Leibniz-Institut für
Astrophysik Potsdam

Particles, Universe,
NuClei and Hadrons
for the NFDI

PUNCH4NFDI : AAI + (Accounting/Assignment)

H. Enke + O. Michaelis & EScience Team | AAI Meeting PUNCH | 27.06.2025

AAI: High level Policy Questions

1. Top Level (Communities)

   Can we accept more than one source of AAI

   1. Current policy: only PUNCH-AAI (Unity Helmholtz) is accepted
      1. But: all Helmholtz-AAI VO in principle can ask for e.g. a gitlab/intranet account
      2. Possible to also accept (via EDUGain) more collaborators from other institutions via DFN/EDUGain Identification
      3. Mapping via Group assignment in VO-Groups
   2. Other communities (or parts of ‘our’ communities)
      1. ILDG: Indigo + Policy engine
      2. Belle 2 : Indigo
      3. Lifescience IAM (e.g. with de.NBI)
      4. IVOA is working on own implementation

AAI: High level Policy Questions

1. Agreements with resource providers
    1. PUNCH-AAI accepted by :
        - In-Kind Contributors (type 1)
        - CP4 with additional MyToken requirement
        - S4P with additional OIDC token
        - S3 storage with extra authorization/assignment
        - REANA / Kubernetes by policy / assignment
        - E.g LRZ with special setup) (for Astro experiments ..), Göttingen/NHR
        - U Münster
    2. In-Kind Contributors (type 2):
        - E.g. FZ Jülich with own Account requirements
        - Same situation with most NHR

Resource Providers:
Evaluating / Managing AAI information

- For C4P and S4P : see other presentation
- Proxy Applications: KeyCloak
  - Desy Hamburg,
  - AIP
- For services running at AIP:
  - Intranet, Results,
  - DRP registry
  - Gitlab, CI/CD
  - REANA / Kubernetes
  - Helpdesk

  Use of **KeyCloak** as provider of information, derived from PUNCH-AAI EduPerson information (and additional tokens)

AIP Keycloak Auth flow

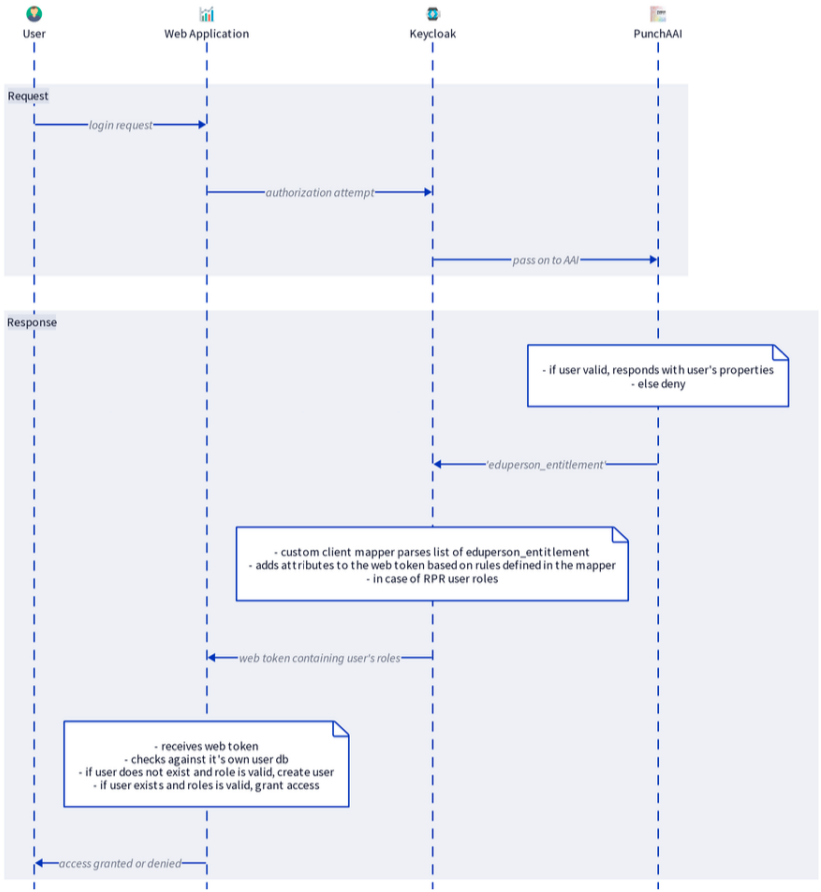
- web application auth that requires specific user information

