

**SSI-based  
diploma  
issuance  
aligned  
with eIDAS  
framework**

**Martina Šestak, M. Inf.**

*Researcher & teaching assistant*

[martina.sestak@um.si](mailto: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/>
- 3-year Horizon 2020 project with 20+ partner institutions
- Member State-driven large-scale pilot aimed at compliance with Single Digital Gateway and aligned with EU eGovernment Action Plan 2016-2020, Tallinn Declaration and EIF Implementation Strategy
- 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

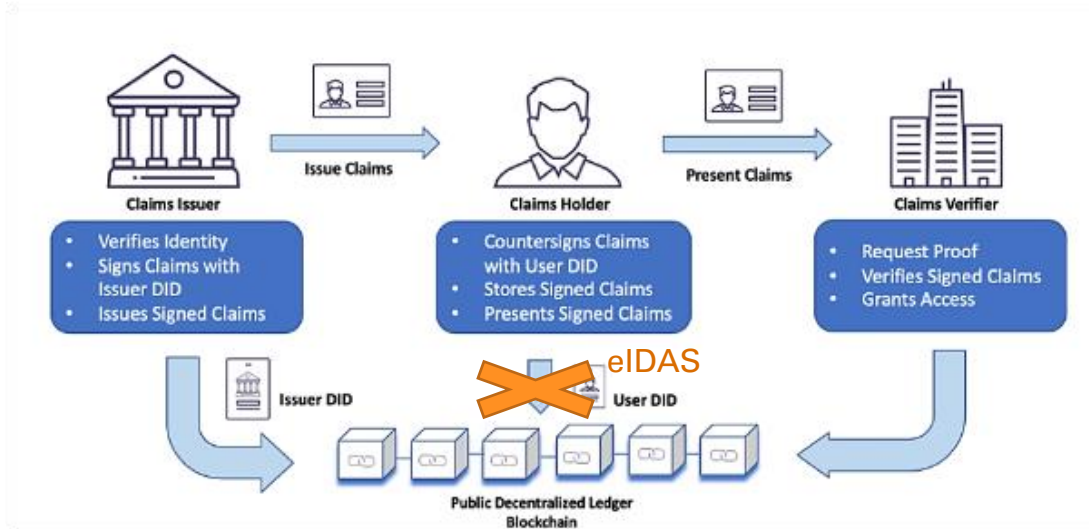


Figure 1: Conceptual overview of SSI. Source: DE4A.

- **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

# eIDAS framework

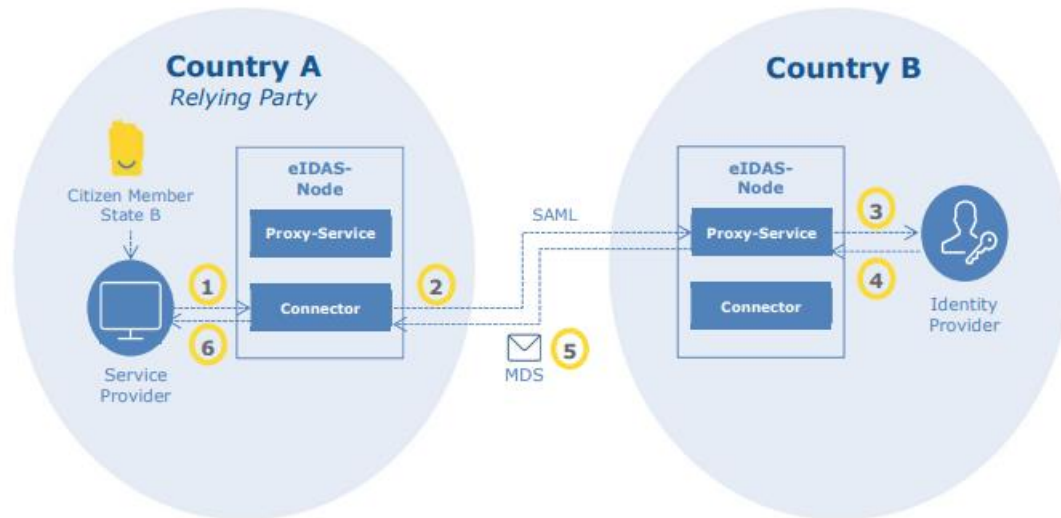


Figure 2: eIDAS supported Self-Sovereign Identity. Source: [https://ec.europa.eu/futurium/en/system/files/ged/eidas\\_supported\\_ssi\\_may\\_2019\\_0.pdf](https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf)

