Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

Federated Identity Management for HEP

David Kelsey

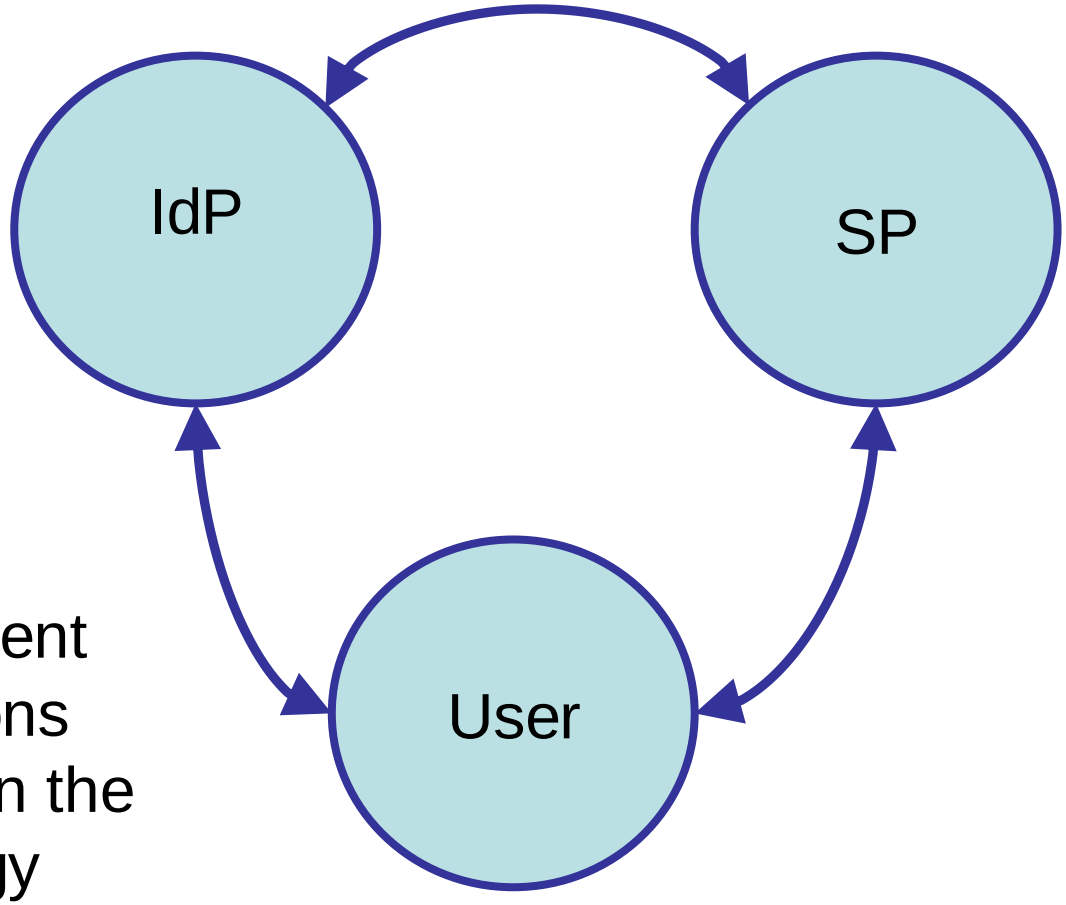
WLCG GDB
9 May 2012

Overview

- A sub-task in the Security TEG
- Introduction to Federated Identity Management (FIM)
- Research Communities Workshops
  - HEP just one of the communities
- WLCG Security TEG
- WLCG endorsement of the FIM paper recommendations

