InCommon Technical Forum
2010 Internet2 Fall Member Meeting
Nov. 2, 2010

Operations Update

Cert Service
- SSL certs are up and running; personal certs and EV certs coming soon
- 64 universities and colleges have subscribed so far.
- TBD – personal certs with various levels of assurance, campus intermediate CAs, code signing CAs

Metadata
- Implemented a metadata change process
- Platform upgrade: XML store
- Upgrade to metadata signing fool (XMLSecTool)
- Looking at metadata host name validation process
- Testing XML submission process
- Implemented support for multiple scopes (need to contact InCommon Ops for this)
- Looking at delegation of metadata submissions with site administrator approvals (much the same as delegated cert request submissions)

WAYF/Discovery Service
- InCommon is testing a new Discovery Service (the current WAYF is limited to SAML1). Information available in the wiki: https://spaces.internet2.edu/x/FgEFAQ

Technical Initiatives

R.L. Bob Morgan introduced the InCommon Technical Initiatives, a comprehensive wiki developed by the Technical Advisory Committee (TAC), listing a wide variety of technical activities to improve the operations of InCommon and to extend its reach. The information includes the relative priority and effort anticipated to bring each item to reality. https://spaces.internet2.edu/x/XIU0

Bob reviewed some of the items on the Technical Initiatives list.

XML Submission – permits site administrators to submit blocks of XML-formatted data rather than (or in addition to) using a web-based form.

Metadata Key Management – automatic and timely notice of expired certs.

Support for User Interface Elements in Metadata – Providing schema support in InCommon metadata management for UI elements related to names, descriptors and logos.

Technical Support for InCommon Identity Assurance Profiles – Using existing metadata to express an IdP's qualifications with respect to bronze, silver and other IAPs.

Cryptographic Algorithm Agility – A proposed OASIS metadata extension for facilitating a move from SHA-1 to SHA-2 (which may be required by the U.S. government).

Clarification/Extension of Contacts – The use of existing contact types within the metadata is inconsistent across sites. Additionally, there is a proposal to add a new type of contact for security incident reporting.

Review of Participant Operational Practices (POP) – The POP questionnaire needs to be refined, particularly in relation to Silver and other proposed identity assurance profiles.

This item led to a discussion about verifying POPs and, in general, the federation's role in encouraging sites to do the right thing – such as moving to SAML2 and populating the contact information in the metadata. R.L. Bob asked if we should publish a list of "the right things to do" and create some sort of "gold star" list of sites that exhibit all of these good community behaviors.

Scott Cantor suggested that we need to be clearer about the standards that we support. Right now, for example, the only software that behaves the way we expect SAML software to behave is Shibboleth. The use of other software impacts the rest of the federation because deficiencies require extra effort and work-arounds at individual institutions. Should InCommon be helping participants identify and deal with problems because of the software choices that others make? Perhaps a site needs to meet a set of standards in order to be present in the metadata.

Metadata Driven Attribute Release – suppose a professor is working with a colleague at another campus and using an SP there, requiring the release of attributes. Currently, the professor needs to find the local IdP administrator and have a new Attribute Release Policy added in order to access the remote SP. The vision: an SP element in the InCommon metadata that lists required attributes. On attempting to access the SP, the professor consents to the release of these attributes and gains access. Local administrators are not involved.

Some suggestions – Steve Carmody said he believes the Japanese federation has a bundle of required attributes and a bundle of optional attributes. Perhaps a UI could be developed that would have check boxes by the optional attributes, but not next to the required attributes. Another option would be to have sets of attributes for the user – if you allow the release of this set, you get access to this. If you allow this additional group, you can access these other sites.

Enhanced Metadata Interpretation – We would like to have a web-based metadata viewer.

The TAC is taking comments and suggestions at the Technical Initiatives wiki page: https://spaces.internet2.edu/x/XIU0