant inefficiencies. Consequently, students in some cases may be left with a bad experience, as they face significant waiting times until they can enter a subsequent job or study program that requires a final diploma.

On the side of verifiers, verification processes of paper-based or unstructured digital documents such as university diplomas constitute a persistent challenge. In a world where anything can be forged, tampered with or fake-university diplomas have become a veritable problem. Verifiers often struggle with identifying these fraudulent diplomas as, in many cases, they cannot be spotted through simple visual checks. Furthermore, verifying diplomas in the form of unstructured documents is highly inefficient as related processes cannot be automated and need to be conducted manually.

To simplify and enhance the reliability of diploma verification processes, the European Commission now aims to leverage the use of digital wallets and blockchain technology. In this context, the European Blockchain Services Infrastructure (EBSI) develops a technical solution for issuing, storing, and presenting digital diplomas that can be cryptographically verified. Technically, EBSI explores a combination of verifiable credentials – credentials in the form of structured files that are cryptographically signed, digitally verifiable, and more tamper-evident than physical credentials – and the EBSI blockchain – as a 'trusted' registry for providing information to support the verification of credentials.

EBSI's approach is currently prototyped by 18 universities across the European Union (EU) within a 'multi-university' pilot. On the national level of Luxembourg, the EBSILUX project – a collaboration between Luxembourg's Ministry for Digitalisation, Infrachain, Luxembourg Institute of Science and Technology, and the University of Luxembourg – took part in EBSI's multi-university pilot. The EBSILUX project developed a prototype for Luxembourg to evaluate the feasibility of verifiable credentials and blockchain technology for exchanging digital diplomas. The EBSILUX system comprises software components for issuing and verifying diplomas and a web-based digital wallet that allows students to manage and use their verifiable credential-based diplomas.

The EBSI multi-university pilot and the EBSILUX project demonstrate the feasibility of using verifiable credentials and blockchain technology for digitising university diplomas. Several best practices have been identified by the EBSILUX team and other projects of EBSI's multi-university pilot. However, to achieve large-scale adoption on a European level and beyond, EBSI will have to extend its functionalities and align with related initiatives and regulations. The following whitepaper provides insights from EBSI's multi-university pilot and the EBSILUX project, in particular.

Table of Contents

1. Introduction

Although digital has become the new normal in many areas of our daily lives, Europe's educational sector still lags behind in digitalising administrative processes. European universities heavily rely on manual processes for issuing and verifying university diplomas. Moreover, these diplomas are mostly handed out as physical paper-based documents, which often complicates and significantly slows the issuing of diplomas.

University administrations typically need to circulate physical documents among different internal administration units until the diploma can finally be physically signed and issued to the student. This inefficient practice may also cause bad experiences for students who, in some cases, must wait for several months until they receive their final diploma. For some students, these long waiting periods may also prevent them from entering a subsequent study program or a professional career, as some institutions will not admit students until they can provide a final diploma.

For verifiers, paper-based diplomas are even more challenging. In a world where anything can be forged, tampered with copies or fake-university diplomas have become a pivotal challenge for verifiers (Clifton et al., 2018). The problem lies in the difficulty of carrying out a quick and simple authenticity check. Applicants typically submit their diplomas as a scanned PDF document or in some cases even a physical notarised copy of the original diploma. Since diplomas are unstructured documents, verifiers continuously face challenges with the automated processing and verification of prior academic records and, in particular, the identification of fraudulent diplomas. To verify the authenticity of a scan or a physical copy of a diploma, institutions mainly employ simple visual checks for spelling and other errors. Some also make use of QR codes provided on the diploma that allow them to check the integrity of the document. However, these QR codes are not standardised and unavailable on many diplomas. Moreover, universities often lack information that is required for interpreting the diploma. To this end, verifiers, in some cases, also rely on repositories that provide information on acknowledged issuing institutions (e.g., foreign universities), their applied grading schemes, and requirements for obtaining a specific credential. Yet, these repositories do not provide any information on whether a specific diploma has truly been issued by the given institution or in the form it has been submitted. Consequently, current verification processes cannot reliably identify fraudulent or tampered-with diplomas. Furthermore, they are highly inefficient as verification processes need to be conducted manually.

To simplify and enhance the reliability of diploma issuing and verifications processes, the EU now aims to provide digitally verifiable educational credentials. With the Europass platform[1], a first approach to digitising educational and professional credentials has been introduced. Educational institutes can connect to the Europass platform and create digital credentials. Students can store their credentials in a corresponding mobile application and use the platform to share a link to the diploma stored on Europass with another party. However, these centralised platforms leave students with limited control over their documents (Chakroun & Keevy, 2018; Rieger et al., 2021).

As part of its larger strategy on digital identities, the EU now actively invests in providing sufficient user-centric means for the management and digital exchange of citizens' personal information. To this end, the EU explores decentralised digital identities and the use of digital wallets to enable a digital identity management that is similar to our physical identity management of today (Sedlmeir et al., 2021). This concept of decentralised identity management is currently being investigated for multiple use cases, including university diplomas. In particular, the European Blockchain Services Infrastructure (EBSI) – a joint initiative from the European Blockchain Partnership (EBP) and the European Commission (EC) – is currently developing a technical solution for issuing, storing, and presenting digital diplomas that can be cryptographically verified.

