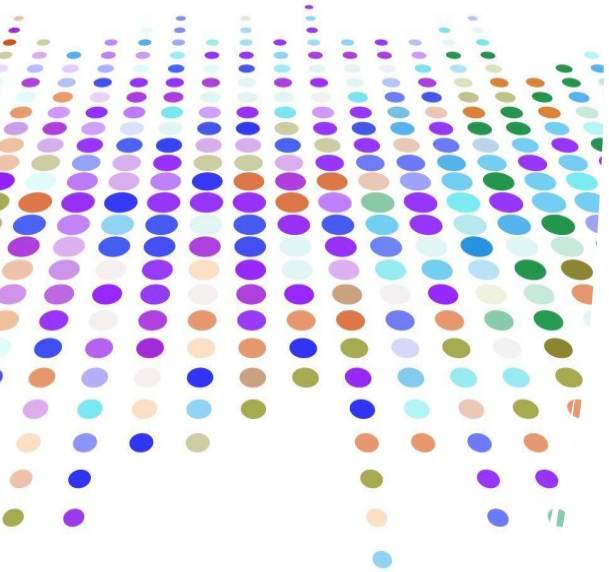
Keycloak-SSI: Post-Authentication Attribute Verification in Federated Identity Management Using Self-Sovereign Identity



The 23rd IEEE International Symposium on Network Computing and Applications, November 5, 2025

