Karlsruhe Institute of Technology

Account Linking Service ALISE

Diana Gudu, Marcus Hardt,
Paul Millar, Gabriel Zachmann

Mar 2025

ALISE

Karlsruhe Institute of Technology

Account LInking SErvicE (ALISE)

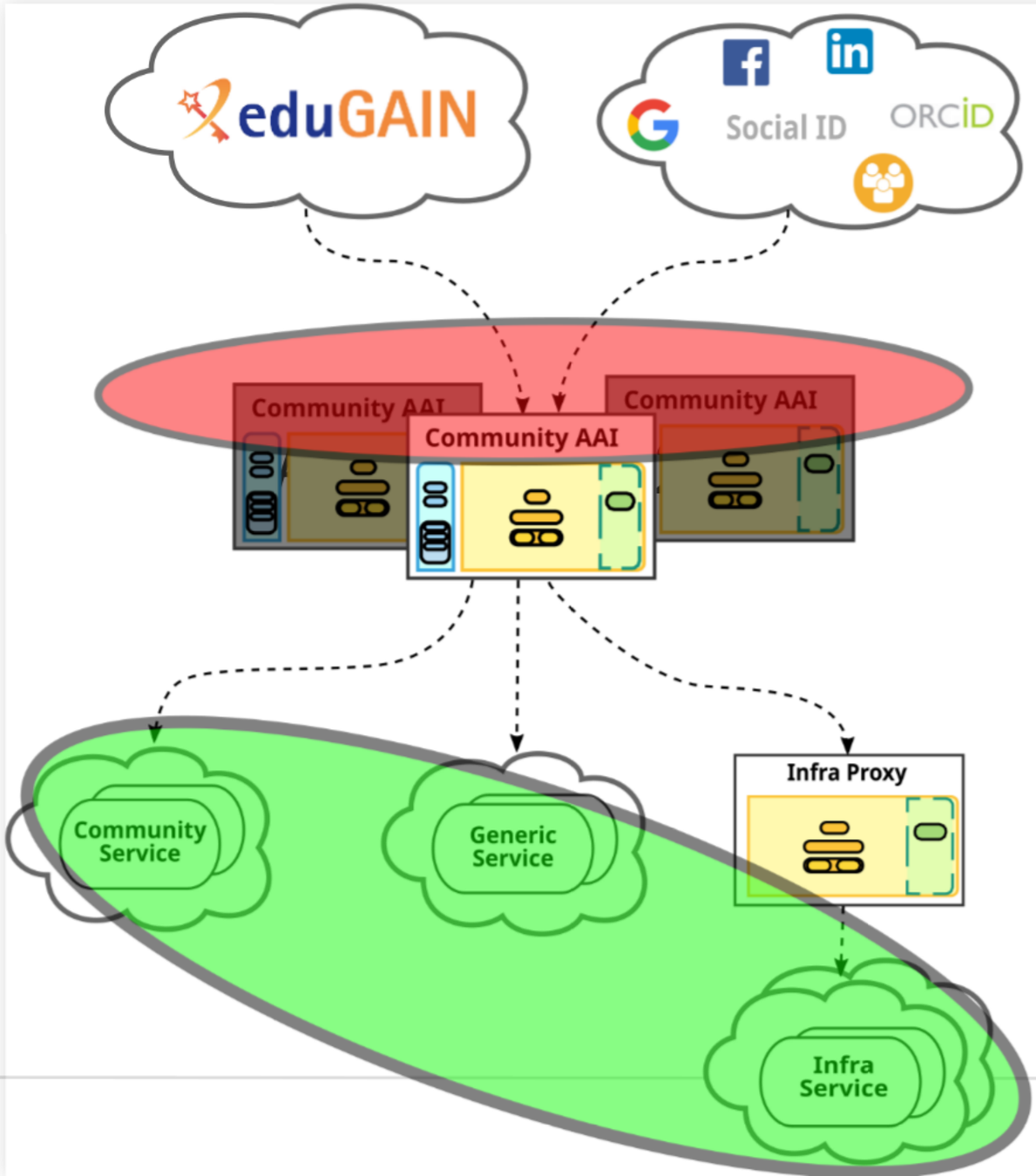
Account Linking Wonderland

Background

Different types of Account Linking

- Link federated identity to
  1. another federated identity
     - There is a logical relation between both identities
     - e.g. link an ORCID to your Home-ID
  2. a technical account
     - e.g. link Home-ID to unix account on an HPC Cluster

Where is ALISE linking accounts?



