MAGIC Meeting Minutes
November 15, 2016

Attendees

Tom Barton	U. Chicago/Internet2
Jim Basney	NCSA
David Bernholdt	ORNL
Ian Foster	U. Chicago
Dan Katz	U. Ill.
Padma Krishnaswami	FCC
Stephen McNally	ORNL
Grant Miller	NCO
Alan Sill	Texas Tech
Derek Simmel	Pittsburgh Supercomputing Center
Steve Tuecke	U. Chicago/GLOBUS
Von Welch	IU

Action Items

Proceedings
This MAGIC meeting was coordinated by Grant Miller of the NCO. This meeting focused on Identity Management in an international context.

Identity Management Update: Von Welch

InCommon:

Von Welch remains an advisor to the InCommon Steering Committee. InCommon joined EduGain global interfederation. See: https://www.incommon.org/edugain/
The NSF is still planning to join Research and Scholarship (R&S) of InCommon.

An IAMOnline session was held in August 2016: https://incommon.org/iamonline/
It advocated attribute release, scalable consent and user convenience.

A security Incident Response Trust Framework for Federat3ed Identity (Sirtifi) enables the coordination of incident response across federated organizations. A Sirtifi proof of concept was held among NCSA, U. of Chicago and LIGO.

Lack of attribute release to science SPs is still a big problem. There are over 900 InCommon participants (organizations). The Global R&S category has 55 InCommon SPs. 122 InCommon Identity Providers release attributes to R&S services. It is common for SPs to report <50% of researchers able to use FedIdM. The InCommon Steering Committee released a resolution for InCommon Identity Provider Operators to release an identified set of attributes to all InCommon Service Provider Operators.

The NSF Cybersecurity Center of Excellence issued a guide for developing cybersecurity programs for NSF Science and Engineering projects which contains an Identity Attribute Management section. The Center also maintains a blog on Identity Management best practices. The Center partners with the EU Authentication and Authorization for EResearch and Collaboraiton project: https://aarc-project.eu/

In summary:

- IdM/IAM is an ongoing challenge but maturing
- InCommon enabling R&S is slow going
- 2 Factor Authentication is becoming common with soft tokens
- Social identities via OAuth is not going away
- It is likely an Ecosystem will evolve rather than a single system

For the complete briefings, please see the MAGIC Team Website at:
https://www.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2016#November_2016

InCommon and Global Federation Issues: Tom Barton

Global Federation demands are leading to evolving the roles of federation operators and federation members in producing trust in federation. EduGain now has over 2200 IdPs, 1380 SPs and 38 Federations. Errors in one federation can impact all others. Issues being addressed include:

- What should be published to EduGain and what should be filtered?
- Which parts of Metadata should federation operators police?
- What autonomy should members have over their own entity attributes?

The global metadata aggregate that fed ops sign is becoming too big for some SPs and IdPs.
A bite-sized metadata is being developed for metadata queries. Metadata is dynamic; both federation operators and members have roles in anchoring trust.

There is a low uptake of FICAM-style Level of Assurance in R&E. MFA needs to be separated from scalar LoA value. For MFA interoperability, we need a standard for how SP signals that it wants MFA and IdP response. The InCommon WG defined a standard profile. REFEDS is working to make this a global standard. The standard builds on International Grid Trust Federation, eIDAS, and Kantara. A complete draft is to be released this month (November 2016).

Sirtifi is a federated security incident response. It establishes basic security practices that each member self-attests to. There is a standard representation of security contact in metadata. The Dutch and Swedish federations are 100% compliant. InCommon pilot production is expected imminently.

Trust in federation will need to be based on:

- A short list of simple high-level statements that are to be true of IdPs, SPs and federation operators
- Finalization in InCommon after broad community consultation
- Developing an implementation plan
- Expanding it globally by taking it to REFEDS

For the complete briefings, please see the MAGIC Team Website at:
https://www.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2016#November_2016

CILogon 2.0: Jim Basney

CILogon 2.0 is a 3 year NSF CICI project that began January 2016. It provides an integrated open-source Identity and Access Management (IdAM) platform for cyberinfrastructure. It supports international collaboraitons.

CILogon OSG Certificate Authority (CA) began January 2016. The CA policy is accredited by the IGTF. It passed XSEDE Operations Acceptance and the OSG CA uses CILogon operated by XSEDE. They are using the CILogon HTTPS API for issuance of certificates by the OSG front-end. The SAML to OpenID Connect Gateway entered production in January 2016. It supports e-science clients. User consent is based on requested scopes: applications requested: See www.cilogon.org/oidc

GLOBUS uses CILogon and encourages Federated logins; they began listing InCommon IdPs directly. This resulted in a doubling of InCommon/CILogon use. Some users include: Atlas, CMS Concept, LIGO, OOI, XSEDE, Globus,…

Global federation is used for Research and Scholarship, security contacts in metadata, and security incident response trust (Sirtfi). CILogon supports international IdPs as a result of InCommon joining eduGAIN.

CILogon monthly usage is now 3200 active users per month.

Visit www.cilogon.org to sign up.

For the complete briefings, please see the MAGIC Team Website at:
https://www.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2016#November_2016

Globus Authorization: Steve Tuecke

The cloud has transformed how software and platforms are delivered. Globus enables cloud services for users. Globus transfers files reliably and securely. It controls access to shared files on existing storage without having to move files to cloud storage. The researcher selects files to share, selects users and groups, and sets access permissions. Collaborators log into Globus to access shared files and downloads via Globus. Results are published via Globus. The next-generation portal will leverage the science DMZ. Globus Web App functionality is implemented via public transfer API. Requests are authorized via OAuth2 access token.

Globus Auth is foundational identity and access management (IAM) platform service. It brokers authentication and authorization interactions among end users, identity providers, services, applications, and services acting as clients. It is based on OAuth 2.0 and OpenID Connect Core 1.0 (OIDC).

A Globus account is a set of identities. Log-in with Globus is similar to log-in with Google or Facebook using existing identities and providing access to community services.

Globus Auth supports mobile applications.

For the complete briefings, please see the MAGIC Team Website at:
https://www.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2016#November_2016

Next MAGIC Meeting

December 7, 2:00-4:00 Eastern, NSF, Room TBD