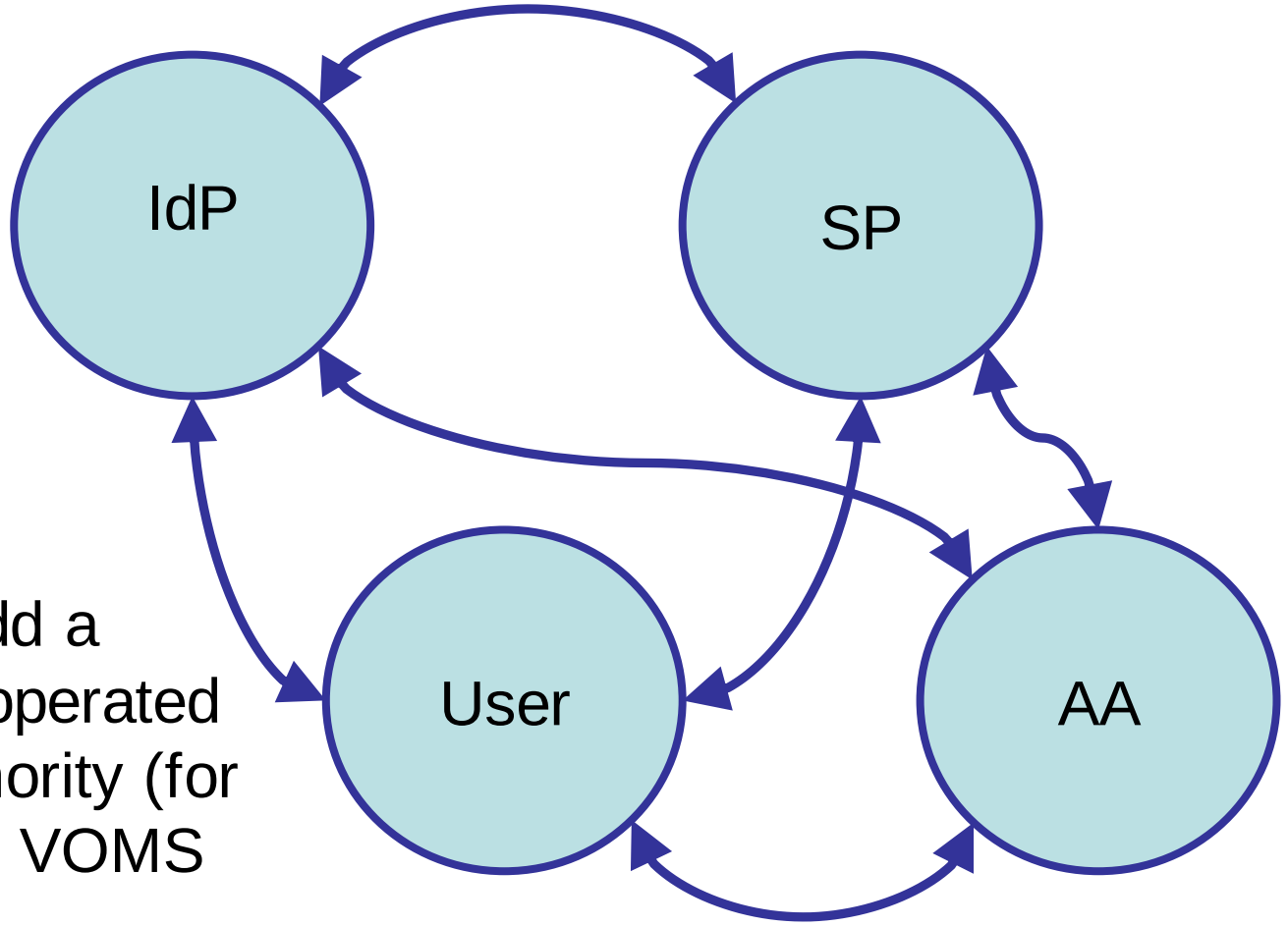
Introduction to IdM

- Remove identity management from the service
  - Identity managed in one place, typically by employer
  - Benefits (and drawbacks!) of single sign-on
- Identity Provider (IdP) manages and provides attributes about Users
  - For AuthN and to some extent AuthZ
- Service Provider (SP) consumes attributes for access control and offers services to users
- Federation: a common trust and policy framework between multiple organisations, IdPs and SPs
- Federations also manage and distribute information (metadata) about the various providers



Many different permutations depending on the technology

Then add a community operated attribute authority (for AuthZ), e.g. VOMS



Some example federations

- Grid X.509 certificates in WLCG and elsewhere
  - International Grid Trust Federation
- European higher education (Shib, SAML etc)
  - UK Access Management Federation, SWITCHaai, SURFfederatie
  - And many other Education & Research federations
- USA education and research: InCommon
- TERENA Cert Service connects national identity federation to a CA for personal certs (and similar CIlogon in USA)
- eduGAIN is linking national federations
- Social networking (OpenID, Oauth)

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*

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

- *To Research Communities*
  - Must perform a risk analysis of using federated IdM
    - Together with technology providers, IdPs and SPs
  - Perform pilot studies
    - In collaboration with FIM providers

Recommendations (2)

- *To technology providers*
  - This includes REFEDS and national federations
  - Separation of AuthN and AuthZ
  - Revocation of Credentials
  - Attribute delegation to the research community
  - Levels of Assurance

Recommendations (3)

- *To funding bodies*
  - An agreed funding model
  - An agreed governance structure

Federated IdM in HEP

- X.509 certificates for Grid services
  - 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.
- Today CERN has to manage thousands of user accounts, many are “external”
- eduroam is one possible federated solution (for wireless)
- What about other services/federations?
  - Using Shibboleth, SAML, OpenID, etc
- Technology appropriate to required level of assurance

WLCG Federated Identity

- Security TEG started on this task
  - Very much linked to the collaborative work
- Trust is essential!
  - not just technology
- How to involve IGTF?
- We need to agree a good HEP pilot project to get some experience

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

Questions?