Date: March 2019

Cherenkov Telescope Array
AARC2 Pilot

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

About CTA

The Cherenkov Telescope Array (CTA) will be the major global observatory for very high-energy gamma-ray astronomy over the next decade and beyond. CTA will be operated as an open, proposal-driven observatory, with all data available on a public archive after a predefined proprietary period.

CTA is a collaboration between 1350 scientists and engineers from 32 countries, set up with the mission to direct CTA's science goals and array design. When in production, CTA will collect the data scientists need to understand the role of high-energy particles in the most violent phenomena of the Universe and to search for annihilating dark matter particles.

CTA Pilot Description

CTA is a community of astrophysics users which already had its own AAI solution in place, and represents for AARC, in this respect, a very good example of how to address the needs of a community who already developed an AAI. In this case their AAI solution was based on a SAML stand-alone, catch all Identity Provider, integrated with a Group management tool used for Authorization on selected service providers.

This pilot propose to provide a non-invasive solution to simplify access to CTA services from eduGAIN and the CTA community.

The requirements which have been identified from the beginning to add the CTA community to eduGAIN, from the CTA perspective, are:

- Implement a user-friendly enrolment flow
- Manage both CTA and eduGAIN identities for users
- Link identities under administrator approval
- Keep supporting Grouper as the main authorization front end towards SPs
- Include guest identities (Social IDs) - (light requirement)
- Support OIDC RP - (light requirement)

The work which has been carried out in the CTA pilot of AARC is aimed at providing to the CTA community the eduGAIN authentication services ensuring at the same time a way to onboard this scientific community into eduGAIN. An infrastructure has been deployed based on the model proposed by the AARC Blueprint Architecture to enable the management of users coming from both eduGAIN Identity Providers and the CTA standalone IdP. The core component of the new infrastructure is the SATOSA IdP/SP proxy, as the central AAI layer to serve the CTA community of users. In addition to that, an external attribute authority (COmanage) has been plugged to the proxy, in order to manage user enrolment process, ensure injection of additional user authorization attributes, allow for account linking whenever appropriate, requested by the users and granted by the manager of the collaboration.

This pilot perfectly fits with AARC's goals:

- It helps to solve issues related to authentication from different IdPs but logically related to the same scientific community

- The proposed solution uses only existing technologies, without the need of creating new ones
- It does not change the global approach for the CTA community

The proposed components within this pilot are highly flexible, which means that other scientific communities can easily adapt the components to fit their own authentication and authorization needs.

Pilot Implementation Phases

While onboarding the CTA community, to reach the desired AAI model (based on a central proxy and a community Attribute Authority (COmanage), two main streams of work have been designed and implemented:

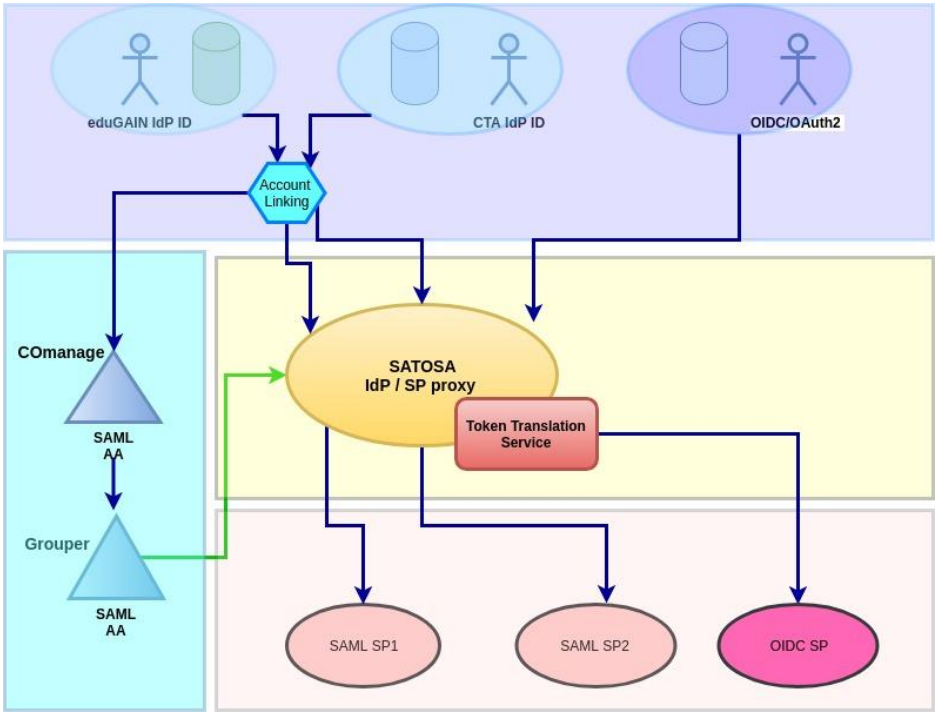
A) Provisioning into COmanage the already existing CTA identities inside the catch-all Identity Provider

To provision IDs of already existing CTA users into COmanage, we have made use of a temporary LDAP server and the LDAP user provisioning plugin of COmanage.

B) Model and implement an enrolment workflow for eduGAIN users (not already inside CTA IdP) - Functional integration of Comanage

The first step implemented in this phase of the pilot consisted of the integration of COmanage and Grouper. Grouper is a Group management tool used by the CTA community to manage Authorization. One of the requirements for CTA is to keep making use of this tool as a front end to their services. COmanage is a comprehensive Attribute Authority, managing the enrolment of users via their IdPs through different configurable workflows. For CTA user self-enrolment via a moderator admin user has been implemented.

CTA Pilot Architecture



Results

The AARC CTA pilot system has been succesfully tested by the CTA AAI experts which have been able to succesfully authenticate and get authorized on specific CTA service providers.

The designed workflow, supported by the SaToSa proxy and its implemented microservices, has proven to work and be reliable, supporting the desired authentication and authorization processes.

The main benefits for the CTA community are:

- Succesfully exploited an architecture capable of onboarding the whole CTA community to the eduGAIN trust model and flows.
- Include COmanage and Grouper as community tools to support attribute management and highly grained authorization processes
- Succesfully integrating legacy and new Service Providers of interest for the CTA community
- Generation of the required ePUID as a unique, reliable identifier for the CTA users
- Linking of identities between already existing CTA IDs and eduGAIN identitfiers

The AARC Blueprint Architecture was used as a model to design the pilot by clearly separating each component and its role in the system architecture. The pilot and its testbed will be maintained by INAF.