Astronomical Data Analysis Software and Systems XXVI
ASP Conference Series, Vol. 521
Marco Molinaro, Keith Shortridge, and Fabio Pasian, eds.

ASTERICS/OBELICS Authentication and Authorization: Investigations and Status

C. Knapic,[1] A. Costa,[2] M. Molinaro,[1] F. Pasian,[1] and G. Taffoni[1]

[1]*INAF-Astronomical Observatory of Trieste, Trieste, TS, Italy;*
cristina.knapic@inaf.it

[2]*INAF-Astrophysical Observatory of Catania, Gravina di Catania, CT, Italy*

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 topics 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 proficient 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.

1. What is A&A task and the ESFRI Projects

Authentication and Authorization processes are critical topics in Astronomy. Several types of authentication and authorization mechanisms have to be considered to facilitate users when accessing different services and resources offered by the Astronomical community. Depending on the requirements of the different ESFRI projects and possible available solutions offered by previously approved European projects, 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. General approaches, trends and best practices for A&A are being investigated:

- 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 issues with the ESFRI projects.

Most of the results come from the investigations performed (done or under study) over the preliminary and official documentation on use cases and requirements of the following ESFRI projects: SKA, CTA, KM3NeT, E-ELT, Euclid, LOFAR, Virtual Observatory.

1.1. SKA related investigations

In the scope of the SKA project the necessity to have a general purpose Authentication and Authorization service emerged. The team involved in the definition of the main use cases and in charge of identifying the main requirements reported that many actors and users will have different roles and privileges to access the SKA services. In the general case, the user's identity will preferably be extracted from remote Identity providers, implying multiple protocols. More than one person will share the same privileges and roles over the same kind of services and data, so an Authorization mechanism will require the ability to create groups and groups of groups of users in an hierarchical way. The services offered will involve several entities (different SKA Elements) so the A&A service will assume an enterprise role. In more detail, the extracted requirements could be summarized as follows:

- Authentication to access resources: possibility to use different authentication protocols (EduGain, OAuth2, etc.), self registration, available to all SKA elements, available off line, support the generation of user's credentials, provided by a management system interface, support the change of credentials (username/ password), allow cancellation of users, highly available (about 99.999%), centralized management logical location.

- Grouping service: available to all SKA elements, provided by a management system interface, able to handle different user's roles, groups and privileges, shall follow the SKA Policy statements, shall allow some group users to generate subgroups and assign privileges to them, should be customized at each telescope site since some users, like operators, could in principle operate in one location only.

- Enterprise solution: identity identification and authorization mechanisms will also involve Observatory facility access, wifi connection, human resources management, VPNs and so on, so in principle an interoperable technology or an interoperable layer will be required.

1.2. IVOA and EuroVO

In the scope of the Virtual Observatory standard, the main recommendations on the way to develop an interoperable system do not concern technological stacks or give specific requirements but suggest best practices. The main valuable ones suggest using Single Sign On and Credential Delegation. Another valuable suggestion is to try to separate as much as possible the authentication from the Authorization part. 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 etc. A possible standard protocol to investigate the grants of a users in an Authorization system is under study and will be proposed soon.

1.3. CTA related requirements

The Cerenkov Telescope Array Authentication and Authorization systems are related to all the interactions between the Telescope facility and the users in the area of data and computing resources access. The main actions to define the systems are based on use case collection, requirement elicitation, system requirement definition. Authorization and Authentication Requirements are grouped in the following categories: a. Authentication Capabilities; b. Authorization Capabilities; c. Management Capabilities; d. Availability, d. Performance, e. Security, f. Portability.

1.4. EUCLID

As with all the preceding space telescopes from ESA, the EUCLID mission data will be handled by the ESA data center. In this case the currently forseen A&A mechanism will be provided by ESA. The authentication mechanism is SAML based, uses a custom based authorization and a peer to peer mechanism (certificates) for computing purposes. In this scenario the system is accessible by known users but currently does not rely on trusted federated systems. EUCLID digital identities management via a Federated approach will be investigated, but no actions on Authorization are needed.

2. General Requirements

The evaluation of the different ESFRI projects analyzed highlighted some common and general requirements that could be summarized as follows:

- Authentication
  - widely used systems in the Educational and Research scope;
  - stable and reliable solutions;
  - open source solutions;
  - possibly connected with social applications authentication products such as Google, FaceBook, Twitter etc.
  - minimum set of protocols: SAML2,OAuth2.0, OpenId Connect, Certificates (X509).
- Authorization:
  - Grouping management systems able to support the creation and manage groups of users;
  - open source solutions;
  - available outside the authorization domain in a federated environment.

3. European Projects suggestions

Several suggestions come from the deliverables of other EU projects like H2020 Indigo-DataCloud and AARC. Both the two projects make a detailed analysis of the current available technologies and their deliverables are both a list of compliant technological stacks and a freely available software tool that tries to integrate several Authentication protocols.

4. ASTERICS deliverables

During the first year, the Asterics project featured some already available items, all open source, as first deliverables. Moreover, a fundamental approach has been chosen in order to guarantee feasibility and interoperability of quite all the mechanism, suggesting the adoption of a federated paradigm for Authentication and delegating to an internal authorization mechanism the management of groups of users since it is much more strictly linked to the application side (project domain) than to a federated ecosystem. More in detail, a list of suggested mature, reliable, standard implementations and tools were tested and are:

- 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)

In the same way, a list of Authorization tools and standard implementations were tested:

- Unity
- Grouper V2.2.1 [1]
- Grouping Management System (CADC development)
- Macaroons (flexible authorization credentials for Cloud services that support decentralized delegation between principals)
- VOMS (Virtual Organization Management System)

5. Conclusions

In the scope of the European ESFRI projects, the ASTERICS H2020 project aims to make a list of useful suggestions and best practices that could fulfill the astronomical use case in terms of Authentication and Authorization. Following the deep analysis conducted over the cases and requirements of the major participating European astronomical projects, and the ongoing activities on testing and developing new tools and new features for the existing one, Asterics WP 3.4.2 will be able to suggest interesting solutions to the Astronomical community in order to enhance the data access and interoperability and the collaborative users experience.

Acknowledgments. The authors acknowledge their work within the ASTERICS project, Horizon 2020 grant agreement n. 653477. The Authors would like to thank all the people involved in the A&A topic on the several ESFRI project, and in particular F. Tinarelli, for the great help, hints and suggestions given.

[1] `https://spaces.internet2.edu/display/Grouper/Grouper+2.2+Release+Announcement`