CNRS - Toulouse INP - UT3 - UT1 - UT2

Institut de Recherche en Informatique de Toulouse

eIDAS in the context of Self-Sovereign Identity

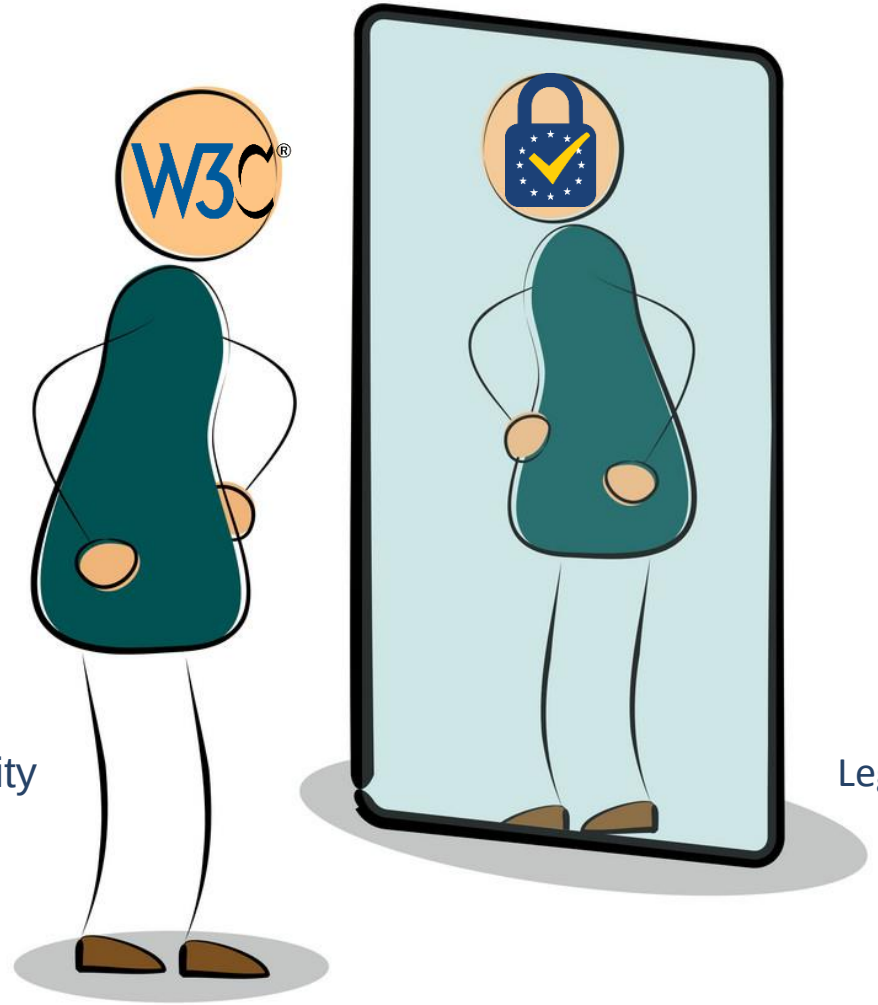
CONVERGENCE 2023

Cristian Lepore, IRIT

Brussels, 1 December 2023

SSI and the Legal Identity

Self-Sovereign Identity at the mirror.

