SSI EduWallets

Zwischenbericht | Call 17 | Projekt ID 6344

Inhalt

1 Einleitung

The SSI (Self-Sovereign Identity) EduWallets project aims to revolutionize the way we manage our personal information and privacy in the digital age of the Web 3.0. By harnessing the power of decentralized and distributed technologies such as blockchain and self-sovereign identity, this project seeks to give users complete control over their data, freeing it from the silos of third-party storage and therefore build a more transparent and trustworthy digital ecosystem.

The project focuses on creating a user management system that allows users which has an identity credential in their wallet, which can be presented to different platforms for access. This approach, based on W3C DIDs (Descentralized identifiers) & VCs (Verifiable credentials) and ESSIF (European Self Sovereign Identity Framework) standards, ensures interoperability and security between different systems within the European Union.

The platforms that implement this system can issue a certificate for the users upon course completion, which can be stored in their wallet for future verification. By digitally signing each certificate and ensuring standardization of formats, the project seeks to end the problems of forgery and inconsistency that plague traditional certificate systems.

The incorporation of the SSI wallet to a platform follows the following process:

1. The SSI wallet kit is incorporated in the defined platform to allow the onboarding of SSI wallet users.
2. The platform act as an issuer and verifier, the first step is to set a DID (Descentralized Identifer) for the issuer, within the EBSI ecosystem its needed that an TAO (Trusted Accreditation Organisations) allow the platform “issuer” as a Trusted Issuer to issue Verified credentials to the users.
3. When the TAO allow the issuer to issue verifiable credentials the accreditation is stored on the ebsi ledger and can be verified later, also the DID generated by the issuer is stored on the ledger.
4. The TAO also allow the platform to act as a trusted verifier to verify any VC that the user shares with it.
5. Once the user wants a VC from the completed course, the platform will issue a VC with the DID of the user,the DID of the platform, the sign of the issuer and the other fields that compose the VC.

6. Through the protocols OIDC/SIOP the issuer exchange the VC with the user wallet, and then the user acepts of reject the VC
7. Once the user accept the VC, the user hold in its wallet this credential that can be verify by other party using the EBSI ledger.

2 Status der Arbeitspakete

2.1 Arbeitspaket 1 - <Projektstart>

- **Start of the project**
- **Assessment of the project** to begin planning & define the tasks to be carried out.
- **Development of a website to inform about the project.**
- **Creation of a blog** to summarize the creation process/objectives and the phases of the project.

2.2 Arbeitspaket 2 - <Anforderungsanalyse, Konzept & Design>

- **Research about the Self-Sovereign Identity (SSI) paradigm in the context of web technologies.** How it works, Why to use SSI paradigm, advantages over the issuance of verifiable credentials.
- **Research about European Digital Identity wallets (EUDI) programme** and their current status & use cases for them. Future of the conformant wallets with the EU standards, review the scope of the project to unify different daily tasks in a single app following a defined standards from the EU, focus on the issuance of verifiable diplomas to replace current titles.
- **Research about the European Self-Sovereign Identity Framework (ESSIF).** How ESSIF works, how to be conformant with the framework, which advantages ESSIF has, review the interoperability with other systems that follow this framework, privacy concerns.
- **Research about European Blockchain Service Infrastructure (EBSI) ecosystem.** How EBSI is implemented, which standards EBSI follows, how blockchain or Distributed Ledger Technologies (DLT) works out, how to be compliant with EBSI ecosystem, current status of EBSI, how EBSI is integrated to be used in a SSI wallets, why to use the EBSI ecosystem.

- **Research about the Decentralized Identifiers (DIDs) & Verifiable Credentials (VCs).** Standards that they follow from the W3C, how DIDs are generated, which different methods we have to create a DID, how DIDs are stored and where, why the DIDs are essential in SSI, how DIDs can be resolved, which information the DID contains, which types of VCs exist, which standards the VCs follow, how VCs are generated, how VCs are secure & how VCs are signed to be tamper-proof, where VCs are stored, how the VCs are shared.
- **Research about the current wallets** that are compliant with ESSIF/EBSI ecosystem to implement a solution that leverages on them.
- **Research about the verifiable credential schemas** that exist or are defined by an authority, which types are defined in EBSI ecosystem, which fields are mandatory, how to use schemas to verify that the verifiable credentials are compliant with the chosen schema.
- **Research about pre-build wallet solutions** that follow ESSIF/EBSI ecosystem to make a test pilot and check if it is possible to leverage on them.
- **Research the implementation of the SSI wallet** that allow verifiable credentials issuance, planning & design the architecture of the implementation.

The achievement on this work package was the knowledge how the new paradigm of web 3.0 fits in the current context to the status of the EUDI wallets program, how this implementation works and the architecture behind it.

The major problem of this work package was to research about a lot of different approaches and new concepts and unify them to understand how SSI and the architecture that composes it works. This work package was developed without any deviations from the initial planning.

