Authentication and Authorisation for Research and Collaboration

Migration to a SP-IDP-Proxy in the DARIAH AAI

David Hübner, DAASI International / DARIAH

DI4R 2018
2018/10/10

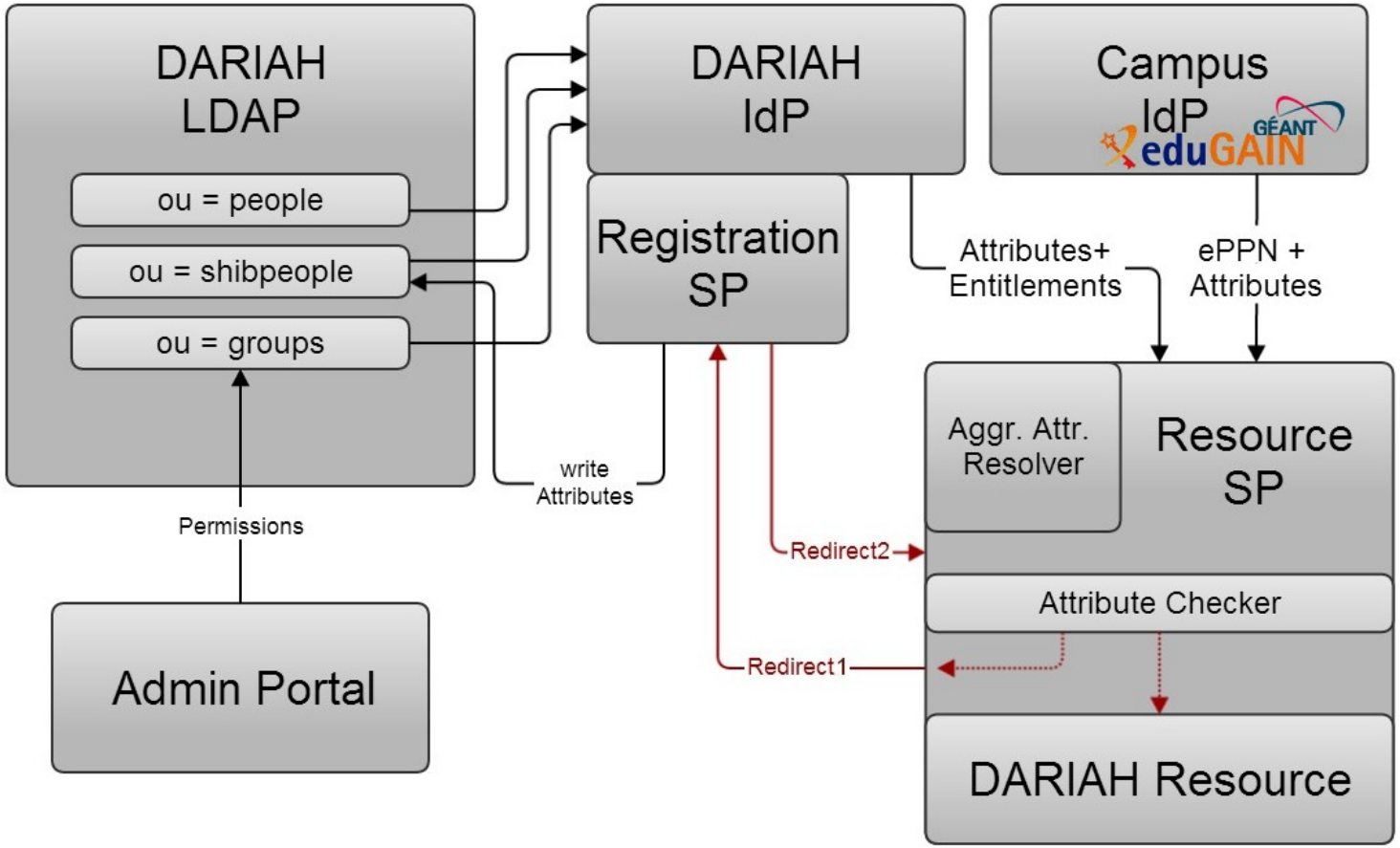
Content

- Short introduction to the DARIAH AAI
- Migration to a SP-IDP-Proxy architecture
  - Why? (→ Goals)
  - How? (→ Process and experience)
- Conclusion and future plans

