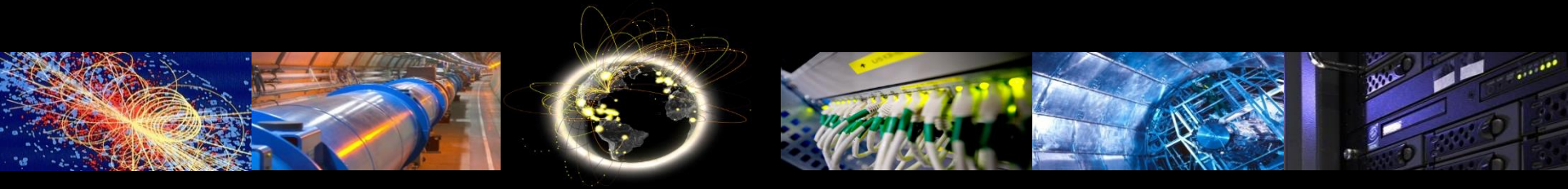
WLCG Auth WG pre-GDB

Short, Valsan, Wartel

November 7th 2017



Agenda

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

Motivation

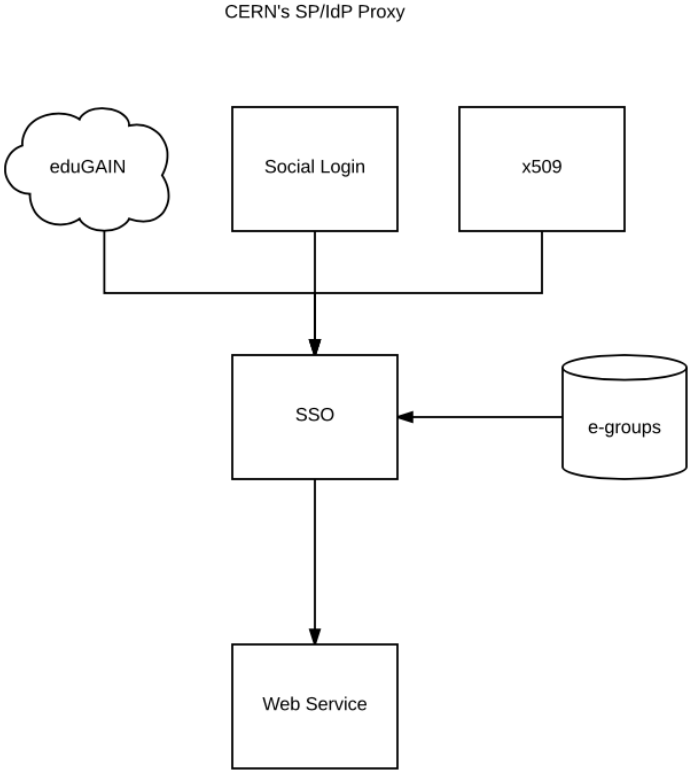
- Evolving Identity Landscape
  - User-owned x509 certificates -> Federated Identities
  - Federated Identities linkage with existing VOMS authorizations not supported
  - Maintaining assurance and identity vetting for federated users not supported
- Central User Blocking
  - Retirement of glexec removes blocking capability (& traceability)
  - VO-level blocking not a realistic sanction
- Data Protection
  - Tightening of data protection (GDPR) requires fine-grained user level access control

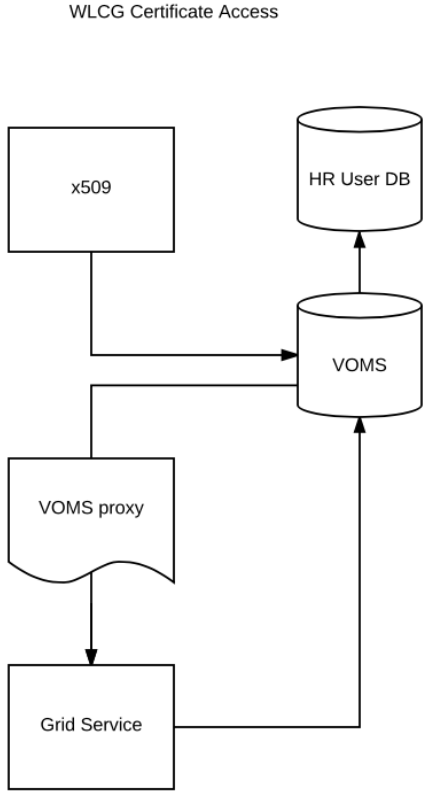
Understand & meet the requirements of an AuthZ service for WLCG experiments – focused on serving the 99% of our researchers