[1] https://europa.eu/europass/en

Technically, EBSI makes use of a combination of verifiable credentials – credentials that are cryptographically signed, digitally verifiable, and more tamper evident than physical credentials (W3C, 2022) – and the EBSI blockchain – as a 'trusted' registry. In doing so, EBSI intends to enable cross-border verification of educational credentials, meaning that an educational credential issued in one Member State can be verified by an institution from another Member State. On the national level of Luxembourg, the EBSILUX project[2] – a collaboration between Luxembourg's Ministry for Digitalisation, Infrachain, Luxembourg Institute of Science and Technology, and the University of Luxembourg – is participating in the EBSI diploma multi-university pilot to improve issuing and verification processes of educational credentials in Luxembourg.

This whitepaper describes the current practice of issuing and verifying diplomas at the exemplary case of the University of Luxembourg. It provides the technical foundations and conceptual basis of digital diploma systems based on blockchain and verifiable credentials. Building on these concepts, the whitepaper describes the EBSILUX proof-of-concept (PoC), which was deployed at the University of Luxembourg. Furthermore, this whitepaper summarises best practices and challenges of implementing EBSI's digital diploma solution identified by the EBSI community.

[2] The EBSILUX project is co-financed by the Connecting Europe Facility of the European Union (Grant Agreement no 2287601) and Luxembourg's Ministry for Digitalisation. Website: https://ebsilux.lu/

2. Background

2.1. Current Diploma Issuing and Verification Processes

When it comes to educational credentials, universities are key entities, as they act as both – issuers and verifiers – where they must handle thousands of diplomas per year. Universities thus represent an interesting sandbox for digitising educational credentials. This section provides a simplified description of the current practices for issuing and verifying diplomas at the University of Luxembourg.

As soon as students complete all modules required for graduation, the University of Luxembourg typically triggers the issuance of a diploma. To this end, students typically receive an attestation of successful completion of all modules and eligibility for graduation. The student administration asks the students to verify the attestation and confirm that all grades are listed correctly. Upon confirmation, the student administration starts the issuing process of the diploma and diploma supplement. In doing so, it extracts the records from the student management system and sends it to the faculty for cross-checking. In case adjustments are necessary, they are included in the student management system. In case no or no further adjustments are required, the student administration prints the physical paper-based diploma and diploma supplement. Afterwards, the student administration manages the physical signature of the printed documents. Once per year, the university hands over the diplomas to the students at a graduation ceremony.

Within the application and admission process, applicants send a scan of their diploma and diploma supplement to the student administration by uploading it within the service portal or via email. Upon receipt, the student administration verifies whether the documents follow the Bologna regulation. Depending on whether an applicant received a diploma that is compliant with the EU's Bologna regulation, or the diploma follows a different educational framework, the verification process at the University of Luxembourg may differ.

In the case of Bologna-compliant documents, the student administration verifies the dates indicated on the diploma and checks the scans of the diploma and the diploma supplement for spelling and other errors. If the student administration cannot spot any errors within the diploma and diploma supplement, the admission process continues. These checks are solely conducted on a visual basis with no technical support available. Thus, these checks are often time-consuming and their thoroughness is often restricted by the student administration office's capacities.

In the case that the diploma and diploma supplement do not comply with the Bologna framework, the student administration undertakes additional steps for verifying these documents. The student administration checks the diploma for the date of issuance as well as spelling or other errors. In addition, the student administration office instructs the student to check the diploma with Luxembourg's Ministry of Higher Education and Research (MESR). For verifying the diploma, the MESR checks the diploma against a repository (Anabin)[3] that provides information on accredited universities and their underlying grading schemes. It then sends a validation or a refusal letter back to the student. The applicant forwards the validation or the refusal letter to the student administration, who confirms the applicant's final acceptance or rejection.

2.2. Decentralised Digital Identity Management and Verifiable Credentials

With the increasing use of digital services, identifying individuals online becomes more and more important. Since the invention of the internet, digitally identifying individuals and verifying specific identity attributes, e.g., age or educational degrees, remains a pertinent challenge (Chaum, 1985; Sedlmeir et al., 2021). To date, identity-related information is mainly locked in centralised databases with limited opportunities for individuals to control their data. In recent years, the idea of decentralised digital identity management has evolved as a response to challenges of existing mainly centralised digital identity management systems, such as unauthorised processing of

[3] https://anabin.kmk.org/anabin.html

personal data or identity theft. Decentralised digital identities are intended to provide subjects with enhanced control, privacy, and portability of their digital identities (Allen, 2016).

On a technical level, the central building blocks of any decentralised digital identity solution are digital certificates. One emerging standard for modelling and exchanging machine-verifiable digital credentials for such certificates is verifiable credentials (VC), as defined by the World Wide Web Consortium (W3C, 2022). A VC is a digitally signed object containing one or multiple claims of attributes about a subject. These claims can be selectively disclosed or presented in the form of zero-knowledge-proofs (ZKP) (Goldreich & Oren, 1994). ZKPs allow a subject to prove an identity claim to another entity without disclosing any additional information than required. For instance, one can prove being older than 18 without providing any further information about the current age or the date of birth.

VCs are not limited to natural persons, and thus subjects can be an individual, an organisation or any other legal entity, as well as a physical or digital object. VCs can be either self-attested – i.e., the credential's subject creates and digitally signs the credential and attributes about itself, or third-party attested. As in the case of diplomas, third-party attestations are VCs whose attributes are certified and digitally signed by an entity other than the subject.