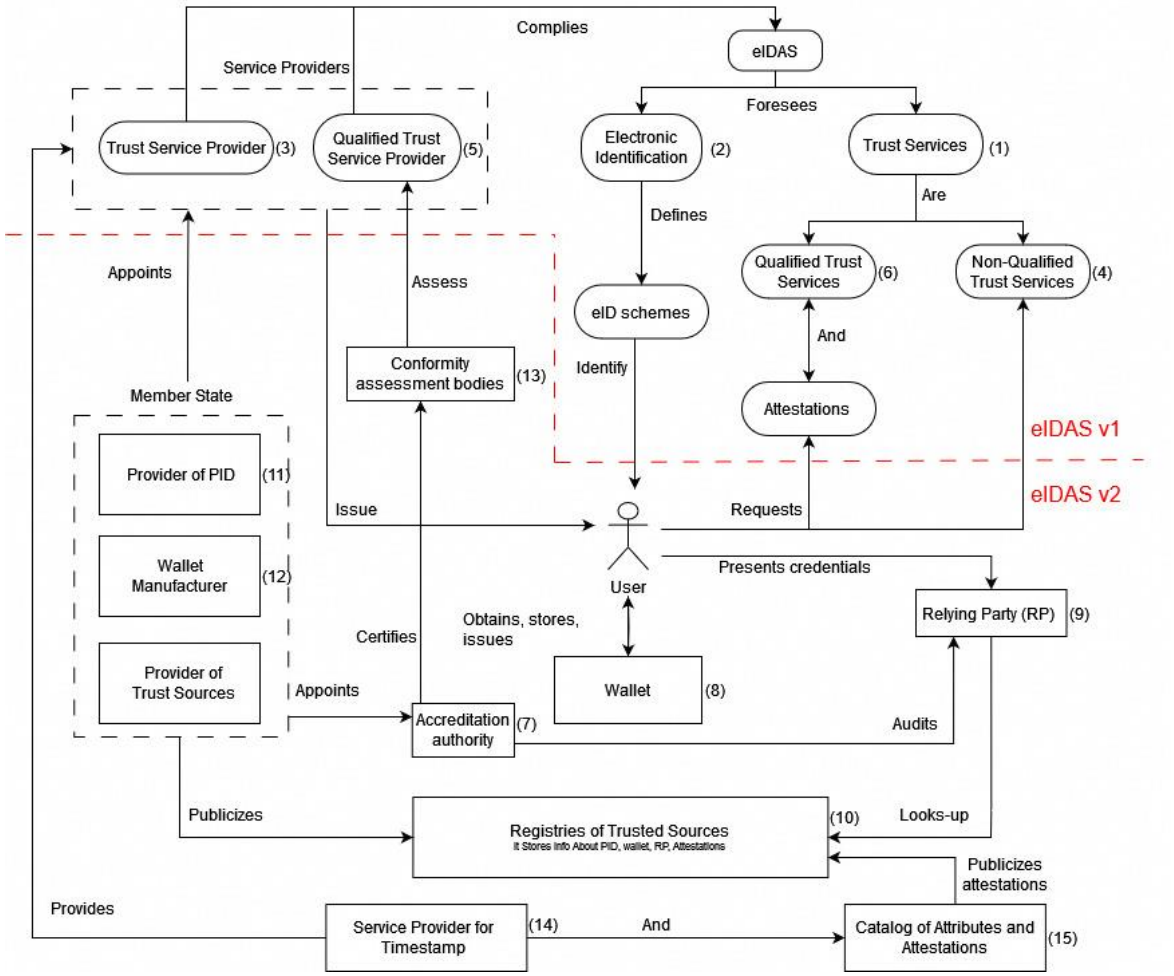


Self-Sovereign Identity solutions

Legal identity

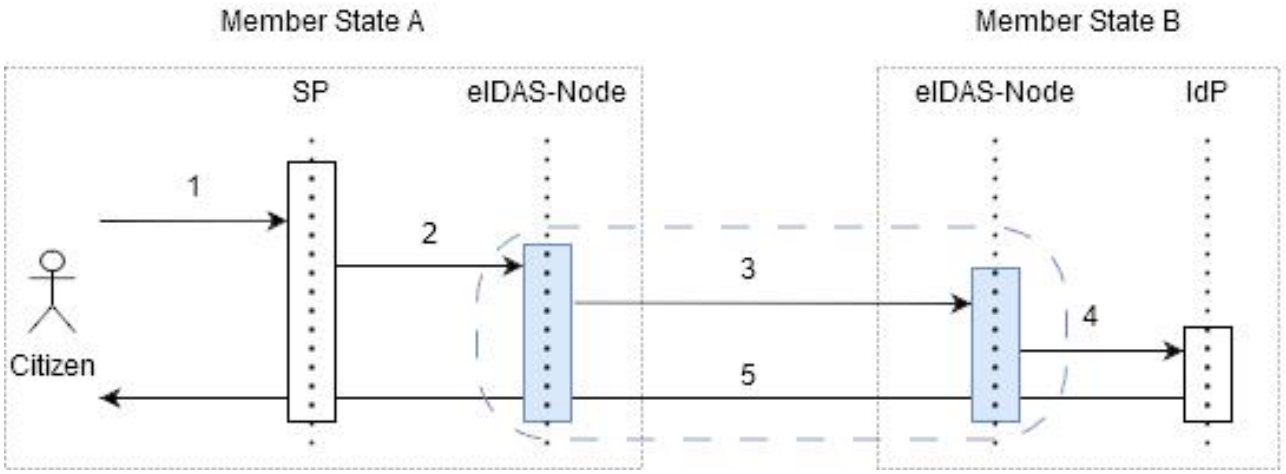
eIDAS - Ontology

The ontology of eIDAS (2018) and the new revision from February 2023. Rectangles with rounded corners are concepts defined in the regulation before 2018. Rectangles with squared corners are the EU wallet ecosystem entities. Arrows mean relationships.



eIDAS – Interoperability of eIDs

The data flow in the eIDAS Proxy-Service scenario. SP stands for Service Provider. IdP is the identity provider. The rounded dashed square encloses elements of the eIDAS solution.



1. A citizen requests an online service in Member State A.
