AAI & SSH Open Marketplace notes

MP & MyAccessId integration - what happened and how to proceed

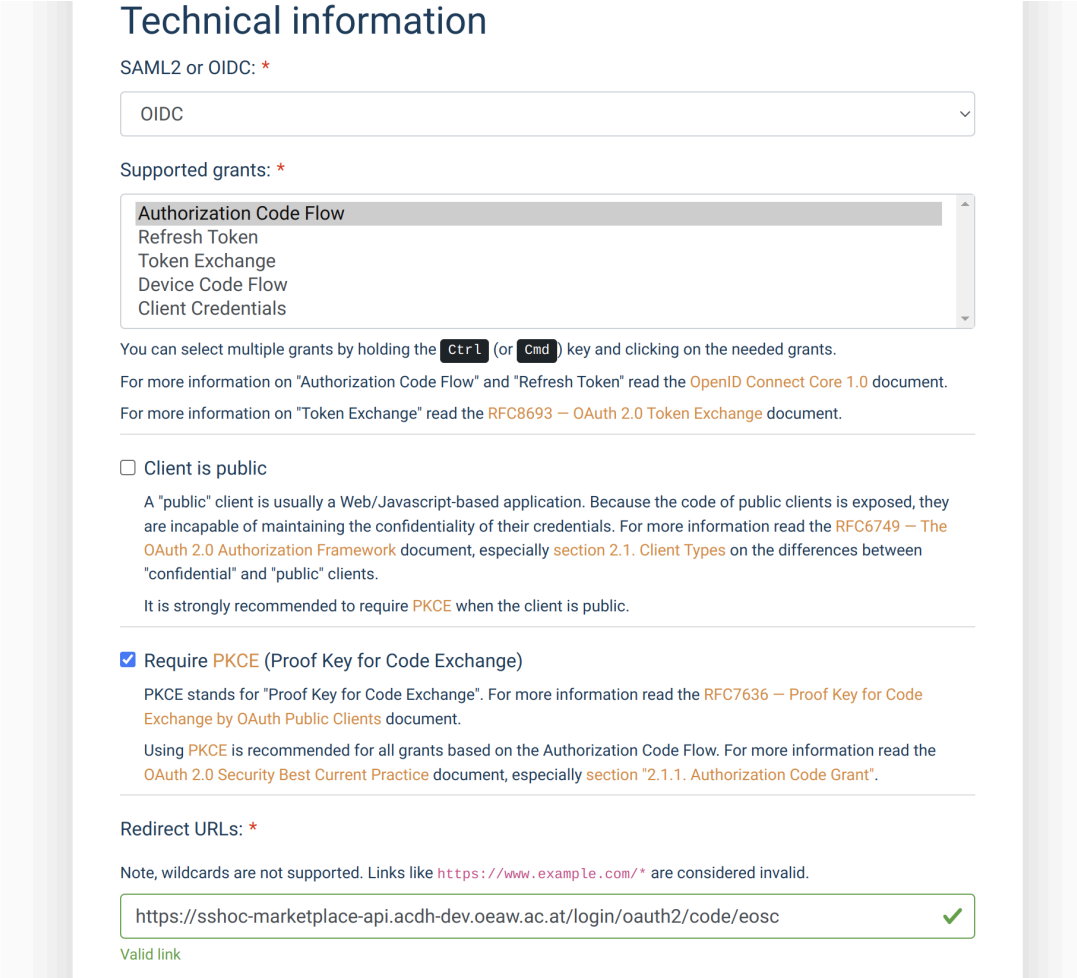
Integration process so far

1. Ola registered localhost/dev instance using acceptance MyAccessId, got clientId & secret.
2. There were slight changes in the backend (but only in configuration): https://github.com/SSHOC/sshoc-marketplace-backend/commit/ea4f41498ea6e6c73e09c066adc7a9c3bba9feb7
3. And another slight changes in frontend https://github.com/SSHOC/sshoc-marketplace-frontend/commit/b857d540b4b2f46440136dec863e661a78ae9a8c (it brings back the login button but only for localhost and dev)
4. Secrets/variables in github secrets were changed LC_K8S_SECRET_EGI_SECRET, LC_K8S_SECRET_EGI_ID, LC_K8S_SECRET_AAI_BASE_URI
5. Code was deployed on the dev instance by github pipeline.
6. As a result using MyAccessId is available here: https://sshoc-marketplace.acdh-dev.oeaw.ac.at/auth/sign-in (I was able to successfully log in via PSNC's idp as well as dariah.de. For PSNC the process goes smoothly but with Dariah.de it showed me the confirmation page several times, but I don't think it's connected to the marketplace configuration.)
7. **PKCE warning**: ATM PKCE is not enabled yet on the dev instance but it would be good to have it as it increases security. Unfortunately it requires some code changes (mainly because MP uses and old version of Spring) and is currently under construction.

