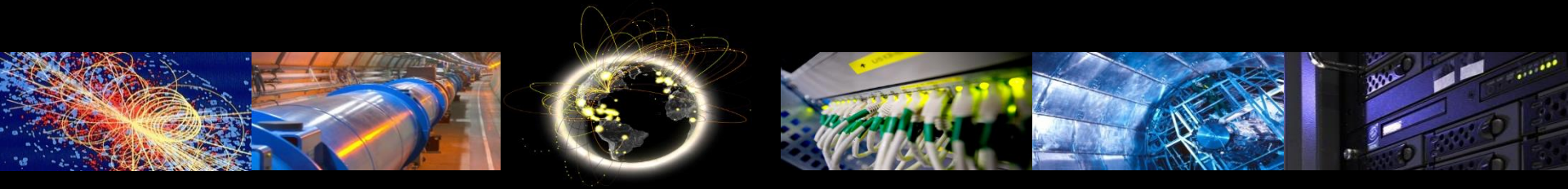
Auth WG pre-GDB Summary

Short, Valsan, Wartel

November 8th 2017



Auth WG

- project-lcg-authz
- Currently 22 members
- Started ~6 months ago

Auth WG Motivation

- Evolving Identity Landscape
  - User-owned x509 certificates -> Federated Identities
- Central User Blocking
  - Retirement of glexec affects blocking capability & traceability
  - VO-level blocking not a realistic sanction
- Data Protection
  - Tightening of data protection (GDPR) requires fine-grained user level access control

WG Aim - Understand & meet the requirements of an AuthZ service for WLCG experiments, focused on serving the 99% of our researchers

Pre-GDB Overview

- Intro
- WLCG Authorisation Requirements Discussion
- Lunch
- Analysis of Current Solutions
- Consensus, conclusions and next steps
- Drinks

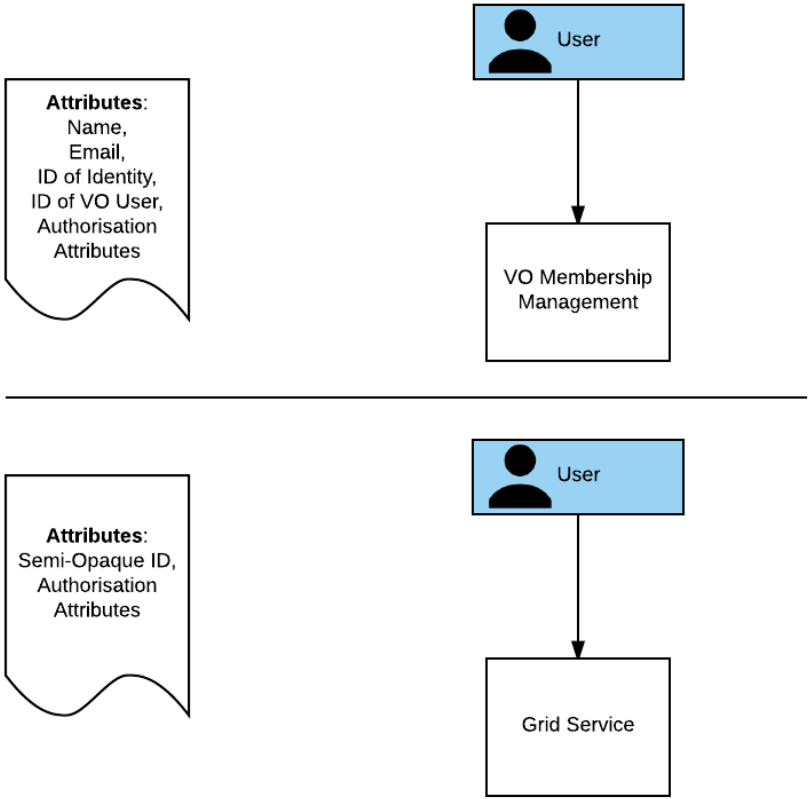
- First face-to-face meeting of Auth WG
- ~ 35 people attended
  - Sites, VOs, Infrastructures, Security
- Minutes online at https://indico.cern.ch/event/578976/ (thank you to Michel and Liviu in particular)