2. At the authentication stage, the service provider discovers that the citizen's electronic identity pertains to Member State B and forwards the request to the eIDAS-node of Member State A.
3. The eIDAS-node in Member State A translates data and forwards it to the citizen's country of origin (here, Member State B).
4. The eIDAS-node in Member State B deserializes data and sends it to the identity provider (IdP) for authentication.
5. Authentication result is returned to the service provider through the eIDAS solution.

Research Questions

We pose the following research questions:

RQ1. What is a definition of SSI?

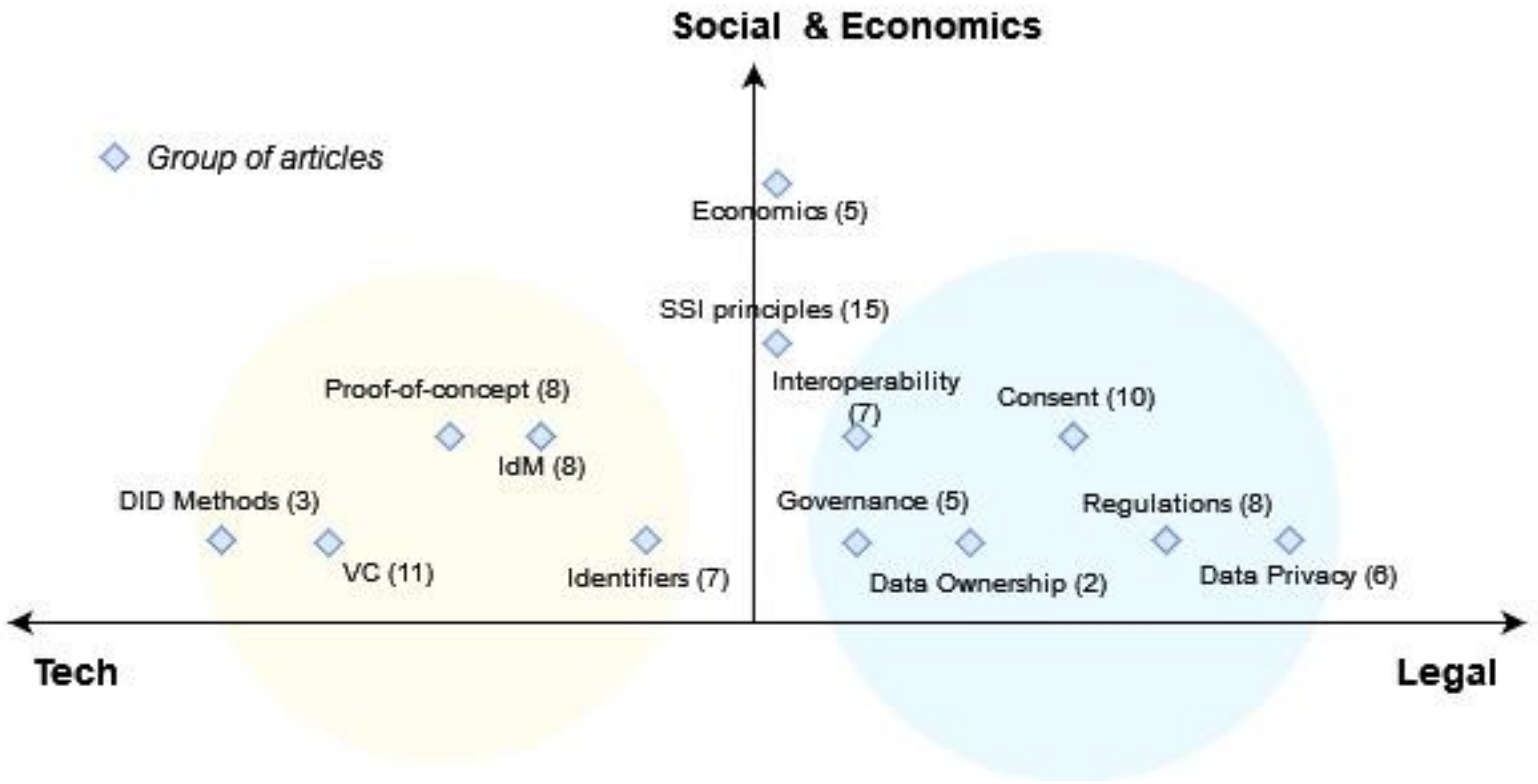
We aim to provide a rigorous definition of SSI, outlining concepts, relationships, and rules governing identity ecosystems' entities.