Mauladi, Ramin Yahyapour

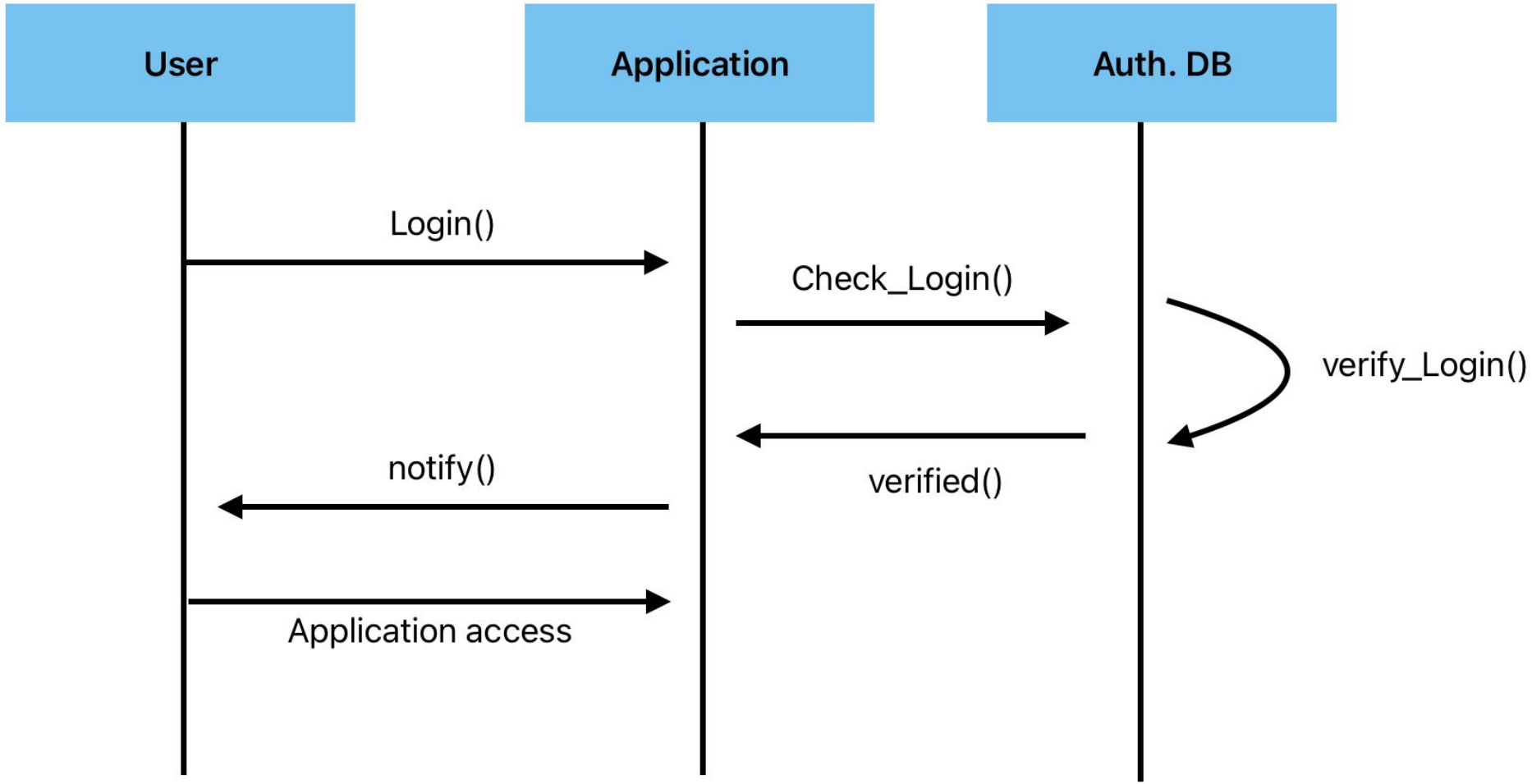
University of Göttingen, Germany

eScience group GWDG, https://gwdg.de

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

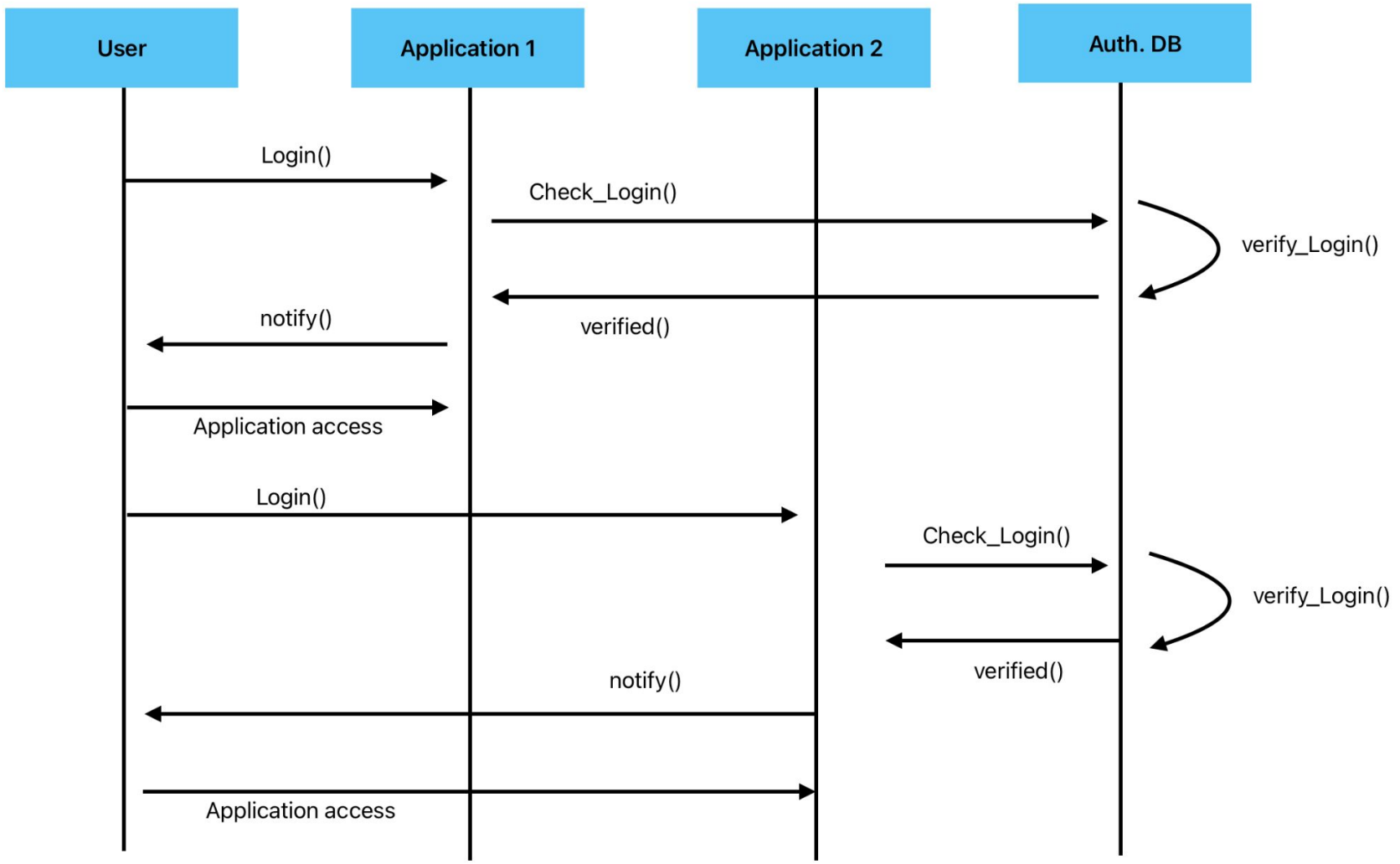
GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Single-App Login