Short introduction to the DARIAH AAI

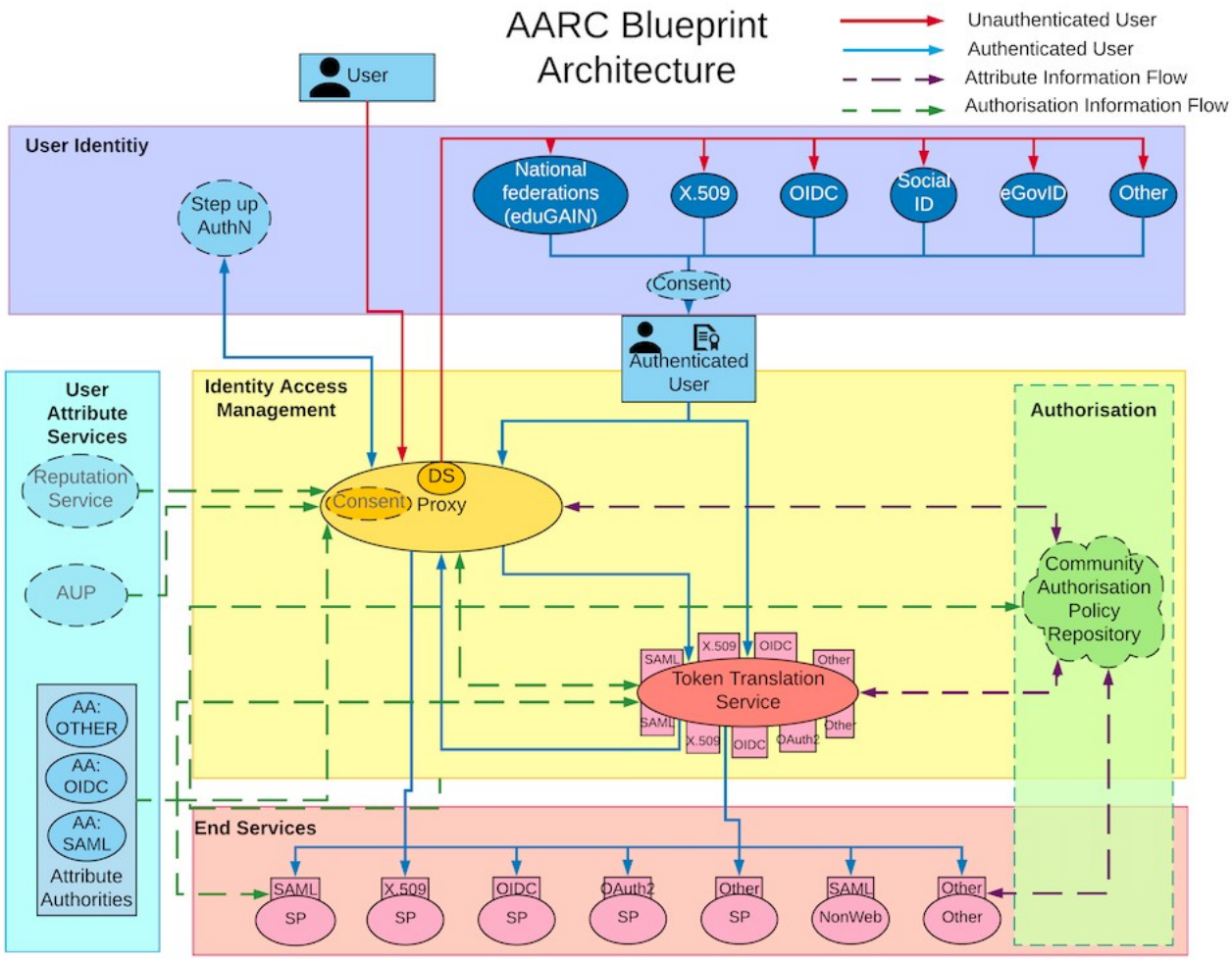
- Requirements for V1 of the DARIAH AAI included (~5 years ago):
  - Provide federated single sign-on to various services within the DARIAH research community
  - Manage authorization within DARIAH thorugh group memberships and PDP
  - Allow researchers to use their institutional account through eduGAIN…
  - ...and also provide a ‘Homeless’ IdP (which is also in eduGAIN → validation of accounts)
- Helpdesk to deal with user support and account registration requests
- Userbase ~4-5k users
- New requirements emerged...

