Implementation Obstacles of Self-Sovereign Identity

VTT

Erik Hieta-aho, Valtteri Lipiäinen, Anni Karinsalo

30th September 2025 **VTT – beyond the obvious**

Biography of Erik Hieta-aho

- Senior Scientist at VTT, the Research Centre of Finland, with research focused on post quantum cryptography, including implementation, testing, and security.
- PhD in mathematics, on error-corrected coding theory, in 2018 at Ohio University, USA.
- Recently taken part in a variety of research projects including implementation of digital credentials and self-sovereign identity.

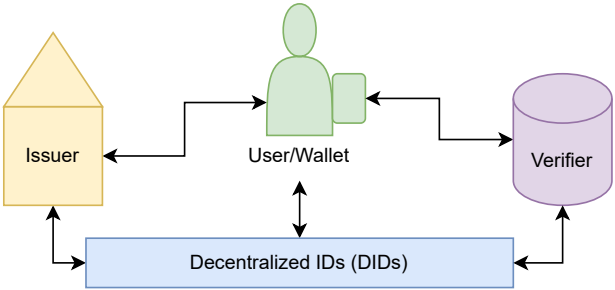
Overview

- Article title: Obstacles In Implementing and Integrating Self-Sovereign Identity and Proposed Solutions
- Self-Sovereign Identity
- Example Use case
- Current standards landscape
- Obstacles of Integration
- Proposals
- Future Work

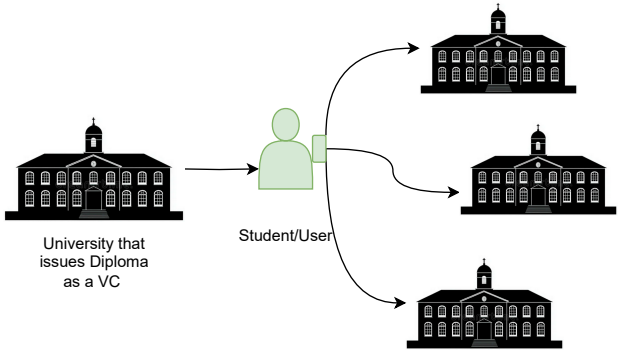
Self-Sovereign Identity

- Self-Sovereign Identities (SSI) allows users to control their identity
- Users have verifiable credentials (e.g. digital driver's license)
- An SSI ecosystem requires a software stack
  1. Wallet
  2. Issuer
  3. Verifier
- Verifiable credentials need to be signed by issuers

Self-Sovereign Identity



Example Use Case



Current standards landscape

- Standards for encoding data:
  - IETF standardized JWT and JWS
  - W3C standardized JSON-LD
- Data model standards:
  - W3C has standardized the core verifiable credentials data model
- Standards for verification and presentation:
  - Open-ID Foundation: Verifiable Credential Issuance and Verifiable Presentations.

Openness in standards brings opportunity

- In the public sector:
  - EBSI has defined a set of conformance tests for software, which specify the interaction between the components,
  - EU digital identity wallet places requirements for member states in the EU.
- In the private sector, the following organizations define SSI used together with data spaces.
  - International Data Spaces Association
  - GAIA-X

Standards and Organizations

TABLE I. STANDARDS AND ENTITIES RELEVANT FOR SSI

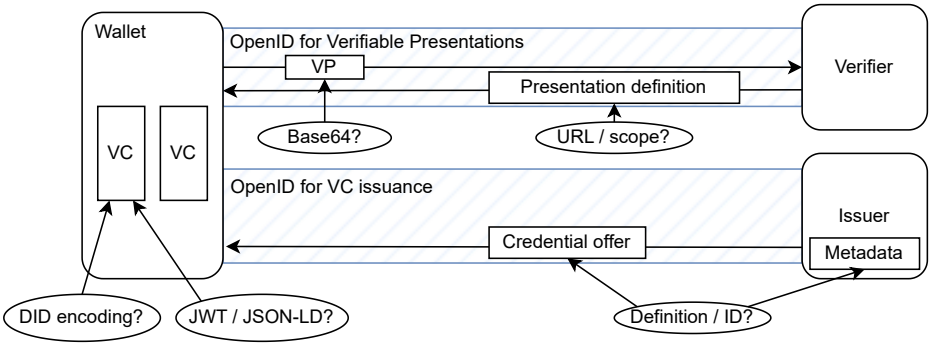
Standard	Layer	Role	Standards body or Entity
JOSE	Technical	Defines basic data objects	IETF
JSON-LD	Technical	Format for data objects	W3C
multicodec	Technical	Encodes key data	W3C
Verifiable Credentials Data Model	Credentials	Defines basic credential and presentation data formats	W3C
OIDC	Identity		OpenID Foundation
EBSI	Institutional	European Blockchain Services Infrastructure	European Commission
DID	Identity		W3C
EU digital identity wallet	Institutional		European Commission
IDSA	Institutional	Standards organization	International Data Spaces Association
GAIA-X	Institutional		GAIA-X Association

Obstacles to integration

- JWT vs JSON-LD
- Signature types and encodings
- Presentation format
- Metadata, breaking backwards compatibility

Problematic ambiguities in SSI flows

Each oval label identifies an area of divergence across implementations.



Possible Solutions

- Standard and draft versions should be included in machine-readable metadata of applications implementing SSI.
- Standards and technical specifications should together include exact technical details necessary for interoperability.
- Standard drafts and technical specifications should clearly state which details are settled and which are not.
- A standard draft should specify any significant point which differs from those in a previous version.
- Requirements related to user privacy should be set clearly by either standards or technical specifications.

Impact of standards

- SSI is decentralized, so standards are very important.
- Verifiable credentials have to be encoded. Two options are JWT and JSON-LD.
- The signatures themselves have to be encoded and transmitted in interoperable ways.

Proposals:

To make takeup of SSI possible, the following should be standardized:

- JSON-LD cryptosuite
- JOSE algorithm types
- A new multicodec format

Future Work

- These are results from our horizon europe project TANGO https://tango-project.eu/
- Continued support of SSI ecosystems
- Research and implementation of more advanced features in verifiable credentials (ZKP, selective disclosure, unlinkability etc)
- Research revocation of credentials
- Post-Quantum Cryptography transition

VTT

beyond
the obvious

Erik Hieta-aho
erik.hieta-aho@vtt.fi
+358 50 462 4005

@VTTFinland

vttresearch.com