Some background

- AuthN & AuthZ for WLCG
- Membership Management
- Ongoing projects elsewhere

AuthN & AuthZ for WLCG

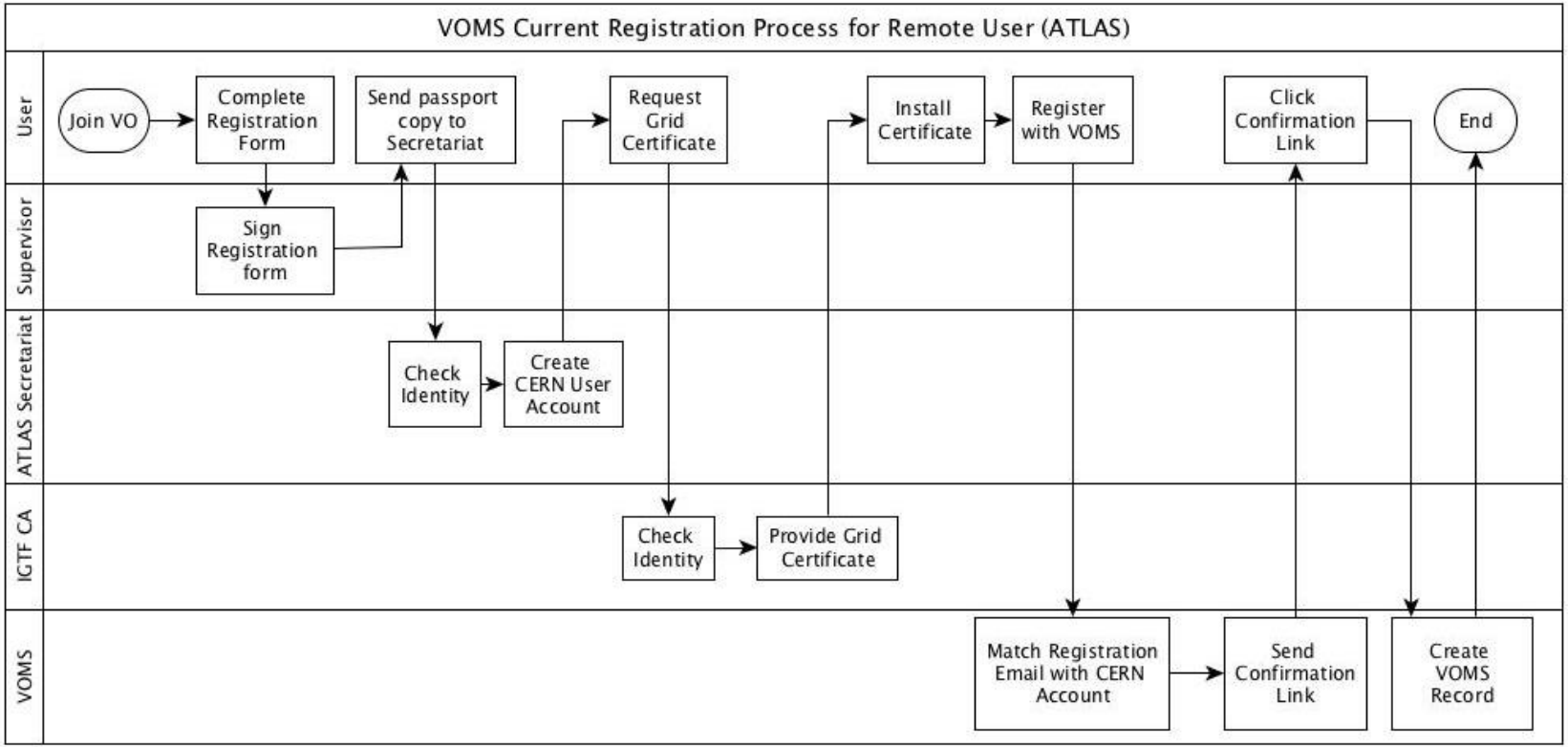




Options

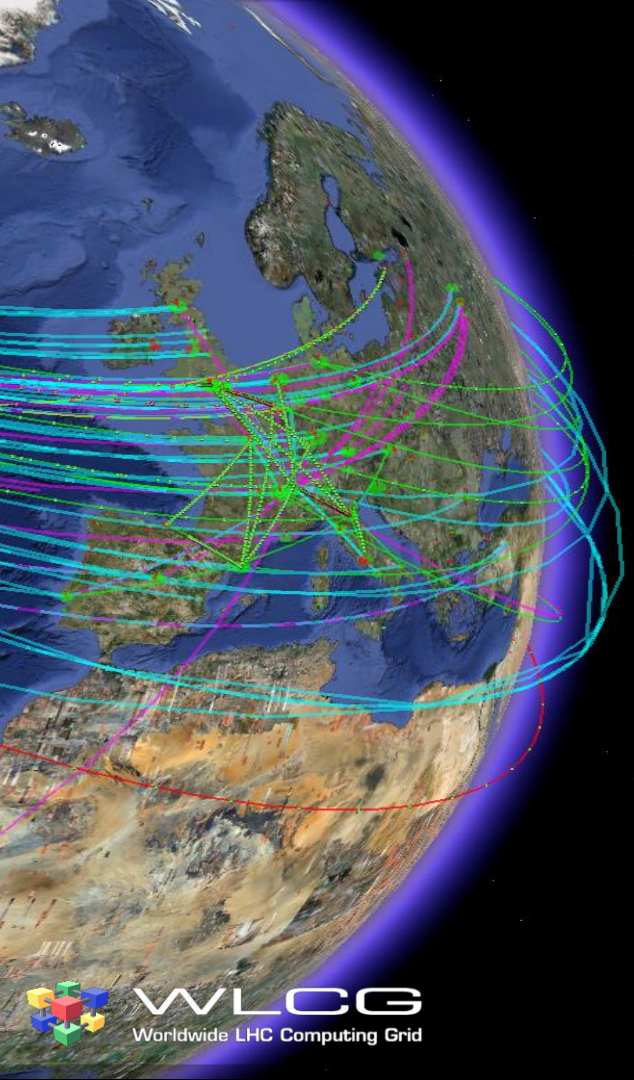
WLCG Service Type	
Web	Move behind SSO & include VO group and role information in e-groups (or future service)
Web service with delegation	Move behind SSO & include VO group and role information in e-groups (or future service) & translate credential for downstream service
Non-web	1. Move behind a web portal 2. Transparently provision user with expected token 3. Alter service to accept new user credentials

VOMS Registration Process



Ongoing projects

- Multiple efforts
  - INDIGO
  - EGI Checkin
  - SciTokens/OSG
  - CoManage
- Unclear where there is room for overlap with WLCG or possibility to leverage existing infrastructures
- Do they cover what we need?



Aims for today

- Agree on our requirements for an AuthZ service (morning)
- Identify whether any existing projects meet those needs (afternoon)
- Come up with a consensus on a few key conclusions