Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

Federated Identity Management for HEP

David Kelsey

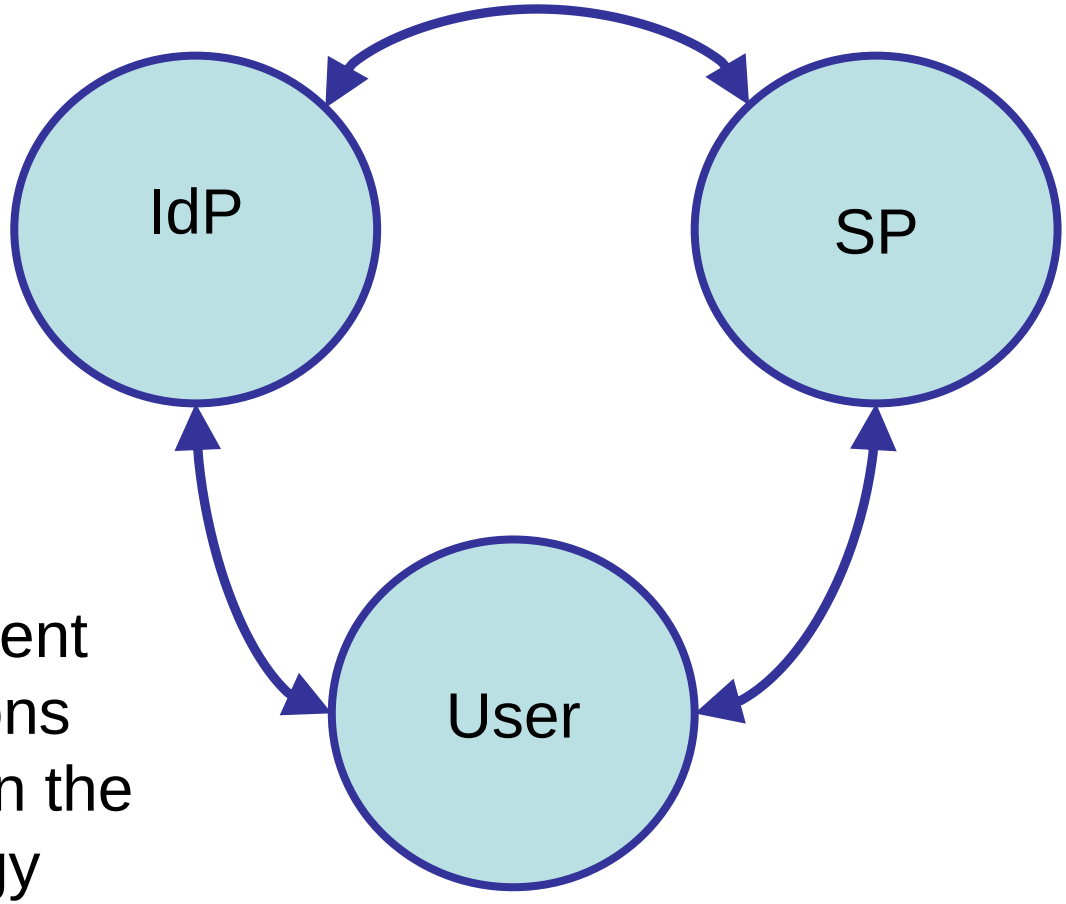
HEPiX, IHEP Beijing
18 Oct 2012

Overview

- *Update on Federated Identity Management (FIM) since Prague HEPiX*
- Federated Identity Management for Research (FIM4R)
- WLCG FIM pilot project

