**InCommon Update**
**Internet2 Member Meeting**
**Monday, October 8, 2007**

## Introduction

The InCommon Federation formed in 2004 as a pilot, with about 10 participants. The federation has since grown to 64 participants (including both Identity Providers and Sponsored Partners), as of September 2007. There are several potential participants in the pipeline, as well.

InCommon has 46 higher education participants and 17 sponsored partners. The National Institutes of Health has recently joined – the first government/research agency to do so. There is a lot of interest from such agencies in both providing and accessing resources.

Other new members include:

- The chancellor's office of California State University. The intention is for all 23 campuses to join InCommon.
- Several universities in Virginia, driven by a movement to share library resources.
- Students Only (www.studentsonly.com) – This new SP specializes in automated student enrollment verification.
- NAS Recruitment Communications – an SP specializing in human resources communication and recruiting.

## InCommon Challenges

InCommon is a young federation and still developing. The level of activity, and number of participants, continues to grow. The federation plans to do more case studies about the federation and demonstrate the benefits to participants, their IT departments and campus stakeholders. Other case studies and materials will demonstrate how participants are using and benefiting from federation participation.

## Working Groups/Interest Groups

https://spaces.internet2.edu/display/InCCollaborate/Home

InCommon will support groups of participants that wish to explore common interests and/or challenges. The federation will provide wiki space, an email list and access to the conference call bridge for any such group. These are grass-roots groups, which InCommon will continue to support. Any groups of participants with an interest in a vendor or type of vendor, or a set of campus constituencies, should communicate with John Krienke at Internet2.

*Library Services* – This working group includes technical librarians and IT staff focused on library services. The group is currently working at getting technical librarians to federate and use access control that is not IP-based. This allows faculty and staff to access resources from off-campus computers and provides a way to address walk-up users in the library. The group has recently focused on using a combination of SAML-based federating software and authenticated proxies.

*Student Services* – This group is currently focused on transactions involving registrar offices, such as enrollment verification and transcripts. There are standards in place for e-transcripts.

Bob Morgan and Ann West have participated at recent meetings of the American Association of Collegiate Registrars and Admissions Officers (AACRAO) meetings and are looking to engage with large organizations like the National Student Clearinghouse and student loan consortia. The group is also looking at federated access with service providers involved with admissions. Some of these scenarios are detailed on the InC-Students wiki space.

*Federal e-Authentication* – Talks continue with the U.S. government's e-Authentication effort. The e-Authentication effort is a proposed U.S. government federation, which has had talks with InCommon about inter-federating. The government continues to work on the policy issues associated with developing a federation. In the meantime, the National Institutes for Health (NIH) has joined InCommon as both an identity provider and as a service provider.

The NIH has been working with the University of Wisconsin and Johns Hopkins University to test passing attributes with NIH applications. InCommon has also been working with NIH to integrate the SiteMinder identity management system to access a group of NIH applications. NIH is also looking for volunteer identity providers to test with the National Institute of Allergy and Infectious Diseases (NIAID). Contact John Krienke if interested <jcwk -at- internet2.edu>

NIH has different levels of assurance (LoA), depending on the security needed for an application. The levels start at LoA 1 and progress to LoA 4 (most secure). Only LoA 1 applications are available through InCommon, but discussions have started to ramp up LoA 2 applications in conjunction with InCommon's Silver Level (equivalent to NIH LoA 2). InCommon and NIH hope to have this completed in 2008.

Looking forward, InCommon is planning similar discussions with the National Science Foundation and the U.S. Department of Education.

**Corporate Updates – Bob Morgan**

R.L. Bob Morgan, chair of the InCommon Technical Advisory Committee, provided an update on the federation's discussions with several large potential service providers. Agreements with any of these will likely result in a surge of interest in the federation and an increase in help requests from participants, particularly those without Shibboleth installed and in production. John Krienke said that InCommon recognizes that possibility and is exploring the stressors on federation adoption..

**New Attribute Information**

New attribute information pages have been posted to the website in the last month. The attribute information reinforces that InCommon participants must agree on the definitions of such attributes and their use in service access scenarios. The federation will continue to promote attributes that are considered particularly valuable and would like to promote a way in which service providers can publish their own attributes and have them consumed by IdPs. One suggestion is to developed profiles based on interest areas – if you are an SP in the library space, for example, the profile would outline what your peers have done in this area.

**Certificates and Metadata**

John Krienke reviewed InCommon's plan for a new way to handle certificates. The federation is testing placing the certificates inside of the metadata. The testing phase will include getting each administrator to make sure the latest certificate is being used. The administrator can go to

the site administration interface and make any corrections or adjustments. This method for handling certificates should make for a much cleaner way of handling any compromised certificate. The site administrator can make the change in the metadata. As part of this process, InCommon will recommend that all participants download the metadata nightly. The target is to have testing completed and the new process implemented by the end of 2007. https://service1.internet2.edu/siteadmin/manage/

**Levels of Assurance**

David Wasely, a member of the InCommon technical advisory committee, provided information about higher Levels of Assurance under development at InCommon.

