Universal SSI-to-OIDC Bridge

Felix Hoops

10.07.2024, GX OSS Community

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

About me

PhD

- Working full-time at the chair of Prof. Dr. Florian Matthes since June 2021
- Research interests evolved from Distributed Ledger Technology to Self-Sovereign Identity
- Involved in maintaining, updating, and teaching our “Blockchain-based Systems Engineering” lecture (ca. 500 students)

Prof. Dr. Florian Matthes
Head of sebis

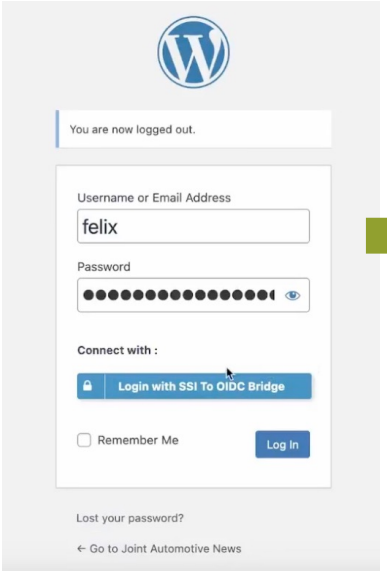
Felix Hoops
Research Assistant
& PhD Candidate

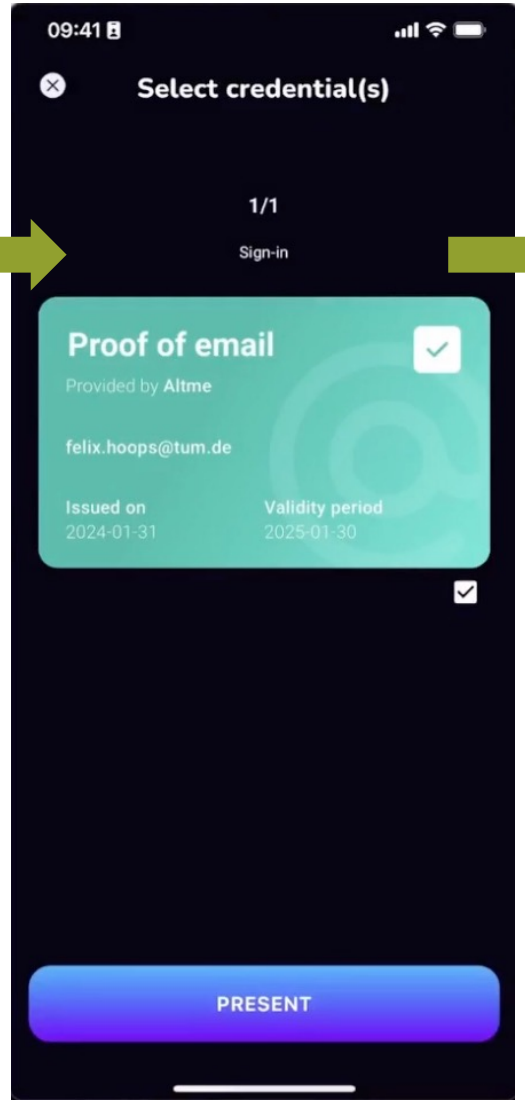
Current Industry Project

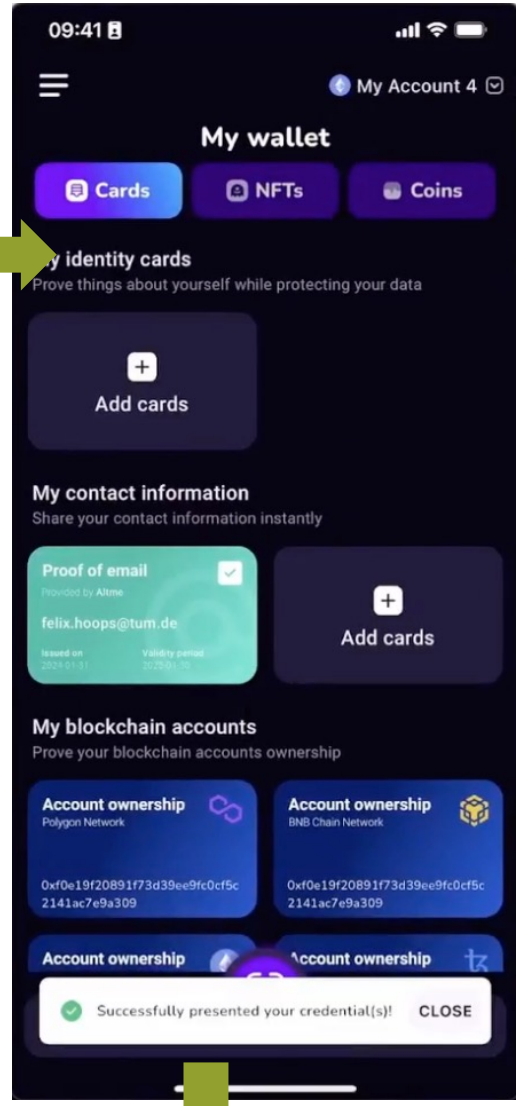
GAIA-X 4 Production, After-Sales and PLC - Across Automated Driving