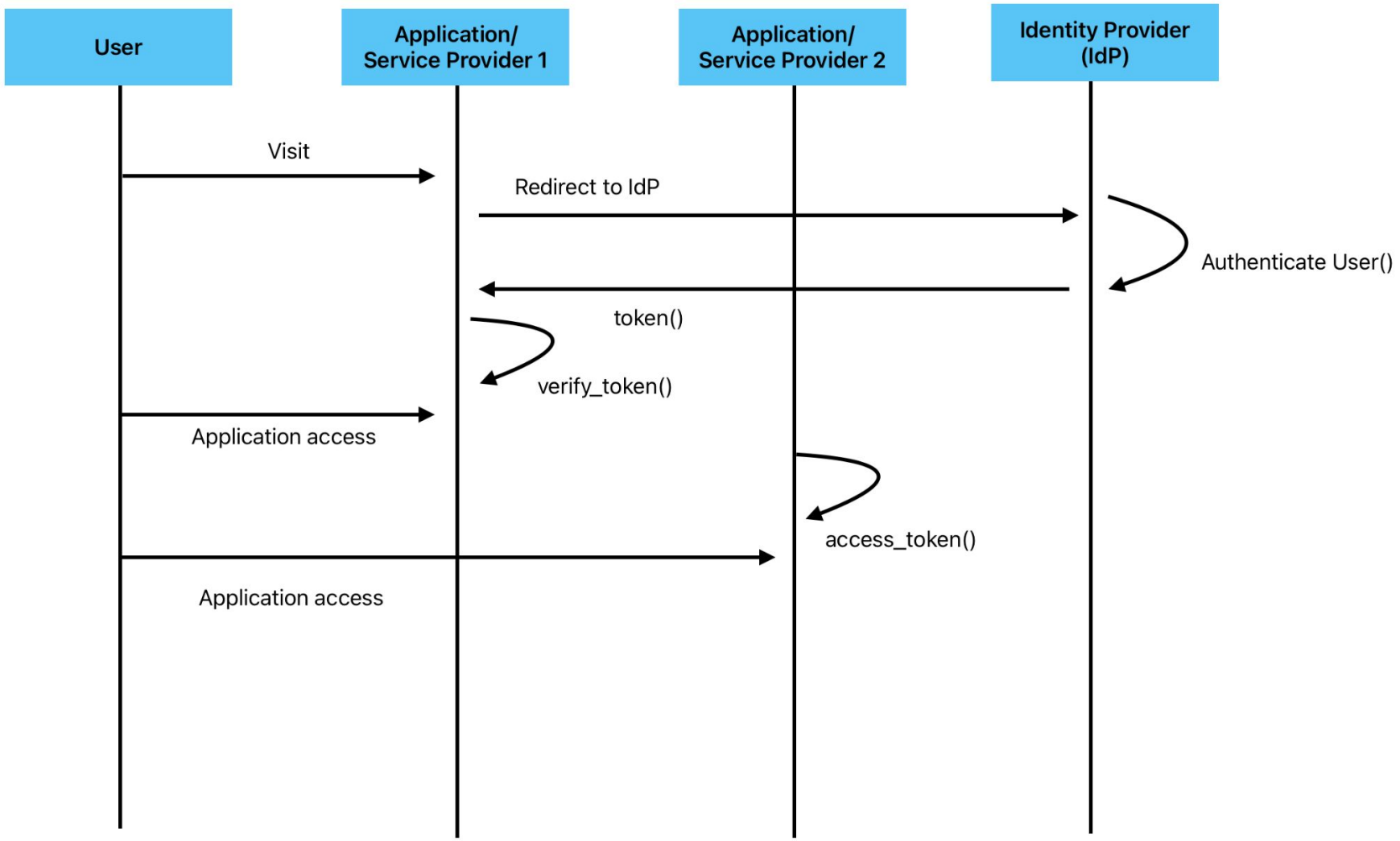
- Application requires direct access to Auth. DB