These VCs can be managed by users with the help of so-called digital wallets (Sedlmeir et al., 2021). A digital wallet is a mobile or web-based software application enabling users to manage and store cryptographic keys as well as verifiable credentials and to execute all necessary interactions with other entities within a decentralised digital identity management system. These interactions include, among others, signing messages, authenticating other entities, receiving VCs and presenting a VC in the form of a verifiable presentation.

To technically enable communication between entities, many digital wallets rely on decentralised identifiers (DID) (W3C, 2021). DIDs are unique universal identifiers that can be used to identify an entity and establish channels for secure communication. DIDs are typically linked to DID documents which contain cryptographic information such as public keys and metadata to authenticate the controller of a DID and establish secure communication channels with the DID controller. These channels can be used for further communication with the corresponding entity (DID controller). However, the use of a single DID for multiple connections may cause privacy risks, as it enables the correlation of activities. To prevent such correlation, users can generate a new pseudonymous DID when establishing a new connection.

In general, along the life-cycle of VCs, three roles exist which communicate and exchange credentials in secure bilateral communications[4] (Mühle et al., 2018). *Issuers* certify certain attributes and issue a VC to a holder (e.g., a university that issues a bachelor's degree to a student). *Holders* store and control the VCs to present them to another entity that aims to verify a specific identity attribute or certificate. For university diplomas, holders are the students who obtain the diploma, and thus the holders are typically the subject of the VC[5]. *Verifiers* request a verifiable presentation (VP) from holders to validate the possession of a VC that certifies specific attributes (e.g., educational or public/private institutions which aim to verify a person's educational degree as part of an application). In doing so, verifiers check the credential's signature, date of expiration, and state of revocation. For this, verifiers typically rely on public registries which provide additional information that allow for verifying a VC's issuer and state of revocation. Here, many current SSI implementations leverage blockchain technology as a distributed database.

[4] To technically enable secure bilateral communications SSI implementations typically rely on protocols like the DIDComm protocol, or OpenID connect that lever public-private key cryptography to establish encrypted bilateral communication channels.

[5] Note that in some cases holders are not always the subject of the VCs, e.g., parents (holder) that manage the credentials of their children (subject).

2.3. The Role of Blockchain Technology for Decentralised Identity Management

Many decentralised digital identity management implementations, such as Canada's Verifiable Organization Network (VON) or the European Self-Sovereign Identity Framework, use blockchain technology as 'trusted' registries. These registries contain information required for verifying a VC's issuer and authenticity, as well as to ensure standardisation among credentials. Using blockchain for these registries is interesting as it enables transparent, tamper-resistant, and distributed operation (Hoess et al., 2022).

Blockchain-based registries typically provide three core functionalities. First, the blockchain serves as a registry for issuers and provides cryptographic material (e.g., DIDs or issuers' signing keys) that can be used to verify the digital signature and authenticity of a VC. Second, issuers can make use of a blockchain to publish privacy-preserving revocation lists. Third, many initiatives also leverage blockchain as a supporting means for ensuring interoperability. More specifically, issuers and standardisation bodies can use a blockchain-based registry to publish credential schemas that provide information on the attributes contained in a specific type of VC.

Concerning decentralised digital identity management, it is essential also to note potential risks that may arise when using blockchain. In particular, the replicated and tamper-resistant storage of information on a blockchain may infringe users' privacy and contradict with the EU's General Data Protection Regulation (GDPR) – especially its right to erasure (Rieger et al., 2019). More crucially, the transparent storage of personally identifiable information on a blockchain might allow for traceability and profiling of users. Thus, decentralised identity management systems need to ensure that blockchains do not store any information related to natural persons – for instance their DIDs or verifiable credentials itself (Rieger et al., 2021).

2.4. The European Blockchain Services Infrastructure and Multi-University Pilot

In 2018, the EU Member States, Norway, and Liechtenstein formed the European Blockchain Partnership to jointly explore the prospects of blockchain technology for Europe. To this end, the EBP has begun developing a European Blockchain Services Infrastructure – a blockchain network with nodes distributed among all EU Member States, Norway, and Liechtenstein. EBSI is intended to provide a technical infrastructure for building interoperable and trustworthy cross-border (public) services.

EBSI has a particular focus on decentralised identity management. In this context, EBSI develops the European Self-Sovereign Identity Framework (ESSIF), which serves as a generic building block for all of EBSI's identity-related use cases. The framework defines a set of roles and rules for using EBSI as a 'trusted' registry. Moreover, it provides technical specifications for the development of EBSI-compliant digital wallets and the issuance, exchange, and verification of identity-related credentials. ESSIF builds on relevant standards such as W3C's VC model and the DID standard.

EBSI's most prominent and advanced use case is digital university diplomas. The use case is currently being piloted at 18 European universities from 15 different countries. This 'multi-university pilot' serves as a sandbox for testing EBSI and ESSIF. Furthermore, the multi-university pilot allows to test the interoperability of EBSI-based applications among various issuers, holders, verifiers, and wallet providers on a cross-border level.

3. EBSILUX Prototype

To evaluate the feasibility of VCs and blockchain technology for the exchange of digital diplomas, the EBSILUX consortium took part in EBSI's multi-university pilot and developed a prototype for Luxembourg. This section illustrates the technical architecture of the EBSILUX prototype and the resulting workflows for the University of Luxembourg (issuer), its students (holders), and verifiers when using VC-based diplomas.

