MAGIC Meeting Minutes
April 3, 2013

Attendees

Jim Basney	NCSA
Rich Carlson	DOE/SC
Dan Gunter	LBL
Ken Klingenstein	Internet2
Miron Livny	OSG
David Martin	Northwestern U.
Shawn McKee	U. Mich.
Josh Moore	CNBC
Don Middleton	UCAR
Grant Miller	NCO
Don Riley	U. Maryland
Alan Sill	TTU/OGF
Von Welch	Indiana U.

Action Items

Proceedings

This MAGIC Meeting was chaired by Rich Carlson of DOE/SC.
Ken Klingenstein provided a briefing on Updates on Identity and Access Control Management. The briefing is summarized below. For the complete briefings, please see the MAGIC Wiki site under the April 3, 2013 Meeting at:
http://www.nitrd.gov/nitrdgroups/index.php?title=Middleware_And_Grid_Interagency_Coordination_(MAGIC)#title

Identity and Access Control Management: Ken Klingenstein

Everyone has many identities, roles and attributes as researchers, scholars, citizens, consumers, users,… In any of these roles, a person may need different applications, different identifiers, different levels of authentication, different privacy regimes, and, perhaps, different identity providers. Across all these different possibilities the user experience needs to be consistent.

Scalable access control is catalyzed by federated identity. Lists of identifiers are problematic to maintain. Use of attributes and entitlements can simplify control. The creation of groups with federated members and groups helps create attributes.

Privacy issues are ubiquitous spanning security cameras, access control, GPS, third party use of data, minimization of data spills,… Laws and regulations regarding privacy are merging, receding, and in endless loops. International inconsistencies are particularly problematic.

The Identity Needs for the research community include doing experiments, collaborating, publishing, doing outreach and submitting grants and grant management.

Social identity is reaching saturation and the protocol may be shifting from OpenId to OpenId Connect. Oauth is used to handle all non-web and mobile applications. Federated ID continues to grow and dominate inter-organizational interactions. Hybrids are growing, e.g., Social2SAML and SAML2Social. New aggregators are appearing, e.g., PingOne. Some legal actions in both the U.S. and Europe are having consequences on behavior.

FICAM provides identity services for government uses. It is successful and steadily growing. It includes PIV cards, PKI, and federated identities. NSTIC is aimed at the next generation of services and privacy. It is providing governance and pilots.

InCommon today includes 500+ universities and 650+ participants with over 20 million users. FICAM is certified at Level Of Assurance (LOA) 1 and 2 (Bronze and Silver levels). New services in InCommon include SSL and personal certificates, InCert (lifecycle management) and certification marks (to facilitate attribute release). InCommon provides silver level of assurance. Multi-factor authentication provides a variety of tokens. InCert manages certs for provisioning, mobility and renewal. InCommon provides Social2SAML gateways.

NSTIC (National Strategy for Trusted Identities in Cyberspace) is a White House initiative on citizen-government security and privacy. It has governance and developments components. See: www.nist/gov/nstic NSTIC is intended to define the rules for electronic identity transactions for the federal government and as an anchor for the general marketplace to provide privacy, security, robustness, usability, and standards. NSTIC is developing pilot capabilities for a variety of applications including monetization of attributes and scalable privacy. The privacy work is promoting 2-factor authentication, privacy managers for users to control release of their attributes, implementing anonymous credentials at scale, and metadata standards.

Interfederation progress is slow and steady. Key packages are emerging: PEER, MDX, MDA. There are initial discussions of interoperation among exchange points. Policy and privacy are difficult, especially internationally.

Identity for scholars includes:

- Eduroam
- FIM4R
- Cyberinfrastructure identity: ORCID, Cllogon, ScienCV, and science agency data set access controls.

Collaboration platforms include VO IdM and CoCoA

A primary issue is that lack of communication among projects and programs leads to reinvention of capabilities by each group. More open discussion and awareness is needed among scholarly groups.

LIGO has developed a list of applications where Id and Access Control Management are required. It includes: Wiki/web, mailing list, repository, ticketing system, voting system, calendaring, polling, document control center, command line tools, grid space, guests, Google apps, conferencing, activity streams, and roster.

Note: Steve Wolff of Internet2 is looking for applications where SDN makes an application possible.

AI: if you know of applications that are enabled only through the use of SDN, please contact Steve Wolff of Internet2.

Upcoming Meetings
April 21-24 Internet2 Member's Meeting, Arlington, Virginia
July 22-25 XSEDE Meeting, San Diego
Week of July 30-Aug 2, OGF Workshop, Miami, Florida
Week of July 30-Aug 2 Federated Cloud Workshop, Germany
November 11-15 InCommon Identity Week, Silicon Valley

OSG and XSEDE are offering a summer school to provide understanding of the principles, concepts and applications. A link to this meeting is provided on the XSEDE Web page.

Next MAGIC Meetings

- May 1, 2:00-4:00, NSF, Room II-415
- June 5, 2:00-4:00, NSF, Room II-415