Multi-App Login



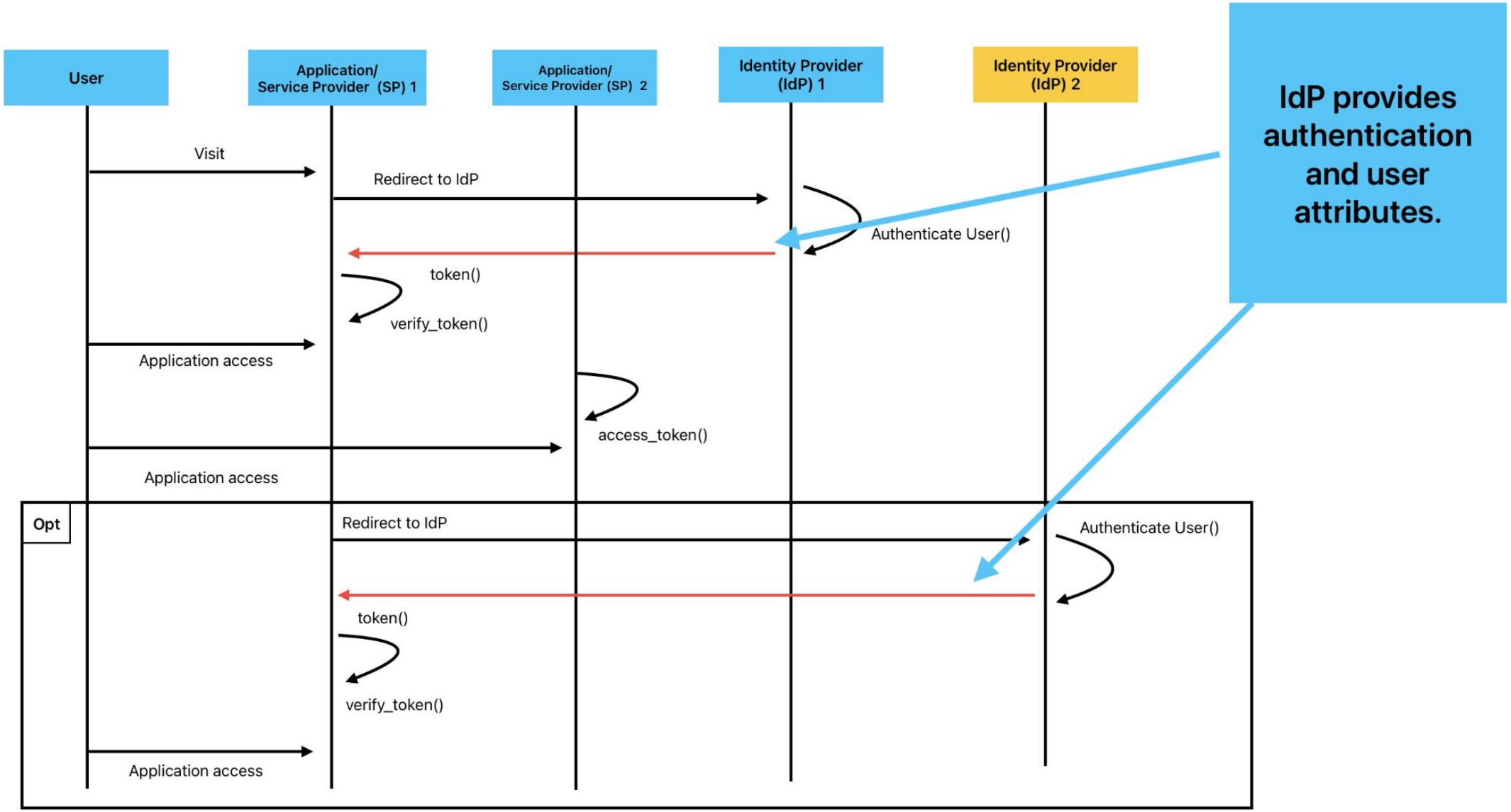
- Application requires direct access to Auth. DB
- User needs to log in to every application.

