MAGIC Meeting Minutes

April 6, 2016

Attendees

Jim Basney	NCSA/UIUC
Rich Carlson	DOE/SC
Dan Gunter	LBL
Randy Heiland	IU
Ken Klingenstein	I2
Padma Krishnaswami	FCC
Grant Miller	NCO
Kevin Morooney	Internet 2
Kevin Thompson	NSF

Action Items

Proceedings

The meeting was chaired by Rich Carlson, DOE. Ken Klingenstein discussed Identity. Ken Kllingenstein gave a presentation on Internet Identity and Collaboration Support.

Grant Miller discussed a number of changes of the NITRD Subcommittee, parent of LSN and MAGIC, and in the National Coordination Office that supports the NITRD Subcommittee.

- The current NCO Director (Keith Marzullo) and Associate Director (Peter Lyster) will be rotated out in July 2016 and October 2016 respectively. A new director and associate director will be named by OSTP and the National Science and Technology Committee.
- NCO has been hosted by the NSF for the past 15+ years. The NSF is moving to new quarters and will not be hosting the NCO after October 2017. GSA is seeking new office space for the NCO in downtown DC. There will be one-time charges for moving the NCO in FY 2017 and FY 2018
- The President's Council of Advisors for Science and Technology (PCAST) made recommendations to change the NITRD groups and Program Component Areas (budget reporting categories). The LSN and MAGIC structure will not be changing.
- All NITRD groups are re-chartered every 2 years. A charter was drawn up for MAGIC. Review by legal counsel identified that teams like MAGIC, with input from university, commercial and private members, should not be chartered. They also identified that it is allowed for the teams to hear from commercial companies about their technology and plans.

Update on Internet Identity Collaboration and Support: Ken Klingenstein, kjk@internet2.edu

FICAM serves gov/gov and biz/gov. Their PKI Bridge provides high assurance and pharma mechanisms for controlled substances. Large SAML federations, e.g. NIEF, serve law enforcement, health, justice,…

NSTIC has been enfolded into NIST. The IDESG (Identity Ecosystem Steering Group) creates trust frameworks, schema certifications for IdP, Relying Parties (RPs), intermediaries. They have produced an initial trust framework and associated self-asserted listing service

General Data Production Regulation (GDRP) applies to all European states. It applies to all EU customers or clients worldwide and provides for massive fines for non-compliance. It provides revocable consent, clearly informed consent, the right to be forgotten, data portability between IdPs and sets the age of consent from 13 to 16. Some implications are:

- Cloud-based processors share responsibilities with data controllers for 72 hour breach notification to authorities
- Back-end Contracts need to be approved by the data controller
- Risk-based requirements on companies for data protection assessments on full data life-cycle
- Almost one-stop shopping for multi-jurisdictional resolutions
- Data protection officers are required
- PrivacyShield (Safe Harbor 2.0) is proposed

InCommon has 842+ participants in academic research institutions with over 8 million users. There are 100s of service providers. Certificate services are important, Multi Factor Authentication (MFA) devices and licenses are increasing and campus use is increasing rapidly. Metrics for MFA and InCommon need to move to the number of relying parties per IdP and the number of critical apps protected by MFA.

InCommon joined eduGAIN which has 41 national R&E federations with 31 million users and the number of IdPs for InCommon has gone from 400 to 300. Issues include system stress due to the metadata bundle size, semantics across national borders, and data movement across national borders.

Social identities are increasingly being used in protocols (Shib IdP v3 extension that issues OpenIdConnect tokens) and in identities (Social2SAML gateways). Issues include the strength of identity proofing, LOAs filtering out attributes and data sovereignty concerns.

Attribute release is the highest barrier to use and is a key dimension of privacy. It presents a complex set of legal, technical, international, and financial issues. Selective release of values from a multi-valued attribute (group memberships) is challenging.

Federated incident handling is important for major science service providers. SIRTIFY, developed by CERN, is working with major labs and science facilities to define requirements. It is moving toward becoming part of composable trust frameworks (e.g., InCommon + R&S + EduGAIN + SirTiFi).

ORCID provides a persistent unique scholarly identifier to connect a researcher as they change affiliations and institutions. It is being increasingly used and ORCID identities can be freely obtained from orcid.org.

Access control can be implemented using attributes of users. ACLs are provided by group membership, role, citizenship, clearances and other attributes..

Collaboration support provides integrated identity management across the set of applications of a VO. It provides participant life-cycle management and privacy preservation by leveraging identity and security infrastructures. Platforms provide identity and group membership via protocols, e.g., COmanage,, Globus Nexus, Google+,… They may be deployed by a VO, by local infrastructure (campus, lab), of by a national or trans-national infrastructure (GEANT, SURFnet, JISC). LIGO was an early adopter of COmanage for federated identity management, MFA, highly managed access controls and managed social identities.

Next steps include:

- Services and identity providers in eduGAIN
- Adhere to federation interop guidelines (e.g., Kantara)
- Leverage R&S tags for attribute release.
- Particiapation in SirTiFi

- Application security moves to MFA
- Promotion of ORCID identifiers for researcher identities.

For the complete briefing please see the MAGIC Website at:
https://www.nitrd.gov/nitrdgroups/index.php?title=MAGIC_Meetings_2016#April_2016_Meeting

Discussion among the MAGIC members

Jim Basney has seen a strong move to OpenIDConnect. Refeds is developing the attributes we need for secure identity. Jim Basney is coordinating with the Opensource COmanage platform for VO management. They started NCSA MFA cooperation last week. How do we specify our users are using MFA? XSEDE funding is supporting a free tier for COmanage.

Kevin Thompson is developing the next proposal for the CC-DNI program

Next MAGIC Meeting

May 4, 2016, 2:00-4:00 Eastern, NSF Room TBD