Karlsruhe Institute of Technology

naco

The “N” Attribute COnformity checker

Marcus Hardt, Gabriel Zachmann

Mar 2025

Technical Overview

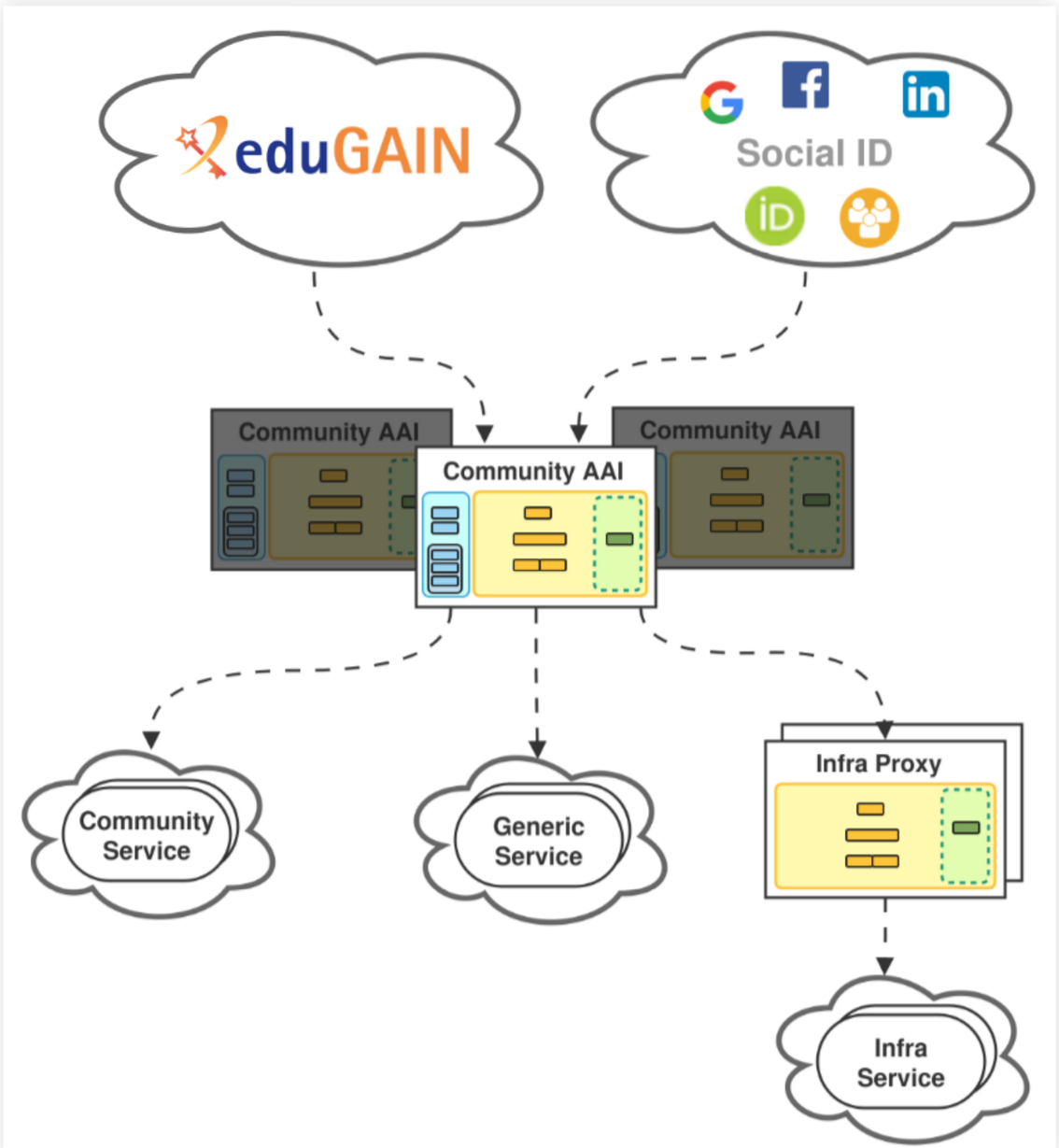
Motivation

Why am I showing this in here in Taiwan / Asia?

1. Interoperability!
2. Interoperability!
3. Interoperability!

Global Interoperability!

AARC BPA


eduGAIN
Social ID
Community AAI
Community AAI
Community AAI
Community Service
Generic Service
Infra Proxy
Infra Service

Context

- Federated Identity Management in Research
  - ~~Community AAIs~~ Collaboration Management Platforms
    - act as proxies between IdPs and services
  - S
- Attr
  - D
  - C
  - N
- Risk

Service Interoperability

- Inconsistent attributes make service development more complex
- This leads to: less services / bad user experience
- Which threatens the success of independent ID-Management in science

How does **naco** help?