RQ2. Can we assess any (non) SSI system based on this definition?

We fill the gap between SSI theory and practical design, delineating a model based on our tweaked definition of SSI. In the long run, we aim to enable future startups and governments to rank solutions, spot weaknesses, and intervene accordingly.

Systematization of Knowledge

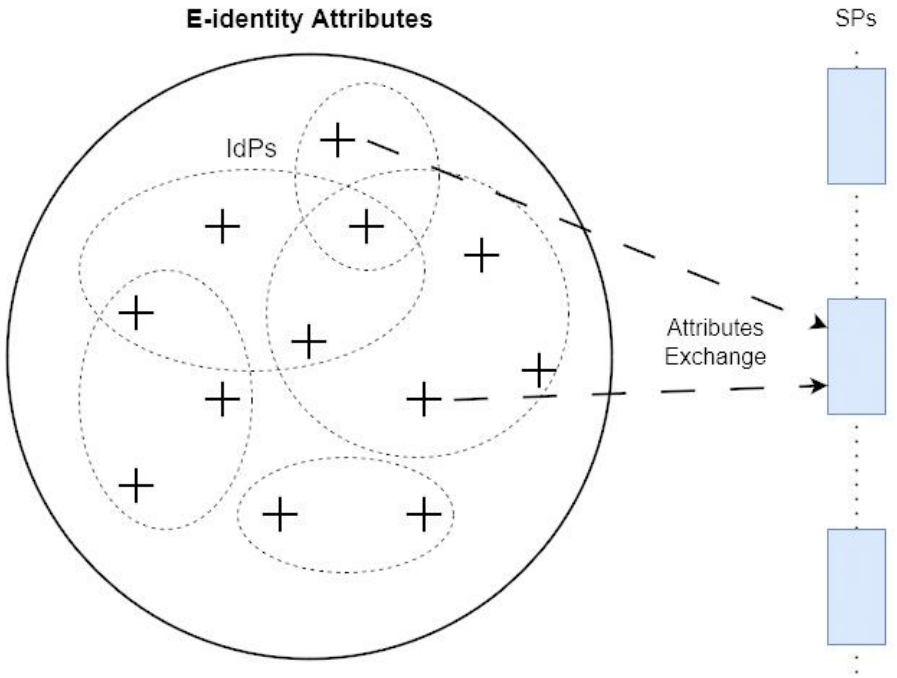
A systematization of knowledge in a two-axes chart. The dashed circle is the SSI topic. Diamonds represent groups of articles, and numbers define instances of articles in each group.



