InCommon BoF (InCommon 101)
2007 Fall Member Meeting
October 10, 2007

Susan Neitsch, Texas A&M
David Walker, University of California Office of the President
David Bantz, University of Alaska
Mark Miller, Penn State University
James Crampton, Brown University
Asbed Bedrossian, University of Southern California
David Wasley, retired, University of California Office of the President
Brendan Bellina, University of Southern California
Mike Austin, University of Vermont
John Krienke, Internet2
Iljun Kim, Internet2
Ann West, Internet2
Renee Frost, Internet2
Ken Klingenstein, Internet2
Dean Woodbeck, Internet2 (scribe)

This session was provided as an introduction to InCommon for new or potential participants. It also provided an opportunity for questions and information exchange among current participants.

InCommon Governance

InCommon is an LLC (form of corporation) with Internet2 as the sole member of the LLC. InCommon is the federation operator and deals with credentials and certificates and metadata.

The InCommon Steering Committee provides oversight and governance of the service and currently consists of 10 people representing a mix of private and public universities that are geographically diverse. The steering committee has appointed a technical advisory committee (TAC), which provides recommendations relating to the operation and management of InCommon with respect to technical issues. You will find information about InCommon governance at www.incommonfederation.org/about.cfm.

Joining InCommon

InCommon is open to higher education institutions, research entities and government agencies; and their sponsored partners. Joining InCommon involves a management process and a technical process (see www.incommonfederation.org/join.cfm). The management process involves a legal agreement and policies/procedures related to being part of a federation (www.incommonfederation.org/docs/policies/incommonpop.html). The length of time to implement the agreement varies – it usually takes a few conversations. With the increasing number of participants and precedents set, it is generally a quick and smooth process, depending mainly on the institution's legal counsel. Current fees include a $700 registration fee and a $1,000 annual participant fee.

The technical process involves installing SAML-based federating software for authentication and authorization. Most institutions use the open-source Shibboleth, developed by the Internet2 Middleware project (www.shibboleth.internet2.edu). The technical process can take place at the same time as the management process. Some campuses already use Shibboleth for internal sign-on, which expedites the federating process. As part of this process, an identity provider supplies metadata to the federation. Metadata, or data about data, includes such things as the providers's top domain name, URL of its single sign-on service, error page, and information about the digital certificate. Complete information about metadata can be found at http://www.incommonfederation.org/metadata.html.

InCommon Roadmap

The roadmap refers to the common data that is exchanged among InCommon participants. It includes information about the eduPerson attribute schema required for operating with InCommon.

There was a general discussion about directory information at multi-location institutions and how the multi-campus nature of the data relates to InCommon. The University of California system provides an example of how multi-campus universities can interact with one-another and InCommon. Under this model, and because of the decentralized nature of UC, each university in the system joins InCommon. The University of California system has more than 375,000 computer users. By building UC Trust on top of InCommon, these users can take advantage of system-wide resources, campus-specific resources and outside resources like library databases or services offered specifically to students. UC Trust also allows users to access any of these resources (for which they are authorized). A case study of UC Trust is available on the InCommon web site (www.incommonfederation.org).

InCommon Member Services

The InCommon metadata lists 105 available services for InCommon participants. Another member service is the single sign-on advantage of SAML-compliant software like Shibboleth, which prevents the proliferation of user IDs and passwords for end users. It was suggested that InCommon list these services, or at least some of them, as part of its outreach efforts.

In terms of outreach, InCommon and Internet2 staff are discussing providing additional services, particularly for those institutions that may have joined InCommon but either have not installed Shibboleth or are not using Shibboleth with a service provider. InCommon's goals include not only increasing membership, but increasing members that are actively participating in the federation (in other words, they have federating software installed and have an association with a service provider).

As part of its outreach, InCommon has set up the InC-Collaborate wiki (https://spaces.internet2.edu/display/InCCollaborate/Home) for the sharing of documents, presentations and other electronic resources. Such information might include RFP language campuses use when negotiating with potential service providers or presentations to on-campus stakeholders explaining the benefits of federating and single sign-on.

One question came up – from a service provider perspective, once the SP joins, can InCommon just turn on access to all of the member IdPs? The answer is: not necessarily – it depends on individual campus policies and procedures and how the campus views the release of attributes.

Fine-tuning Authentication

Brendan Bellina, from USC, discussed a desire to have more granular control over the release of attributes. For example, currently a service provider may want to know whether or not someone is a student at a specific institution. But, there are cases where not all students at the institution would have access to that resource. Perhaps it is just a handful of students who need edit access to a wiki. He would like to see the identity provider have the ability to release only information about individuals who are authorized to actually use the service in question.

One suggestion is to have a more extensive handshake as the IdP is negotiating with the SP. Perhaps a general identifier is presented first, identifying the group of people who are potentially authorized to use a service then, later in the handshake, more detailed information is exchanged to narrow it down to those are actually authorized to use a service.

Managing non-members at the campus level

There is interest among some campuses in registering a second identity management system with InCommon to use for groups who are not members of the campus community. One large university, a potential InCommon participant, would like this available before they join. InCommon's business processes are about ready for this feature, which should be ready to roll-out sometime in 2008.