Service providers rely on identity providers to follow best practices and comply with trust agreements made through the federation. Some services require more formal rules and a higher level of assurance from those seeking access.

InCommon is developing enhanced identity services, with additional requirements and assessment criteria for identity providers. Part of this is driven by the federal eAuthentication effort, which has developed four levels of assurance, from one (lowest) to four. The National Institutes of Health (NIH), an InCommon Participant, will require federal level 2 for some of its applications. InCommon is developing bronze and silver levels, which correspond to federal levels 1 and 2, respectively.

There are a number of areas considered for the identification assurance requirements, including:

1. Business, policy and operational factors
2. Identity proofing
3. Digital electronic credential technology
    a. How strong are your passwords
    b. PKI and secure IDs
4. Credential issuance and management
    a. How will a person obtain a credential?
    b. Renewal of credentials
    c. Validation of credentials
5. ID information management
    a. ID info will change over time
    b. Needs to be up to date
    c. Needs to be secure
6. Security and management of authentication events
    a. Example—password should never be sent in the clear
7. Identity assertion content
    a. Privacy issues
    b. FERPA – is this covered by FERPA and, if so, how does an IdP obtain permission to pass attributes about a person?
8. Technical environment
    a. security of equipment
    b. security of network
    c. backup and redundancy

Achieving higher levels of assurance will require an Identity Assurance Assessment of the IdP. This is essentially an independent audit, using criteria defined by InCommon. An institution's internal auditor may perform the assessment, if that office is sufficiently independent. External auditors may also be used and InCommon may develop an audit manual for their use. InCommon has no plans to do audits.

The process of achieving a higher level of assurance will involve:

1. The IdP notifying InCommon of the intent to achieve a higher LoA
2. The IdP having an Identity Assurance Assessment performed
3. The IdP providing InCommon with the audit results or a summary of the results
4. InCommon verifying the audit and providing an addendum to the participation agreement
5. InCommon adding the Bronze/Silver qualifiers to the IdP metadata
6. The IdP can optionally include additional qualifiers in assertions (such as differentiating students from faculty).

**Participant Services** – John Paul Robinson

John-Paul Robinson is a lead systems programmer at the University of Alabama-Birmingham. He is interested in providing applications from his university to other universities, which would require identity management. He would like to act as a service provider and not operate a separate identity management system.

His example is the UAB Grid, which faculty and students use for collaboration. UAB is also considering using wikis for collaboration. To facilitate this with students from other campuses, he would need a unique identifier from an identity provider to provide access to the resource. From the perspective of an ID provider, such as another campus, are there barriers to entry for such relationships?

The response was, in general, directory information can be released unless the student has asked for it to remain private, under FERPA. At some campuses, no student attributes can be released without the involvement of the registrar's office.

While attribute release policies involving students can get complicated, in light of privacy laws, they are not insurmountable. One Australian university, for example, has a system that allows students to manage the release of their own attributes via a web page. Part of the challenge is educating students on the need to release some attributes to enable collaboration with other institutions or entities.

**InCommon Outreach**

InCommon's outreach efforts focus on supporting working groups and other participant groups with like interests. Currently, for example, there is a group looking at federated library services and another involved with federated student services, such as those involving the registrar. InCommon will support any such interest group with wiki space, conference call capability and email lists.

Other outreach efforts include development of two InCommon value propositions: one aimed at campus CIOs and the other at CIO-level executives at service providers. Outlines of both are on the InCommon Collaboration wiki (https://spaces.internet2.edu/display/InCCollaborate/). Please comment on them and tell us what can make them better.

The InC-Collaborate wiki is a resource for participants for use in collaborative projects. It is also the home of toolkits – resources to use when working with campus stakeholders or with potential sponsored partners. The wiki also includes case studies demonstrating the benefits of federating. InCommon will continue to develop such case studies. Participants are encouraged to contact the federation if they have suggestions for such documents.

**Wikis and Privacy**

Ken Klingenstein provided comments about the exponential increase in the use of wikis. Federated wikis provide some interesting challenges, in terms of identity management. He was at a meeting in Prague last month that involved federations from around the world. Other federations are able to speak for their members and have requirements for the way members perform their access control and identity management. InCommon, at this point, is not able to place similar requirements on its members.

Privacy is driving some policies, including the potential that users may gain more control over release of their attributes. There may come a time when federations require pop-up windows that tell users they are about to release their identity to another federation. In such a scenario, will InCommon participants allow the federation to require them to support these pop-ups? This is one example of policies a federation may need to adopt and require of its members.