Single sign-on (SSO)



- One login for all applications in one organization.

Federated Identity Management (FIM)



What kinds of attributes can the IdP share with the SP?

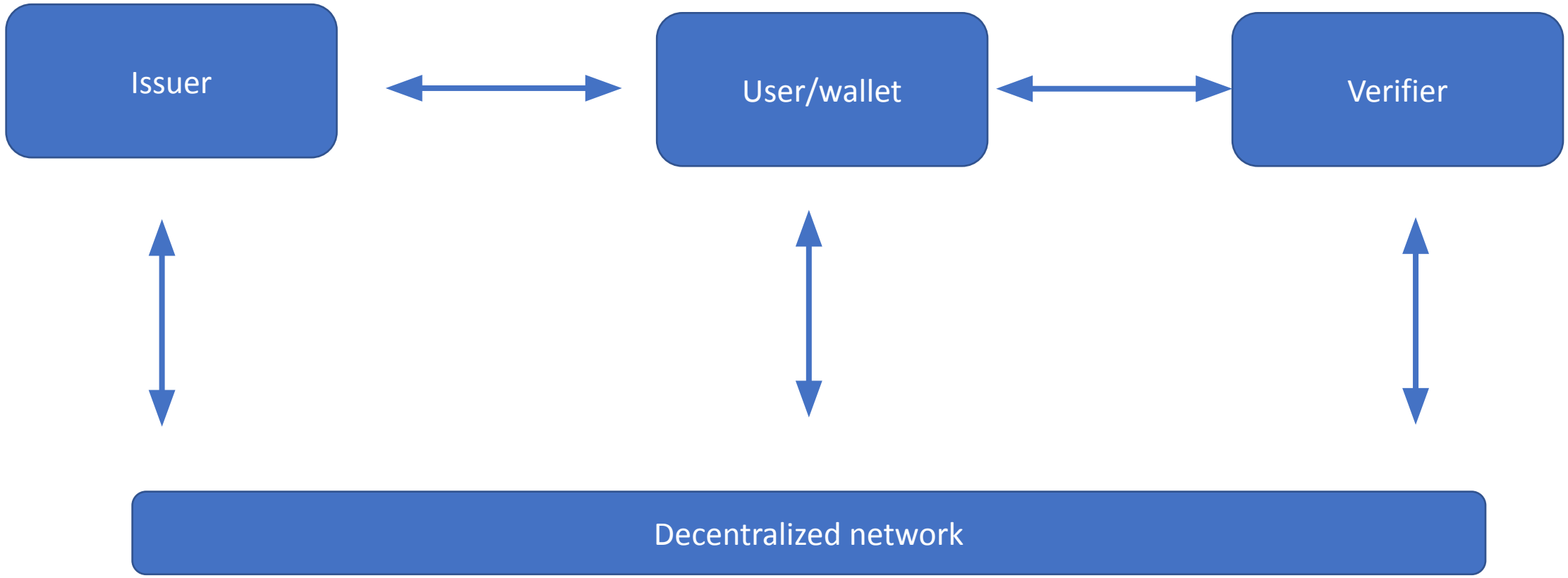
- First and last name
- Phone number
- Address
- Identity number
- Birthdate

