Chair of Software Engineering for Business Information Systems
Department of Computer Science
School of Computation, Information and Technology
Technical University of Munich

# A Decentralized Identity Bridge for Usable Blockchain-backed Self-Sovereign Identity

Felix Hoops, Florian Matthes
felix.hoops@tum.de, matthes@tum.de

## Motivation

Simple logins are the foundation of today's Internet and are mainly centralized, which endangers privacy. Blockchain communities have already explored decentralized solutions such as "Sign-in with Ethereum"[1] and connections to established identity and access management (IAM)[2]. Self-Sovereign Identity (SSI)[3] offers a way to attach claims to (blockchain-based) identifiers, making them more useful in real-world IAM.

**PROBLEMS**

- Integration Complexity
- Ecosystem Lock-in
- Interoperability and Maintainability Concerns
- Complexity of Existing Bridges

**GOAL** A bridge that makes Verifiable Credentials (VCs)[4] backwards compatible with existing single-sign-on (SSO) solutions relying on OpenID Connect (OIDC)[5]. This system would simplify the adoption of SSI for old and new services.

## A Gaia-X Use Case

Companies explore decentralized "coopetition" models where no participant holds centralized control of another one's data[6].

**EXAMPLE** An employee wants to buy from a Gaia-X marketplace for sensor simulation assets, such as 3D street maps, to support a project:

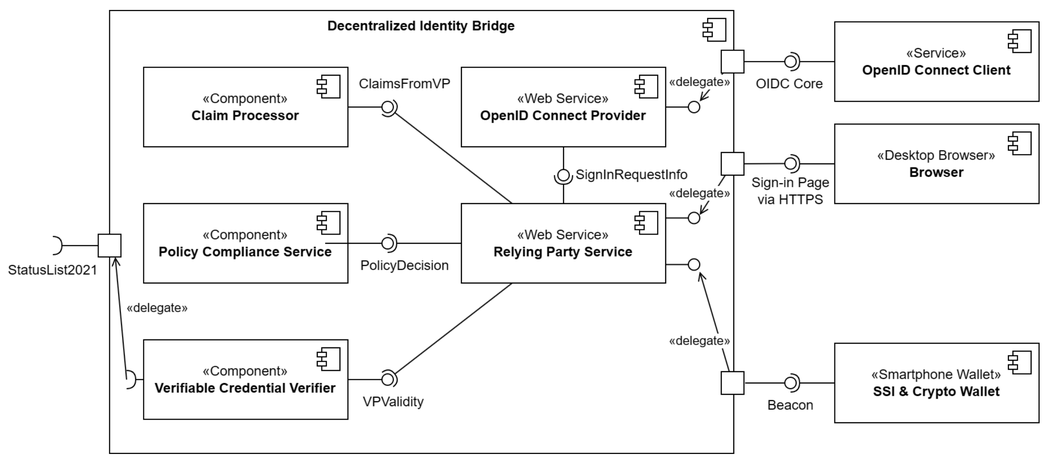
1. Employee navigates to the page in his browser and clicks the "Login" button
2. Employee scans the shown QR-Code with a smartphone wallet and chooses to present his employee VC
3. Employee is redirected to the marketplace site with an active session

Finanziert von der Europäischen Union
NextGenerationEU

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

## Architecture

We propose a bridging architecture that acts as an OpenID Connect Provider (OP) towards any given service supporting OIDC for sign-in. To obtain user claims during the sign-in procedure, a connection with a smartphone wallet via Beacon Protocol is supported.




**COMPONENTS** The bridge consists of the following logical components:

1. The *OpenID Connect Provider* adheres to OIDC Core to provide sign-ins.
2. The *Relying Party Service* is responsible for coordinating the overall sign-in procedure. It relies on the claims made by issuers in the form of VCs.
3. A *Verifiable Credential Verifier* handles all syntactical and cryptographic checks involved in verifying a Verifiable Presentation (VP) and its VCs. This includes an optional status list check using W3C StatusList2021[7] to ensure a given VC has not been revoked. Additionally, a simple holder binding is enforced.
4. The *Policy Compliance Service* enforces that all presented VCs are from trusted issuers.
5. The Claim Processor extracts all subject claims from the presented VCs and aggregates them for their inclusion in the *access_token*.

**DEPLOYMENT** Acting as an OIDC Provider towards service clients, the bridge has full authority over transmitted user information without any mechanism to enforce accountability. Thus, the only feasible deployment option is for every service provider to deploy one themselves.

