MAGIC Meeting Minutes
November 18, 2015

Attendees

Tom Barton	U. Chicago
Jim Basney	NCSA
Richard Carlson	DOE/SC
Vince Dattoria	DOE/SC
Jill Gemmill	Clemson U.
Jim Marskeleve	PSC/CMU
Don Middleton	NCAR
Grant Miller	NCO
Amy Starzynski	IU/CTSC
Steve Tuecke	U. Chicago
Nick Watts	Clemson U.
Von Welch	IU

Action Items

Proceedings
The meeting was chaired by Rich Carlson, DOE. Tom Barton, Jim Basney, Steve Tuecke, and Von Welch presented the status of Identity Management (IdM) and international cooperation on IdM.

Identity Management (IdM) Update: Von Welch

InCommon Research and Scholarship Update

The InCommon Research and Scholarship (R&S) members increased by 2 members last year. NSF is joining R&S as a Service Provider (SP). R&S increased by 15 IdPs and 6 SPs in 2015. R&S growth is not keeping up with InCommon growth.

There were 667 InCommon members in October 2014, which grew to 810 members today. InCommon appointed Von Welch to the Steering Committee as their advisor for research.
InCommon is joining EduGain to enable international use of identities. They are currently addressing legal issues of the participant agreements.
NSF made a number of CCIE awards affecting IdM including to FeduShare and Vassar IdM.

A number of InCommon services exist:

- Globus Nexus
- AuthO
- SciGap
- Google, etc. social media
- ORCID

Management is specific to workflows especially for Identity Access Management (IAM).
At the NSF Cybersecurity Summit, IAM was a focus topic. Two factor authentication for smart phones is inexpensive and widely used. It, increasingly, is likely to become the default IdM. HIPAA plays an increasing role in research and will drive 2-factor authentication. Data sharing is a driver for IdM both for big data and small data. There is no convergence on IdM solutions by the global community.

Policy decisions are difficult and generally require a CIO for higher level decision but the CIOs and higher are not used to making these decisions. It would be useful to routinize access requests with a semi-automatic response on behalf of the CIO (educating the CIO is implied here.)

CILogon: Jim Basney

CILogon enables use of federated identities for access to cyberinfrastructure. It translates across federations and protocols. CILogon IdPs number over 160 now with over 50 IdPs added via Research and Scholarship (R&S). There are over 6500 CILogon users now.

NSF awarded a 3-year CICI award for January 2016 to December 2018 to provide an integrated open-source Identity and Access Management IdAM) platform. This includes CILogon for federated IdM and COmanage for collaborative organization management. This will support international collaborations. Science partners include NANOGrav Physics Frontier Center, LIGO, and DataONE. Cyberinfrastructure partners include XSEDE and AARC. Project deliverables include:

- CILogon-Comanage integration
- VO collaboration
- International federation through EduGAIN
- Linking ORCID identities
- Supporting LDAP and SSHKey management
- Multi-factor authentication and Levels of Assurance
- Web Single Sign-On Gateway with IdPoLR, SAML, AA, SAML-OIDC

International federation will be approached through international IdPs with US CILogon or EU CILogon linked with GEANT's Trusted Certificate Service. A pilot project with AARC is underway.

Multi-Factor Authentication (MFA) will be used and signaled in CILogon assertions.

Web Single Sign-On Gateway will be an IdP of last resort (IdPoLR) adopting InCommon-recommended IdPoLR providers. SAML Attribute Authority (AA) will provide VO-specific attributes and group membership for authorization and Shibboleth SP to query multiple SAML AAs.

Next steps are to work with science projects, standardize OIDC claims, interfederation (InCommon will be EduGAIN-ready in February), and ORCID-ID linking.

For the full briefing, please see:
https://www.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2015
Under the November 18, 2015 meeting

InCommon and Global Federation Issues: Tom Barton

InCommon is implementing.

- Attribute release
- IdP/SP practice requirements
- International federation

They are developing IdP for researchers without federated credentials, operational security and operational continuity, a community practice trust framework and a federated incident response.

Attributes include email, name, and a persistent identifier. They are developing frameworks for attribute release. Barriers include the inability of central IT to address policy questions and accept risks, a lack of communication between researchers and central IT, data privacy for the EU to non-EU transactions and a lack of technology to implement correct behavior. There is a Federation Interoperability Working Group that promotes:

- IdP-SP interoperability
- Participation by EU and U.S. R&E, Ping., Microsoft, OCLC
- SAML V2.0 implementation profile for federation interoperability

Next steps include REFEDS consultation, WG focus on deployment practices and In-Common Fed-Lab

Sirtfi and Federated Security Incident Response enable R&E organizations to coordinate security incident response. First step is to establish a global standard. Sirtfi Trust Framework v1.0 defines low-bar security incident response. It is under REFEDS consultation now. Sirtfi Phase 2 will provide security contact information in R&E federation metadata. Sirtfi Phase 3 will provide proactive notification by IdP to SP of account breach on a need to know and private basis.

Baseline trust needs to provide assurances to R&E Feds to enable mutual trust. FICAM/Kantara is too heavy. InCommon's Participant Operating Practices are too light and hard to verify. A new approach is needed. The Internet2 TIER project should help organizations with this.

For the full briefing, please see:

https://www.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2015

Under the November 18, 2015 meeting

Globus: Steve Tuecke

NCAR Remote Data Access (RDA) is improved with Globus Authorization by:

- Removing the need for Globus identity
- Integrating RDA and Globus Transfer API.
- Leveraging other Globus Auth-enabled services
- Removing the need for RDA identity
- Integration with RDA REST APIs.

Meetings:

Next MAGIC Meeting

December 2, 2015, 2:00-4:00 Eastern, NSF Room II-575