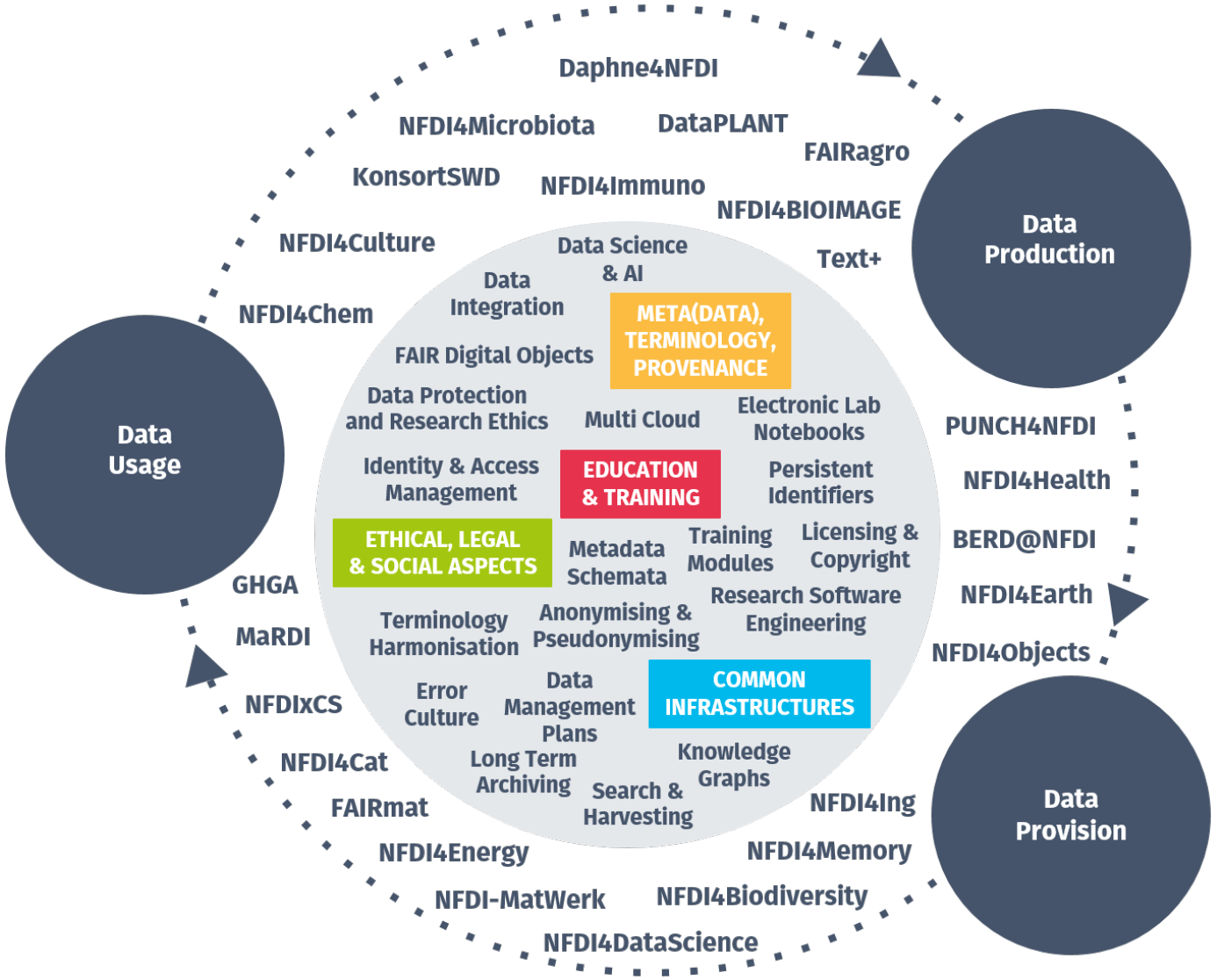
base4 nfdi Basic Services for NFDI

Experiences of the CAAI Operators

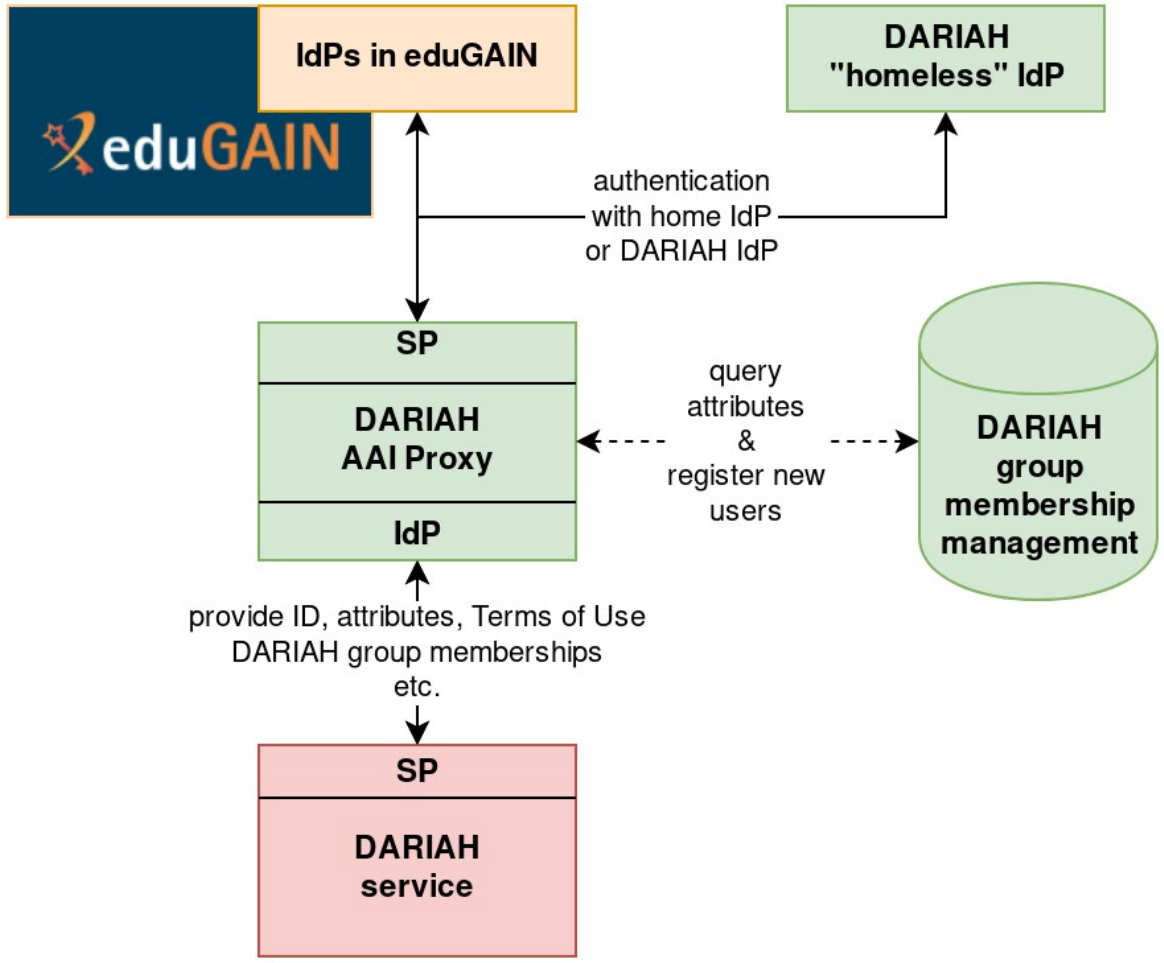
Workshop IAM Basics #2, 24.08.2023



Funded by DFG as part of NFDI.
Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232