The Gaia-X project aims to build a federated data infrastructure for Europe. As part of the GAIA-X 4 Future Mobility project family, this project focuses on the secure implementation of digital twins for the automotive sector in the context of automated driving through an open distributed data ecosystem (ODDE). Spanning the entire product lifecycle, these twins are envisioned to improve product verification, validation, and update strategies. more here ...

Functionality

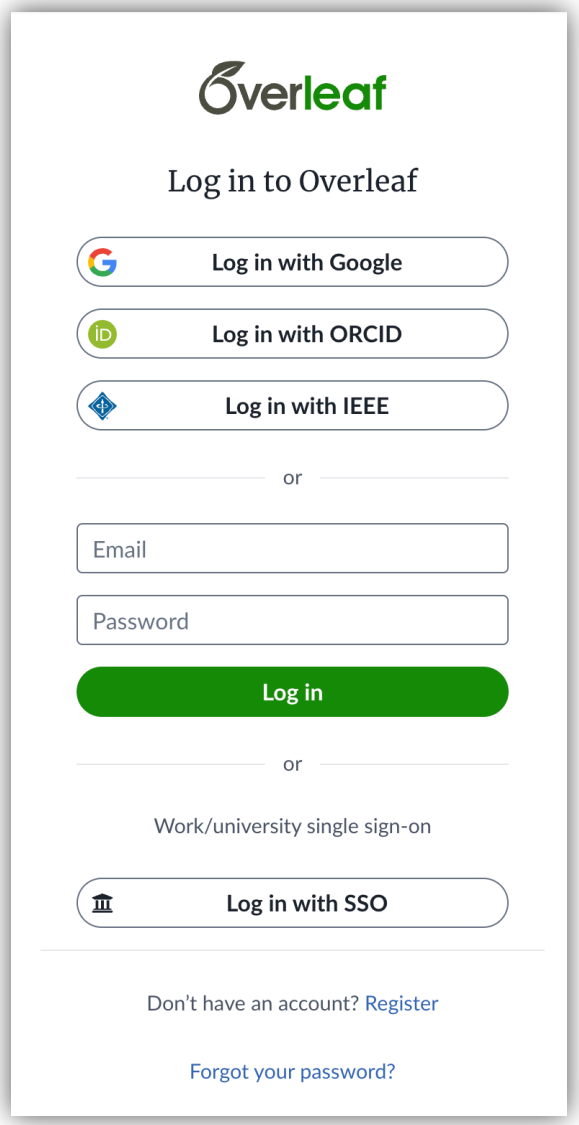






Usually takes about 6 seconds
(technical bound much lower)