How to proceed

1. Wait until PKCE is resolved (?)
2. Decide about what to do with the old accounts because they will not be merged automatically. (MyAccessId returns it's unique identifier "user_name" which is different from the already existing accounts even if the email is the same)
3. Do a proper change in frontend that will work for production/stage with change of name, logo etc., removing the red warning text
4. You have to register service provider for stage and production here: https://webapp.myaccessid.org/sp_request (for stage env there has to be a note in "Additional information" ~ "this is staging/sandbox instance of MP", no note for production

😉). After submission the page shows client secret & id and these have to be **stored safely.**



Redirect url: https://{link-to-mp-backend-app-behind-http-server}/login/oauth2/code/eosc

5. Wait for the email with confirmation.
6. Config change (in github secrets). Use client id & client secret in and url in LC_K8S_SECRET_EGI_SECRET, LC_K8S_SECRET_EGI_ID, LC_K8S_SECRET_AAI_BASE_URI (for appropriate environment). Dalibor or someone with permissions high enough can do it.
7. Deploy the newest version of code (from github pipeline) + frontend.
8. In case of a config change you can email MyAccessId support support+myaccessid@eduteams.org in a response to their confirmation email (there is no way to do it by yourself).

Important: using social network integration is possible ATM in MyAccessId but it strongly discouraged due to future problems that will appear on migrating to EOSC AAI

23.07.2024, 9h30 CEST

https://dariah.zoom.us/j/89821409457?pwd=IqJ5EXBeJc3dtiWQASj1Mjf4UOE7zF.1

Christos Kanellopoulos (GEANT), Sally Chambers (DARIAH), Matej Durco (DARIAH), Laure Barbot (DARIAH), Ola Nowak (PSNC), Marcin Helinski (PSNC), Tomasz Kuczynski (PSNC), Michal Stava (GEANT)

Suggested agenda:

1. EOSC AAI shut down - Grace period possible?

Not shut down completely yet. But should be. Up and running for some services till mid-August

New EOSC EU node AAI launched mid-October @EOSC symposium

2. SSH Open MP log in function, requirements (social accounts, OIDC) - https://marketplace.sshopencloud.eu/auth/sign-in
3. MyAccessID https://wiki.geant.org/display/MyAccessID/MyAccessID+Home

MyAccessID is also solution used by the EOSC AAI

Users IDs will change - last change

MyAccessID Home

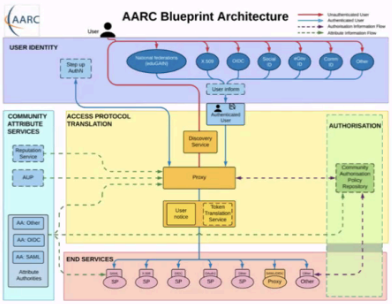
The main goal of the AAI

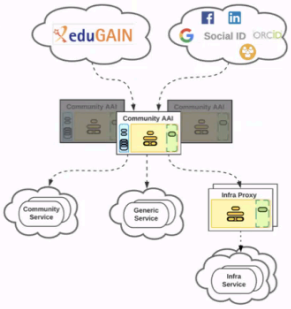
- **Science Clusters, Research Infrastructures and e-Infrastructure Providers** have been been implementing their AAIs using the **AARC Blueprint Architecture** in order to manage their users and the access rights to resources
  - The **AARC Blueprint Architecture (BPA) provides a set of building blocks** for software architects and technical decision makers who are designing and implementing access management solutions for international research collaborations.