Technical Note

- This kind of linking is actually provisioning
- This kind of linking MIGHT happen automatically
- We mean: “Site-local account linking”

ALISE

Use Case

Example

- File on storage service:

```
-rw-r--r-- 1 marcus ant-researchers 210 Oct 4 09:19 /projects/ant-science/alise.py
```

- Access this file locally:

```
cat /projects/ant-science/alise.py
```

- Access this file via federated service:

```
curl https://hpc.example.org/projects/ant-science/alise.py -H "Authorization:
Bearer 'oidc-token egi'"
```

- This requieres correct and consistent mapping of
  - Federated users to local accounts
  - Entitlements / Groups / VOs to local groups

How does ALISE work?

- ALISE drives the transition
- For this to work, an existing local account is required
- ALISE web app offers two logins
  - First with techical computer centre account
  - Then with (multiple) federated accounts
- ALISE enabled tools use REST interface to obtain mappings
- ALISE may be self-hosted, or used as a service
  https://alise.data.kit.edu

Life demo (WEB)

- Account LInking SErvicE (ALISE)
  https://alise.data.kit.edu

Life demo (REST)

```
curl  https://alise.data.kit.edu/api/v1/target/vega-kc/mapping\
      /issuer/$(urlencode.py https%3A%2F%2Flogin.helmholtz.de%2Foauth2)\
      /user/$(urlencode.py 6c611e2a-2c1c-487f-9948-c058a36c8f0e)\
      ?apikey=bnginyourdreamsinyourdreamslxbmu | jq
```

Example output


```
{
  "internal": {
    "sub": "3c498039-1754-4f9d-b71c-5c13739e8875",
    "iss": "https://sso.sling.si:8443/auth/realms/SLING",
    "username": "marcush",
    "last_seen": -930016800,
    "display_name": "Marcus Hardt"
  },
  "external": [
    {
      "sub": "d7a53cbe3e966c53ac64fde7355956560282158ecac8f3d2c770b474862
      "iss": "https://aai-demo.egi.eu/auth/realms/egi",
      "last_seen": 13552005600,
      "display_name": "Marcus Hardt"
    },
    {
      "sub": "104223951181002749851",
      "iss": "https://accounts.google.com/",
      "last_seen": 13552005600,
      "display_name": "Marcus H"
```

API Key

Getting an apikey is simple:

```
curl  https://alise.data.kit.edu/api/v1/target/vega-kc/get_apikey \
      -H "Authorization: Bearer $(oidc-token egi)"
```

Timeline

Current state

- Suppported Computer Centres:
  - VEGA
  - KIT
  - KBFI
  - PSNC (self-hosted instance)
- Supported Identity Providers:
  - EGI-Checkin
  - Google
  - Helmholtz-ID
  - (it’s trivial to add more)
- Services making use of ALISE:
  - dCache

Future Work

- Include more sites
- Support LDAP
- Integrate with **`ssh-oidc`**
- Support **`entilement`** / group based mapping

Questions

- https://alise.data.kit.edu
- codebase git@codebase.helmholtz.cloud:m-team/tools/alise.git
  https://codebase.helmholtz.cloud/m-team/tools/alise
- github git@github.com:m-team-kit/alise.git
  https://github.com/m-team-kit/alise

Since we're at it

Account linking

(on the higher level)

- Should NOT be used for establishing a second login path
  - Deprovisioning WILL be your nightmare
  - Freshness of some attributes is critical
- Instead:
  - Use the second login only to “obtain additional attributes linked to the same user”
  - be creative!