Contribution ID: **392** Type: **Poster**

The INDIGO-DataCloud Authentication and Authorisation Infrastructure

Thursday, October 13, 2016 4:30 PM (15 minutes)

Contemporary distributed computing infrastructures (DCIs) are not easily and securely accessible by common users. Computing environments are typically hard to integrate due to interoperability problems resulting from the use of different authentication mechanisms, identity negotiation protocols and access control policies. Such limitations have a big impact on the user experience making it hard for user communities to port and run their scientific applications on resources aggregated from multiple providers in different organisational and national domains.
INDIGO-DataCloud will provide the services and tools needed to enable a secure composition of resources from multiple providers in support of scientific applications. In order to do so, an AAI architecture has to be defined that satisfies the following requirements:

- Is not bound to a single authentication mechanism, and can leverage federated authentication mechanisms
- Provides a layer where identities coming from different sources can be managed in a uniform way
- Defines how attributes linked to these identities are represented and understood by services
- Defines how controlled delegation of privileges across a chain of services can be implemented
- Defines how consistent authorization across heterogeneous services can be achieved and provides the tools to define, propagate, compose and enforce authorization policies
- Is mainly targeted at HTTP services, but can accomodate also non-HTTP services, leveraging token translation

In this contribution, we will present the work done in the first year of the INDIGO project to address the above challenges. In particular, we will introduce the INDIGO AAI architecture, its main components and their status and demonstrate how authentication, delegation and authorisation flows are implemented across services. More precisely, we will describe:

- The INDIGO Identity and Access Management (IAM) service, a central service responsible for user authentication and authorisation, supporting multiple authentication mechanisms (SAML, X.509, OpenID-connect);
- How identity information is exposed to services leveraging the OpenID-Connect standard;
- How we leverage and extend OAuth2 to support flexible delegation of privileges across services;
- How account linking and identity harmonisation is implemented centrally and at site-level;
- How identity provisioning and de-provisioning is implemented leveraging the System for Cross-Domain Identity Management Standard (SCIM);
- How Non-HTTP services, or services requiring different credentials/authentication flows, are integrated with the INDIGO AAI via the INDIGO Token Translation Service;
- How the INDIGO AAI relates and integrates with existing production infrastructures and with architectures being developed in the context of other projects in support of scientific research (e.g., the AARC and EGI-Engage projects)

Secondary Keyword (Optional)

Computing middleware

Primary Keyword (Mandatory)

Security and policies

Tertiary Keyword (Optional)

Primary authors: CECCANTI, Andrea (INFN-CNAF); WEGH, Bas (Karlsruhe Institute of Technology); Mr ERTL, Benjamin (Karlruhe Institute of Technology); VIANELLO, Enrico (INFN-CNAF); CABERLETTI, Marco (INFN-CNAF); HARDT, Marcus (Kalrsruhe Institute of Technology); MILLAR, Paul (DESY); LICEHAMMER, Slávek (CESNET)

Presenter: MILLAR, Paul (DESY)

Session Classification: Posters B / Break

Track Classification: Track 8: Security, Policy and Outreach