2.3 Arbeitspaket 3 - <Infrastruktur & Setup>

- **Setup the wallet API architecture.** Definition of the architecture that the project will follow, how the project will be implemented, which approach we follow (microservices or other).
- **Testing some use cases** for our proof of concept, what will be needed to perform verifiable credentials issuance, how users are signed up in the platforms through an SSI wallet, how the platform can verify the verifiable credentials that the users send to / share with the platform.

- **Issue Verifiable Credentials.** How it'll be issued, which steps are needed to issue a verifiable credential to a user, which fields are essential within verifiable credentials.
- **Verify Verifiable Credentials.** How the verifiable credentials that the users share with the platform are verified, which steps are needed to verify a VC, what happens after the verification process is finished.
- **Setup a basic web interface** to create a test pilot of a real user claiming a verifiable credential to the platform.
- **Implementation of the endpoints** for the registration/login using a SSI wallet, issuance request, issuance of a verifiable credential, verifiable credential request, verification of verifiable credentials.
- **Setup of the hardware.** Which hardware is needed and how it'll hold the API, how many resources are needed, which budget is needed, how it will be configured.

The achievement on this work package was to setup an API that allow us to implement an SSI Kit to perform the task of creating DIDs, VCs, issue the VC to the users and verify the VC that the users send to the verifier.

The major problem was to read and understand all the documentations about how to implement the workflows with the SSI wallets for issue a signed credential and verify it, also we are trying to get access to the EBSI ecosystem to implement a whole solution based on the Europe Union infrastructure to be fully compliant with European Union standards and ensure interoperability. Our request to the EU/EBSI team is under review.

This work package was developed with some deviations to become compliant with the EBSI ecosystem.

2.4 Arbeitspaket 4 - <Prototypische Entwicklung>

- **Implementation of writing the verifiable credentials** to the user's wallet, once the verifiable credential is created: how the exchange between platform (issuer) and the user (holder), how the user stores its verifiable credential in his/her wallet.
- **Implementation of the reading a verifiable credential** from a user's wallet, how the exchange process between user (holder) and the platform (issuer) is created, how the issuer API verify the verifiable credentials that the user share with the platforms, how the data of the verifiable credentials are managed inside the platforms.

- **Documentation the code** that we are implementing, how the wallet kit needs to be implemented in our ecosystem (PoC), which API calls are defined in the application, instructions on how to integrate the project in ecosystems.
- **Implementation of open API** to serve as an intermediary to communicate the user request with the platform and the issuer wallet.
- **Implementation of authentication system** that allows users to sign up and sign in on the platforms, integration of an IDP kit to allow users to perform those actions using an SSI wallet.
- **Build and link whole SSI ecosystem.** Build the open API and integrate the IDP API and SSI wallet API.
- **Implementation of the EBSI onboarding** integrate the project with the EBSI ecosystem.
- **Implementation of UI components** to perform the actions of sign up / sign in, verifiable credentials issuance and verification of verifiable credentials

This work package is still in progress meanwhile we are waiting to achieve access to the EBSI ecosystem.

The major challenges are related to the steps needed to exchange a verifiable credential with the wallet of the user.

2.5 Arbeitspaket 5 - <Projektmanagement & Dokumentation>

- **Documentation and report of the project.** Creation of a general documentation about the project and their features.
- **User documentation.** Creation of a user manual to introduce this target audience to the project, this documentation is an abstraction of the technical architecture of the project.
- **Developer documentation.** Creation of a developer manual to introduce this target audience to the implementation and integration of the project and convey details to be enabled to reuse the SSI approach.
- **QMS integration.** How to reuse the Qualification Metadata Schema in context with wallets.
- **ESCO integration.** How to reuse the European Skills, Competency & Occupations Taxonomy in context with wallets.

This work package is still in progress.

2.6 Arbeitspaket 6 - <Qualitätsmanagement, IT Compliance & Datenschutz(richtlinien)>

- **EBSI assessment**. Onboard to the EBSI ecosystem into the project and validate the data on the European blockchain infrastructure, compliance to their rules, regulations and standards.
- **Check the compliance of SSI & GDPR**. Review the compliance of the SSI paradigm and the GDPR to fulfill the current data protection laws in the scope of European Union.
- **Evaluation of the European Learning Model (ELM).** Matching different data formats to be ELM and wallet kit compliant, compare differences between LOM (IEEE1484.12.1) with Learning Opportunities Metadata Schema (LOMS), importance of EQR/QDR, compliance & structure of EU diplomas

The major achievement was the assessment of the architecture & technical details about the EBSI ecosystem & its impact on GDPR compliance, as well as, identifying relevant ELM data models and their schemata in terms of compatibility.

2.7 Arbeitspaket 7 - <Dokumentation und Formales am Projektende>

- This work package is not reached yet.

3 Umsetzung Förderauflagen

- not applicable

4 Zusammenfassung Planaktualisierung

- Extension of project timeline to 15.7.2023 (1-2 months) (see tab “Arbeitspakete” red marked)
- Reordering of tasks within working packages, new project management plan (see tab “Projektübersicht”)

5 Öffentlichkeitsarbeit/ Vernetzung

- Skipped (tmp)

6 Eigene Projektwebsite

- Skipped (tmp)