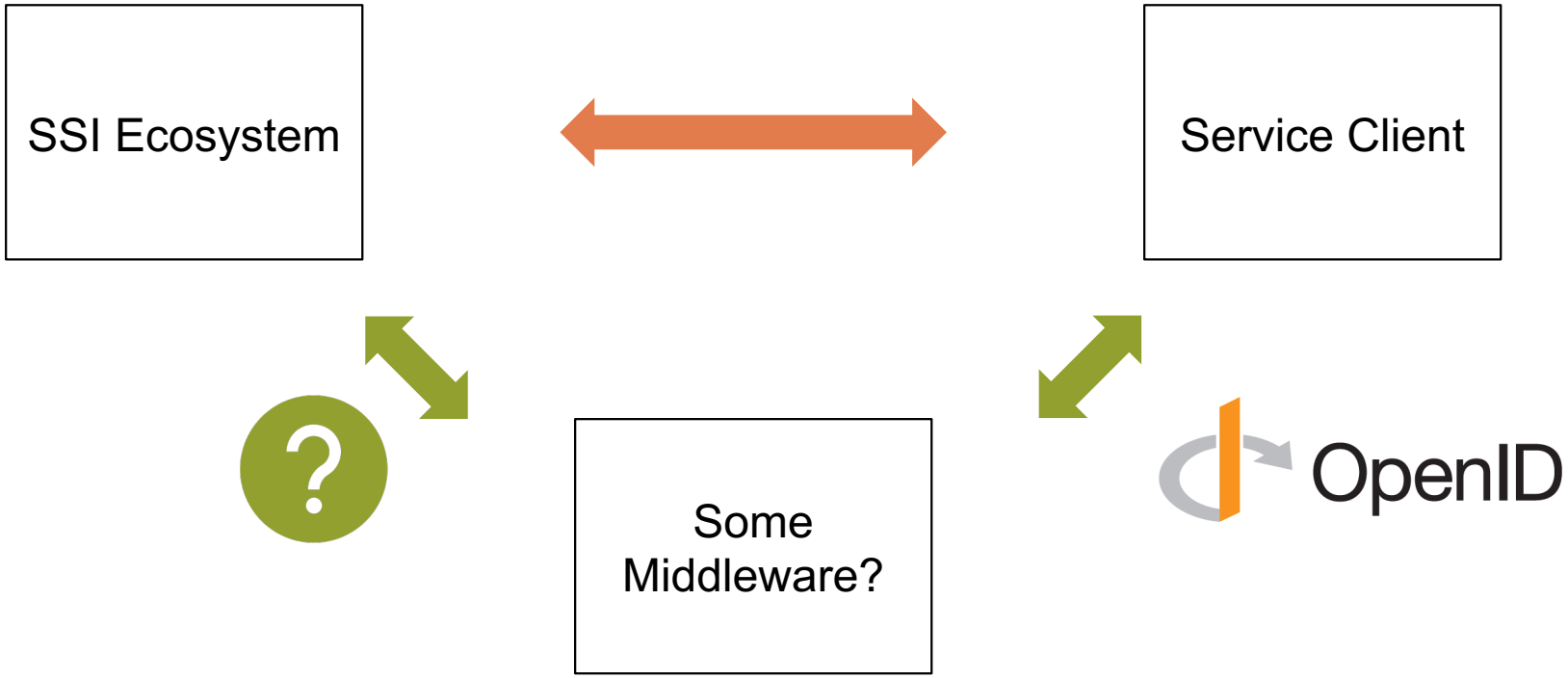
Today's Digital Identity



Screenshot illustrating federated logins.

- In the digital age, we need digital identity for offline and online services.
- While SSI is promising, **adopting SSI as a verifier is not trivial**
  - verification itself
  - use case dependent constraints
  - exchange of VPs
- While some services need more complicated authorization processes, **most services just need a sign-in** that is simple:
  - Navigate to sign-in
  - Scan QR code with phone (or press link if on phone)
  - Choose (preselected) VC(s) to present and confirm on phone
  - Page refreshes with session

The Idea of Bridging to Established Systems



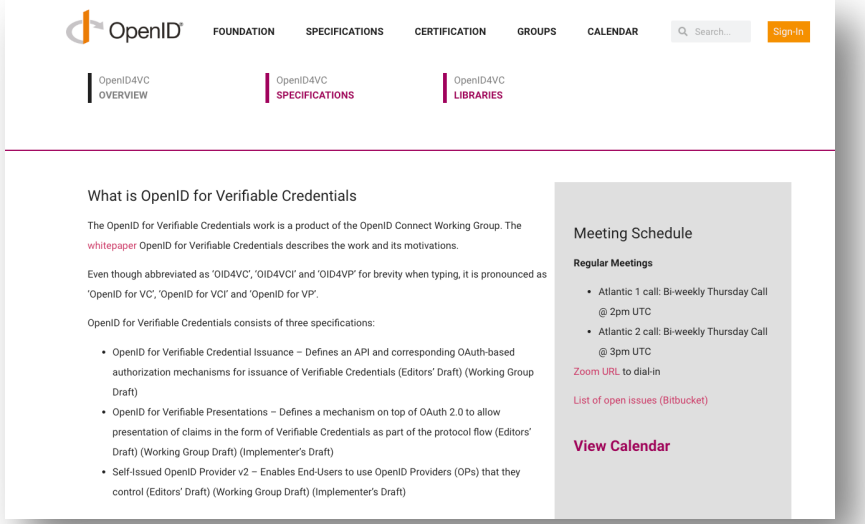
A general survey of the state of SSI from 2022 by Schardong et al. notes that protocol integration into established IAMs is vital to pave the adoption for SSI.

