Help Your PIs: Put InCommon's Research-Enabling Tools in Your Campus CI Plan

By Tom Barton, Internet2 and the University of Chicago

This year, the National Science Foundation's proposal solicitation for its Campus Cyberinfrastructure (CC*) program has new InCommon-related requirements. These requirements help ensure that campus researchers can successfully use their campus credentials to access research related services available via global federation (InCommon and eduGain).

The solicitation says this about campus cyberinfrastructure plans:

> The plan should include the campus status and plans with respect to federated identity and specifically InCommon, including: if the campus is registered with InCommon as supporting the Research and Scholarship (R&S) Entity Category to streamline integration with research applications; and if the campus meets the InCommon Baseline Expectations for Trust in Federation.

Meeting the Research & Scholarship Entity Category Requirement

What and Why

Many federated research services require a few user attributes to successfully complete login, usually name, email, and a persistent user identifier (called the "R&S attribute bundle"). A common example is CILogon, which enables a user's campus credential to be used to access a variety of research infrastructures such as XSEDE.

A global program and standard for the R&E sector has been established to facilitate meeting this need to share these attributes. That's the Research & Scholarship Entity Category (R&S). That standard enables research services to request that their national R&E federation (as InCommon is for the US) "tag" them with the R&S entity category and specifies the vetting that R&E federation operators perform to ensure that such a tag is appropriate. It also provides a means by which a campus federated login system (called an Identity Provider or IdP in federation lingo) can automatically release the R&S attribute bundle to research services that have been tagged R&S, and a corresponding R&S tag to be given to an IdP to signal that it participates in this global program. This is important because some research services will only permit a login to proceed if the user's campus IdP is so tagged.

Here are links to the R&S Entity Category specification and an FAQ addressing both IdP operators and Service Provider (SP) operators.

How

Check to see if your IdP or SP is listed

as already meeting the "REFEDS R&S Entity Category specification" by being displayed as "research-and-scholarship" on a green background. Those shown a red background are a legacy from before there was global agreement on the R&S Entity Category. Their R&S attributes are limited to InCommon services only, hindering user access to international research services.

A wiki page describes how to enable an IdP to automatically provide the R&S attribute bundle to R&S tagged services. Once you have done so, email admin@incommon.org to request that your IdP be tagged as REFEDS R&S.

If a research service operated within the campus needs to support federated access for users elsewhere, fill out this application to be given the R&S tag.

Meeting the Baseline Expectations Requirement

What and Why

When service providers rely on federation, they are relying on those who operate IdPs to do a reasonable job of ensuring that their logins are trustworthy. In other words, that an account is used only by the user to whom it is assigned, and that the user is currently authorized to use it. Similarly, when IdPs send user attributes to an SP, the IdP operators rely on the service provider to use those attributes only for the stated purpose and to reasonably prevent unauthorized disclosure. Federation users rely on IdP and SP operators to operate their services in a manner that makes it as easy as possible for them to access the services they need.

The Baseline Expectations for Trust In Federation is a small set of high level statements that describe how InCommon participants expect InCommon IdPs and SPs to be operated to embody reasonable trust and usability, and how InCommon Federation operators should support this objective. The statements themselves as well as an extensive implementation program are detailed on the Baseline Expectations for Trust in Federation wiki page.

How

Step 1: Metadata review & update

There are several clearly defined requirements of an IdP's or SP's federation metadata that should be reviewed to ensure they meet Baseline Expectations. One or more campus IT people are InCommon Site Administrators, which authorizes them to manage campus IdP and SP metadata using InCommon's Federation Manager. They should login, review entity metadata, and make any changes that may be needed. The most common updates that are needed or strongly recommended are supplying an institutional logo (for both IdPs and SPs) and an error URL (for IdPs). These are key enablers of good user experience. Other common needs are to provide security contact information and a privacy policy URL.

Step 2: Operational practice review

Good institutional judgment is used to address some of the other Baseline Expectations. Some guidance is provided here, but please note that further interpretation may occur as consensus of the InCommon participant community about these statements develops. If you are unsure whether your operations currently or will reasonably soon meet these expectations, please raise your question on the InCommon Participants mailing list.

For IdPs, the following Baseline Expectations express what constitutes a reasonable job of ensuring that IdP logins are trustworthy.

1. The IdP is operated with organizational-level authority
2. The IdP is trusted enough to be used to access the organization's own systems
3. Generally-accepted security practices are applied to the IdP

The first statement holds when responsibility for operating the institution's IdP is assigned appropriately, usually to the central IT organization. The second statement asserts that the quality of the IdP operation is equivalent to the quality of any other authentication service that is used to login to important systems, such as HR, course management, or grants administration systems. And the third one recognizes that user accounts are points of potential compromise, so reasonable security protections and security incident response measures should apply to IdP operations in a manner equivalent to how other authentication services are protected by the organization.

For SPs, the following Baseline Expectations express what constitutes a reasonable job of ensuring that attributes are used only for the stated purpose and are protected from unauthorized disclosure.

1. Controls are in place to reasonably secure information and maintain user privacy
2. Information received from IdPs is not shared with third parties without permission and is stored only when necessary for SP's purpose
3. Generally-accepted security practices are applied to the SP

As with the IdP statements, these express the expectation that an SP system that collects user data will protect it in alignment with how your organization determines protections for other systems that store or process personal information.

Note that there are at present no external standards covering statements 1-3 (for IdPs or for SPs) that all InCommon participants are required to meet. Basically, these statements amount to an "eat your own dogfood" expectation. If you don't, why should others trust you?