Asterics / Obelics Authentication and Authorization: investigations and status

C. Knapic[1], A. Costa[2], M.Molinaro[1], F. Pasian[1], G. Taffoni[1]
1- INAF - Osservatorio Astronomico di Trieste; 2 – Osservatorio Astronomico di Catania
Contacts: knapic@oats.inaf.it - http://ia2.oats.inaf.it/

Abstract :
ASTERICS aims to address the cross-cutting synergies and common challenges shared by the various Astronomy ESFRI facilities (SKA, CTA, KM3NeT & E-ELT) and other world-class experiments (LOFAR, Euclid, etc.). The major objectives of ASTERICS are to support and accelerate the implementation of the ESFRI telescopes, to enhance their performance beyond the current state-of-the-art, and to see them interoperate as an integrated, multi-wavelength and multi-messenger facility. OBELICS (OBservatory E-environments LInked by common ChallengeS - WP3) work package aims to enhance the interoperability and software re-use for the data generation, integration and analysis of the ASTERICS ESFRI and pathfinder facilities. One of the most relevant topic in this is the user accessibility to data acquired, particularly in the scope of user and digital identity recognition addressed by the OBELICS WP. Several technologies are available nowadays and a deep and proficuous work has been done in WP3 to investigate different requirements, aspects and constraints imposed by the projects. An overview of the investigations is exposed and some architectural solutions are described.

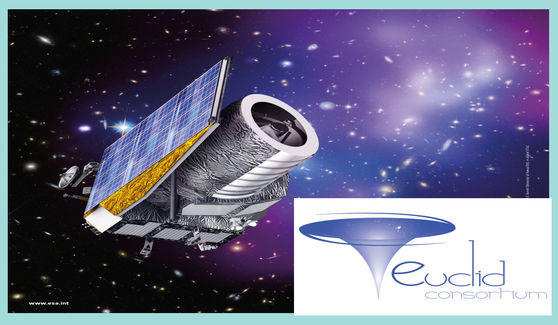
What is A&A task and the ESFRI Projects

Authentication and Authorization processes are critical topics in Astronomy. Several type of authentication and authorization mechanisms have to be considered to facilitate users when accessing at different services and resources offered by the Astronomical community. Depending on the requirements of the different ESFRI projects and possible available solution offered by previously approved European project, ongoing activities and experiences, the A&A task team suggests both protocols and their implementations, technologies to merge different solutions and available open source products.

Activities:
- Investigate general approaches, trends and best practices for A&A;
- Collect ESFRI projects requirements;
- Collect ESFRI projects use cases;
- Analyze ESFRI projects technical solutions, prototypes and activities;
- Contribute to implement the most flexible solution common to the ESFRI projects issues.

Investigation performed over the requirements of the following ESFRI projects:

SKA : Authorization and Authentication is under revisit
- Federated access to resources / self registration;
- Grouping service
- Enterprise solution.
- Authentication service
  - available to all SKA elements
  - available off line
  - support the generation of user's credentials
  - provided of a management system interface
  - support the change of credentials (username/password)
  - allow cancellation of user
  - highly available (about 99.999%)
  - centralized management logical location
  - Based on Federations (SAML2.0) but able to handle also other kind of identities (OpenID, ...)
- Authorization service
  - available to all SKA elements
  - provided of a management system interface
  - able to handle different user's roles, groups and privileges
  - shall follow the Policy statements
  - shall allow some group users to generate sub-groups and assign privileges to them
  - should be customized at each telescope site since some users like operators could be in principle operate in one location only.



IVOA and **EuroVO** :
Recommendations for:
- Single Sign On, Credential Delegation;
- Authorization under discussion;

SSO recommendation "is a profile against existing security standards". No authentication required. If any: HTTP Basic Authentication, Transport Layer Security (TLS) with passwords, Transport Layer Security (TLS) with client certificates, Cookies, Open Authentication (Oauth), Security Assertion Markup Language (SAML), OpenID

CTA :
- Use Case Collection
- Requirement Elicitation
- System Requirement Definition

Authorization and Authentication Requirements are grouped in the following categories:
- Authentication Capabilities
- Authorization Capabilities
- Management Capabilities
- Availability
- Performance
- Security
- Portability

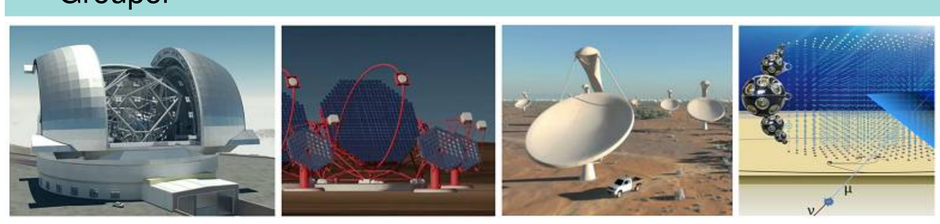
EUCLID : Currently A&A foreseen mechanism will be provided by ESA
- SAML based Authentication ;
- Custom based Authorization ;
- Peer to peer mechanism using certificates for computing purposes.

