MAGIC Meeting Minutes
November 18, 2014

Attendees

Tom Barton	U Chicago
Jim Basney	NCSA
Rich Carlson	DOE
Bob Cowles	Indiana/CACR
Dan Katz	NSF
Mark Luker	NCO
David Martin	Argonne
Grant Miller	NCO
Adam Slagell	NCSA
Harold Teuneson	SurfNet
Kevin Thompson	NSF0
Steve Tuecke	Globus
Von Welch	IU
Ann West	Internet2

Action Items

Proceedings

 This MAGIC Meeting was chaired by Rich Carlson of DOE and Dan Katz of the NSF... Thanks go to Von Welch for organizing a discussion of Identity Management with an international perspective.

InCommon Federation: Ann West

 The InCommon Federation has been enabling global identity management for 1.5 years. They are currently addressing policy issues.
 EduGain coordinates identity management. The actors in identity management include:
- Users
- Identity provider
- Service provider
- Federation operator

The Federation operator provides the "phone book" for the identity management/coordination. Federation is primarily distributed. InCommon has 695 organizations. Trust and risk are shared. InCommon provides privacy, membership, and risk control among the partners in collaboration. InCommon provides an interfederation phone book with over 2000 entries. EduGain is a lightweight interfederation that aggregates all metadata into one file. It is focused on metadata exchange. The intent is to be totally transparent and to publish what you do. Users are bound by the metadata they provide to their organizations. Federation principles are consistent with international requirements. EduGain covers most countries in Europe, North America, much of South America, and Australia. InCommon joined EduGain and is establishing a pilot with 5 service providers. They have completed the technical and transparency requirements. They are finishing a legal and policy position paper.

FOR OFFICIAL GOVERNMENT USE ONLY
c/o National Coordination Office for Networking and Information Technology Research and Development
Suite II-405 · 4201 Wilson Boulevard · Arlington, Virginia 22230
Phone: (703) 292-4873 · Fax: (703) 292-9097 · Email: nco@nitrd.gov · Web site: www.nitrd.gov

Next steps for InCommon joining EduGain include:
- Complete the policy/legal education materials to work with the InCommon community
- Work toward attribute release globally for the research and scholarship communities
- Work in the US on scale, diversity and community education
- Work to align federation operators: they currently may have different levels of rigor

SurfNet Security: Harold Teunissen
Surf is the basis for European federation.   Surf is an umbrella for SurfNet, Surfmarket, and SurfSara (computation and big data). They provide an interface to identity federations worldwide.
Collaborations do not have national boundaries so you need an international interfederation framework. Federations work but there are challenges including attribute aggregation, attribute release, levels of assurance, bridging communities, homeless users, credentials translations, user friendliness, and non-Web browsers.
The EU works on 2 tiers, a national basis and the EU scale.
At a global level interfederation is supported by REFEDS . GEANT coordinates EU academia. It creates a simple service to validate affiliation, provide Web-shops discounts, free access to some cloud services, and to validate affiliation. An academic pilot provides attributes within a federated logon to validate membership within the academic community but the user needs to join a federation. The federated service gets attributes directly from the user (self-assertion) and then verifies the user affiliation with his institution. Identity providers use SAML and are connected via EduGain. REFEDS is a Research and Education Federation which provides the mutual needs of research and education identity federations worldwide. It groups federation identities that share common criteria into categories. Two categories have been approved.
A security response is based on a characterization of a security incident and developed methods to respond to that security type.

Federated Security Response: Tom Barton, U. of Chicago
A federated security response requires a global a global access management infrastructure across users (research and education). REFEDS provides a basis. Much remains to be done:
- Global coverage (100%) or R&E organizations
- Standards
- Ubiquitous federated authentication for non-browser users
- Authentication assurance and strong authentication
- Federated security incident response
There is an increasing need for federated infrastructures. NSF cyberinfrastructure uses InCommon. It configures IP auditing to support debugging and security. CERN provides a federated Identity management. Considerations include:
- Scale: currently the same or a small set of affiliated organizations
- Unaffiliated organizations
- Why should I trust a request to share security incident information?
- How can organizations know who to contact? Currently th3e identity provider initiates the incident response across identity types.
Current work includes:

- Sirtfi provides a security incident response trust for federated identity
- Sirtfi has a draft trust framework providing foundational documents.
- A basic problem is to promote trust among federated organizations by self-asserting
- They need processes and tools for a federated security response (technology)
- Multifactor authentication is effective but there are still security incidents

Globus Identity Management: Steve Tuecke

User communities need faster international coordination. A user's GLOBUS identity at the U. of Chicago is his U of Chicago identity. They plan to coordinate with InCommon next year Over 1000 Globus users are members of InCommon. Issues they are addressing are:
- Account recovery if my account is compromised. How do I establish my identity to continue to access services?
- How do I deal with linked identities?

New Zealand eScience Infrastructure: Nick Jones

Tuakiri is the New Zealand national identity federation service for higher education and research. It developed out of the Grid computing environment. Tuakiri collaborates with REFED and AAF (Australian identity federation). It launched a pilot service in 2011. In 2012 there were 16 research institutions federated under Tuakiri in New Zealand. In 2014 all New Zealand research institutes participate in Tuakiri. The University of Aukland hosts the national service. The research institutes seek to work cooperatively with public sector entities. In 2014, there are 16 member research institutes, 42 federated services and over 135k transactions to date. 2015 target areas include:
- Online services for teaching and learning
- Amazon Web services
- Microsoft Azure
- Research and Office 365
- Dropbox

They are building a pilot EduGain interfederation and increasing cooperation with REFEDS and GLOBUS
. Attribute granularity is not fine grained. They can not currently distinguish between a professor and a student

Upcoming Meetings:

Next MAGIC Meetings:
January 7, 2:00-4:00 NSF, Room II-565
February 4, 2015, NSF