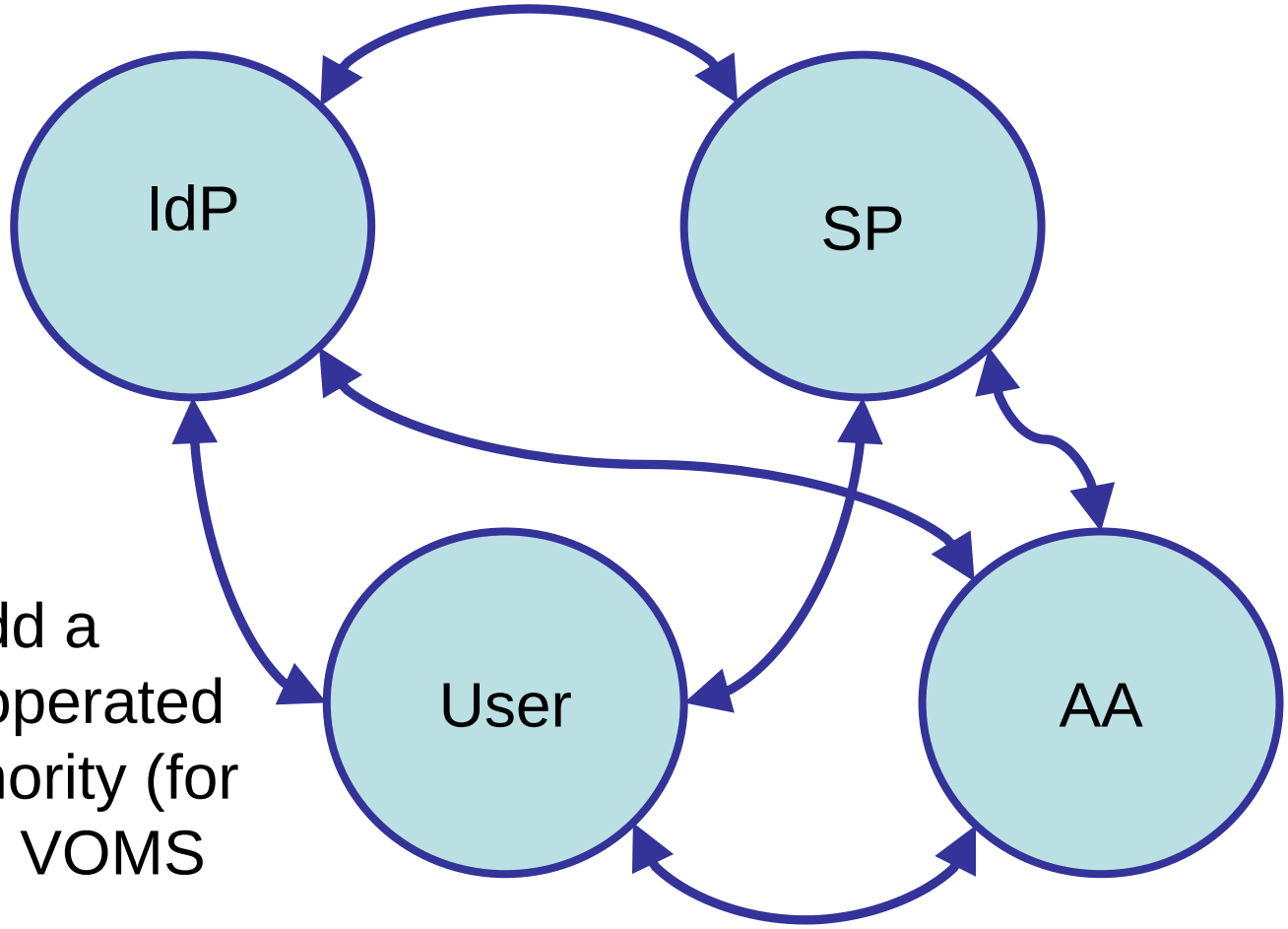
Introduction to FIM

- 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/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
- eduroam
- European higher education (Shib, SAML etc)
  - UK Access Management Federation, SWITCHaai, SURFfederatie
  - And many others
- 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 for "Research" (FIM4R)

- A collaborative effort started in June 2011
- Involves photon & neutron facilities, social science & humanities, high energy physics, climate science and life sciences
- 4 workshops to date (next one in March 2013)
- https://indico.cern.ch/conferenceDisplay.py?confId=177418
- Documented common requirements, a common vision and recommendations
- Accepted by the REFEDS community as an important use case for international federation
- CERN-OPEN-2012-006: *https://cdsweb.cern.ch/record/1442597*

Last 6 months

- FIM4R presented at REFEDS meeting, TERENA VAMP meeting, TNC2012, CHEP2012 and WLCG GDB/MB
- HEP (ie WLCG MB) has endorsed the paper
- FIM4R has prioritised the requirements
- We await a response from REFEDS
- Pilot projects by each community are the best way forward
  - In collaboration with eduGAIN, academic federations, ...

Common Requirements (High priority, Medium)

- End-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

Federated IdM in HEP

- X.509 certificates for Grid services
  - Using TERENA Cert Service in many places
- But many other services (not just Grid!)
  - E.g. collaboration tools, wikis, mail lists, webs, agenda pages, etc.
- Today CERN has to manage 10s of thousands of user accounts, many are “external”
- eduroam (for wireless)
- What about other services/federations?
  - Using Shibboleth, SAML, OpenID, etc
- Technology appropriate to required level of assurance