- Validate attribute release
- Focus is on OIDC tokens
  - SAML assertions can be uploaded via API
- Continuously monitors many Community AAIs
- Your AAI HERE!!!

Drop me an email: hardt@kit.edu

`naco` Features

- Highly configurable attribute specifications
- Distinguishes mandatory vs. optional attributes
- REST Interface to interface with external tools
  (e.g. https://aarc3.cat.argo.grnet.gr)
  - More details here (Slides 82-89)

Supported Specifications

- AARC-G056 (Draft)
  - AARC Attribute guidelines
  - Interoperability requirements for federated access
  - Community-defined attribute expectations
  - Defines basic and extended attribute sets
- NFDI Attribute Profile
  - Attribute requirements
  - Based on an early draft of AARC-G056
  - Additional optional attributes

Attribute Specification System

- Make use of Attribute Catogories
  - Example: Name
    (`flaat-userinfo --oidc login | grep -Ei "(marcus|hardt)"`

    - “display_name”: “Marcus Hardt”,
    - “family_name”: “Hardt”,
    - “given_name”: “Marcus”,
    - “name”: “Marcus Hardt”,
    - “preferred_username”: “marcus”,
    - “sn”: “Hardt”,
- **`naco`** (actually G056 likely) is happy, if a name is found

Where `naco` gets information

- OIDC
  - User Info endpoint
  - Access Token body
  - Token Introspection
- Validation Checks
  - Attribute presence (single or compound keys)
  - Type correctness (string, list, bool, dict)
  - Scope correctness (external vs community scopes)
- Result Generation
  - Per-attribute and per-source results
  - Summary verdict per Community AAI
  - Colour-coded: green=OK, red=missing/error

Attribute Sets

- Mandatory Attributes (Basic Set)
  - Identifier (**sub+iss**, **eduperson_unique_id**, **voperson_id**)
  - Name information (**name**)
  - E-Mail (**email**, **voperson_verified_email**)
  - Home organisation affiliation (**voperson_external_affiliation**)
  - Assurance levels (**ass**, **assurance**, **eduperson_assurance**)
- Optional Attributes (Extended Set)
  - Groups and roles (**eduperson_entitlement**)
  - Capabilities (**entitlements** (**eduperson_entitlement**)
  - Agreement to policy (**voperson_policy_agreement**)
  - ORCID identifier (**orcid**)
  - Preferred email (**voperson_preferred_email**)
  - Supplemental Name Information (**given_name**/**family_name**)
  - Authentication Profiles (**acr**)
  - External Idenfifier (**voperson_external_id**)
  - SSH Keys (**ssh_public_key**)
  - Verified Email Address (**email_verified**)
  - The domain name of the users Home-Org. (**org_domain** (**organization_name**) (**schac_home_organization**)
  - Version of the AARC Profile (**aarc_ver**)

Warning: Attribute names are based on an early and old draft of AARC-G056!!!

Currently Monitored Communities

- E
  -
- G
  -
- In
  -

naco - the NFDI Attribute COnformity Checker

Listed are **attribute categories** (e.g. Identifier) and the actual attributes that belong into these attribute categories. Please check the Draft AARC-G056 and the NFDI Attribute Profile for more information.

Mandatory Attributes

Product	Identifier	Name	E-Mail	Affil. at home-org	Assurance	Last Update
didmos (User Info)	sub+iss voperson_id	name	email	voperson_external_affiliation	eduperson_assurance	2026-03-18 04:15
didmos (Summary)	OK	OK	OK	OK	OK	2026-03-18 04:15
Product	Identifier	Name	E-Mail	Affil. at home-org	Assurance	Last Update
RegAPP (User Info)	sub+iss eduperson_unique_id voperson_id	name	email	voperson_external_affiliation	eduperson_assurance	2026-03-24 15:15
RegAPP (Access Token)	sub+iss	---	email	---	---	2026-03-24 15:15
RegAPP (Introspection)	---	---	---	---	---	2026-03-24 15:15
RegAPP (Summary)	OK	OK	OK	OK	OK	2026-03-24 15:15
Product	Identifier	Name	E-Mail	Affil. at home-org	Assurance	Last Update
Helmholtz-Login (User Info)	sub+iss eduperson_unique_id voperson_id	name	email	voperson_external_affiliation	eduperson_assurance	2026-03-24 15:15

https://cvs.data.kit.edu/~naco

Use Cases

- Compliance Monitoring
  - Continuous validation of attribute release
  - Early detection of configuration drift
- Service Provider Onboarding
  - Verify Community AAI meets requirements before integration
- Federation Operations
  - Compare attribute coverage across Community AAIs
  - Support standardisation efforts

The Future Is

- Add more CAAIs
- Ensure full AARC G056 compatibility
  - Once AARC G056 is final(ly final)
- Board of Shame
  - (for the home-IdPs)