Short introduction to the DARIAH AAI

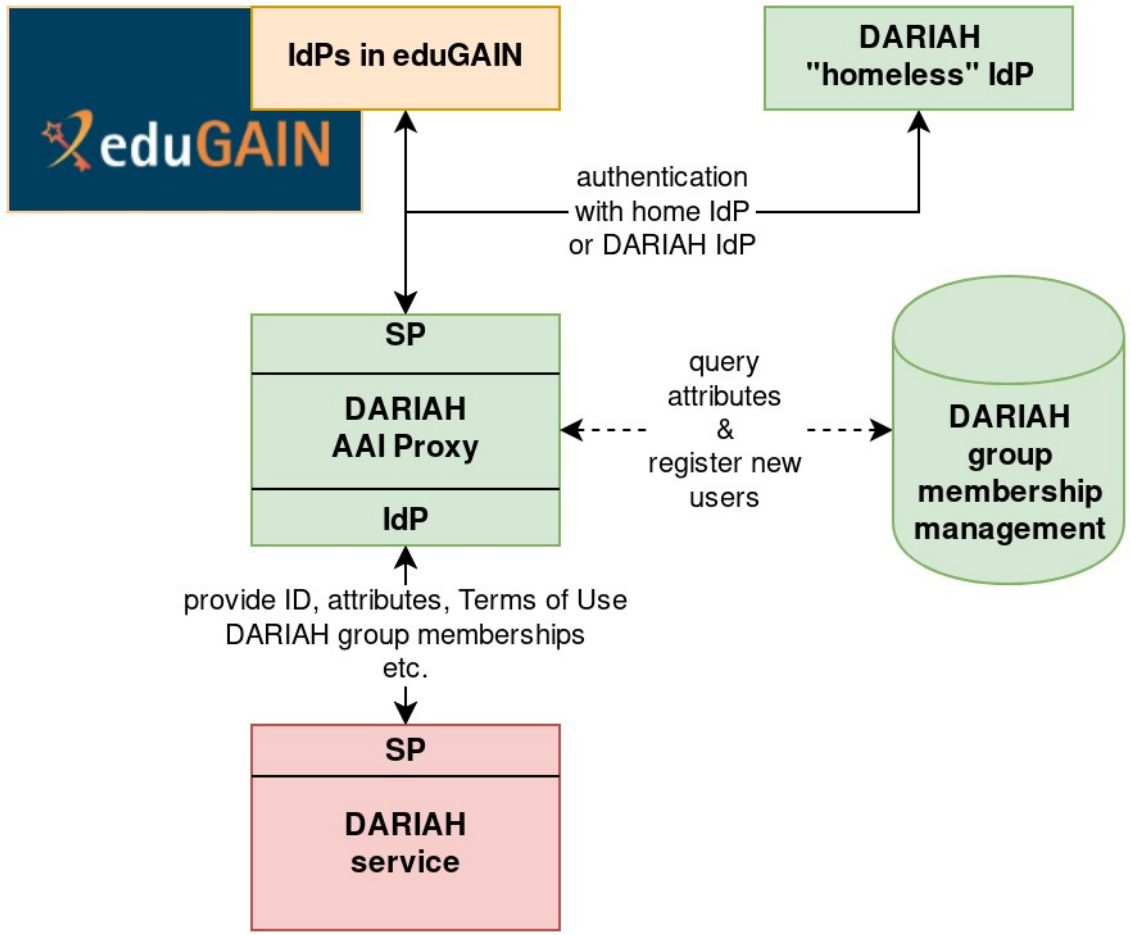


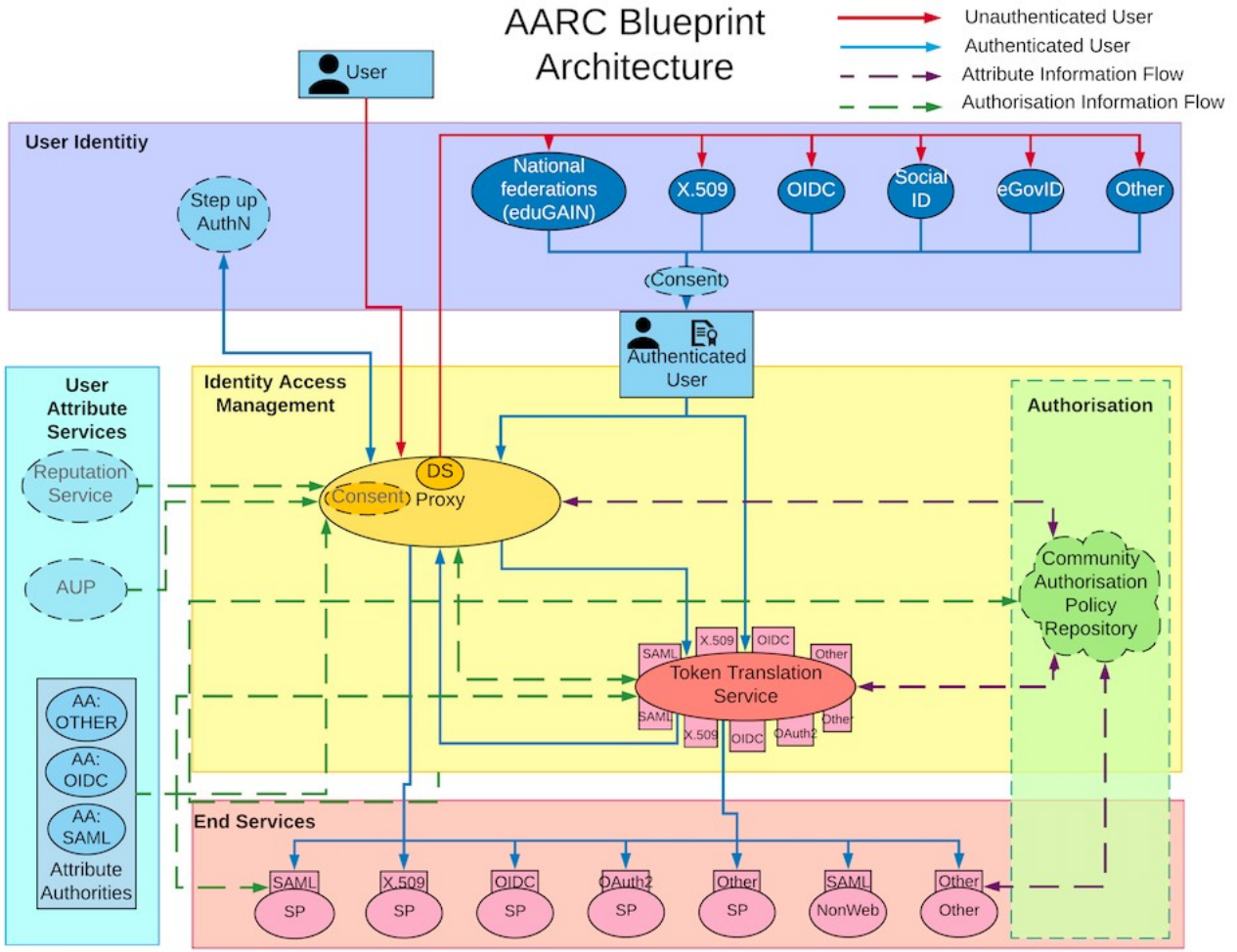
Reasons for migration to a SP-IDP-Proxy

- Scaleable solution to...
  - ...add more services
  - ...deal with policy decisions centrally
- Encourage non-homeless users at the ‘homeless’ IdP to actually use their institutional IdP
- Adoption of AARC results
- Be interoperable



Overview of the DARIAH AAI V2





Migration to a SP-IDP-Proxy

- In May 2017 we started planing implementation as an AARC pilot with two phases
  - Phase 1: Migration to SP-IDP-Proxy
  - Phase 2: Use the proxy for an interoperability pilot with EGI
- Sept. 2017 – April 2018: Implementation based on Shibboleth IdP and SP
- May 2018: Interoperability tests with existing DARIAH service
- July 2018: Move to production (it's the official way to connect a service to the DARIAH AAI now)
- In parallel: Work on Phase 2 (the EGI-DARIAH interoperability pilot)
  - Adoption of relevant AARC guidelines for infra-infra communication

Our experience with the process

- Changing a critcal infrastructure is not easy
  - Ensuring compatibility or upgrade paths for existing services
  - Which is especially challenging for end-services
  - This means trade-offs
- Technology-agnostic blueprint architecture + individual requiremets = tricky implementation
- Technical solution is one thing…
- ...policy is another

Conclusion

- It was the right decision
- Feedback since going live has been positve
- No major issues
- There's still work to be done
  - … finalize the EGI-DARIAH interoperabilty pilot
  - … keep up-to-date
  - … new internal requirements

Thank you

Any Questions?

david.huebner@daasi.de

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).