Karlsruhe Institute of Technology

Institute AIFB
Web Science

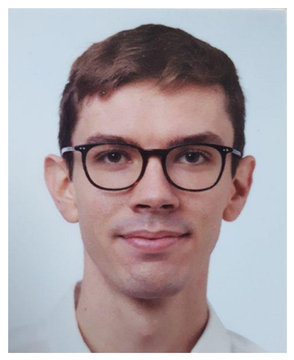
Towards realizing Attested Attribute-based Access Control on Solid Pods using Verifiable Credentials

Supplementary Poster to the Demo

Valentin Betz, **Christoph Braun**, and Tobias Käfer
*valentin.betz@student.kit.edu, **braun@kit.edu**, tobias.kaefer@kit.edu*

Say hi to this guy!

He has long hair now...

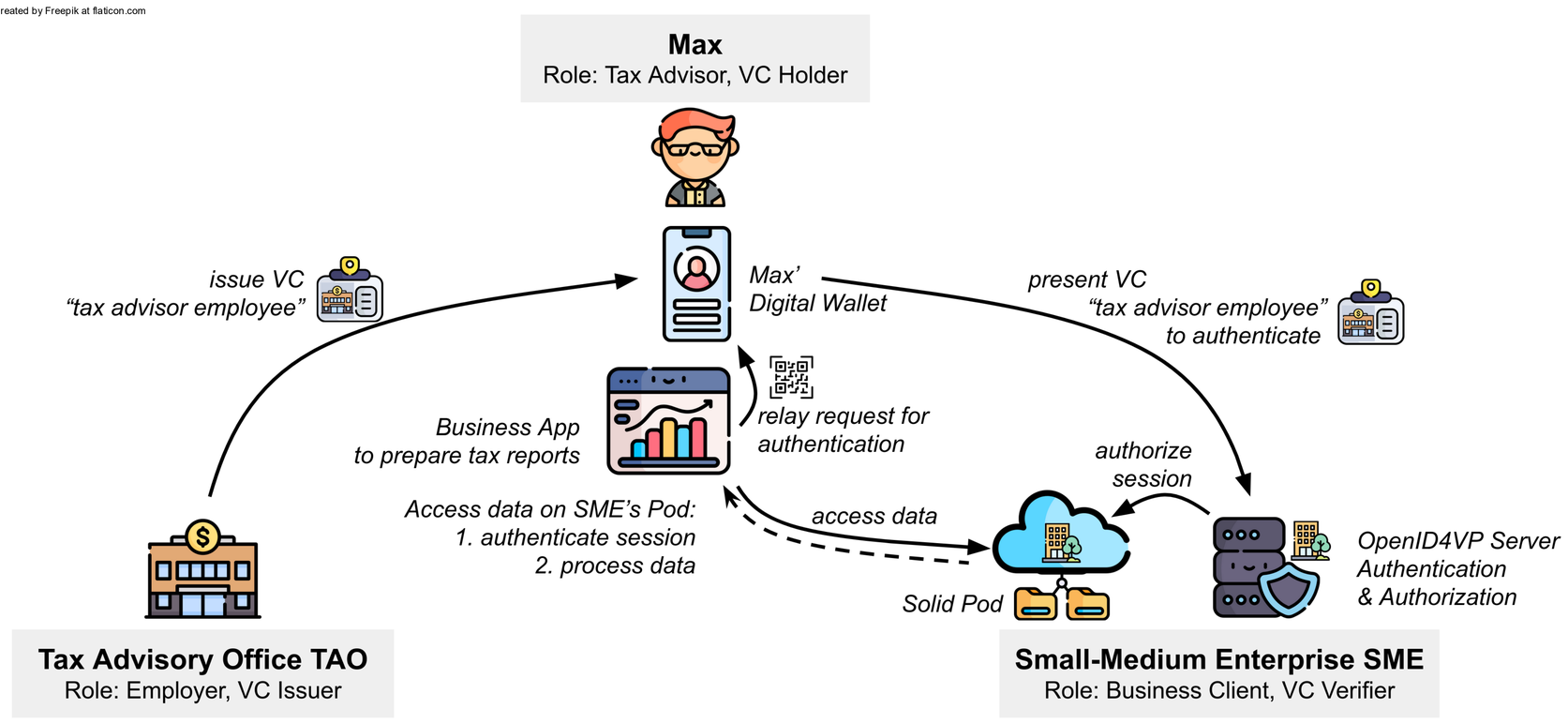


Problem: In the Solid Protocol, granting access to private and dynamic (attribute-based) agent groups is undefined.

Question: How can we grant access to resources stored on a Solid Pod based on some attested attribute (e.g., age, organizational membership, ...) using web standards?

Solution: Use **Verifiable Credentials** and **SHACL** in **OpenID for Verifiable Presentation (OID4VP)**

Attested Attribute-based Access Control



Live Demo!

- ***Verifiable Credentials*** *to attest user attributes*
- ***SHACL*** *to specify required attributes in access control rule*
- ***OID4VP*** *as protocol to authenticate using VCs*

Figure 1: A high-level illustration of the system architecture in our example use case.

Walkthrough

SME stores and manages their financial data on their **Solid Pod**.
SME hires a Tax Advisory Office (**TAO**) to prepare the business' tax reports.

TAO employees – the actual tax advisors preparing and singing off the tax report – require access to SME's financial data.

SME, however, is not aware which of TAO's employees will be working SME's case.
Maybe TAO only schedules tasks just-in-time such that it is hard to predict which employee should have access to SME's data.
Therefore, SME restricts access to the Pod-stored data to TAO employees – unable to only whitelist who will actually prepare the tax report.

Max, the tax advisor, uses a business application to prepare the tax report:
Attempting to access SME's data via the business app, a QR code is displayed asking Max to authenticate as a TAO employee.
Max scans the code using their phone with the digital wallet.
Max' digital wallet prepares the required VCs; Max only needs to check who will receive the VP and consenting to the disclosure.

SME's OID4VP server processes the presented VC to authenticate and authorize Max's business app session as a TAO employee.
Max is thus allowed to access the Pod-stored financial data to prepare the report using the business app.

References

Capadisli, S., Berners-Lee, T., and Kjernsmo, K.: *Solid Protocol*. Version 0.11.0. W3C Solid Community Group (2024)

Sporny, M., Noble, G., Longley, D., Burnett, D.C., Zundel, B., and Den Hartog, K.: *Verifiable Credentials Data Model*. W3C Recommendation, W3C (2021)

Knublauch, H., Kontokostas, D.: *Shapes Constraint Language (SHACL)*. W3C Recommendation. W3C (2017)

Terbu, O., Lodderstedt, T., Yasuda, K., and Looker ,T.: *OpenID for Verifiable Presentations*. OpenID Digital Credentials Protocols Working Group, Editor's Draft, (2025)