3.1. Conceptual Architecture

The EBSILUX system comprises software components for all three entities in the ESSIF framework: issuer, holder, and verifier. For each entity, the components are structured in two layers: a front-end layer and an integration layer. Furthermore, the overall architecture relies on EBSI as a 'trusted' registry.

3.1.1. Issuer Components

The university runs a set of 4 components that support the generation and issuance of diplomas as VCs. Members of the student administration can interact with the EBSILUX system through an *Issuer Frontend.* This front-end is connected to an issuer integration layer which comprises a *Backend for Issuer Frontend* component, a *Diploma Data Connector,* and an *Identity Management Module*[6]. The *Backend for Issuer Frontend* coordinates all workflows initiated via the *Issuer Frontend*. Moreover, it triggers the other components on the integration layer. To reduce manual effort and potential mistakes, the *Diploma Data Connector* automatically retrieves all information required for creating digital diplomas from the university's system for student data management. The *Diploma Data Connector* transmits this information to the Identity Management Module via the *Backend for Issuer Frontend* to create a digital diploma. The *Identity Management Module* provides all cryptographic tools allowing the university to create DIDs, establish secure communication channels, as well as to generate and sign digital diplomas in the form of VCs. Furthermore, the *Identity Management Module* can connect to EBSI to publish its DIDs and to view or store credential schemas[7] and definitions[8] that act as a blueprint for generating credentials.

3.1.2. Holder Components

In order to access and make use of their VC-based diplomas, students have access to web-based digital wallets. These wallets comprise two layers, a *Wallet Frontend* and a wallet integration layer. The *Wallet Frontend* is an interface which allows students to interact with the EBSILUX system and manage their VCs. The *Wallet Frontend* provides students access to the wallet integration layer required for generating DIDs, establishing secure connections, requesting, storing, and presenting VCs.

The wallet integration layer includes a *Backend for Wallet Frontend* and an *Identity Management Module*. The *Backend for Wallet Frontend* processes the user input and incoming messages and triggers the *Identity Management Module.* The *Identity Management Module* provides cryptographic tools required for receiving VCs and generating VPs. Received VCs can be securely stored in the local storage of the browser or on the local device and presented later to a verifier. Furthermore, the holder's *Identity Management Module* can connect to EBSI to view and verify an issuer's or verifier's DID and related meta-information (DID documents).

Although not within the scope of the EBSILUX prototype, holders may alternatively use a mobile wallet comprising all wallet components which can be downloaded and run locally on a smartphone.

3.1.3. Verifier Components

The verifier system can be integrated by any institution that aims to verify EBSILUX digital diplomas. Similar to the issuer and holder system, the verifier system consists of two layers: the frontend layer and the integration layer.

The verifier integration layer includes a *Backend for Verifier Frontend* component, an *Identity Management Module* and a *Verifier API.* The *Backend for Verifier Frontend* coordinates all verifier workflows and related components. The *Verifier API* serves as an interface for connecting the EBSILUX system to existing recruitment tools. The *Verifier API*

[6] The EBISLUX *Identity Management Modules* rely on the open-source frameworks provided by walt.ID (https://walt.id/). We gratefully acknowledge walt.ID's advice and support in using their frameworks.

[7] A credential schema is a standardised document that provides the structure, data model, and format of a specific type of credential.

[8] A credential definition is a credential schema enhanced by a specific issuer's meta-data such as DID and signature. It thus provides information on how credentials of a specific issuers will look like.

provides information on required proof requests as well as verification processes which can be executed via the *Identity Management Module*.

To this end, the *Identity Management Module* allows the verifier to establish secure communication channels with the diploma holders, generate proof requests, and provides cryptographic tools to verify a VC-based diploma. To ensure reliable verification, the *Identity Management Module* can connect to EBSI and verify additional information provided on-chain such as trusted issuer information or a diploma's state of revocation. Furthermore, the *Identity Management Module* can send required data to the verifier back-end system for further processing.

A complementary *Verifier Frontend* facilitates the interaction with the system and displays the current state and the final result of a specific verification processes.

3.1.4. Trusted Registry

EBSI serves as the 'trusted' registry for the EBSILUX system. More specifically, EBSI comprises three different registries: a *Trusted Issuer Registry*, a *Trusted Accreditation Organisation Registry*, and a *Trusted Schemas Registry*. The *Trusted Issuer Registry* provides all information required for authenticating an accredited issuer (e.g., university) and verifying related VCs. This information includes issuer DIDs, public keys, their legal names, and accreditations. Issuers can receive an accreditation/authorisation to issue diplomas via a Trusted Accreditation Organisation. To allow for traceability of accreditations, EBSI maintains a *Trusted Accreditation Organisation Registry* which indicates the organisations that are eligible to authorise institutions as trusted issuers (e.g., the national ministry providing accreditation to universities in the country). To this end, the *Trusted Accreditation Organisation Registry* contains similar information as the *Trusted Issuer Registry.* Furthermore, issuers can make use of existing or publish new credentials schemas and definitions on EBSI's *Trusted Schemas Registry.* The *Trusted Schemas Registry* provides verifiers with meta-information required for understanding and verifying credential attributes.