- Organization name
- Tax number
- Bank account
- Others depend on the organization’s needs

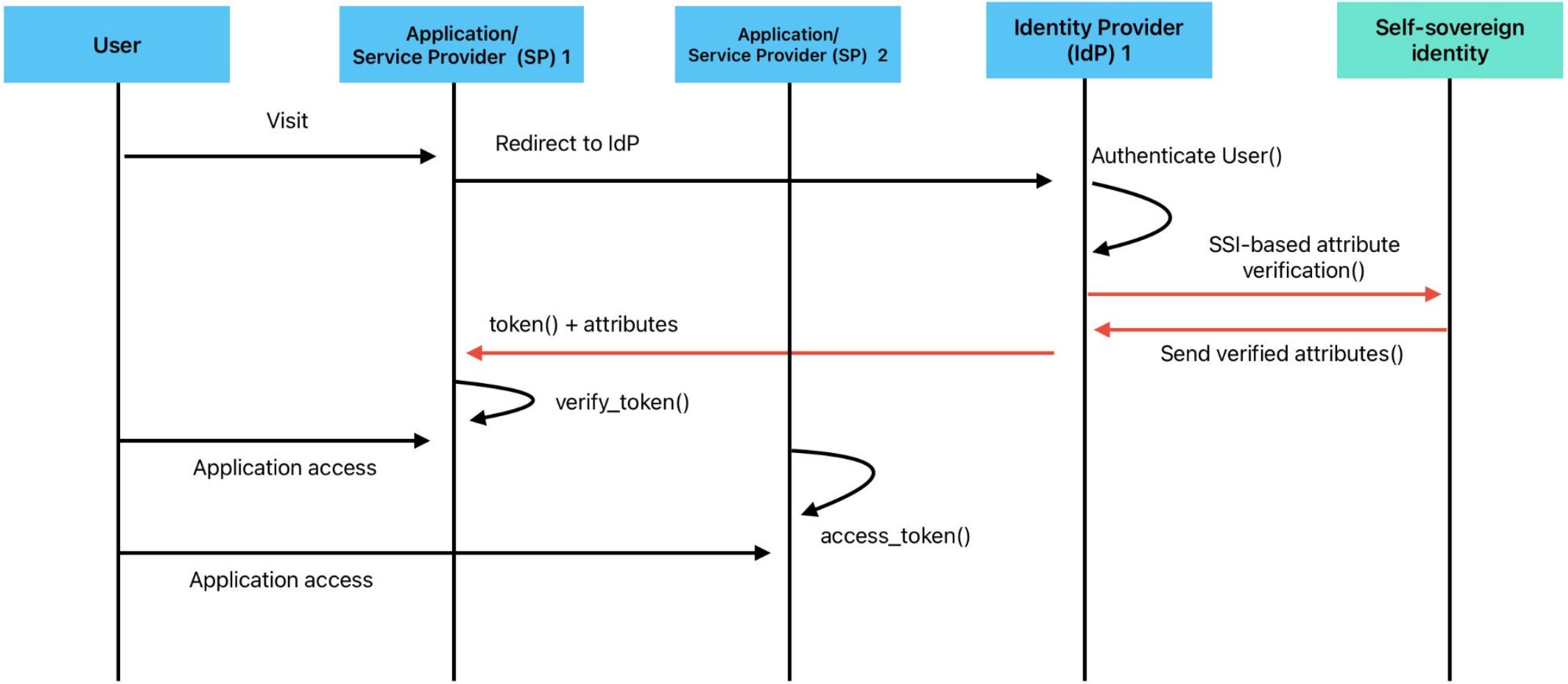
Research problems

- User: control the attribute data from user side
- IdP: reducing the burden on the IdP regarding protection of user attribute data.