But…

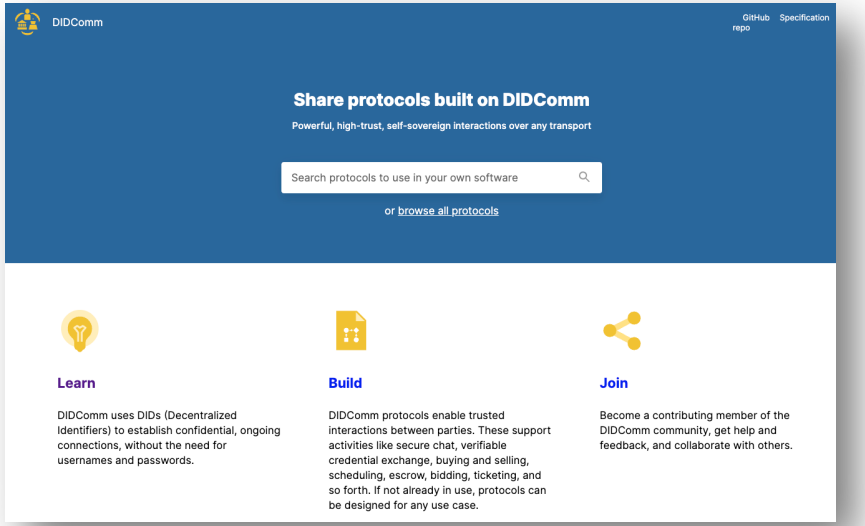
A survey by Kuperberg et al. (2022) looking at SSI integrations for established IAM protocols identifies only **seven relevant candidates**.
The majority are commercial, and only **2 of them are available as open-source software**.

Protocols for Verifiable Credential Exchange

- Issuance and presentation processes need standardized protocols
- There are two fundamental approaches:
  - Client-server
    - Web-based exchange via HTTP
    - *Example*: OID4VC
  - Peer-2-peer
    - Direct and symmetric message exchange
    - *Example*: DIDComm