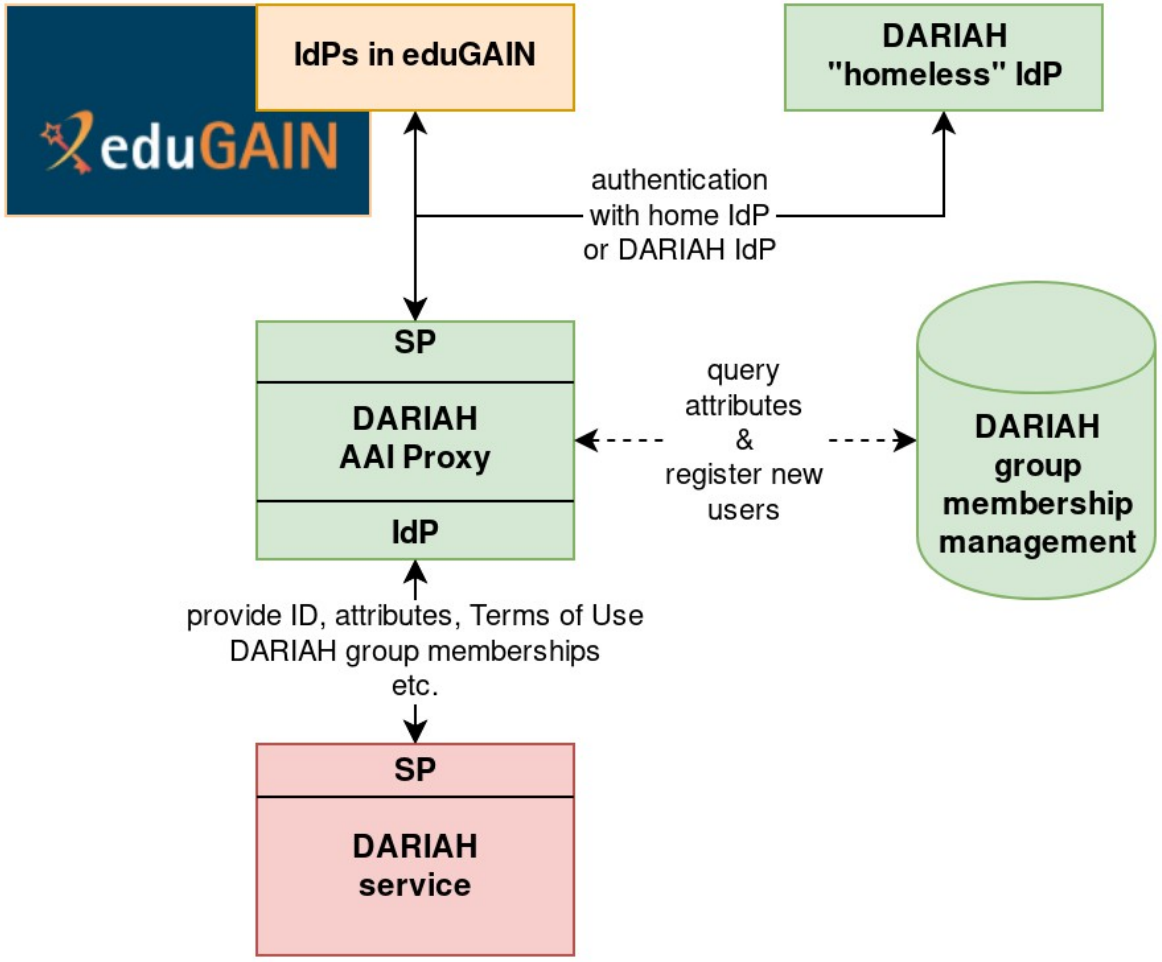
Operating the DARIAH-AAI

- In the DARIAH-AAI we offer a “homeless” IdP for users with no HO IdP identity from eduGAIN. This poses additional challenges.
- A lot of users do not have a HO IdP for various reasons (e.g. guest researchers)
- For these users vetting of identities is difficult, since we can’t rely on the information provided by the HO
- We use a combination of whitelisted email domains from known organisations and manual vetting based on information provided by the researchers
- Due to the DARIAH homeless IdP being in the DFN-AAI federation this vetting process is particularly important



Operating the DARIAH-AAI

- Service operators sometimes struggle to implement federated authentication (SAML or OIDC) in their applications
- To assist them, we provide documentation, incl. “How-To” tutorials for e.g. Shibboleth SP, technical trainings and workshops
- We set up and operated a Helpdesk:
  - for technical questions, including service integrations
  - for end users, including account vetting on the “homeless” IdP
- Due to open standards (SAML2, OIDC, AARC guidelines, etc.) the actual technical solution is of less importance. We changed the AAI proxy component from Shibboleth to SimpleSAMLPHP without much problems
- Generally, sustainable and pemanent funding is needed for operating the service, which usually is difficult in research projects