SSI Definition

Legend

- **Cross symbols (+)** are attributes
- **Outer circle** represents the set of e-identity attributes
- **Dotted circles** are Identity Providers (IdPs)
- **Squares** are service providers (SPs)
- **Dashed arrows** indicate attributes attestations



Model

Individuals' Rights (a)			
Principle	**Challenge**	**Dimension**	**Eval.**
Existence	- What attributes can attest to an e-identity?	- Assigned attributes/ID tokens (Username and Password)	●
		- Multi-Factor Authentication (e.g., One-Time Password)	●
		- Combine attributes for a new credential	○
		- Legal credentials (e.g., x509/QWAC)	●
		- Other credentials (e.g., JWT-based, AnonCreds, ntQWAC)	●
		- Know Your Customer (KYC)	●
Persistence	- Who can issue attributes?	- Qualified Trust Service Providers (QTSPs)	●
		- Trust service providers (Non-Qualified)	●
		- Other public bodies (e.g., government agencies, Univ.)	◐
		- Other private bodies (e.g., Microsoft, Financ. Inst.)	◐
		- Foundations & intergovernmental organizations (IGOs)	○
		- Non-Governmental Organizations (NGOs) and others	○
		- Self-issued	○
Protection	- Who maintains the list of IdPs and SPs?	- Private sector (e.g., banks, credit bureaus)	○
		- Consortium of organizations (e.g., Kantara)	○
		- Government agencies (e.g., national identity authority)	●
		- Supranational organization (e.g., EU Commission)	○
		- Foundations & intergovernmental organizations (IGOs)	○
		- Open community of contributors/NGOs	○
		- Nobody	●

Trustworthiness (b)			
Principle	**Challenge**	**Dimension**	**Eval.**
Access	- How users obtain information about their attributes? - Can users access the list of IdPs?	- Local agent (wallet)	●
		- Shared ledger of IdPs	●
		- History of attributes	○
Control	- Do users negotiate the release of attributes to SPs?	- User negotiates attributes but PIDs	○
		- User negotiates PIDs	○
		- Users can choose the service provider	○
Transparency	- Are policies, rules, protocols and algorithms to manage ecosystem members open and clearly stated?	- Guidelines only	●
		- Transparent rules and procedures	●
		- Open protocols	○
		- Transparent algorithms	○
		- Open code/sftw	○
		- Open APIs	●

Score System

Algorithm 1 Functional dependency (pseudo-code)

Data: $w_1, ..., w_n \in W$ s.t. $w \in \{5, 7, 8, 10, 15, 20\}$; /* set of weights */

Input: mini-batches β_i, β_i is a Ring $\{w|w \subseteq W$ weights of dimensions $\}$
$\beta_i = \{[(w_1, c_1), (w_2, c_2), ...], [(w_j, c_j), ...], [...]\}$ where $\forall_{i=1...n} c_i \in \{0, 0.5, 1\}$

Output: $\Sigma = \{\sigma_1 \rightarrow \sigma_2 \rightarrow \sigma_3 \rightarrow \sigma_4\}$; /* functional dependency */

$\Sigma \leftarrow \emptyset$

In parallel for *each mini-batch* β_i **do**

  for *each challenge* C **do**

    Step 1: multiply weights by coefficients
    $w'_j = w_j \times c_j$ for each dimension $d_j \in C$

    Step 2: sum results
    $S_c = \sum_{d_j \in C} w'_j$

    Step 3: normalize weights
    $\|S_c\| = \frac{(S_c - w_{min})}{[w_{min}, w_{max}]}$; /* Min-max normalization */

  end

  Step 4: compute weighted avg
  $\sigma_i = Avg \sum \|S_c\|$; /* Avg of norms in mini-batch */

