How to Get Started in the InCommon Federation

Introduction

Thank you for your interest in the InCommon Federation. The process of joining will likely raise issues for various areas of your institution, potentially affecting technology, policy, and operations. However, none of these are particularly onerous; your institution has probably addressed most, if not all, of them already. Here's a 10,000 foot view of the process.

1. Review Your Identity-Related Policies and Practices. While it is likely that you already an Identity and Access Management (IAM) program, now is a good time to review it in light of your current requirements and those of the federation.
2. Join InCommon. Ensure that your institution is prepared to commit to InCommon's multilateral trust framework and sign the InCommon Participation Agreement. As mentioned above, this will likely involve coordination among technology, policy, and operations personnel, not only the person with the institutional authority to actually do the signing.
3. Designate Organizational Contacts. Designate the people who are authorized to act on behalf of your institution and each of its Identity Providers (IdPs) and Service Providers (SPs) in technical, security, management, and administrative roles.
4. Deploy Software. If you haven't already done so, deploy the IdP and/or SP software that you will be using in the federation.
5. Register Federation Metadata. Enable your IdPs and SPs to interoperate with the rest of the federation by registering them in the federation metadata.

The remainder of this document provides additional detail for each of these steps, including advice that should help you avoid operational problems and end-user difficulties in the future. You should also review Things to Do After Getting Started in InCommon for follow-on activities that can enhance your participation in InCommon.

The Details

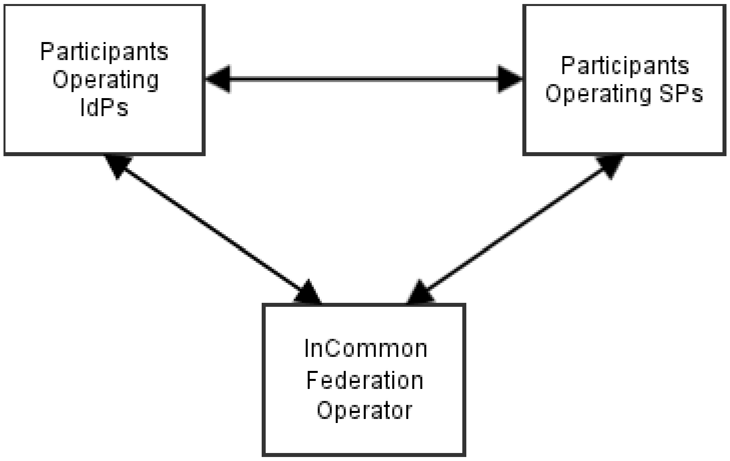
Background

The InCommon Federation

"*The InCommon Federation is the U.S. education and research identity federation, providing a common framework for trusted shared management of access to online resources.*" - InCommon Federation

InCommon's "common framework" creates multilateral trust among all federation Participants, facilitated by the Federation Operator, to exchange identity information in a secure manner. Service Providers trust Identity Providers to provide accurate information, and Identity Providers trust Service Providers not to misuse the information they receive. Community Members trust both Identity Providers and Service Providers to respect their privacy, making use of their identity information only as needed, according to legal and institutional policy. Trusted Relationships for Access Management: The InCommon Model provides a comprehensive introduction to this framework, including definitions of many of the terms used in this document.

InCommon's Participants (member institutions) operate Identity Providers (IdPs - network-accessible services that authenticate users and provide identity information, according to local policy, about Service Providers' current users) and Service Providers (SPs - network-accessible services that rely on information from IdPs for the purpose of making access decisions and/or personalizing the user's experience). In order to facilitate this exchange, the Federation provides about all IdPs and SPs, and the Participants that operate them, to all Participants. This creates a three-way flow of trust and information:


Participants Operating IdPs
Participants Operating SPs
InCommon Federation Operator

Review Your Identity-Related Policies and Practices

When you sign the InCommon Participation Agreement, you will be agreeing to comply with various requirements related to InCommon's multilateral trust framework, including:

- Deployment of conformant software
- Use of common syntax and semantics for Identity Assertions
- Provision of accurate information for the Trust Registry
- Provision of accurate contact information
- Respect for intellectual property rights
- Respect for privacy of identity information
- Adherence to Baseline Expectations for the mature, secure, and privacy-protecting operation of your institution's IdPs and SPs, and that those IdPs and SPs are duly registered with InCommon.