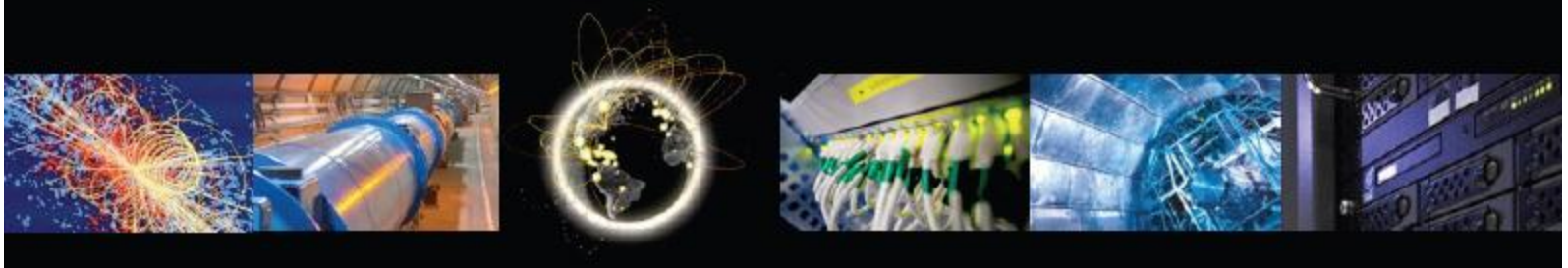
WLCG FIM pilot

- Romain Wartel (CERN) is leading this
- Mail list created with current volunteers
- First meeting happened on 5th Oct 2012
- See next slides from Romain

WLCG Group

WLCG Security Update

EGI Technical Forum, Praha, 17th September 2012, R. Wartel

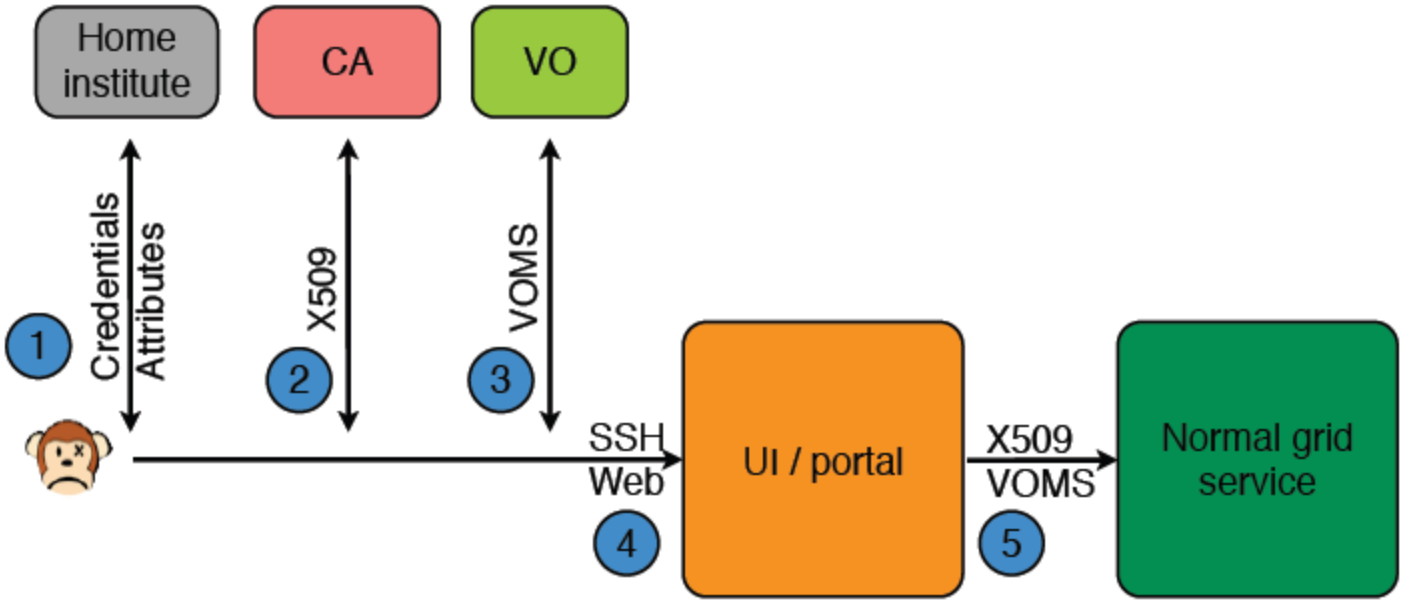


WLCG Worldwide LHC Computing Grid

Identity Federation

- Federated Identity Management document
  - Common vision, requirements and recommendations
  - https://cdsweb.cern.ch/record/1442597
  - Endorsed by the MB on 5th June 2012
- WLCG planning a non-browser based pilot project
  - a service enabling access to WLCG resources using home-issued federated credentials.