Operating unity

- Used at EUDAT B2ACCESS, Helmholtz AAI, Clarin IdP, …
- Offers upstream authentication based on SAML, OAuth2/OIDC, LDAP
- Pre-configured “social” IdPs
- Offers accounts to “homeless” based on X.509 or username/password
- Build-in extensions for account linking, Policy management, group management, MFA using TOTP or FIDO
- Powerful configuration makes it easy to follow multiple standards and guidelines like SAML2, OAuth2/OIDC, AARC, ...

base4 nfdi

Operating unity

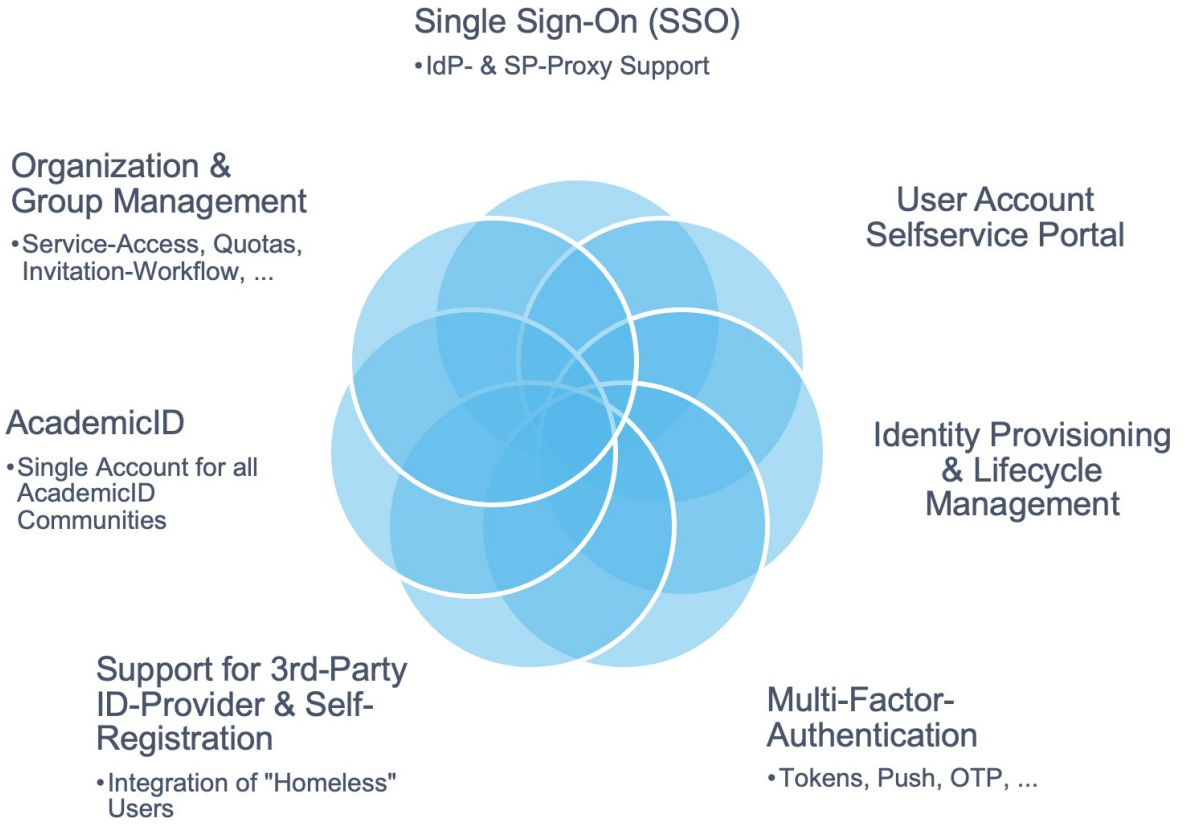
- X.509 handling is difficult since DN changes in renewal and can’t rely on information provided by the HO
- “Social” IdPs deliver different information and not all guarantee persistent identifiers
- Linked accounts are tricky in deprovisioning, if resources were bound to one of the upstream identities
- Deprovisioning based on an additional tool
- MFA needs some improvements in signaling and honoring MFA from upstream IdPs