Self-sovereign identity (SSI)



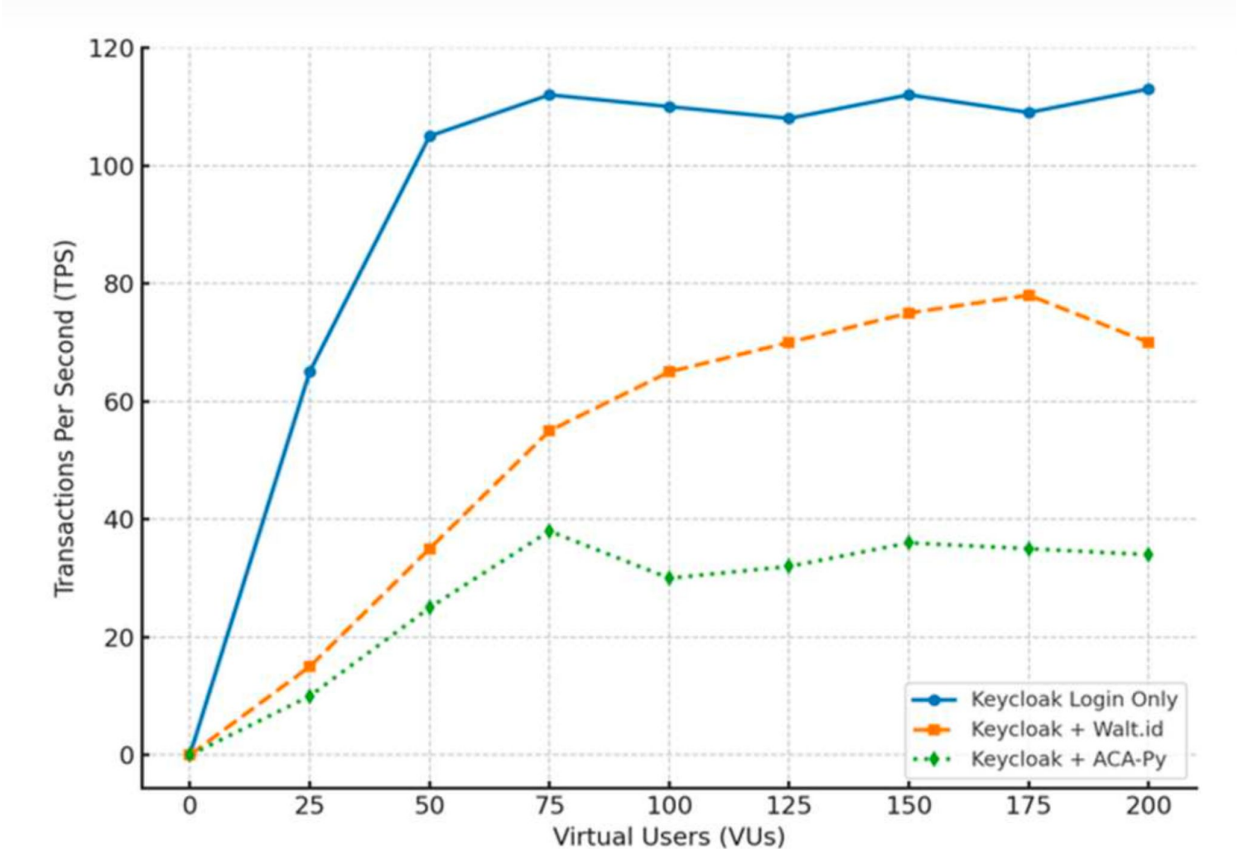
Post-Authentication Attribute Verification in FIM Using SSI