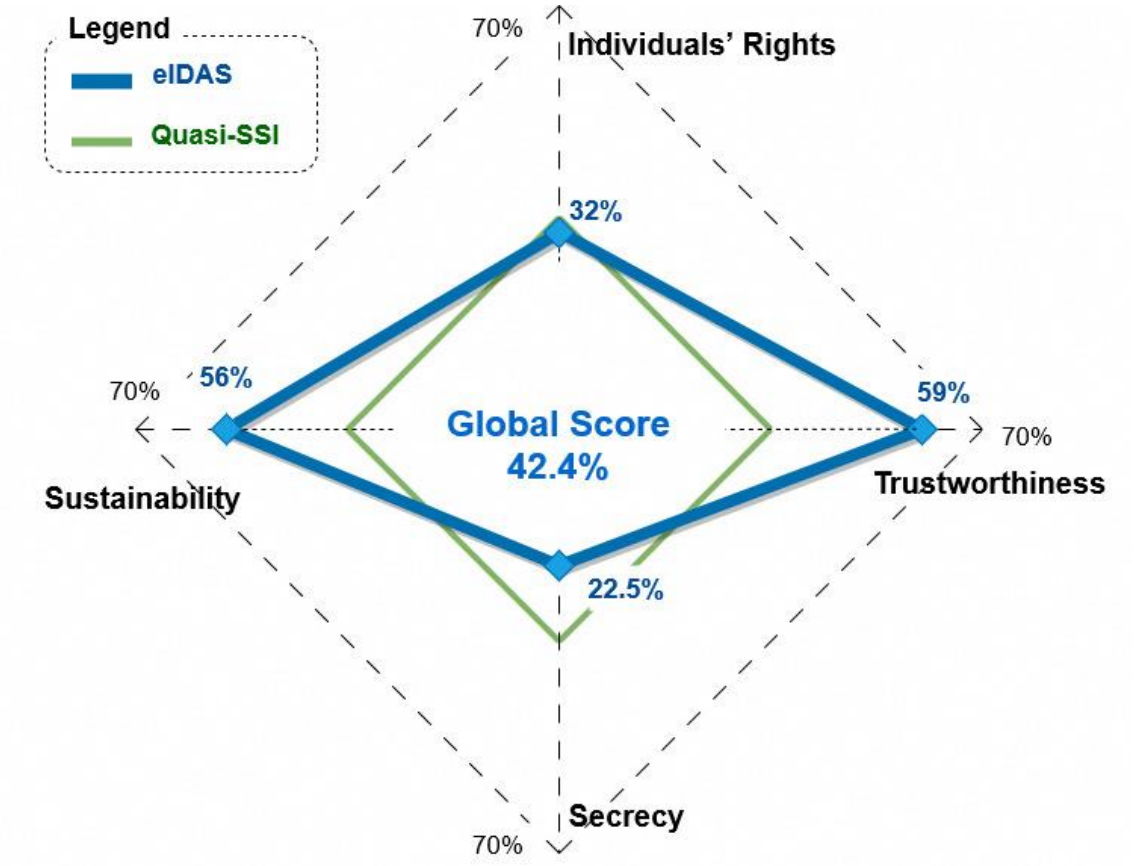
  Step 5: collect results as a power of ten
  $\Sigma \cup \{\sigma_i 100\}$; /* Cartesian product of 100 */

end

Return: $\Sigma \leftarrow \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$

Results

A Kiviat chart reporting the Global Score and each category sigma value. The thicker (blue) rumble is the outcome of eIDAS. The inner thinner (green) rumble is our pragmatic definition of SSI. The dashed (outer) rumble represents the guideline for a fair SSI solution.



Recommendations

Legal and technical recommendations for eIDAS

- The Commission should work to decrease the ambiguity of LoA, specifying parameters that are unique for Member States to follow.
- Streamline the procedure for service providers to become TSPs.
- Move the management of the list of service providers from Member States to a ”super partes” entity of the European Union or an open community of contributors.
- Add a chapter in eIDAS that specifically addresses governance-related issues and portability to embrace and help quickly adopt coming standard
- Negotiation of PID.
- Implement data minimization through Verifiable Credentials.
- Update the consent management.

Limitations of our work

- The ratio of parameters.

Thank You

Any questions?