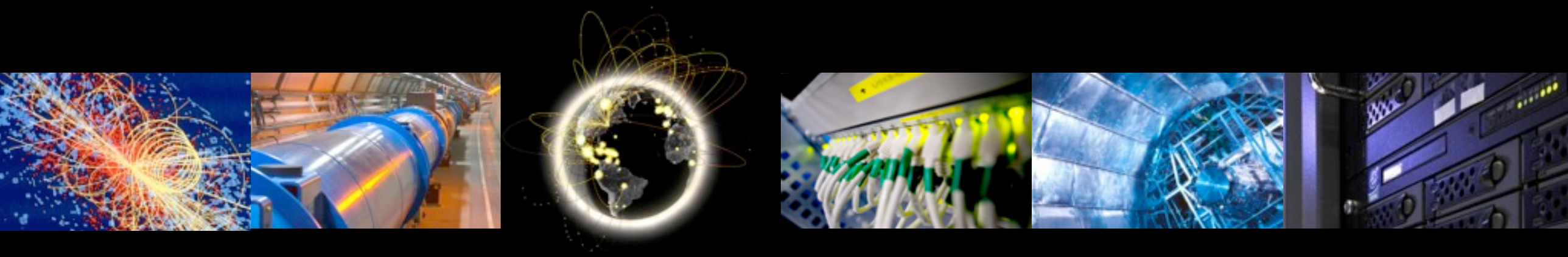
WLCG Group

Federated Identity Management Vision

WLCG Management Board, 5th June 2012, R. Wartel



WLCG
Worldwide LHC Computing Grid

Overview

- Federated Identity Management (IdM) (slide 2 and 3)
  - In research communities and HEP/WLCG
- Overview of the document (slide 4 to 8)
  - Common vision, requirements and recommendations
  - https://cdsweb.cern.ch/record/1442597
- Pilot project in HEP/WLCG?

The goal of this presentation is to obtain the MB endorsement of the document

Science & Technology Facilities Council

GridPP UK Computing for Particle Physics

Federated IdM in “Research”

- A collaborative effort started in June 2011
- Involves photon & neutron facilities, social science & humanities, high energy physics, climate science and life sciences, fusion energy
- 3 workshops to date (next one in June 2012)
- https://indico.cern.ch/conferenceDisplay.py?confId=177418
- Documented common requirements, a common vision and recommendations
  - To research communities, identity federations, funding bodies
- An important use case for international federation
- CERN-OPEN-2012-006: https://cdsweb.cern.ch/record/1442597

Federated IdM in HEP/WLCG

- X.509 certificates for grid services
  - Federated through the IGTF
  - Working and well established
  - Using TERENA Cert Service in some places
- But many other services (not just Grid!)
  - E.g. collaboration tools, wikis, mail lists, webs, agenda pages, etc.
- eduroam - federated solution for wireless
- Today CERN has to manage thousands of user accounts, many are “external”
- X509 complicated for end users
  - Users have two “maintain” several sets of credentials
- Need to interact with services/federations
  - Using Shibboleth, SAML, OpenID, etc

Common Requirements

- User friendliness
- Browser and non-browser federated access
- Bridging between communities
- Multiple technologies and translators
- Open standards and sustainable licenses
- Different Levels of Assurance
- Authorisation under community and/or facility control
- Well defined semantically harmonised attributes
- Flexible and scalable IdP attribute release policy
- Attributes must be able to cross national borders
- Attribute aggregation for authorisation
- Privacy and data protection to be addressed with community-wide individual identities

Operational Requirements

- Risk analysis
- Traceability
- Security incident response
- Transparency of policies
- Reliability and resilience
- Smooth transition
- Easy integration with local SP

Common vision statement

A common policy and trust framework for Identity Management based on existing structures and federations either presently in use by or available to the communities. This framework must provide researchers with unique electronic identities authenticated in multiple administrative domains and across national boundaries that can be used together with community defined attributes to authorize access to digital resources

Recommendations

- For research communities (including HEP/WLCG):
  - Conduct a risk analysis
  - Conduct pilot studies
- For technology providers (e.g software developers, national federations, HEP/WLCG, IGTF, etc.)
  - Separate Authentication and Authorization
  - Enable credentials revocation
  - Enable attribute delegation (to the research communities)
  - Support different levels of assurance
- For the funding agencies (of the research communities)
  - Agree on a funding model

Next steps

- WLCG Security TEG
  - Has agreed in principle to the vision and recommendations in the draft paper
  - We still need to identify a good pilot project for WLCG/HEP/CERN
- WLCG MB "endorsement" required
  - Before the June workshop

WLCG endorsement

- Does the MB agree in principle on the common vision, requirements and recommendations?

- Need to decide on a pilot project, for example:
  - Browser based: a pilot using a WLCG collaborative Web application where users authenticate via their home-issued federated credential (e.g. https://refeds.terena.org/ (click "Login"))
  - Non-browser based: a service enabling access to WLCG resources using home-issued federated credentials. Different technologies are being worked on (e.g. Project Moonshot, EMI STS)

  - Topic for discussion/agreement at the next GDB?