Although not implemented yet, EBSI further foresees including a *Revocation Registry* which will allow for generation and verification of proofs of revocation for digital diplomas. To access information on these EBSI registries, EBSILUX uses the *EBSI connector.* The *EBSI connector* allows issuers, holders, and verifiers to connect to EBSI and read and/or write information on the ledger.

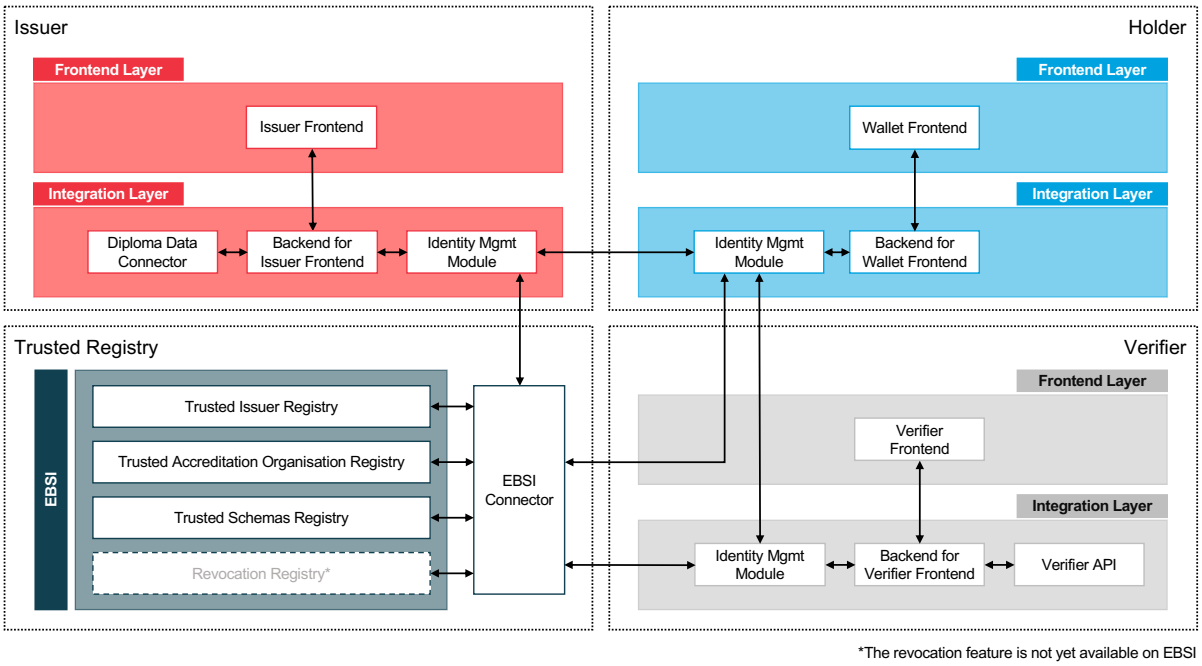

Figure 1. EBSILUX technical architecture

3.2. Issuance and Verification of Verifiable Credentials

3.2.1. Issuance of a verifiable credential

Analogous to today's physical diploma issuance, the issuance of a VC-based diploma through the EBSILUX system starts with the student administration that collects and checks all diploma relevant information. In addition to the physical diploma, the student administration transfers the diploma and diploma supplement into a VC with the help of the Issuer Frontend. When generating the VC, the university makes use of standardised credential schemas that can be accessed through EBSI's Trusted Schemas Registry. In case no schema is available on EBSI, the university creates a new schema and publishes it on EBSI. The university digitally signs the credential and notifies the student that a VC-based version of the diploma is now available.

To receive and store their digital diploma, students must setup an account for a web-based EBSILUX wallet. After successfully setting up their digital wallet, students can request the VC-based diploma via the university's student portal. To this end, students log in to the university's student portal and use the wallet to request their diploma VC by clicking on a personalised link or scanning a personalised QR-code with their mobile phones. The link or QR-code triggers the web-based or mobile wallet to connect and establish a secure connection between the student's wallet and the university and to request the issuance of a VC.

As soon as a new connection has been established, the university issues the diploma VC to the student's wallet. The student receives a notification and a credential offer that displays the credential which will be issued to the wallet. The student can review the VC to check that all information included in the credential is correct. If all information is correct, the student accepts the VC and stores the credential. Otherwise, students can decline a credential and request an updated VC.

3.2.2. Verification of a verifiable credential

Verifiers can make use of diploma VCs to enhance the reliability and efficiency when screening applications. To this end, verifiers can complement their recruitment portals with additional features like a link or a QR code that allow students to present their diplomas digitally in the form of a VP. When clicking a link or scanning a QR code, the student receives a request to provide a VP of a diploma VC. Students can open this request with their web-based or mobile wallet and review the set of diploma attributes that is requested by the verifier. In case the student agrees to share this information with the verifier, the wallet derives a VP from the diploma VC and sends it to the verifier.

The verifier receives the VP and verifies the corresponding VC's schema, the attribute values, and university's digital signature included in the VP. To verify the signature, the verifier makes use of the issuer information provided in EBSI's Trusted Issuer Registry and checks whether the signature was derived from a private key that matches the issuer's public key. If needed, the verifier can additionally verify the VC's state of revocation based on the information provided on the EBSI ledger (Revocation Registry)[9]. The result of the verification process can be accessed by the verifying institution's responsible employees through the verifier frontend.