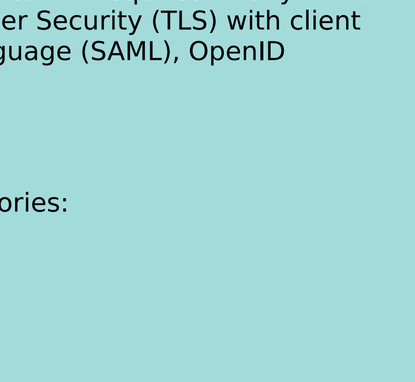
Investigation on EUCLID digital identities management via Federated approach, no actions on Authorization.

General Requirements

•Authentication:
- Widely used systems in the Educational and Research scope;
- Stable and reliable solutions;
- Open source solutions;
- Possibly a connection with social applications authentication products (Google, FaceBook, Twitter etc..);
- Protocols:
  - SAML;
  - OAuth2.0;
  - OpenId Connect
  - Certificates (X509);

•Authorization:
- GMS (CADC)
- Grouper



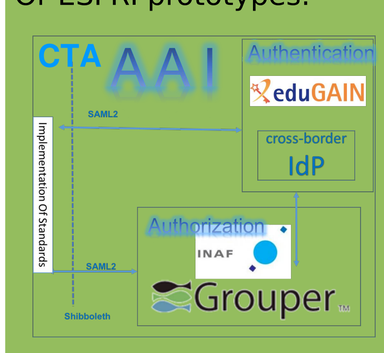


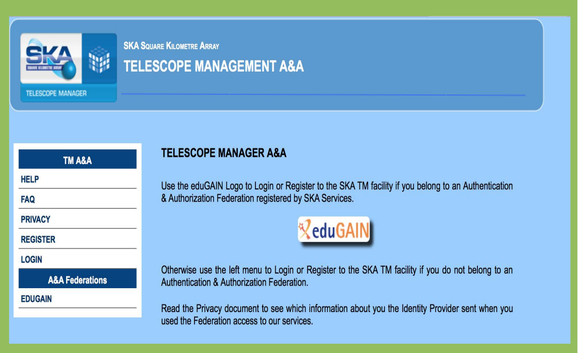
Most of the results came from the deliverable of other EU projects like :

INDIGO - DataCloud

AARC

Or ESFRI prototypes:





Deliverables for Authentication and Authorization

List of standards and protocols
- **SAML2.0** (Security assertion markup language)
- OpenID (open standard and decentralized authentication protocol)
- **OAuth** (open standard for authorization)
- **OAuth2** (open standard for authorization)
- **X.509** (standard for a public key infrastructure to manage digital certificates and public-key encryption)
- **XACML** (eXtensible Access Control Markup Language)
- **OpenID-Connect** (authentication layer on top of OAuth 2.0, authorization framework)
- **SCIM/VOOT** (System for Cross-domain Identity Manage)

List of Authentication tools and standard implementations
- **Django** framework with EduGain support (SAML2.0)
- **Shibboleth** service provider V 2.5
- Cross border Identity provider ApacheDS V 2.0 + Shibboleth IdP v 2.4
- **OpenID**
- **OAuth**
- **OAuth2**
- **Unity** (http://www.unity-idm.eu/site/support)

List of Authorization tools and standard implementations
- **Unity**
- **Grouper** V2.2.1 (https://spaces.internet2.edu/display/Grouper/Grouper+2.2+Release+Announcement)
- **Grouping Management System** (CADC development)
- **Macaroons** (flexible authorization credentials for Cloud services that support decentralized delegation between principals)
- **VOMS** (Virtual Organization Management System)

List of A&A ecosystems
- **PERUN** (application developed to manage users, groups and access to the services in highly distributed environments - https://www.egi.eu/news-and-media/newsletters/Inspired_Issue_16/perun.html)
- **UNITY-IDM** (http://www.unity-idm.eu/site/)
- **Cloud Foundry UAA** (User Account and Authentication Service)
- **WSO2 Identity Server** (http://wso2.com/products/identity-server/)
- **ForgeRock OpenAM** (https://www.forgerock.com/platform/access-management/)
- **Argus Authorisation Service**

Asterics
Astronomy ESFRI & Research Infrastructure Cluster