MAGIC Meeting Draft Notes
January 4, 2012

Attendees

Menee Altimee	FermiLab
Rachana Ananthakrishnan	ANL
Jim Basney	CSA
Scott Brim	
Rich Carlson	DOE/SC
Ken Klingenstein	Internet2
Scott Koranda	LIGO
Craig Lee	Aerospace
David Martin	ANL
Grant Miller	NCO
Alan Sill	Texas Tech Un
Kevin Thompson	NSF

Action Items

1. Grant Miller will send a message to the MAGIC members to solicit their suggestions for topics for future MAGIC meetings.

Proceedings

Welcome by Rich Carlson, Co-chair of MAGIC and a reminder to provide comments on the MAGIC minutes from November.

Discussion: Identity Management Systems for Collaborations and Virtual Organizations; Ken Klingenstein facilitator

Internet Identity

Consumer marketplace identity management is led by Google with participation by Paypal, Yahoo and others. It is based on the Open Internet Exchange (OIX) using a new standard OpenIDConnect. Open ID Connect is based on Shibboleth with additional capabilities in JSON. It uses SAML attributes and metadata which enables integration. Other major players are sitting on the sidelines including Facebook and Twitter. ISOC is interested in moving forward cooperative Identity Management internationally regardless of what is happening in the U.S. It fosters a comprehensive integration of roles and communities.

Consumers are individuals with their roles and attributes. They retain their identity even when they assume different roles, different policies and different governance.

NSTIC (http://nist.gov/nstic/) provides a well-crafted architecture and approach. OMB issued a fall 2011 directive that the Federal agencies should move to external identities where appropriate. An IDTrust Conference will be held in Gaithersburg March 13-14, 2012.

InCommon currently has 250+ universities and 450+ participants and continues to grow rapidly with over 10 million current users. It has 300 university providers versus 4

providers for Google. New uses are being developed for InCommon including Wikis, shared services, cloud services, calendaring, command line apps, UHC and others. Certificate services bind the InCommon trust policies to new applications including signing and encryption. FICAM certified at LOA 1 and 2 (bronze and silver). New InCommon developments include uApprove (end user attribute management), Social2SAML coordination and personal certificates for authentication, signed mail, signed documents, encryption, etc. Silver service provides a higher level of assurance to support financial and other valued resources. Silver service is used for grants administration, TeraGrid, OSG and medical records.

Basic attributes for science applications include: high-level affiliation, opaque, persistent and non-correlating identifiers (ePTID), a persistent and human-suable identifier (e.g. kjk@internet2.edu), name, email address and an open-ended set of entitlements assigned by the institution including group membership. Attributes tend to travel in bundles. For research and scholarship (R&S) the bundle contains: name, email, authenticated identity, and affiliation.

Approaches are being developed for non-Web applications. Challenges for this space include discovery, trust anchors in the clients, attribute release and privacy management. Three categories of approaches include:

- Moonshot- GSS over Radius and maybe SAML
- Oauth and OpenID Connect
- SAML ECP (extended client profile)- Kitten

There are no turn-key deployments yet.

Interfederation provides connection among autonomous identity federations. This is critical for global scaling, accommodating state and local federations and integration across vertical sectors. Operational capabilities include Kalmar2 Union and eduGAIN. Key technologies are being developed and used: PEER, metadata enhancements and tools and discovery.

Virtual Organization Identity Management

There are three contexts for VO ID Management:

- Internet-scale
- Campus/enterprise
- Virtual Organization

Primary issues are how to leverage the Internet and enterprise to serve the VO. Including leveraging security, privacy, efficiency, ease of use, sustainability… while identifying and engineering what is unique about the VO. VO ID Management needs to provide:

- Control of access to VO resources to properly authenticated and authorized users
- Serve deep, wide, and international communities
- ID Management applied to non-Web applications
- Integrated with scholarly identity
- Rely on limited support resources, legacy apps, ad hoc authority and processes
- Goals are to:
    - -- Leverage existing IDManagement technologies
    - -- Leverage existing deployed infrastructure

-- Drive identity and access control for both general collaboration and domain-specific apps.
-- Connect to the scholarly record
-- Offer implementation and deployment options

Collaboration Management Platforms include SurfNet and COmanage.

Discussion among the MAGIC members identified that:

- There are 2 scenarios for managing IDManagement for VOS. For LIGO, groups from universities (MIT, Cal Tech) write up an MOU with other universities for access to resources. They join wholesale into the VO. Under an alternative scenario. External to the VO set up collaboration for a specific application, e.g., sharing notes, findings, postings, developing research papers. Use resources such as CoManage to establish the collaboration.
- Institutions have to be primary for identity management for specific applications, e.g., for the Higgs Boson collaboration.
- How do we get VOs working across many organizations and apps? Identity management and attribute authorities are outsourced to assert individual identities. Your identity is established close to your home institution but is adopted for other uses like VOs. Universities are looking to the future where they rely on Google identities. The Google identity is then decorated with university attributes.
- Assume that Globus will not be replaced. The movement is toward acceptance of outside entity authorities.
- Non-Web IDManagement: Current development is all for Web-based apps. There are no turn-key non-Web uses yet. Discovery and attribute release need to be based on SSH. You can bring attributes into the local service. How are the attributes retrofitted to the local app? Is there a reasonable mapping between what attribute providers can provide and what the application server can use? Federal agencies have a role to provide this bridge. A modest investment might provide a real gain. COmanage and Assert Connect can manage attribute release. MAGIC could profile existing standards
- OGF has a Federated Security Group that deals with integrating IDManagment capabilities and establishing security standards.
- Open Science Grid and EuropeanGrid are developing a common document to identify how federated security is provided across US and European groups.

AI: Grant Miller will send a message to the MAGIC members to solicit their suggestions for topics for future MAGIC meetings.

Future MAGIC Meetings
February 1, 2:00-4:00, NSF, Room II-415
March 7, 2:00-4:00, NSF, Room II-415