[9] By the time of writing this whitepaper, the revocation feature was still under development and has not been available on EBSI.

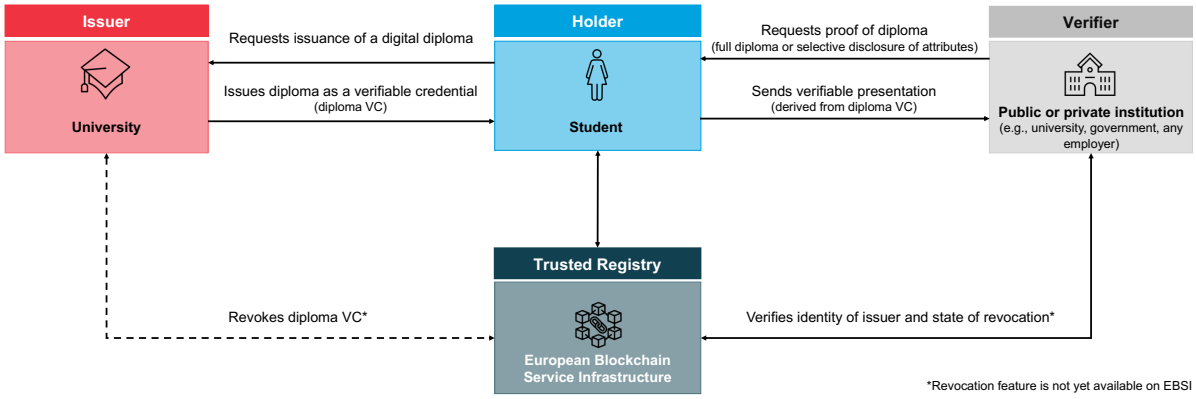

Figure 2. Roles and activities in the EBSI-based diploma system

4. Evaluation – Best Practices and Prevailing Challenges

The EBSI multi-university pilot and the EBSILUX project demonstrate the opportunities of using VCs and blockchain technology for digitising educational credentials. Several best practices (BPs) have been identified by the EBSILUX team and other project teams from the EBSI multi-university pilot. At the same time, piloting occurred in a pre-production environment and on a national level. Hence, multiple challenges remain that need to be overcome to achieve large-scale adoption on a European level and beyond. This section summarises the best practices from the multi-university pilot and the prevailing challenges of EBSI.

4.1. Best Practices

Along the multi-university pilot, the EBSI community has identified multiple best practices for developing and operating a distributed digital infrastructure for cross-border services and use cases such as digital diplomas.

Firstly, the piloting universities did not approach the multi-university pilot as a purely technical project related to the development of digital diplomas. Instead, they viewed EBSI as a vehicle to **establish viable governance (BP1)** frameworks for VC-based diplomas. They were particularly concerned with how to ensure trust in digital diplomas and avoid issuance of diplomas by fake universities. To this end, EBSI developed an accreditation scheme for trusted issuers. This accreditation scheme prescribed that only universities that have been authorised by the corresponding national public authority (e.g., the Ministry responsible for higher education) can register their DIDs and public keys to the EBSI ledger for public verifiability. Thereby, issuance of diplomas by fake universities could be prevented.

Furthermore, the EBP established a clear **distribution of responsibilities (BP2)** between infrastructure providers, piloting universities, and wallet providers. More specifically, EBSI's technical scope is clearly defined as a decentralised infrastructure and corresponding APIs for trusted registries, while other aspects remain out of the responsibility for EBSI. This clearly defined scope of EBSI allows to keep the project manageable. Accordingly, universities themselves are responsible for the local integration with EBSI. In a similar vein, the EBSI team considers the development of digital wallets to be out of scope of EBSI itself. While EBSI provides overall requirements and frameworks for EBSI-compliant digital wallets, the development of wallets remains the responsibility of wallet providers in close partnership with universities and national governments. Establishing such **collaborations** between the different stakeholders enabled the different projects to leverage different expertise and develop more efficient solutions.

Exploring EBSI and related implementation strategies in **a limited number of small-scale projects (BP3)** facilitated manageability of the multi-university pilot. In particular, the limited number of participants allowed the EBSI team to maintain a strong and close relationship with

piloting institutions like universities and digital wallet providers. Piloting institutions were able to reach out to the EBSI team to discuss issues and identify solutions that help to overcome prevailing challenges and successfully deploy their prototypes while ensuring conformance with EBSI and ESSIF. Although EBSI focused on relatively small-scale projects, **involving all relevant stakeholders** and **gaining political support** from the beginning was important. In doing so, the EBSI team could ensure that decisions on the governance and technical implementation were made in consultation with the concerned stakeholders and their respective needs.

Building upon existing data models (BP4), such as the European Learning Model (ELM), which is also used in Europass, helped to speed up the prototyping process. In this sense, negotiations for agreeing on a new standard or data format could be avoided and interoperability among projects could be enhanced. For instance, in an interoperability test between Luxembourg and Germany both projects could successfully verify each other's VC-based diplomas. Furthermore, selecting ELM allowed universities to rely on existing technical components that retrieve and process diploma data, as the required data for a diploma remained the same. However, while ELM provides an overarching framework of diploma attributes, the selection of attributes still differs across projects. **Agreeing on a single schema** may support interoperability among pilots in the future and facilitate the automated processing and interpretation of credentials.

