Contribution ID: **543** Type: **presentation**

Beyond X.509: Token-based Authentication and Authorization for HEP

Thursday 12 July 2018 10:00 (30 minutes)

X.509 certificates and VOMS have proved to be a secure and reliable solution for authentication and authorization on the Grid, but also showed usability issues and required the development of ad-hoc services and libraries to support VO-based authorization schemes in Grid middleware and experiment computing frameworks. The need to move beyond X.509 certificates is recognized as an important objective in the HEP R&D roadmap for software and computing, to overcome the usability issues of the current AAI and embrace recent advancement in web technologies widely adopted in industry, but also to enable the secure composition of computing and storage resources provisioned across heterogeneous providers (e.g., Grid, private and commercial clouds, HPC centers) in order to meet the computing needs of HL-LHC.
A flexible and usable AAI based on modern technologies (such as OpenID Connect, OAuth 2, Json Web Tokens (JWTs)) is a key enabler of such secure composition, and has been a major topic of research of the recently concluded INDIGO-DataCloud project.
In this contribution, we will present an integrated solution, based on the INDIGO-Datacloud Identity and Access Management (IAM) service and other software components, that demonstrates how a next generation, token-based VO-aware AAI can be built in support of HEP computing use cases while maintaining compatibility with the existing, VOMS-based AAI used by the Grid.
We will describe and demonstrate:
- The base technologies and standards used (OpenID Connect, OAuth, JWTs)
- IAM support for multiple authentication mechanisms (SAML, social logins,X.509 certificates)
- the IAM account linking functionality, which allows users to link multiple different credentials to their VO membership
- the IAM registration service, which provides VO enrollment flows similar to the ones in use today but that do not impose X.509 certificate management on users
- the IAM VO management service, used to organize the VO structure and organize users in groups and grant privileges to users;
- How IAM can directly be integrated with existing Grid software leveraging on-demand X.509 certificate and VOMS provisioning;
- How token-based VO-based authentication and authorization can be implemented at relying services using off-the-shelf software compliant with the OAuth/OpenID connect standards.
Finally, we will discuss how this work is positioned with respect to other AAI solutions (e.g. the EGI CheckIn service) and standardization efforts being pursued in the context of relevant European and American projects (AARC, SciTokens).

Author: CECCANTI, Andrea

Co-authors: Mr CABERLETTI, Marco (INFN); VIANELLO, Enrico; GIACOMINI, Francesco (INFN CNAF)

Presenter: CECCANTI, Andrea

Session Classification: Plenary

Track Classification: Track 3 –Distributed computing