https://openid.net/sg/openid4vc/

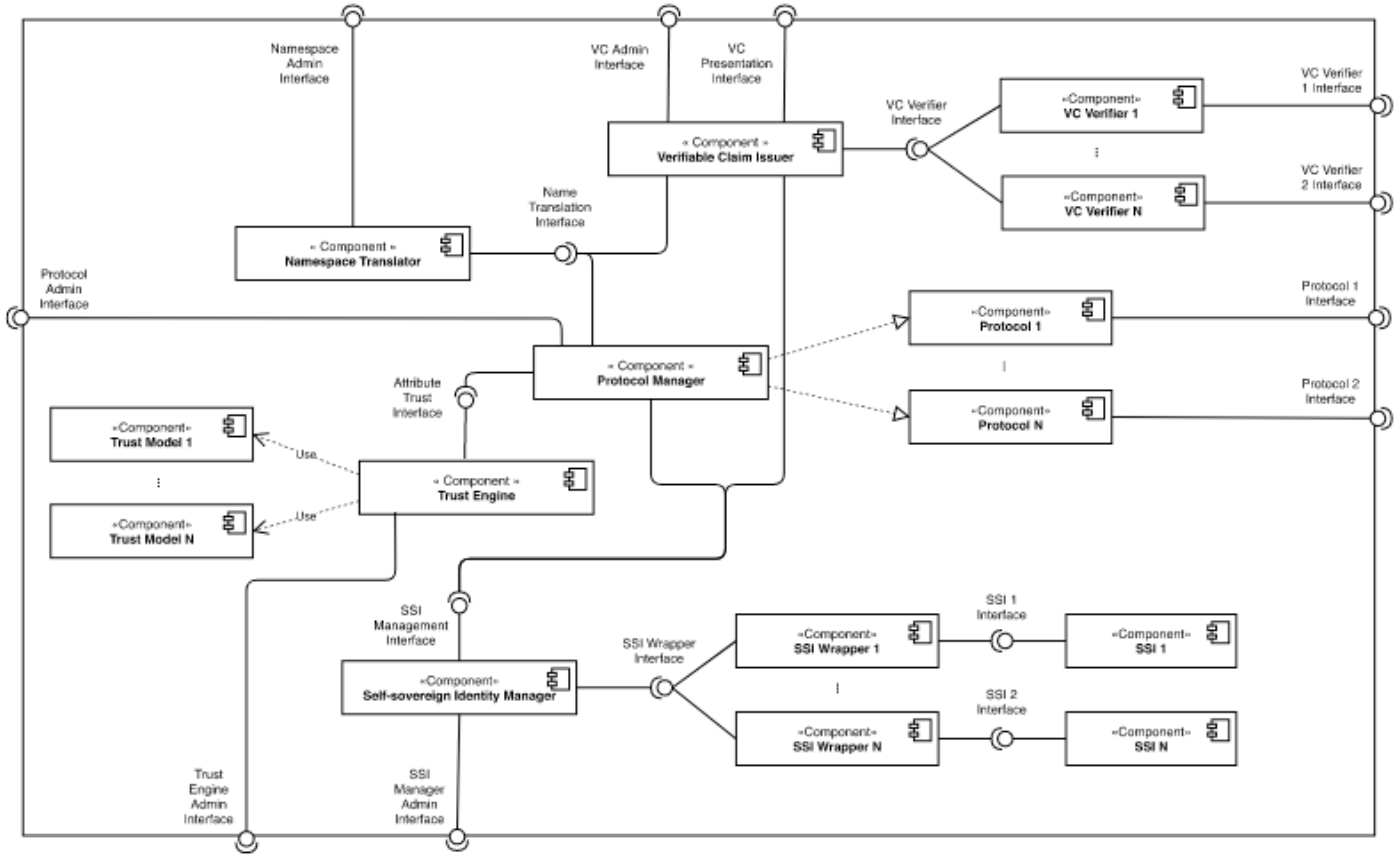


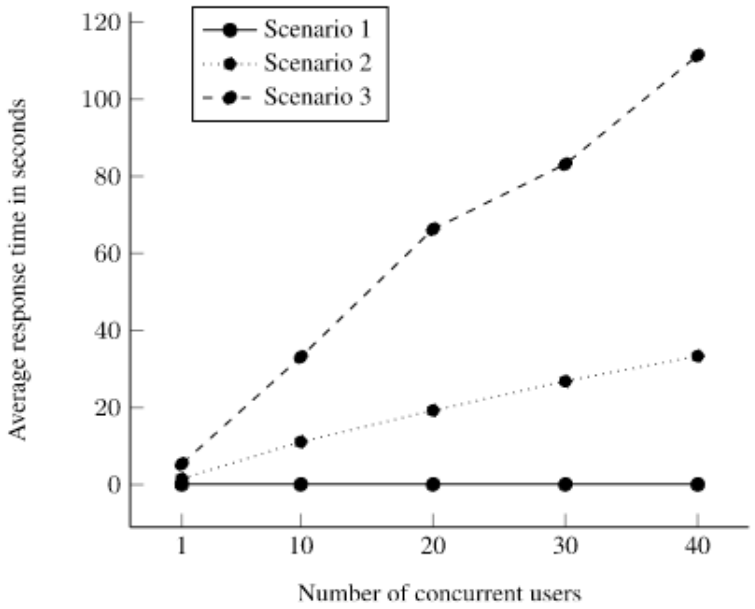
https://didcomm.org/

Protocols for Verifiable Credential exchange have been developed, and there are very different philosophies behind them. For truly interoperable SSI, everyone must support the same set of protocols.

Complexity of Existing IAM Bridges

Grüner et al. (2019, 2021) have created one of the most extensive works so far. However, there is still no adoption.





Grüner, A., Mühle, A., & Meinel, C. (2021). ATIB: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider. *IEEE Access*, *9*, 138553-138570.

Complexity of Existing IAM Bridges (ctd.)

Grüner et al. (2019, 2021) have created one of the most extensive works so far, but required configuration is excessive.

TABLE 3. Verifiable claim names in distinct domains.

Claim	uPort	Jolocom	OIDC
Email	email	ProofOfEmailCredential	email
Name	name	ProofOfNameCredential	name
Firstname	firstname	ProofOfFirstnameCredential	given_name
Lastname	lastname	ProofOfLastnameCredential	family_name

TABLE 6. Trust model characteristics for OpenHPI.