Although the ELM could be re-used, the multi-university pilot had to build knowledge of implementing new technologies like blockchain or emerging specifications such as the W3C's standard for VCs. **Sharing knowledge between the projects (BP5)** helped to increase technical and conceptual understanding of EBSI, VC-based diplomas and digital wallets. Regular knowledge sharing and feedback sessions also allowed the EBSI team to identify shortcomings of EBSI and the need for improvements. This agile approach helped to constantly improve EBSI and ESSIF as well as to accommodate the requirements in EBSI and ESSIF. These regular exchanges also enabled the EBSI team and the multi-university pilot to develop a common vision of the EBSI diploma use case and its future.

Concerning the implementation of the multi-university pilot, ensuring students' privacy is a key objective of EBSI. To this end, EBSI performed a privacy risk assessment and critically reflected on the needs for processing students' personally identifiable information on the ledger. This investigation revealed that a reliable issuing and verification of verifiable diplomas does not require storing any personal identifiable information such as natural persons DIDs or verifiable credentials – even in hashed form – on EBSI. Consequently, similar to other projects, EBSI opted for a model that **only stores information of legal entities (BP6)** – i.e., diploma issuers and accreditation organisations – on the ledger. This practice helps EBSI to ensure students' privacy and be compliant with related regulations such as EU's General Data Protection Regulation.

4.2. Prevailing Challenges

The multi-university pilot provides an important first step for the adoption of EBSI and VC-based diplomas within Europe. However, along the pilot, the EBSI community discovered several challenges that will need to be overcome for bringing EBSI into production and reaching large-scale adoption.

To date, EBSI's features are still limited. To fully exploit the potential of EBSI, additional technical features need to be implemented. In particular, ensuring the integrity and validity of digital university diplomas requires features for a **privacy-preserving revocation** of credentials. Likewise, the availability and functionalities of EBSI-compliant digital wallets is still limited. Therefore, wallet providers will have to align with EBSI's upcoming features, to make them available for issuer, holder, and verifier.

Reaching a critical mass of issuers and verifiers will be essential to realize the potential of digital diplomas. However, implementation of EBSI-based issuer and verifier tools currently requires high integration efforts and, therefore, constitutes a current barrier for organisations to adopt EBSI. Consequently, EBSI is currently investigating opportunities for providing **easy to integrate and user-friendly toolkits** to reduce barriers of entry for issuers and verifiers.

Such tooling would allow a multitude of organisations – be it a small family company or a well-established large cooperation – to quickly make use of EBSI-compliant digital diplomas.

Another essential aspect for large scale adoption of EBSI-compliant digital diplomas is interoperability among the different projects. Yet, these multi-university pilot projects are not fully interoperable. In particular, they differ based on their implementation of the user workflows and interactions between digital wallets and issuer as well as verifier tools. **Unification among workflows and interoperability among EBSI-conformant digital wallets** will be essential to allow for a seamless use of digital diplomas across Europe. Here, the upcoming European Digital Identity Wallet might step in as a generic building block to allow for unification of workflows and enabling a seamless user experience along the different projects.

Consequently, ensuring **compliance between EBSI and the upcoming European Digital Identity Wallet** will be essential. In this context, being recognised as a registry of trust sources within the eIDAS v2 reference architecture will be a pivotal aspect for the future of EBS in the context of digital identities. Therefore, EBSI will have to align with the requirements of the European Digital Identity Wallet toolbox and the related registries of trust sources. This, for instance, implies certification of EBSI's node operators according to the required security management guidelines. Moreover, issuer and verifier toolkits should be aligned with eIDAS' technical specifications for electronic attestation of attributes providers (i.e., diploma issuers) and relying parties (i.e., diploma verifiers). In doing so, interoperability between EBSI's diploma use case and similar projects in domains apart from educational credentials could be ensured.

Overall, the development of new EBSI features and advancement of digital wallets as well as issuer and verifier tools will demand extensive resources. However, to date financing is mainly provided on a grant project basis. A **stable long-term financing** model between the EC and the member states, for instance for node operation, will be essential to secure EBSI's long-term success and to ensure availability of resources for development and maintenance of EBSI's cross-border services. Open source frameworks for digital wallets as well as issuer and verifier tools developed by the European Commission may lower the size of this funding model as well as barriers to make use of EBSI-based diplomas. Such open source tools may also mitigate an uneven distribution of cost and benefits between issuers, holders, verifiers. Moreover, the provisioning of an open-source digital wallet could prevent future business models that might harm holders by charging high user fees, or monetising data stored or presented with a wallet.

The transition towards digital diplomas is also challenging form a legal perspective. Although according to the eIDAS regulation, a diploma-VC, which is an electronic document, "shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form" (Domingo, 2020). However, this does not automatically imply that a VC will be legally recognised for a specific purpose. In many countries, there is no legal basis today for digital credentials like VC-based diplomas or other electronically signed documents. Instead, many countries still insist on physical documents with a physical seal, stamp, or a wet-ink signature. Consequently, European and national **legislations will need to be revised** and updated to ensure that digital diplomas will be fully legally recognised and can ultimately be in everyday life.

All in all, EBSI is still in its early stages and only limited knowledge and experience is available regarding the implementation and productive use of EBSI services. To foster the adoption of EBSI services, the EBSI community will actively need to **collect and share their experiences** with new EBSI adopters to enable a more seamless deployment and use of EBSI services. For the diploma use case, this will also demand creating awareness on the university, verifier, and student side to encourage all relevant stakeholders to make use of EBSI.