Summary

- World is moving to OAuth2 and JWT, we should go with them - let's not invent our own solution
- Although Certificates have been a simple and functional solution, there are now more user friendly alternatives that we can employ to the benefit of our researchers
- Topics can be split into requirements for VO Membership Management and for Services (+ suspension)

Draft Requirements Document available for comment at
https://indico.cern.ch/event/578976/

User Attributes



VO Membership Management

- Registration must be possible with different credential types (but it's up to the VO which ones they allow – must meet assurance)
- For LHC VOs
  - Propose leverage CERN SSO
  - Link to HR db

Services

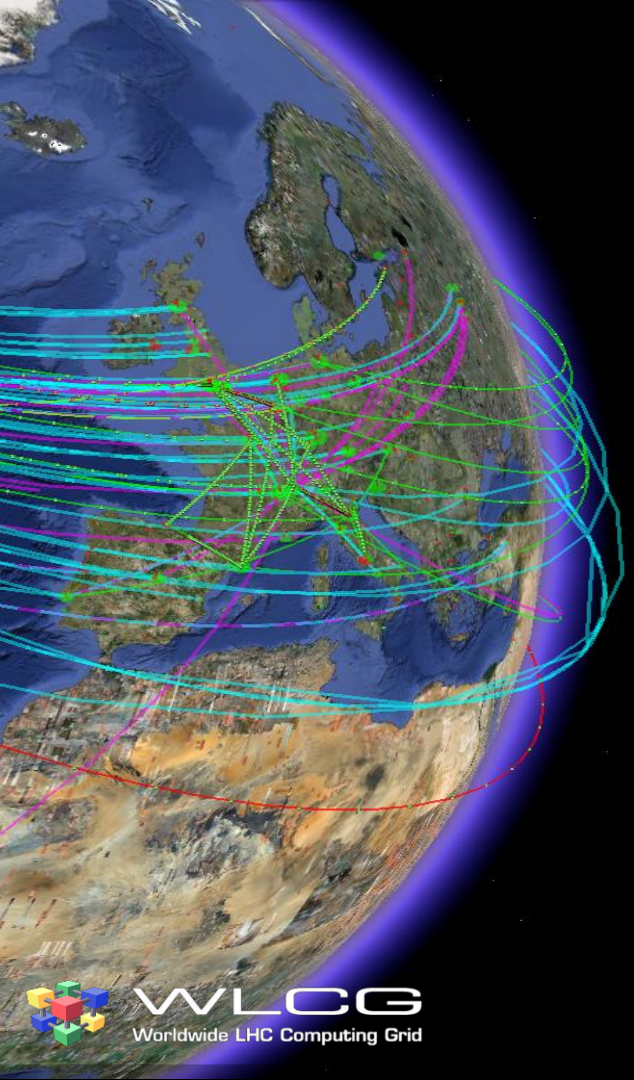
- Approach should be simple, standard and easily integrated
- Users should not have to actively manage tokens (e.g. x509/JWT) beyond session login (e.g. command line workflow)
- Tokens should be verifiable by service and resolve to an individual for security purposes

Suspension

- Sites/Services should be able to suspend users locally
- VOs and Infrastructures (e.g. EGI CSIRT) should be able to suspend users across all sites/services

Next Steps

- Call week of December 11th
  - Review comments on requirements
  - Andrea (INDIGO) and Nicolas (EGI) to demo full JWT workflow (including VO registration) at next meeting
- Areas of collaboration
  - Ensure our approach consistent with WLCG's input to FIM4R
  - Jointly (EGI/OSG/WLCG) define a profile for OAuth2 content of the access token including OAuth2 proof of concept of interoperability between OSG and EGI retrieving a token/sending the token (Can be supported by AARC)
  - Provide command line solution to allow users to submit jobs without certificate management (AARC Pilot with Mischa, transparently provision proxies using ssh)
- Tasks for the group
  - WG to define requirements for VO Membership Management Tool and assess solutions (such as INDIGO IAM or CoManage) against them
  - WG to consider Token Translation services



What would we like from you?

- Join the mailing list project-lcg-authz
- Provide your comments on the requirements doc