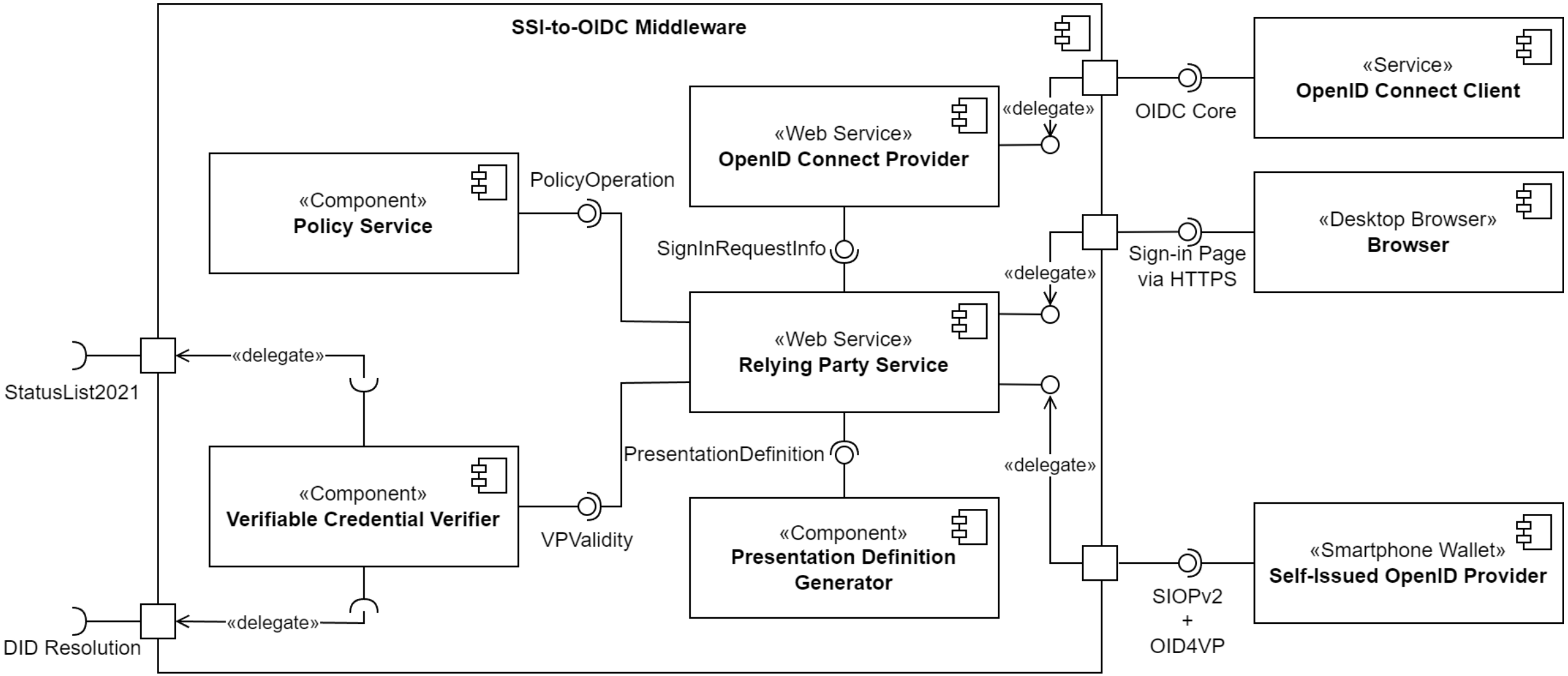
Attributes	Providers	Acceptance Rules
$\mathbb{A} = \{email, name\}$	$\mathbb{P} = \{ATIB, anonym\}$	$\mathbb{S} = \{\Theta \geq 1 \Rightarrow email, \Theta \geq 0 \Rightarrow name\}$

Definition 1 (Acceptance Rules): Let $\mathbb{S}$ bet a set of acceptance rules to decide at a threshold $t \in (0 \ldots 1)$ on the use of an attribute $a \in \mathbb{A}$ under n attestations of distinct providers $p_1 \ldots p_n \in \mathbb{P}$. An element $s_i \in \mathbb{S}$ is defined as follows.

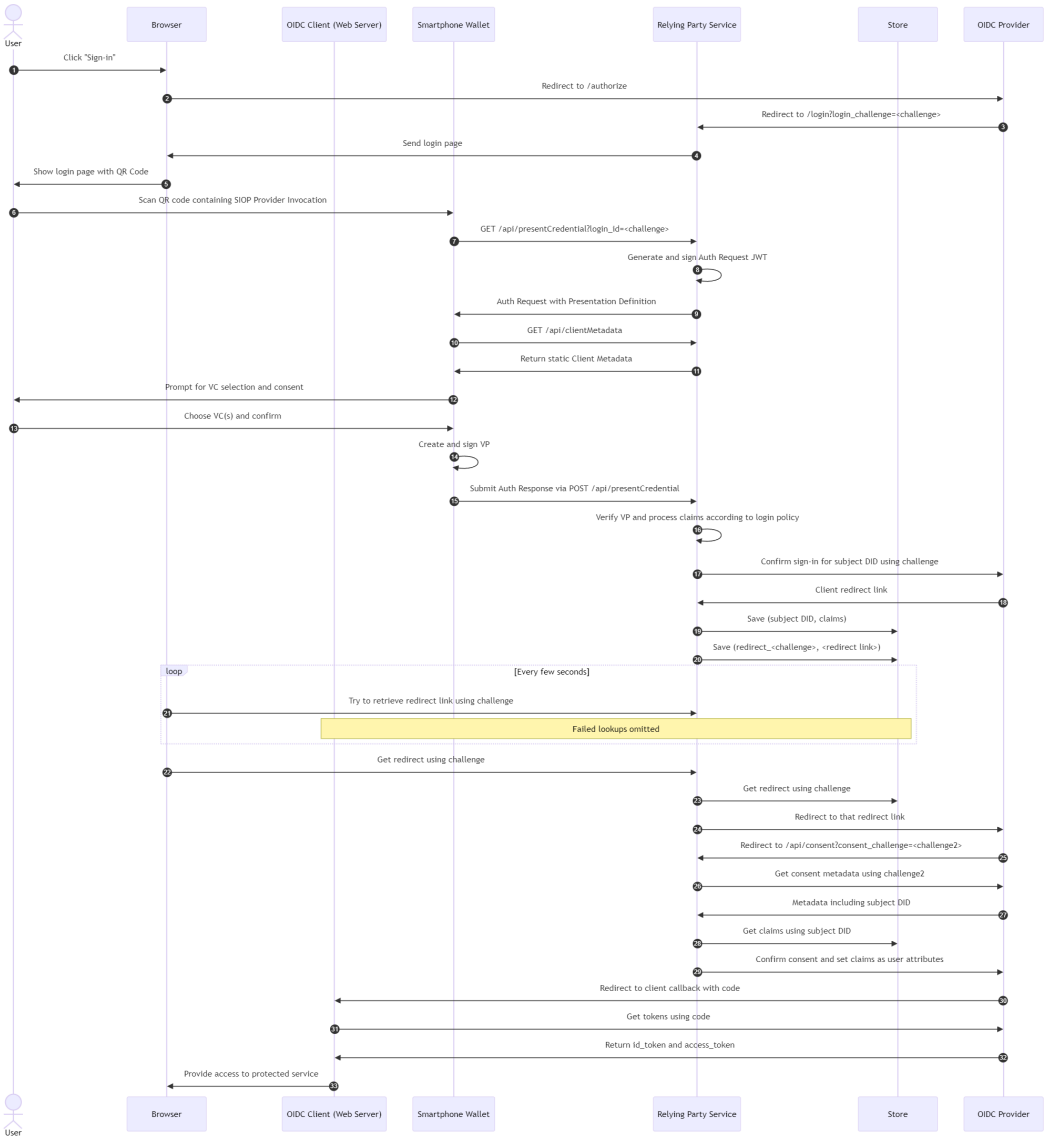
$$s_i : \Theta(\mathcal{P}_{p_1}, \ldots, \mathcal{P}_{p_n}) \geq t_{a_i} \Rightarrow a_i \quad (1)$$

