NITRD

Networking and Information Technology
Research and Development

MAGIC Meeting Minutes

November 14, 2012
At SC12 Room 250-AB

Attendees

Jim Basney	NCSA
Rich Carlson	DOE/SC
Keith Chadwick	FNAL
Rory Eigenmann	NEES/Purdue U
Terry Fleury	NCSA
Ian Foster	ANL/U Chicago
Dan Gunter	LBNL
Shantenu Jha	Rutgers U.
Dan Katz	NSF
Kate Keahey	ANL/U Chicago
Scott Koranda	U Wisconsin - Milwaukee
Archit Kulshrestha	Cycle Computing
Cees de Laat	UVa (NL)
David Martin	ANL
Steve Newhouse	EGI
Grant Miller	NCO
Ruth Pordes	FermiLab
John Townes	NCSA/XSEDE
Von Welch	Indiana U.

Action Items

Proceedings

This MAGIC Meeting was Cochaired by Dan Katz of the NSF and Rich Carlson of DOE/SC. This meeting was organized by Von Welch and focused on Identity Management with an international perspective.

Identity and Access Management for LIGO: International Challenges: Scott Koranda

LIGO is the Laser Interferometer Gravitational-wave Observatory. It seeks to detect gravitational waves. There are LIGO facilities in Hanford, Washington; Livingston, Louisiana; and Caltech in California. An additional facility in India is scheduled to begin operations in 2020. The LIGO collaboration seeks to detect gravitational waves and use them to explore the fundamental physics of gravity. The collaboration currently has 1000 members at 70 institutions worldwide.

The LIGO Identity and Access Management (IAM) Project knits together existing technologies and tools. Its goals are:

- Single identity for each LIGO person
- Single source of identity information
- Single credential for each LIGO person
- SSO across the web, grid, command-line

There is a Kerberos principal for each LIGO member (their LIGO.ORG login). The roster drives creation of principal for each member and pushes principal and details into LDAP. LIGO IAM leverages Grouper from Internet2 which provides Privilege, Role and Attribute support and provisions into LDAP. A single sign-on for LIGO web space uses the Shibboleth System to provide single sign-on, LIGO Identity, and consume federated identities (InCommon for many U.S. institutions).

The Gravity-wave community is larger than LIGO with such facilities as Cascina in Italy, KAGRA in Japan, and researchers in Canada, Australia, Korea, China,…. Peer-to-peer federation is necessary. The only options are peer-to-peer negotiation or joining each national identity federation. IDEM in Italy will be the next federation for LIGO.

LIGO international federation engagement has goals to:

- Document technical and policy changes for a peer-to-peer
- LIGO membership in IDEM
- Prototype interoperability with the UK via InCommon

Peer-to-peer federation with KAGRA in Japan provided metadata exchange and negotiation on attributes. Access control is the central issue.

The complete briefing may be found on the MAGIC web site at: https://connect.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2012

European Federated Identity Management (IdM) : Steven Newhouse

Federated IdM in research is a European collaborative effort started in June 2011. It involves photon and neutron facilities, social science and humanities, high energy physics, climate science, life science and fusion energy. They have held 4 workshops to-date. They documented common requirements, a common vision and recommendations. An important use case for international federation is CERN-OPEN-2012-006. The vision is for a common policy and trust framework for IdM based on existing structures and federations providing unique electronic identities authenticated in multiple administrative domains and across national boundaries. Common requirements include: user friendliness, browser and non-browser federated access, multiple technologies and translators, open standards and sustainable licenses, different leves of assurance, authorization under community or facility control, flexible and scalable IdP. Attribute aggregation for authorization, and privacy and data protection. Operationally, they require: risk analysis, traceability, security incidence response, transparency of policies, reliability and resilience, smooth transition, and easy integration with local service provider.

Recommendations for technology providers include: separation of authentication and authorization, revocation of credentials, attribute delegation to the research community and levels of assurance. European activities include NRENs: https://refeds.org/ and connecting national identity federations: www.edugain.org and federation of federations.

Participants in the European Grid Infrastructure (EGI) (EGI.eu@Amsterdam) include over 35 countries with secure sharing of infrastructure components (computers, clouds, data archives,…). EGI activities include personal certificates (X.509), TERENA certificates and federated IdM access.

For the complete briefing please see: https://connect.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2012

Federated IdM works but is not commonly used. Getting attributes released is difficult.

The Globus Nexus identity and group management hub: Ian Foster

There are a multiplicity of credentials of different types using different federated identity protocols. Some of the identity providers include: InCommon, VeriSign, Google, and XSEDE. Globus Nexus as an identity hub allows users to create Globus online identity and link to identities from other federated IdPs (InCommon (SAML), Google (OpenID), XSEDE (OAuth MyProxy)) It acts as a federated or native IdP to third-party services and caches delegated credentials for unattended operation.

As a Group Hub, Globus Nexus links a set of Globus Online identities. It allows users to self-manage groups, Query and update are via REST API. Import and publish are via LDAP. The hub operates on multiple Amazon availability zones with over 99.9% availability. Other services can outsource identity and group management to Globus Nexus, such as kBase, and BIRN.

The Globus Hub does NOT:

- Provide authorization
- Provide interfaces to support extensible user attributes
- Support HIPAA data.

More information is available at: globusonline.org. For the complete briefing see: https://connect.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2012

CILogon: Jim Basney

CILogon enables campus logon to CyberInfrastructure using existing researcher credentials at their home institution and eases credential management for researchers and CI providers. The CILogon service: https://cilogon.org supports InCommon and OpenID authentication. It provides certificates to desktop, portals and browsers. Certificate lifetimes are from 1 hour to 13 months. It supports close integration with CI projects. It is available now.

The CILogon Delegation Service allows researchers to approve certificate issuance to portals via OAuth. LOA requirements differ across scientific collaborations. CILogon LOA options include:

- InCommon silver
- OpenID OIX
- InCommon Basic
- Second factor authentication (soon)

CILogon CA operations meet IGTF standards.

For non-browser applications use browser-based authentication or use SAML Enhanced Client or Proxy (ECP) authentication outside the browser to download the certificate.

Lessons learned include:

- InCommon today supports browser SSO
- Attribute release is challenging today for service providers that want to support multiple IdPs.
- Google OpenID is a popular catch-all IdP.

More information is available at: www.cilogon.org

The full briefing is at: https://connect.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2012

Next MAGIC Meetings

- December 5, 2:00-4:00, NSF, Room II-415
- January 2, 2:00-4:00, NSF, Room II-415