Now is a good time for a quick review your policies, practices, and software in light of your current requirements and those of the federation. This review will likely involve various areas of your institution, potentially affecting technology, policy, and operations.

If you will be registering an IdP in InCommon, you will particularly want to review your Identity and Access Management (IAM) program, the business processes and technology platforms that your institution uses to manage the life-cycle of identity information your institution maintains about members of its community to control access to online services. If your institution is like many others, that IAM program is the result of many years of often-informal evolution, so this is a good opportunity for some clean up. See the "Your Identity Management System" section of InCommon Basics and Resources for more information.

Join InCommon

By signing the InCommon Participation Agreement, your institution agrees to participate in the framework by complying with multiple aspects of InCommon's multilateral trust, as outlined above.

Baseline Expectations also establishes requirements for the Federation Operator, among them being that "Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions." The first of these practices is to validate that your institution is what it claims to be. Upon receipt of a signed InCommon Participation Agreement, the Federation Operator will reference publicly-available information sources, such as those listed in Accrediting Agencies Recognized by InCommon, to verify this.

See the Join InCommon web page for more information.

Designate Organizational Contacts

The Federation Operator's next task is to the establish identities of the people who will have the authority to perform various functions on behalf of your institution. These are:

- **Executive Contact**. This is the person who is authorized to speak on behalf of your institution for issues relating to its contractural agreement with InCommon. This is typically the CIO or similar institution-level officer who signed the InCommon Participation Agreement, but that may vary, depending on your institution's organizational structure.
- **Site Administrator**. Designated by the Executive Contact, this is the person who approves metadata submissions for all of your institution's IdPs and SPs. This person is also InCommon's primary contact for operational, technical, and security issues relating to your institution's IdPs and SPs and its participation in InCommon overall. For business continuity reasons, institutions are strongly encouraged to designate two Site Administrators.
- **Delegated Administrator**. Designated by the Site Administrator, this is a person who has responsibility for one or more of the institution's SPs. This person perpares metadata submissions for their SPs, subject to approval by the Site Administrator. Any number of Delegated Administrators may be designated.
- **Billing Contact**. This is the person who will receive billing invoices from InCommon.

After validating the identity of your institution, the Federation Operator will arrange a telephone call with your Executive Contact to issue their login credentials for InCommon's site administration tools, and to establish the identities and phone numbers of the institution's Site Administrators. The Federation Operator then arranges phone calls with each of the Site Administrators to issue their credentials for InCommon's site administration tools.

Deploy Software

It is strongly recommended that you utilize software produced by Internet2's Trust and Identity in Education and Research (TIER) program in your service offerings. This standards-based software has been configured for optimal use in InCommon and has been used successfully by many of its participants.

The following resources provide additional detail that may be helpful to you, particularly if you do not adopt TIER software components:

- InCommon's Federation Technical Guide
- Identity Provider Strategies for Common Campus Environments
- SAML V2.0 Implementation Profile for Federation Interoperability
- Upcoming resources from the Deployment Profile Working Group

Register Federation Metadata

Federation metadata is the trusted registry of IdPs and SPs operated by participants for use within the federation. It not only provides technical information to enable interoperation, links to support contacts and documents, *etc*., it also includes information to enhance mutual trust, such as responsible parties and certifications achieved.

Getting your metadata right will make your life much easier. Time spent now will pay you back over the lifetime of your IdPs and SPs; don't skimp on this task. See Metadata Administration for all the details.