5. Conclusion and Outlook

Europe's educational sector still lacks behind when it comes to digitalisation of administrative processes. European universities heavily rely on manual processes for issuing and verifying university diplomas. These diplomas are mostly handed out as physical paper-based documents, which often complicates issuing and verification processes, and also opens a window for fraudulent diplomas. Fake or tampered with diplomas have become a veritable problem. Verifiers often cannot reliably spot fraudulent diplomas through simple manual visual checks on mostly paper-based diplomas. To enable more efficient and reliable verification processes of diplomas, EBSI explores and evaluates the feasibility of digital wallets and blockchain technology.

Within a multi-university pilot, EBSI and various European universities developed prototypes that allow issuers, holders, and verifiers to exchange digital diplomas in the form of verifiable credentials. As Luxembourgish representatives, the EBSILUX consortium took part in this multi-university pilot and developed a prototypical solution for Luxembourg to evaluate this concept on a national level.

EBSI's multi-university pilot and the EBSILUX prototype demonstrate the feasibility of using verifiable credentials and blockchain technology as a basis for digitally verifiable diplomas. The prototype allows the University of Luxembourg to automatically issue diplomas in the form of a verifiable credential. University students can store and make use of their verifiable credentials via a web-based EBSILUX wallet and share a verifiable presentation of their diploma credential with a verifier. Verifiers can digitally verify the authenticity of the credential via the EBSILUX verifier system and with the help of information stored on EBSI's trusted registries.

Overall, the EBSILUX system demonstrates how digital wallets and blockchain can help to increase the efficiency and reliability of diploma issuing and verification processes. Yet, several challenges remain to achieve EU-wide adoption. As an initial step, EBSI is currently developing additional features such as revocation, that will be essential to ensure reliable verification of digital diplomas. Furthermore, EBSI plans to bring its diploma use cases into production and make it available to university students across Europe. In doing so, ensuring interoperability among the various EBSI projects will be a crucial aspect and critical step for enabling large-scale evaluations of the solutions.

In the future, important steps for the adaption of EBSI's solution will be the availability and interoperability of digital wallets. Ensuring interoperability between EBSI and the upcoming revised eIDAS regulation as well as the upcoming European Digital Identity Wallets may help to scale EBSI's solution and build the bridge between different digital diploma solutions, such as EBSI and Europass, and other use cases that will require a digital wallet. Moreover, large-scale adoption of EBSI-compliant diplomas will require simple verifier tools that can be easily deployed in various institution.

Based on the insights form the EBSI multi-university pilot, the EBSI community is planning to undertake active steps to address these problems and extend EBSI's capabilities to support widespread adoption of EBSI across Europe.

6. Bibliography

Allen, C. (2016). *The Path to Self-Sovereign Identity*. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Chakroun, B., & Keevy, J. (2018). *Digital credentialing: Implications for the recognition of learning across borders; 2018*. 45.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, *28*(10), 1030–1044.

Clifton, H., Chapman, M., & Cox, S. (2018). *"Staggering" trade in fake degrees revealed*. https://www.bbc.com/news/uk-42579634

Domingo, I. A. (2020). *SSI eIDAS Legal Report—How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market* (p. 150). https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

Goldreich, O., & Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, *7*(1), 1–32. https://doi.org/10.1007/BF00195207

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or Without Blockchain? Towards a Decentralized, SSI-based eRoaming Architecture. *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., & Urbach, N. (2019). Building a Blockchain Application that Complies with the EU General Data Protection Regulation. *MIS Quarterly Executive*, *18*(4), 263–279. https://doi.org/10.17705/2msqe.00020

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2021). The privacy challenge in the race for digital vaccination certificates. *Med*, *2*(6), 633–634. https://doi.org/10.1016/j.medj.2021.04.018

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, *63*(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

W3C. (2021). *Decentralized Identifiers (DIDs) v1.0*. https://www.w3.org/TR/did-core/

W3C. (2022). *Verifiable Credentials Data Model v1.1*. W3C. https://www.w3.org/TR/vc-data-model/

Imprint

Publisher:
Ministry for Digitalisation, Luxembourg on behalf of the EBSILUX consortium members

Authors:
The EBSILUX consortium members composed of:
- Ministry for Digitalisation, Luxembourg
- University of Luxembourg
- Luxembourg Institute of Science and Technology
- Infrachain ASBL

Publication Date:
November 2022

Design:
Ministry for Digitalisation, Luxembourg on behalf of the EBSILUX consortium members
Cover Photos: pickup / stock.adobe.com n° 197844330
Inna / stock.adobe.com n° 541411807

Recommended citation:
Hoess, A., Howard Maclennan, D., Rieger, A., Ermolaev, E., Fridgen, G., and Roth, T. Issuing and verifying digital diplomas with the European Blockchain Service Infrastructure – Insight from the EBSILUX project. Ministry for Digitalisation, Luxembourg, ed.

For more information:
Ministry for Digitalisation, Luxembourg
4, rue de la Congrégation
L-1352 Luxembourg
Luxembourg

EBSILUX Publication Office
https://ebsilux.lu/news/press-room/

The publication is distributed free of charge and is not intended for sale.

Visit us at

https://ebsilux.lu/

https://www.linkedin.com/company/ebsilux

https://twitter.com/EBSILUX_Project