- is user registered at Helmholtz AAI

- if yes, fetch user's metadata (i.e. *eduperson_entitlement*)

- create user in Keycloak and enrich with metadata

- authorize user, pass on valid token, containing mapped attributes



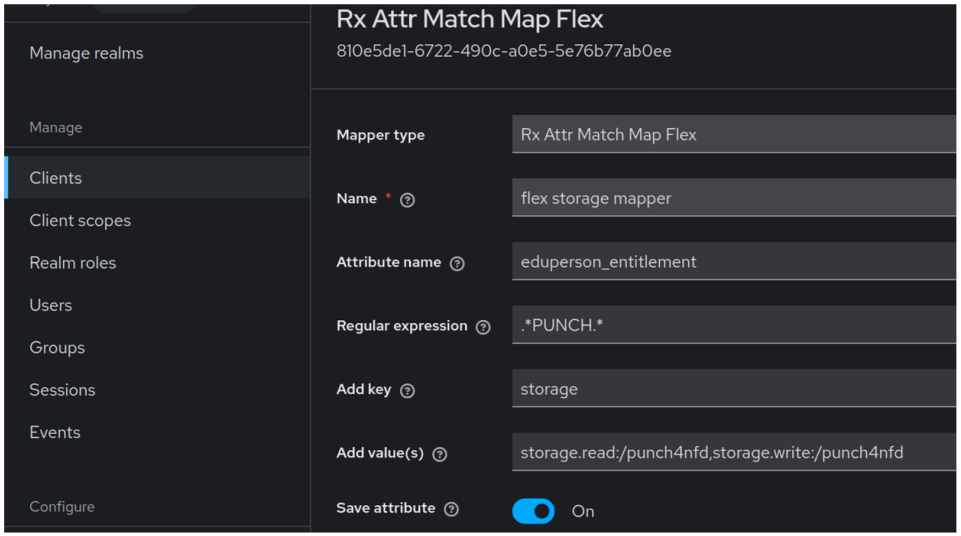
Available Mappers

KeyCloak:

Implemented
Regex-Parser + Mapper

- several custom AIP written mappers are available
- they distribute groups, roles or any attribute based on metadata delivered from the Helmholtz AAI

- for example the regex based flexible attribute matcher



User Token Response Example


```
{
  "acr": "1",
  "allowed-origins": [],
  "email": "omichaelis@aip.de",
  "email_verified": true,
  "groups": [
    "create-realm",
    "p4n_aip_rpr:project_owner",
    "default-roles-master",
    "offline_access",
    "super_user",
    "admin",
    "uma_authorization"
  ],
  "iss": "https://aipoidc.aip.de/realms/punchaai",
  "resource_access": {
    "account": {
      "roles": [
        "manage-account",
        "manage-account-links"
      ]
    }
  },
  "scope": "openid profile email microprofile-jwt",
  "sid": "986da470-e4cb-4833-9cbd-7bcc01457d70",
  "storage": [
    "storage.read:/punch4nfd",
    "storage.write:/punch4nfd"
  ]
}
```


KeyCloak:

Implemented
Regex-Parser + Mapper

Resource differences: How to cope?

Life Cycle of data:

1. Creation / generation => community managed access
2. Preparation of science ready data => community managed access (embargoed data, e.g.)
3. Data Publication => public access, archival management
4. Data exploitation => group/individual start of new Lifecycle
    - Support for publication process:
        - Storage / archive
        - Metadata
        - Curation

Only 1+2 are covered by AAI currently, 4 partially. (<=> DRP)

Resource Allocation

Current Situation:

- no need for assignment and control of resource consumption
- Monitoring of resources is partially done, improvement of presentation to user (and admins) under way
- Accounting by individual groups or on user level can be done by ‘Auditor’ (PUNCH -2.0)
- No concept of allocation up to now
- How to integrate with AAI?