In general, if the overall probability for an attribute exceeds a threshold, the property is accepted from the trust engine. The threshold reflects a risk indicator for the SP. The higher the threshold is set, the higher the assurance that the attribute is correct and valid. In the ATIB database, the considered APs, their DIDs as reference, and the respective probability values as well as the dependency factor are stored as a configuration.

Our Design



The Protocol Flow

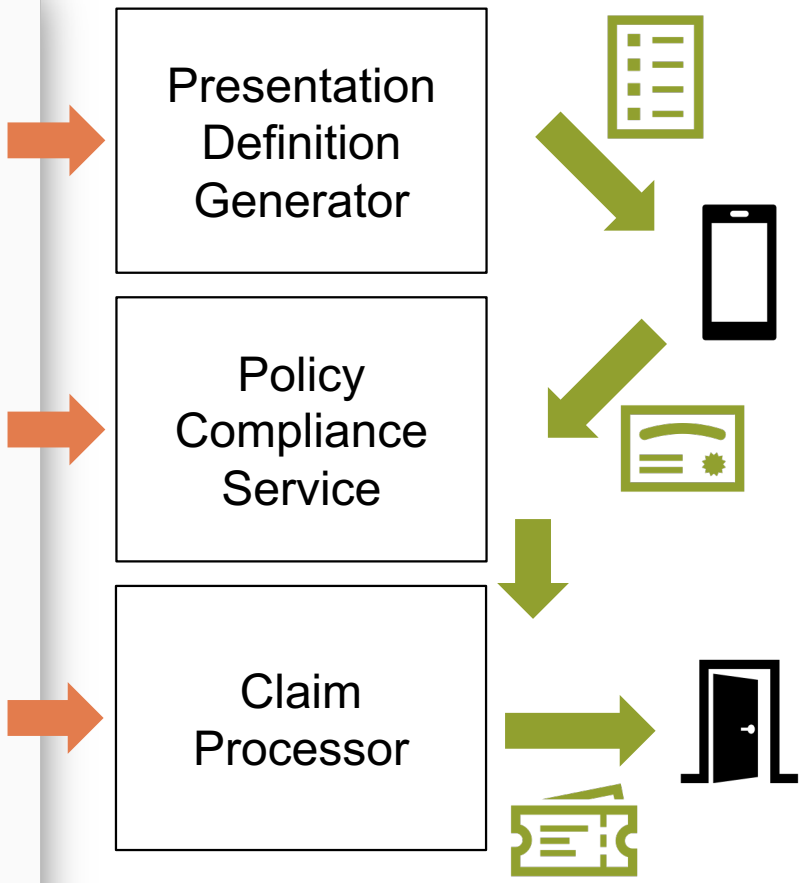


- Modified OAuth 2.0 authorization code flow
- The login challenge from OIDC (in shorter form) is used throughout the entire process
  - We pass it to the phone by encoding it as part of the QR code
- Sign-in page actively polls for completion
- Consent stage of the authorization code flow is skipped by confirming it automatically
  - Users already give consent by sharing VP
- No refresh tokens issued
  - The **bridge remains stateless in the grand scheme**