Audio Video 8 Participants React Chat Share Apps More Leave

Community AAI: The AARC BPA Model

Based on the AARC Blueprint Architecture





Community AAI

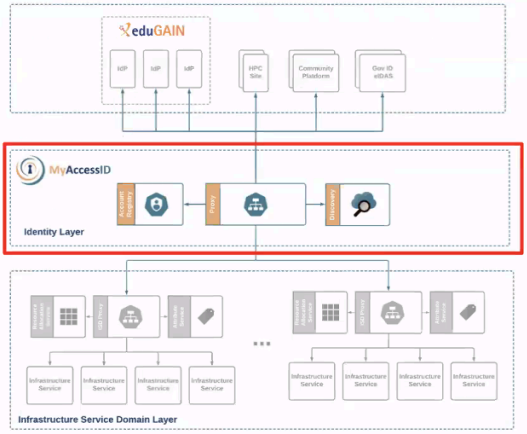
The purpose of the Community AAI is to streamline researchers' access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy

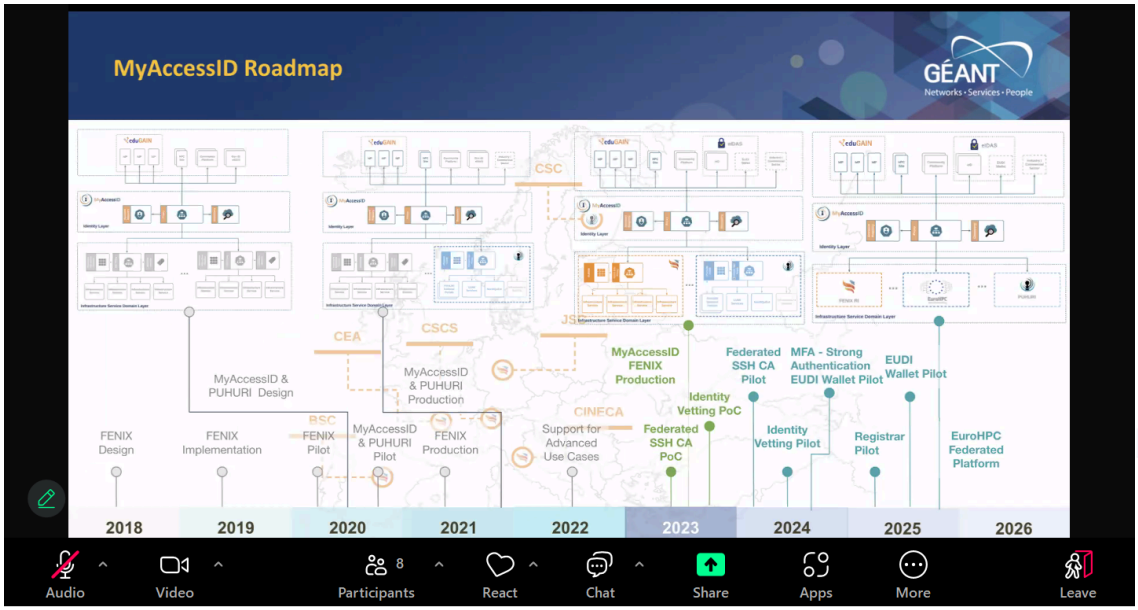
The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant policies and business logic for making available these resources to multiple communities.

