EOSC AAI Implementation

Christos Kanellopoulos - GEANT
Slavek Licehammer - MUNI
Nicolas Liampotis - GRNET
Implementing the EOSC AAI
Relation with the EOSC-A AAI Task Force

EOSC Future

- focus on the implementation aspects of the EOSC AAI based on the HLR and the EOSC Authentication and Authorization Infrastructure (AAI) report published back in January by the AAI Task Force of the EOSC Executive Board Architecture WG.

EOSC-A AAI TF

- focus on the requirements and the further evolution of the EOSC AAI.
Two parallel areas of work

• **Area 1** will be about the EOSC Core and its requirements from the EOSC AAI *(the micro level)*.

• **Area 2** will be about implementing the EOSC AAI at the **macro level**, and we will be working on the cross-infrastructure/domain aspects.
Area 1: EOSC Core

EOSC Security Operational Baseline

Created by Matthew Vlijmen on Sep 26, 2022

Scope
Adherence to this policy is required for EOSC Core services, based on the Core Provider Agreement. All other services should consider this the best practice and are warmly recommended to follow its guidance.

Table of contents
- Table of contents
- Scope
  - Definitions
  - Scope
  - Baseline Requirements
  - Acknowledgements

Scope
To fulfill its mission, it is necessary for the European Open Science Cloud (EOSC) to be protected from damage, disruption, and unauthorized use. This Security Baseline supports these goals by defining minimum expectations and requirements of the behavior of those offering services to users and communities connected to the EOSC, and of those providing access to services or enabling service components through the EOSC. It thereby applies to all participants in the EOSC authentication and authorization infrastructure (EOSC AAI). It aims to establish a sufficient level of trust between all participants in the infrastructure to enable reliable and secure infrastructure operation.
Area 1: EOSC Core

EOSC Core Infrastructure Proxy Attribute Profile

Created by Nicolas Lampoti, last modified on Feb 11, 2022

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>SAML Attribute</th>
<th>OpenID Connect Claim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-reassignable, persistent, unique user identifier</td>
<td>Any of the following:</td>
<td>Any of the following:</td>
</tr>
<tr>
<td></td>
<td>- voPersonID [voPerson-2.0]</td>
<td>- voperson_id [voPerson-2.0]</td>
</tr>
<tr>
<td></td>
<td>- eduPersonUniqueID [eduPerson-202001]</td>
<td>- sub (public) [OIDC-Core] - Deprecated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- sub (pairwise) [OIDC-Core] - Deprecated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- eduperson_targeted_id [eduPerson-202001] - Deprecated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- eduperson_unique_id [eduPerson-202001] - Deprecated</td>
</tr>
</tbody>
</table>

Name information

|                   | All of the following:                                                         | All of the following:                                                              |
|                   | - display Name                                                                | - name [OIDC-Core]                                                                 |
|                   | - givenName + sn                                                              | - given_name + family_name [OIDC-Core]                                             |

Email information

|                   | Either (or both) of the following:                                            | Either (or both) of the following:                                                |
|                   | - mail                                                                        | - email [OIDC-Core]                                                              |
|                   | - voPersonVerifiedEmail [voPerson-2.0]                                        | - email_verified [OIDC-Core]                                                     |

Home organisation information

|                   | schac_homeOrganization [SCHAC-1.5] - TBD                                      | schac_home_organization [SCHAC-1.5] - TBD                                       |

Affiliation

|                   | Either (or both) of the following:                                            | Either (or both) of the following:                                                |
|                   | - eduPersonScopedAffiliation [eduPerson-202001]                              | - edupersonScopedAffiliation [eduPerson-202001]                                  |
|                   | - voPersonExternalAffiliation [voPerson-2.0]                                 | - voperson_external_affiliation [voPerson-2.0]                                   |

Assurance

|                   | edupersonAssurance [eduPerson-202001, RAF]                                   | edupersonAssurance [OIDC-core, RAF]                                             |

Overview

The EOSC Core Infrastructure Proxy is connecting the EOSC Core and EOSC Support Services to the EOSC Federated AAI. This document describes the requirements for integrating SP to the EOSC Core Infrastructure Proxy based on the EOSC Core Infrastructure Proxy - Policy for connecting services.

- Requirements
  - Eligibility
  - Technical and Policy
- Service Provider integration workflow
  - Required Service Information per Environment
- SAML Service Provider
  - Metadata registration
  - Metadata
  - Entity Identifier Format
  - Scope Format
  - Attributes
  - References
- OpenID Connect Service Provider
  - Client Registration
  - Metadata
  - Grant Types
  - Claims
  - REDirection URTs
  - Endpoints
    - Authorization Endpoint
    - Token Endpoint
    - Logout Endpoint
  - Client Migration to Keycloak
    - How to Migrate your Service to Keycloak
  - Common issues
Area 2: The EOSC AAI Federation

- Benchmark the AAI readiness of the Science Clusters and the e-Infrastructures against the policy and technical requirements [*]
- Use cases and requirements from the Science Projects
- Update of the technical and policy requirements based on the input from the Science Projects - Contribute to the EOSC Interoperability Framework
- Plan for each Science Clusters and e-Infrastructure to be ready for joining the EOSC AAI Federation
- First implementation of the EOSC AAI Federation and initial Community AAIs / Infrastructure Proxies connected
AAI Readiness of Science Cluster and Research e-Infrastructures
Goal

- Engage with the key parties
- Make sure the EOSC AAI is adopted
  - Implementation is ongoing process
- Provide consultancy
- Help overcoming obstacles
- Gather feedback and inputs for EOSC AAI evolution
Who we are focusing on?

- European e-infrastructures
- EOSC Science Clusters
  - ENVRI-FAIR, ESCAPE, Lifesciences, PaNOSC/ExPaNDS, SSHOC
- EOSC Science Projects from INFRAEOSC07
  - 10 projects to drive the integration of research data and services across scientific domain
- Open to other communities, projects, etc.
General status

- AAI is recognized as important
  - Interoperability
- Chicken-egg situation
  - Not really a problem
- European e-infrastructures and RIs are heavily engaged
- General agreement on standards
  - AARC standards endorsed by AEGIS (AARC engagement group for infrastructures)
Status in science clusters

• Single AAI available for most science clusters
  • Getting there for the rest

• All science cluster users have access to AAI
  • Not all users might be aware of AAI

• Based on AARC blueprint architecture
  • AARC interoperability guidelines
  • Progress of implementation varies
Area 2: The EOSC AAI Federation

- ESCAPE IAM (ESCAPE)
- Lifesciences AAI (EOSC-Life)
- UmbrellaID AAI (PaNOSC / ExPANDS)
- CESSDA AAI (SSHOC)
- EGI CheckIn
- EUDAT B2ACCESS
- GEANT SP Proxy
- GEANT eduTEAMS
- Infrastructure Proxy for EOSC Core Services
THANK YOU