Login Policy

To not repeat what prior works did, we wanted one central configuration file, that combines trust, required values, and value mapping. For that, we had to develop a custom format.

```
[{
  "credentialID": "expected_credential_for_email",
  "patterns": [{
    "issuer": "did:example:123",
    "claims": [{
        "claimPath": "$.credentialSubject.e_mail",
        "newPath": "$.email",
        "token": "id_token"
    }]
  },
  {
    "issuer": "did:example:456",
    "claims": [{
        "claimPath": "$.credentialSubject.email",
        "token": "id_token"
    }]
  }]
}]
```



The Paper

A Middleware Architecture for Self-Sovereign Identity Authentication and Authorization

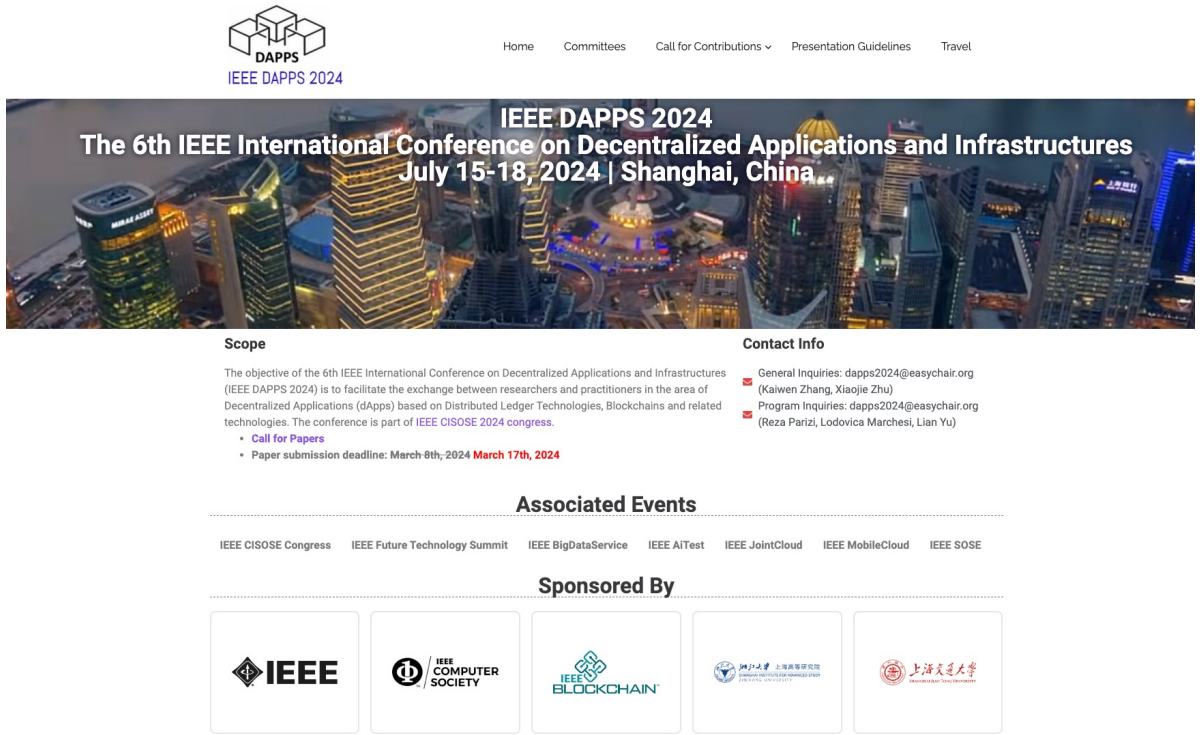
Felix Hoops, Florian Matthes

- Part of our work on Gaia-X 4 PLC-AAD
- Gaia-X creates de–centralized data–spaces and –markets for b2b

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Just accepted as a short paper at the IEEE DAPPS conference.



Conclusion

Currently Used Standard Versions

- OpenID for Verifiable Presentations - draft 18
- Verifiable Credentials Data Model v1.1 – JSON-LD

Newest update on GitHub

Constraints

… and lots of fixes and improvements.

What is next?

Collaborators are welcome.

JWT support.

Testing, testing, testing.

Check out our code!

M. Sc.

Felix Hoops

Technical University of Munich (TUM)
TUM School of CIT
Department of Computer Science (CS)
Chair of Software Engineering for Business Information Systems (sebis)

Boltzmannstraße 3
85748 Garching bei München

+49.89.289.17126
felix.hoops@tum.de
wwwmatthes.in.tum.de