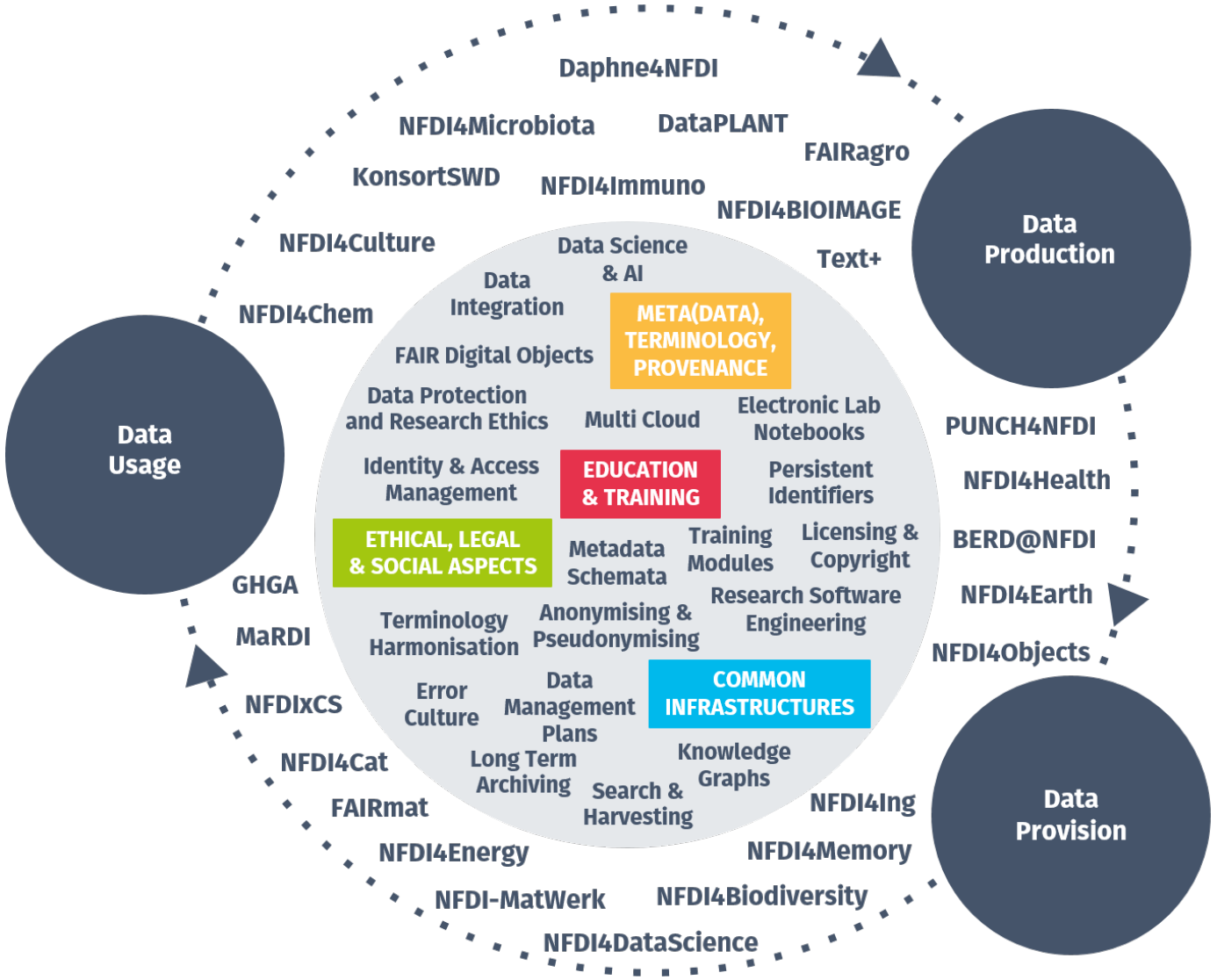
base4 nfdi

Experiences of operating AcademicID

- Availability Management
  - Authentication & authorization services need to be available 24/7. Any interruption of these services needs to be fixed ASAP, otherwise no user can access any IT service. Operation of these services should cover: load-balancing, failover, monitoring (geo-)redundancy, backup, testing
  - Identity (de)provisioning and lifecycle services are less critical, since only a small number of users will usually be affected by an interruption.
- Security
  - IAM infrastructures are “crown juwels” that need a high level of security protection.
  - Restrict administrative access: use MFA, dedicated administration workstations and networks/VPNs, ...
  - Document and regularly audit critical changes, e.g. to administrative accounts.

AcademicID CAAI Solution





Funded by DFG as part of NFDI.
Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232