MyAccessID: Towards a common AAI for Infrastructure Service Domains

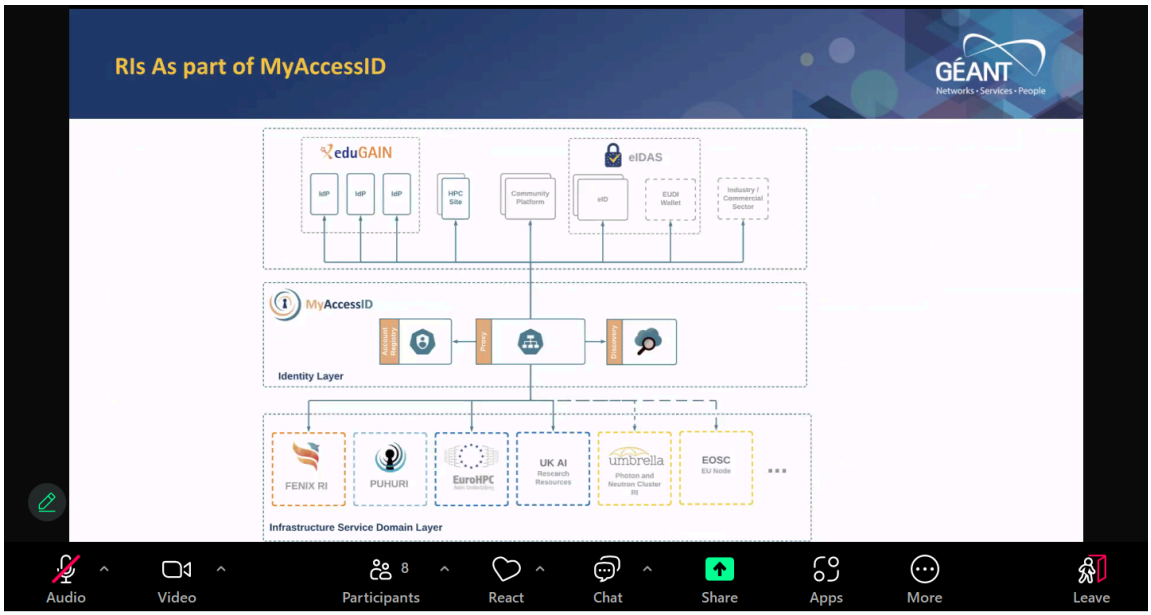
- HPC Datacenters are in the process of transforming to **Infrastructure Service Providers** with **a diverse Service Portfolio**
- These infrastructure services become available in different administrative and policy domains, which we call **Infrastructure Service Domains**
- **A common Authentication and Authorization Infrastructure** enables uniform accessibility to scientists and engineers at European scale



MyAccessID: A common AAI for ISDs in HPC


MyAccessID Roadmap
GÉANT
Networks · Services · People
CSC
CEA
CSCS
JSC
CINECA
BSC
MyAccessID & PUHURI Design
FENIX Design
FENIX Implementation
FENIX Pilot
MyAccessID & PUHURI Pilot
MyAccessID & PUHURI Production
FENIX Production
Support for Advanced Use Cases
MyAccessID FENIX Production
Federated SSH CA PoC
Identity Vetting PoC
Federated SSH CA Pilot
MFA - Strong Authentication
EUDI Wallet Pilot
EUDI Wallet Pilot
Identity Vetting Pilot
Registrar Pilot
EuroHPC Federated Platform
2018
2019
2020
2021
2022
2023
2024
2025
2026
Audio
Video
8
Participants
React
Chat
Share
Apps
More
Leave


EUROPEAN OPEN SCIENCE CLOUD
umbrella
FENIX RI
LUMI
eosc
PUHURI
panosc
PRACE
European Research Infrastructures
High Performance Computing
MyAccessID
Core AAI Platform
MyAcademicID
Student Mobility
EuroHPC
EOSC-Life
LEONARDO
OLA
European Universities Alliances
Erasmus+
erasmus without paper
European Commission



Umbrella = Panosc cluster aai

My AccessID supporting both SAML and OIDC

Business model: GEANT offering available for everyone (same as edugain) - GEANT strategy & commitment. MyAccessID actually outside of the procurement

What is the difference between EduGain and My Access ID? You don't need to negotiate with the individual institutions?

Germany: building national solution (german-eduid)
- possibility to link to MyAccessID

Possibility to use test environment

New endpoints + registration of the client

Through the registration form - terms of use

Where are you from that of MyAccessID

From Ola's email:

changing the configuration of Marketplace should be enough to connect MyAccessId. But to do so we need:

- MyAccessId endpoint address to use in these variables (pasted with current values for better example):

  ```
  token-uri: ${aai_base_uri:https://aai-dev.egi.eu/oidc}/token
  authorization-uri: ${aai_base_uri:https://aai-dev.egi.eu/oidc}/authorize
  user-info-uri: ${aai_base_uri:https://aai-dev.egi.eu/oidc}/userinfo
  jwk-set-uri: ${aai_base_uri:https://aai-dev.egi.eu/oidc}/jwk
  ```

  (I assume they will point to one base uri as they did before)

- for MyAccessId to setup a client that can use authorization grant type of "authorization_code".

4. Alternatively: SSHOMP implementing SAML? (question to PSNC-team)
5. (DARIAH AAI) - possible integration with MyAccessId federation?

