InCommon BOF
April 25, 2007
Internet2 Spring Member Meeting

John Krienke from Internet2 reviewed information from the InCommon Update (held earlier at the Internet2 Member Meeting) and a track session that featured information from InCommon universities and service providers. He also related information on future plans for InCommon, particularly efforts related to access to government resources and levels of assurance.

There is interest among InCommon participants in expanding the use of the federation and federating software both internally and with service providers. Some areas of potential include:

- TeraGrid
- Integration with student processes (registrar, admissions, transcripts, enrollment verification, third-party service providers)
- Library services
- iTunesU
- E-Auth (US government)

InCommon participants are also interested in additional ways to share information and there are plans to establish a wiki. Another thought, in terms of information sharing, is to provide an area where interested parties could view a demo of the InCommon process and federating software.

John also mentioned a testing process, currently underway, to put the certificate information in the metadata as part of the move from Shibboleth 1.2 to 1.3. Universities interested in participating in the test should contact John.

Attribute Release Policies

The discussion turned to attribute release policies and which attributes universities typically pass to a service provider (SP). The response was: it depends on the role and the privacy policies of the SP. In general, universities want to release only the information that is necessary. For example, if an SP needs to know whether someone is a student, but does not need the student's name, the university will pass an attribute that confirms student status but does not provide a specific name or university user ID.

There was discussion about whether any universities have a default attribute release policy – for example, certain attributes that are always "on." Such attributes may include identifying information so a web administrator could see if a person has been to the site before. The information would not identify who the person is – just that they have been to the site before. Universities represented at the BoF do not have such default policies.

This could also be used by service providers that don't have a relationship with the institution but does with the individual. Student Universe, for example, sells discount tickets to students and needs enrollment verification to prove affiliation. An IdP could offer the individual the ability to release affiliation, for example, to anyone for this purpose without a contract.

A concern was raised about university control over attribute release and whether the institution should trump the individual's wishes and default to a more restrictive policy that includes the registrar's approval for all student information released to all SPs, for example. Other

participants felt that the individual controlled this release and should be able to release it if they wished.

One concept would be for InCommon to provide a set of standard attribute release policies for a class of content providers such as what's being done the library publisher space. Perhaps this would include common attribute profiles that would address typical use cases in that field. These could be included on the InCommon web site. For additional services, an SP may ask the user for more information to personalize the experience. This would be optional on the part of the user.

Other topics that bear investigation:

1. Would it be useful to have some sort of self-assessment survey or web tool related to levels of assurance (LOA)? An InCommon participant or potential participant could complete the tool to discover about what LOA they meet, based on current policies and practices.

2. Are their policies or practices in place to contact participants about necessary policy changes? For example, if InCommon pairs with another federation and there are items not covered by the current participant agreement, how do we go to the members and say "we have this opportunity to peer, but need XYZ." In the UK, for example, the federation has greater latitude to make commitments on behalf of its members. That is not the case it the U.S.

The best way to deal with #3 would be the differences in LoA. Participation with another federation, or at some higher level, may require moving to the silver or bronze level. This keeps InCommon from becoming too prescriptive with its members.