SSI-based diploma issuance aligned with eIDAS framework

Martina Šestak, M. Inf.
Researcher & teaching assistant
martina.sestak@um.si

University of Maribor,
Faculty of Electrical Engineering and Computer Science, Slovenia
About the DE4A project

- Digital Europe for All (DE4A) - [https://de4a.eu/](https://de4a.eu/)
- 3-year Horizon 2020 project with 20+ partner institutions
- Solutions for securely sharing relevant-only data once-only across digital-by-default common services when accessing public services
- Studying abroad pilot implements cross-border higher education procedures → Diploma recognition use case
Diploma recognition:

Use case description

• Goal → facilitate the use of diploma information in another Member State (MS)
• Self-sovereign identity approach
• Diplomas issued as verifiable credentials from trusted data sources and stored in mobile digital wallets (Issuer)
• Diplomas submitted as verifiable presentations to be validated by competent authority in another MS (Verifier)
Conceptual overview of SSI

- **Decentralized Identifier (DID)**
  - Portable URL-based identifier that can uniquely identify a Party and is fully under the Party’s control

- **Verifiable Credential (VC)**
  - Set of one or more claims made by the same entity
  - Tamper-evident credential with an authorship and integrity that can be cryptographically verified

- **Verifiable Presentation (VP)**
  - Data derived from one or more VCs that is shared by the Holder with a Verifier

---

Figure 1: Conceptual overview of SSI. Source: DE4A.
eIDAS framework

- Provides a legal framework for cross-border use of eIDs on authentication and signature purposes in public service procedures
  - Major building block for supporting digital solutions and the idea of a single digital market
- Infrastructure:
  - eIDAS nodes in MSs - national entry points that allow federated access to eID schemes and form a circle of trust with other nodes
  - Delegated trust model → MS entities trust only their national eIDAS node

Figure 2: eIDAS supported Self-Sovereign Identity. Source: https://ec.europa.eu/futurium/en/system/files/pid/eidas_supported_ssl_may_2019_0.pdf
SSI + eIDAS in DE4A

- Requirements:
  - Issuers and Verifiers need to provide their services to authenticated users across borders
  - eIDAS Minimum Data Set for natural persons:
    - personIdentifier: 12345,
    - currentGivenName: Martina,
    - currentFamilyName: Šestak,
    - dateOfBirth: 1997-01-01T00:00:00.000Z
  - Issuers need to ensure that the issued diploma corresponds to the correct identity
  - eIDAS record matching process based on available identity attributes for a natural person
**SSI + eIDAS in DE4A**

**Issuer:**
1. Student authenticates with his/her eID on the Evidence Portal.
2. Student establishes a peer DID connection between the Portal and his/her mobile wallet.
3. The Portal issues a Verifiable Credential based on the original diploma.
4. The student stores the issued VC on his/her mobile wallet.

**Verifier:**
1. Student authenticates with his/her eID on the eProcedure Portal.
2. Student establishes a peer DID connection between the Portal and his/her mobile wallet.
3. Student submits his/her diploma as a VP to the Portal.
4. Student’s diploma is validated against the digital signature, issuer, schema and holder information.
THANK YOU

Martina Šestak, M. Inf.
Researcher & teaching assistant
martina.sestak@um.si

University of Maribor,
Faculty of Electrical Engineering and Computer Science, Slovenia