PAUL SCHERRER INSTITUT

PSI

ETH-RAT ORD

Spencer Bliven, Khadidja Malleck

Identity Access Management

2023-06-29 ETH-ORD Workshop on interoperability

Identity and Access Management

- **Identity:** descriptive information about the user (name, email, affiliation, etc.)
- **Authentication:** identifying the user securely and unambiguously to the service
- **Authorization:** defines what rights, permissions, and access a user has on a service
- **Roles:** Organize users into groups with shared authorizations

IAM in Open Research Data

- Most ORD services need IAM
  - Open ≠ Anonymous
  - Track data provenance
  - Limit access, eg. by affiliation
- Interoperable services require interoperable IAM
  - Users experience Single Sign On (SSO)
  - Services receive authentication code and requested identity & authorization info
  - Delegate authorization between services (eg. using JSON Web Tokens)

Authentication

- Multiple existing options for authentication
- EG-SI should require **federated authentication** for all M2 projects
- Identity providers should have strong security (MFA, security audits, etc)

Provider	Target Audience	Technology
eduGAIN	Global academic users	SAML
SWITCH eduID	Swiss residents (primary identity for some Swiss universities; account creation open to the public)	SAML, OpenID Connect
SWITCH AAI	Swiss residents & academic users (using existing university accounts)	SAML, OpenID Connect
Umbrella ID	Users of Photon and Neutron sources	SAML
Globus Auth	Global	OpenID Connect
ORCID	Academics	OAuth2 (No identity features)
Institutional Identity Providers	Limited	Active Directory, LDAP

Identity

- Most institutes maintain their own identity provider with *institute-specific* identities
- Efforts to provide *user-centric identities* (SWITCH eduID, Elixir LS Login, etc) are not fully adopted at ETH and provide limited authorization claims
- Federated identities rely on identity providers for all information
  - Heterogeneous verification of information
  - Lack of standards between different providers (eg claim nomenclature)

Authorization

- Possible to issue authentication claims through the identity provider, but no standardization
- Most authorization handled in application logic currently
  - Often difficult to add claims (may require involvement from central IT)
- No group management

IAM Ideas for M2

- Draft with recommendations for IAM management for M2 projects:
  - https://drive.switch.ch/index.php/f/6020320606
  - Contributions welcome!
- Additional resources for projects to add interoperable IAM to existing services
  - Add central group management system
    - UI to manage groups and roles that are shared between multiple services
    - Integrate with IAM provider to provide standard claims
    - Useful for PSI SciCat data catalog. Other use cases?
  - System to share authorization claims between services at different institutions
    - Need a strong use case, since otherwise it can be done within application logic
  - Integration between storage access (S3) and service authentication (OIDC)