- 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

# SSI + eIDAS in DE4A

```
{
  "id": "http://de4a.eu/credentials/ff7f1798-5162-4f20-9bd7-076b543d69f2",
  "type": [ "VerifiableCredential", "UniversityDegreeCredential" ],
  "issuer": "did:ebsi:zBL9v9AhqUde1ZryUzogcw",
  "issuanceDate": "2021-01-31T00:00:00.000Z",
  "issued": "2021-01-31T00:00:00.000Z",
  "validFrom": "2022-05-03T12:10:10.397Z",
  "expirationDate": "2023-05-03T12:10:10.397Z",
  "proof": {
    "created": "2022-05-03T12:10:10.442420778Z",
    "jws": "eyJhbGciOiJIUzE1IiwiaWF0Ijoi",
    "proofPurpose": "assertionMethod",
    "type": "Ed25519Signature2018",
    "verificationMethod": "did:ebsi:zBL9v9AhqUde1ZryUzogcw#a4f8879be9..."
  },
  "credentialSubject": {
    "currentFamilyName": "Alves",
    "currentGivenName": "Alice",
    "dateOfBirth": "1997-01-01T00:00:00.000Z",
    "personIdentifier": "123456789",
    "achieved": [
      {
        "id": "urn:epass:learningAchievement:1",
        "title": "Mestrado em Engenharia Informática e de Computadores",
        "wasAwardedBy": {
          "id": "urn:epass:awardingProcess:1",
          "awardingBody": [ "Instituto Superior Técnico" ],
          "awardingDate": "2021-01-31T00:00:00.000Z",
          "awardingLocation": [ "urn:Lisboa-Portugal" ]
        }
      }
    ]
  }
}
```

eIDAS MDS



## 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

Figure 3: Example VC issued to student „Alice Alves”.

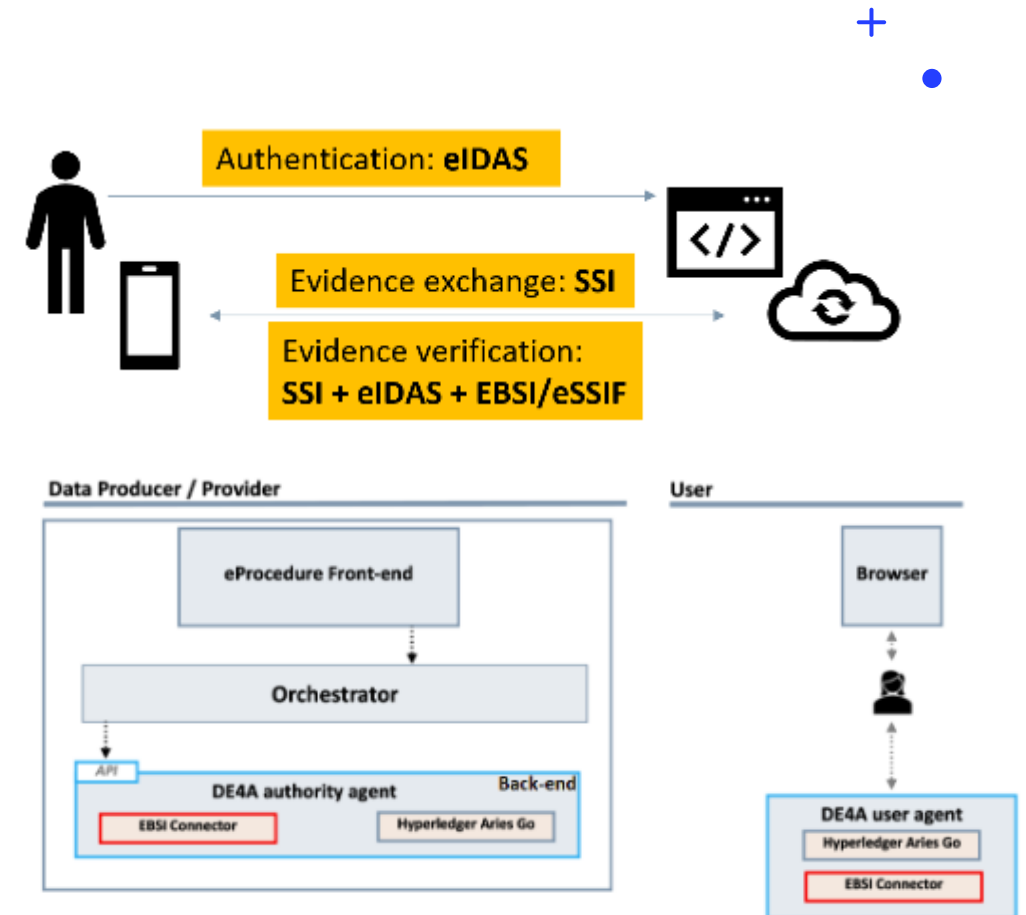
# SSI + eIDAS in DE4A

## 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](mailto:martina.sestak@um.si)

University of Maribor,

Faculty of Electrical Engineering and Computer  
Science, Slovenia