Contribution ID: **40** Type: **Oral Presentation**

Support to experiments in the transition from X.509 authN/Z to SciTokens

Friday, 29 March 2024 09:00 (20 minutes)

X.509 certificates and VOMS proxies are widely used by the scientific community for authentication and authorization (authN/Z) in GRID Storage and Computing Elements. Although this has contributed to improve worldwide scientific collaboration, X.509 authN/Z comes with some downsides: mainly security issues and lots of customization needed to integrate them with other services.

The GRID computing communities have decided to migrate to token-based authentication, a new web technology that has proved to be flexible and secure.
SciTokens, the token model adopted by the GRID communities, are based on JSON Web Tokens (JWT): a compact way to securely transmit information as JSON objects.
JWT are usually short-lived and provide fine-grained authorization, based on "scopes", to perform specific actions.
These scopes are embedded into the token and are specified during the request procedure so they last only until token expiration time. Scopes can be requested based on user groups and permission thus providing the possibility of restricting a group to perform only a subset of actions.
These characteristics make up to a more secure alternative to X.509 proxies.
Being largely used in industries, JWT are also easily integrated in services not specifically developed for the scientific community, such as calendars, Sync and Share services, collaborative software development platforms, and more.
As such, SciTokens suit the many heterogeneous demands of GRID communities and some of them already started the transition in 2022.

In the Italian WLCG Tier-1, located in Bologna and managed by INFN - CNAF, several computing resources are hosted and made available to scientific collaborations in the fields of High-Energy Physics, Astroparticle Physics, Gravitational Waves, Nuclear Physics and many others.
Although LHC experiments at CERN are the main users of CNAF resources, many other communities and experiments are being supported in their computing activities.

While the main LHC experiments have already planned their own transition from X.509 to token-based authN/Z, many medium/small-sized collaborations struggle to put effort into it.

The Tier-1 User Support unit has the duty of guiding users towards efficient and modern computing techniques and workflows involving data and computing resources access.

As such, the User Support group is playing a central role in preparing documentation, tools and services to ease the transition from X.509 to SciTokens.
The foreseen support strategy and the related tools will be presented. Future workflow plans in view of the complete transition will also be presented.

Primary author: Mr PASCOLINI, Alessandro (INFN - CNAF)

Co-authors: Mr CESINI, Daniele (INFN-CNAF); Mr RENDINA, Andrea (INFN - CNAF); Mr PELLEGRINO, Carmelo (INFN-CNAF); Ms MORGANTI, Lucia (INFN - CNAF); Mr LATTANZIO, Daniele (INFN - CNAF); FORNARI, Federico (INFN-CNAF)

Presenter: Mr PASCOLINI, Alessandro (INFN - CNAF)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations