Contribution ID: **40** Type: **not specified**

The new CERN Authentication and Authorization

Tuesday 9 October 2018 11:50 (25 minutes)

The current authentication schemes used at CERN are based on Kerberos for desktop and terminal access, and on Single Sign-On (SSO) tokens for web-based applications.
Authorization schemes are managed through LDAP groups, leading to privacy concerns and requiring a CERN accounts to make possible the mapping to to a group.

This scenario is completely separated from WLCG, where authentication is based on X509 certificates, which are mapped to Virtual Organizations for authorization.
While this solution covers the required use cases, it provides a difficult user experience.
Several initiatives, like Indigo-Datacloud platform or the SciTokens projects, are aiming at providing alternative authentication and authorization schemes based on tokens.

The ongoing redesign of the CERN authentication and authorization infrastructures is an occasion to harmonize the different authentication schemes used at CERN, and close the gap between IT's offer and HEP needs, aligning with the token-based authentication schemes that the WLCG is heading towards, and allowing for a full integration between the two worlds.

The new services will provide full support for a federated environment, where users authenticate with their home institute credentials or social account, and more uniform authorization schemes, with builtin privacy.

Desired length

20

Authors: TEDESCO, Paolo (CERN); ORMANCEY, Emmanuel (CERN); SHORT, Hannah (CERN); SMITH, Tim (CERN)

Presenter: TEDESCO, Paolo (CERN)

Session Classification: Basic IT Services

Track Classification: Basic IT Services