

InCommon Technical Forum
2011 Internet2 Fall Member Meeting
October 5, 2011

RL "Bob" Morgan reviewed the technical initiatives underway, including a number of items that will soon be deployed.

Technical Initiatives

- Default Attribute Bundles to streamline boarding of a subset of service providers (<https://spaces.internet2.edu/x/962KAQ>)
- InCommon recommended practices (introduced at CAMP) (<https://spaces.internet2.edu/x/Z4AXAQ>)
- Additional information in metadata
 - Required attributes - SPs express which attributes they require
 - User interface elements
 - Contacts – clarifying what we want/expect from IdPs
- Assurance – InCommon expects to be ready to certify IdPs for Silver in early 2012
- SP error handling (improving the user experience when attributes are missing and access denied)
- Delegated administration of metadata
- Statistics and business intelligence
 - Gathering/providing more information about the federation and its use.
 - Also deeper issues, such as who is using services and which services are being used.
- POP revision
- FICAM (federal identity initiative)
- Metadata vetting policy
- SAML ECP support
- Decommissioning of the WAYF
- XML submission of metadata
- Participant web pages
- Metadata-driven web pages
- NIH/NSF support
 - Important to evangelize with these and support what they are doing.
- AdmitMe
 - This is a new project that is looking at the possibility of a common identity process for high school students taking standardized tests and using the common application (and whether these students could receive an central identity, vs each school to which they apply providing an identity).
- Client certificate
- Second factor authentication

Recommended Practices

Bob reviewed the recommended practices program, which was first introduced at CAMP 2011 (<https://spaces.internet2.edu/display/InCCollaborate/Recommended+Practices+for+InCommon+Participants>)

There has been quite a bit of discussion about what to include in these practices and how to provide incentives for participants to adopt these practices. The goal is to make things more predictable and to provide increased value by having these practices widely adopted.

Bob highlighted some of the recommended practices:

- Federated security incident response
- Metadata consumption – refresh and verify daily
- SAML endpoints - some new features – new metadata elements, assurance – will only be available via SAML 2.
- Contacts in metadata
 - o Four kinds – technical, administrative, security, support.
 - o We're recommending using aliases, mailing lists, trouble tickets, etc., rather than specific individual emails
 - o Admin contact is now seen as the contact that can deal with attribute release policies.
- We will likely do one or more webinars on the recommended practices.

There are still some questions to be answered, including how a practice gets on the “recommended” list and whether there is a process for vetting such requests. Might there be community voting or some other method?

Demos

There were three demos at the end of the session:

- The forthcoming metadata-driven web pages
- delegated administration of metadata
 - o a proposed central error handling service, targeted at R&S category of SPs, that would provide more information for users as to why they can't get access and what their next step(s) might be.