MAGIC Meeting Minutes
June 4, 2014

Attendees

Jim Basney	Americas Grid Policy Management Authority
Rich Carlson	DOE/SC
Rob Gardner	U. of Chicago, OSG Connect
Dan Gunter	LBL
Craig Jackson	Indiana U.
Klara Jelinkova	U. of Chicago
Minet Klinate	OSG
Scott Koranda	U. Wisconsin-Milwaukee
Don Riley	U. Md
Dan Katz	NSF
Ji Lee	NCO
David Martin	ANL
Grant Miller	NCO
Von Welch	CTSCI

Action Items

Proceedings

This MAGIC Meeting was chaired by Rich Carlson of DOE/SC and Dan Katz of the NSF. Von Welch organized a session addressing Identity Management with the presentations:

- OSGConnect: Rob Gardner, U. Chicago
- Identity and Access Management for LIGO: International Challenges – Scott Koranda, U. of Wisconsin-Milwaukee
- InCommon Update – Klara Jelinkova, Chief' Information Technology Officer, U. of Chicago
- Center for Trustworthy Scientific Computing IdM Activities – Von Welch, CTSC
- eXtreme Scale Identity Management (XSIM) – Craig Jackson, Indiana U.

OSG: Rob Gardner

OSG campus grids deliver distributed high throughput computing capabilities to campuses. OSG Connect is a job and data service to directly connect users to over 120 sites on the OSG. OSG is the leading high throughput computing service in the U.S. with 104k cores, 75.6 PB of storage and 123 compute endpoints. Most sites have 10Gbps or more to I2 or ESnet and utilize science DMZs.

The OSG Connect Platform provides login to the OSG using your campus identity. It leverages Globus, HTCondor, CI-Logon, U-Bolt, and Bosco technologies. It contains:

- A submit host
- Object storage service (90 TB usable)
- Accounting
- Science DMZ

- Globus identity management, group organization, reliable data transfer, data sharing

CI Connect provides access to Globus Online, HT Condor submit host and other services. OSG Connect manages identities, keys and certificates. Groups are mapped to projects of the OSG VO. Full user traceability is provided.

Globus Online integration is built-in in OSG Connect. OSG Connect brings campus, OSG, and cloud resources together.

CI-Connect

CI-Connect provides services for the HPC Center to connect to national ecosystems. It adds campus flocking factories for SLURM, LSF, and SGE local campus schedulers. For more information see:
http://ci-connect.net

Example of CI-Connect: US Atlas for CERN LHC

Users from 44 U.S. Atlas communities are connected through a portal to connect.usatlas.org including:

- Campus Grids, Off-grid Tier3
- Atlas T1 and T2
- TACC
- Cloud AWS

CI Connect leverages the Globus platform to connect users to the OSG. It couples users, data, and distributed computer cycles as a service. CI Connect provides an easy path for campuses to connect or bridge to the national ecosystem.

Identity and Management for LIGO: Scott Koranda

LIGO utilizes SAML for SSO. As a member of the Shibboleth Consortium, it operates a Shibboleth Identity Provider (IdP) 2.4.0. It will, shortly, deploy IdP in a high availability configuration. Three backup IdPs are included at sites. There are more than 100 Shibboleth Service providers.

LIGO joined InCommon in the U.S. It partnered with CTSC to focus on international interfederation. The goal was to support world-wide Gravitational Wave (GW) astronomy efforts. Federated access is provided with about 50 scientists of the Japanese KAGRA Program. Peer-to-peer negotiation was required; InCommon membership enables only U.S. federation. The LIGO goals include:

- Documentation of technical and policy changes for peer-to-peer IdM
- LIGO membership in the Italian Federation (IDEM)
- Prototype interoperability with UK via InCommon
- Research likelihood and timeline for eduGain via InCommon
- Assist LIGO-India with developing use cases.

Peer-to-peer IdP for KAGRA

IdP is managed by the University of Tokyo. Metadata exchange and negotiation on attributes was easy. Access control is the largest issue. COmanage facilitates collaboration. It leverages Internet2, LIGO, iPlant and Bamboo to provide enrollment, onboarding, and management for federated identity. It provides group management targeted at research VOs. It currently provides prototype interoperability with the UK Access Federation. CoManage is a SAML Attribute Authority (AA). CoManage provisions people and groups into LDAP.

Shibboleth IdP reads from LDAP. The SP queries AA using a key identifier. AA returns other attributes managed via COmanage.

eduGain via InCommon: Jim Basney

eduGain interconnects federations to link services and users worldwide. It is:

- A federation of SAML Identity Federations
- Led by GEANT
- Policy last revised September 30, 2013
- Policy framework includes eduGain: Declaration, Constitution, Metadata profile, and Attribute profile.

There are 31 Production Federations and an additional 17 Pilot Federations.

The Gravitational Wave Astronomy Collaboration needed help with facilitating their collaboration especially with Identity Management. COmanage provided support for federated identity. They surveyed 60+ contact persons for the MOUs. So far there are:

- 26 countries
- 161 institutions
- 72 U.S. institutions
- MOUs signed by international VOs

For the U.S. the primary concern is attribute release by the IdP. As a minimum they need ePPN. The experience is that most users will interoperate but only a minority will release attributes.

For federated identity outside the U.S. the goal is to leverage eduGain. First step is to publish LIGO SPs into eduGain metadata. InCommon is not ready to publish. The Swedish federation has agreed to publish SPs in its federation and to push into eduGain.

InCommon Update: Klara Jelinkova

InCommon is a trust framework for U.S. education and research. It provides best practices and mature consumable services. InCommon architecture supports other Internet2 services: Grouper, Shibboleth. MACE, COmanage... InCommon facilitates:

- Federation of IdPs and SPs
- Interfederation
- Putting trust and privacy into identity
- Research support

Current InCommon focus areas are:

- More mature, scalable and resilient operations
- Expand in-house services
- Expand 3rd-party services
- Create more tools
- Enhance the certificate service: Deployment of InCommon IGTF CA for XSEDE.

InCommon is designed for compatibility with U.S. government identity management capabilities: FICAM, TFPAP. InCommon is aligning trust policy and practices via REFEDs (Research and Education Federations). It is also aligning with eduGain metadata aggregation export/import. InCommon and eduGain have signed an agreement to collaborate with an expectation to operationalize their capabilities. TIER (Trust and Identity in Education and Research (TIER) provides a context for disjointed efforts. It provides a place where federation can operate more efficiently. They plan for a charter to be in place by the fall of 2014.

CTSC: Von Welch

CTSC provides the research community with a coherent understanding of cybersecurity and the resources to provide an appropriate cybersecurity program. It is interacting with Globus, Pegasus WMS, DataONE, and LIGO. International identity federation was facilitated by cooperative efforts among LIGO, CTSC, and InCommon. CTSC provides Identity Management best practices: see http://blog.trustedci.org/2014/04/idm.html
CTSC provided a central source of information for the HeartBleed vulnerability.

XSIM is working on VO IdM. The VO plays a role in collaborator IdM implementation. This role alters the direct trust relationship between users and RPs. Trends are toward mediated trust, using the capacity of the VO to represent its members, particularly with transitive trust.

Upcoming Meetings:
July 22-25, XSEDE, San Diego
July, NCAR: Data management for environmental and climate research. Speeding up data movement.
November, SC14, New Orleans: WISPE meeting focused on software

Next MAGIC Meetings:
June 4, 2014, 2:00-4:00 EDT, NSF
July 2, 2014, 2:00-4:00 EDT, NSF