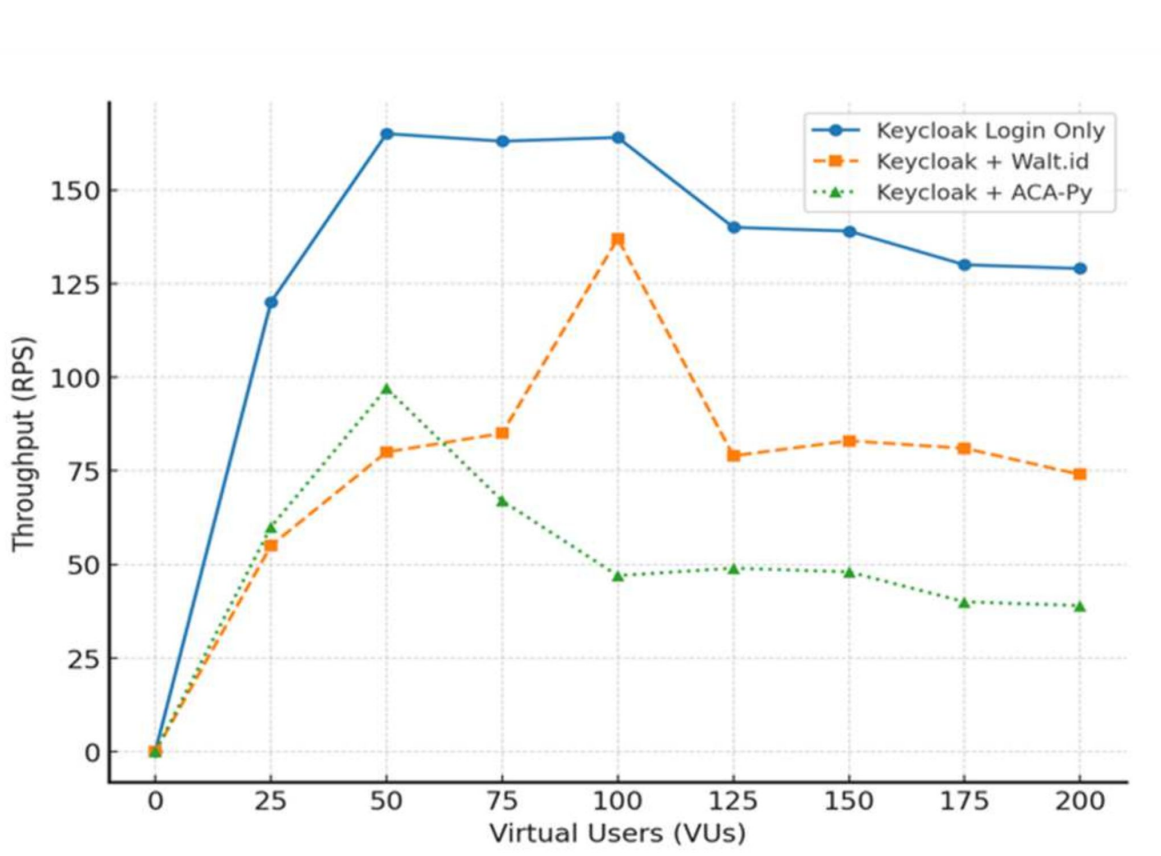
Evaluation (1)

- k6 performance testing (https://k6.io/)
- Keycloak (https://www.keycloak.org/)
- Build a module inside Keycloak for SSI verification
- We applied different virtual user loads ranging from 25 to 200
- compared three authentication configurations:
  - non-SSI Keycloak,
  - SSI with did:sov via ACA-Py, and
  - SSI with did:web via Walt.id

Evaluation (2)



Login And Attribute Verification Success Response Time Vs Virtual Users



Login and Attribute Verification Throughput vs Virtual Users

Conclusion

- We proposed a model and a preliminary implementation demonstrating how Federated Identity Management can be extended to verify credential attributes in the Self-Sovereign Identity ecosystem.
- With this proposed method, users can control their attribute data, and the IdP can reduce the burden of protecting user attribute data.
- This validates attributes without changing IdP authentication, enabling adoption of the new functionality

Q & A

Thank you!

Mauladi
mauladi.mauladi@stud.uni-goettingen.de
University of Göttingen, Germany
eScience group GWDG, https://gwdg.de

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen