Identity Management in Open Science Grid
Challenges, Needs, and Future Directions

Mine Altunay
OSG Security Officer
Fermilab
maltunay@fnal.gov

Current Status of Identity Management in OSG

- OSG uses IGTF accredited CAs + 2 TeraGrid CAs
- Mainly uses DOEGrids CA for issuing personal and service certificates
- OSG does not run its own CA.
  - Runs a Registration Authority for handling requests.
  - Certificates are issued by DOEGrids CA
- 3-5 day approval period per certificate

Open Science Grid

Challenges, Needs

- Desires:
  - Accelerating the approval/renewal period
  - Strong desire to use Federation-enabled CAs (CILogon); leveraging existing university identities
  - Easing user experience, enabling SAML tokens when appropriate

Open Science Grid

InCommon and Educational Identity Providers in the US

- InCommon is the largest identity federation for educational institutions in the USA. (see Jim Basney's talk)
  - Spans DOE National Labs, over 200 major universities, NSF, NIH, and so on
- InCommon has different levels of assurances for Identity Providers: Bronze, Silver, and Basic (http://www.incommon.org/assurance/)

Open Science Grid

Challenges

- Challenges:
  - There are no InCommon Identity Providers who are accredited at Silver or Bronze level; equiv to IGTF levels.
  - All IdPs operate at Basic level.
  - CILogon CA serves InCommon IdPs
    - Two flavors of CILogon CA: CILogon Silver CA serves InCommon Silver IdPs; CILogon Basic serves all IdPs.
  - Expectation is InCommon members will get their accreditations individually, but requirements are heavy and adoption is slow.

Future Directions

- How can we find a common ground between InCommon Basic IdP and IGTF identity vetting requirements?
  - Normally falls under IGTF SLCS profile with requirements for identity vetting
- Can we create a new TAGPMA profile that does not require stringent identity vetting at the certificate issuance from Basic IdPs?
  - Equivalent to NIST LoA1.
  - Certificates does not have to match user's legal name
  - ***User vetting and authorization happens at VO registration***

- Not all the VOs can comply, but LHC VOs already applies stringent identity checks at VO registration step. (Double identity vetting) For example, CMS VO checks
  - CERN id number
  - Birthdate
  - Supervisor approval
  - And then adds the certificate into VOMS
- There is existing work in IGTF for VO registration guidelines
- What about allowing CILogon Basic CA for VOs who operate and comply with IGTF VO requirements?

Future Directions

- OSG is joining InCommon as a member entity.
- While waiting to leverage existing University IdPs, OSG may
  - Run its own IdP as an InCommon member, OR
  - Leverage Identities given out by major US institutions Fermilab and BNL.
  - Fermi and BNL plan on running a Shibboleth IdP
  - We can integrate these IdPs with a Federation-CA such as CILogon
  - Will need IdP accreditation