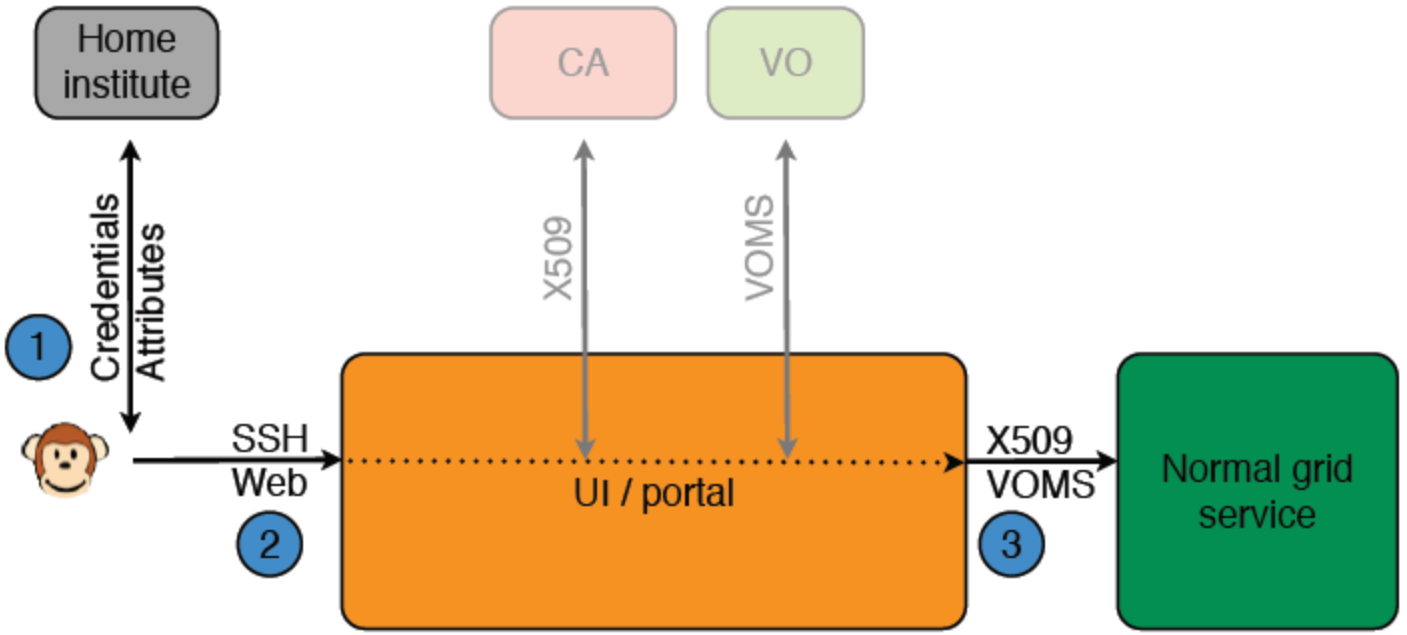
A pilot project for WLCG



Traditional access to grid services

11

A pilot project for WLCG



Federated access to grid services

12

A pilot project for WLCG

- Existing building blocks
  - Credential translation and/or short lived online CA available
  - VO are basically attribute providers
- Certainly a lot of technical questions to be answered
  - Policy, "trust" and standardisation work also needs to continue
- Important to build on top of existing federations/architectures
- Possible starting points:
  - EMI STS
    - http://www.eu-emi.eu/security-token
  - CILogon
    - https://cilogon.org/
- Most users have already have a home institute and credentials issued by them
  - Probably a number of corner cases too

13

A pilot project for WLCG

- Proposed plan
  - Proof of concept
  - Architecture design and integration in WLCG
  - Pilot service
- Working group will start just after the EGI TF
- Interested experts, sites, VOs and federations should step forward!

Results of the1st meeting

- Many issues to look at: requirements, technical feasibility, trust, policy, levels of assurance, etc.
- Focus of the pilot
  - The pilot is not just browser-based (need a CLI)
  - We should incorporate the university-based authentication systems (including SAML)
  - The end-user never sees the certificate

1st meeting (2)

- Goal of the pilot
  - a CLI login tool
    - typically a "voms-proxy-init" or "grid-proxy-init" replacement
  - able to authenticate users based on their home credentials
  - create X509 credentials and proxy
  - optionally add voms extension
- CILogon, EMI Security Token Service (STS), arcproxy
  - All claim to meet the requirements
  - To be investigated further

1st meeting (3)

- focus on defining the requirements and options for a proof-of-concept
- Later two separate subtasks might be defined
  - A trust, level of assurance, policy subtask
  - Software and technical issue subtask

More info – HEP pilot

- https://twiki.cern.ch/twiki/bin/view/LCG/WLCGFedIdPilot
- https://indico.cern.ch/getFile.py/access?contribId=7&resId=0&materialId=slides&confId=190743
- https://indico.cern.ch/getFile.py/access?contribId=18&resId=0&materialId=slides&confId=155069

Next steps

- FIM4R
  - Work with REFEDS and GEANT to make progress on pilot projects and solving the requirements
- WLCG FIM Pilot
  - Start the agreed plan of work
- Volunteers still welcome to join
  - Contact Romain Wartel at CERN

Questions?