12.01.2024

DARIAH_PIDs_AAI_telco

23.02.2022 - AAI & SSHOC Marketplace

Copied from EOSC-Future Teams:
https://technopolisltd223.sharepoint.com/:w:/r/sites/INFRAEOSC-03Proposal/_layouts/15/Doc.aspx?sourcedoc=%7B71E19298-6D91-4C92-853C-8B921111BA58%7D&file=t6.2%20diverse%20notes.docx&action=default&mobileredirect=true

Christos K., Matej, Tibor, Laure

SSHOC MarketPlace

Lack of SSHOC AAI, need to connect to a pre-existing proxy (DARIAH-AAI): this would be one valid procedure.

- Technically easy, but number of users could be an issue.
- Using the community identifier - how does it work in the SSHOC MP? Community aai Idps not a problem, if not the case might be an issue.
    - → seems ok as it is implemented now

Community AAI vs. Infrastructure Proxy?

- Different requirements
- Different policies apply for community aai and infr proxy.
- When a user accesses a service and the user comes from another community (other community AAI)
    - DARIAH AAI should not enforce registration flow - pass through unknown users directly to services.
    - upstream identifier + attributes needs to be passed to to the service. Pre-condition for service continuity.
- Login:
    - If using dariah aai: proxy gives the data
    - If not: (infra) proxy should pass through the identifiers

DARIAH AAI = community AAI + Infra Proxy

Q: How to for SSHOC?

- No cluster proxy at the moment.
- SSHOC ERICs will provide their own proxies - EOSC will not force for one single cluster proxy.

Q: How to with “joint” services, like SSHOC MP?

- For joint service, they should be connected to one proxy, and not 2-3 (actually there MUST be exactly one upstream proxy). DARIAH would be the one to use for the SSHOC MP
- DARIAH AAI will have a double-role: community AAI + Infra proxy

Q: Flow?

1. User goes to Service
2. Upon Login => redirect to DARIAH IP => Discovery page
3. Select IDP
4. Authenticate
5. Coming back to DARIAH IP
6. DARIAH IP Check is a DARIAH user
    1. If not pass through directly to Service
    2. If yes DARIAH IP should check for and add attributes to the response to Service

(Step checking if DARIAH user or not could be passed)

Q: DARIAH AAI in EOSC Federation?

- DARIAH AAI from eosc pov: 2 ways to see it: IdP = community aai; but through dariah aai, possible to offer access to services outside of the dariah users = proxy.
- Connecting to the eosc aai, each aai will have to connect 2 endpoints: users + services declaration.
- Most communities have one implementation that serves both roles. But two functions that serve different purposes.

Q: What if SSHOC cluster proxy would be created in the future?

- Several proxies can be used under one cluster aai. Migration of users from idps to one cluster > life sciences is doing this right now. Change of identifiers for the users. Impact for the users.

Q: How to connect MP and DARIAH AAI?

- Option #1: Direct connection between DARIAH AAI and Service
- Option #2: via national federations.
    - Currently DARIAH AAI part of DFN (preferred way)

- MP? OpenID → national federations support SAML and not OpenID.

Q: EOSC AAI Federation

- Not available yet, new concepts with EOSC Future.
- Now: Connect all proxies among each other.

Q: How to add MP to DARIAH AAI?

-> OEAW / GWDG to register MP as a service through the dariah aai proxy
https://wiki.de.dariah.eu/display/publicde/DARIAH+AAI+Documentation still up-to-date?

register@dariah.eu & dariah@gwdg.de

—----

T6.2 wider discussion:
AAI integration for science projects, science clusters or individual service

Q: What is the message T6.2 should say?

- AAI integration for science projects, science clusters or individual service
- Currently connection between proxies is done based on an opportunistic manner (only if needed)
- **Message to users**: "How to join community AAIs?" → Not T6.2 focus.
- **Message to SP**: "Do you have services to connect?" → contact your cluster and add service to Infra Proxy or to community proxy (depending on your cluster's AAI solution)

Q: What is the cluster-specific AAI solution? Infra proxy or community proxy?

- PaNOSC, ESCAPE, EOSC-Life - cluster aai
- SSHOC - individual RIs
- Envir-FAIR situation unclear

→ WP3 gathered info already

Q: How to keep T6.2 informed about integration? (eg. next deliverable, 10 services)

- By the end of April, goal to have first clusters connected to the Federation

Q: Is AAI a core service or not?

- AAI // other core functions - for other services decision making while AAI is an underlying component of the whole eosc architecture. Despite these differences, integration is still needed