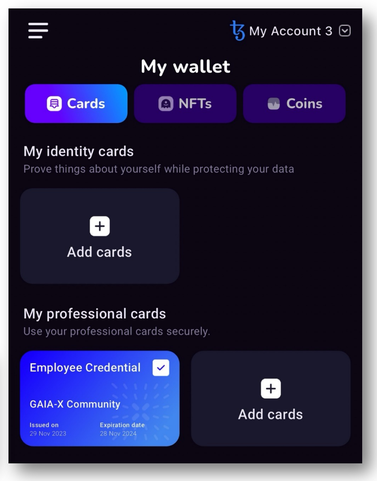
A *Trust Policy* governs what issuers are trusted. It also provides expected VC types to improve the user experience.

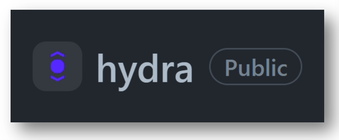
```
[
  {
    "issuer": "did:tz:tz1NyjrTUNxDpPaqNZ84ipGELAcTWYg6s5Du",
    "types": ["EmployeeCredential"],
  },
]
```

## Validation through Implementation

We implemented a proof of concept system, testing it on realistic hardware with existing software. We used:

- **Altme Wallet** as an open-source SSI wallet in production
- **Ory Hydra** as a customizable open-source OIDC Provider in production
- **Ory CLI** offers a simple web-based OIDC Client for testing purposes




```
{
  "acr": "0",
  "at_hash": "cwulOA2eR_-ER-JmBEUBog",
  "aud": [
    "884be2fe-82dc-4f67-9328-1c3110d31ff9"
  ],
  "auth_time": 1702986515,
  "exp": 1702990119,
  "iat": 1702986519,
  "iss": "http://localhost:5004/",
  "jti": "7b5e8c26-1a31-45db-8713-a3cabe4623ca",
  "nonce": "vqcmzeknafpnodbcslhdmhat",
  "rat": 1702986496,
  "sid": "a7cdcaaa-0b63-496a-add3-32914dc66c05",
  "sub": "did:key:z6MkkdC46uhBGjMYS2ZDLUwCrTWdaqZdTD3596sN4397oRNd"
}
```

The bridge issues regular OIDC tokens to provide full compatibility with existing systems. The *id_token* (pictured) contains a DID as the subject. The *access_token* (not shown) includes all other fields.

## Conclusion

We have designed a minimal, focused, practical bridging mechanism to support VC-based logins via OIDC. In particular, we define and implement a detailed protocol flow for integrating a VP-based authentication and authorization into an OIDC flow. Manual testing has confirmed the viability of this approach.

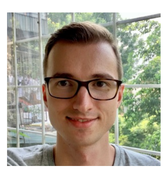
**What is next?**

- Design a more expressive Trust Policy.
- The adoption of OpenID4VP must be explored for a potentially universal exchange protocol between wallets and the Relying Party Service.
- The code base is planned to be open-sourced very shortly.
- Extended testing in the context of the Gaia-X 4 PLC-AAD project.
- Investigate scalable support for fully decentralized revocation mechanisms.

## Acknowledgments

This work has been funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK) under grant 19S21006N. The responsibility for the content of this publication lies with the authors.

## Contact



Felix Hoops
Technical University of Munich, sebis
felix.hoops@tum.de

Technical University of Munich
School of Computation, Information and Technology
Department of Computer Science
Chair of Software Engineering for Business Information Systems (sebis)

[1] https://login.xyz/
[2] e.g., https://github.com/spruceid/siwe-oidc
[3] Allen, C. [Accessed 21-11-2023] "The Path to Self-Sovereign Identity." (2016) URL http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html.
[4] Sporny, M., Longley, D., Chadwick, D. [Accessed 21-11-2023] "Verifiable Credentials Data Model v2.0 — w3.org." (2023) https://www.w3.org/TR/vc-data-model-2.0/.
[5] OpenID Foundation [Accessed 21-11-2023] "OpenID Connect Core 1.0 incorporating errata set 1" (2014) https://openid.net/specs/openid-connect-core-1_0.html
[6] https://www.gaia-x4futuremobility.de
[7] Longley, D., Sporny, M. [Accessed 21-11-2023] "Verifiable Credentials Status List v2021." (2023) https://www.w3.org/TR/vc-status-list/.