InCommon Basics and Participating in InCommon

A Summary of Resources

Updated July 17, 2018

Table of Contents

InCommon Basics

Federated Identity Management Quick Start Checklist

Introduction

This document contains checklists, policy documents, an FAQ, and other information to help you get up and running with InCommon. We begin with a quick start checklist outlining the key areas to address as you adopt federated identity management and join InCommon.

Identify Your Business Case

What is the primary motivator for your adoption of federated identity management? When you start to traverse the policy and technical implementation steps, it helps to have a specific purpose and stakeholder group in mind.

Review Your Practices

A prerequisite to federated identity management is sound campus identity management policies and practices. This resources guide will help with that. You will also find information about the Baseline Practices for Trust in Federation, which includes requirements for all InCommon participants (see https://www.incommon.org/federation/baseline).

Install/Configure a SAML 2-Compliant Federating Software

SAML (Security Assertion Markup Language) is the language of InCommon and SAML2 is the latest version. You will need SAML 2-compliant software (such as the latest versions of the Shibboleth Identity Provider (v3.x) and Service Provider (v3.x) to interact with other federation participants. You will need to install and configure the identity or service provider portion of your SAML2-compliant software depending on what you plan to do. For testing purposes, and a greater understanding of how the identity and service providers work together, you may want to install both.
http://shibboleth.net

Support the eduPerson Schema

The eduPerson schema defines the attributes exchanged by federating partners when authenticating and authorizing access to protected resources. https://www.internet2.edu/products-services/trust-identity/eduperson-eduorg/

Join InCommon

You've covered the basics outlined above. Now it's time to join InCommon and start to enjoy the privacy and security benefits of federating and to provide single sign-on convenience for your students, faculty and staff. https://www.incommon.org/join.html

Federated Identity Management Checklist

This document lists the *minimum (marked with an *)* and *recommended* policy, process, and technical steps required to implement Federated Identity Management and operate within the InCommon Federation. You may use the checklist to assess your organization's readiness for implementation and to serve as a checklist for those tasks that remain to be completed.

Most sections of the checklist have three parts: policy steps, business practice steps, and technical steps. Each batch of steps is sequential.

This document was developed by:
Steven Carmody, Brown University
Jacob Farmer, Indiana University
Eric Jansson, NITLE
Bob Johnson, Rhodes College
John O'Keefe, Lafayette College
Ann West, InCommon/Internet2
Dean Woodbeck, InCOmmon/Internet2

Identity Provider: Identity Management Preparation

Policy Steps

* **Review the InCommon Baseline Expectations for Trust in Federation**
The InCommon community adopted Baseline Expectations for Trust in Federation to improve interoperability. Baseline expectations are in place for Identity Providers, Service Providers, and the Federation Operator. They include policy items, as well as requirements for including certain information in the metadata. Details and links are available at https://www.incommon.org/federation/baseline.

Ensure basic identity management policies are in place, including data stewardship and acceptable use policies
Outside service providers to whom you provide identity information may have questions about your institution's acceptable user and data stewardship policies and how these compare with their requirements. If you plan to provide federated services to the InCommon community, these questions are especially important as they will let others from outside your network understand policies that relate to their use of your organization's resources.

*** Define policies related to single sign-on (SSO) and authentication**
SSO is a method that allows a user to perform authentication once and then use it for access to a variety of resources and applications for some period of time. This reduces the number of identifiers and passwords a user must remember and reduces the number of times he or she needs to log into and out of systems. This convenience requires some security tradeoffs. Your policies in these areas are of interest to your service providers in the federation, but they also help to inform your users of identity risks and best practices. To address these policies, your organization will need to answer questions such as "How long is a sign-on valid (one hour? until a web browser is closed?)"?

*** Define and publish account creation and termination policies**
"What defines a *user* for your organization?" is a question of key interest to service providers. Organizations to which your institution provides identity are likely to want to know the steps your institution uses to establish and create user identity (e.g. What identification does your organization require? How are accounts removed? When a student graduates or leaves, is the student's account removed immediately? In one month?). Service providers may ask for information about account creation, termination or provision in order to ensure your organization's compliance with licensing, published or federation policies, etc. It is a best practice to be explicit about what verification your institution is able to do.

Define policies on log retention for identity management and provision
In relation to the previous policy areas, especially account creation and termination and identity management, service providers may request information related to your logs. Your organization may need to develop policies related to the retention of logs and their use. Practitioners in the IdM space need to be particularly aware of the privacy implications of their log management policies.

*** Join InCommon**
See http://www.incommon.org/join.html for more information.

Business Practice Steps

*** Provision/de-provision accounts for your users (faculty, staff, and students) based on published policies**
Before you provide identity to outside providers, your organization needs to ensure compliance with its published policies. For example, have accounts been terminated which are supposed to have been terminated? Since federated identity is heavily reliant on shared policy statements, it is crucial to ensure that your organization is acting in the expected manner.

Create a problem resolution process for forgotten or lost passwords
As with the authentication problems, your organization likely has such processes, and these should be checked against any policies set above. Pay special attention to users who may need password reset performed when they are in a remote location.

Create Help Desk support procedures for authentication problems and password changes
Your organization probably already has such procedures, but it is best to check these again against the policies in the above steps. Again, special attention is needed for the remote user scenario.

*** Create a process to address reports of abuse**
Incident response becomes somewhat more challenging in the federated scenario, because two organizations have to cooperate to collect the necessary forensic information. It is important that these procedures be in place before an incident occurs. You can see the recommended practices around federated security incident response on the wiki: https://spaces.internet2.edu/x/8o6KAQ

Technical Steps

*** Install/operate/manage the identity provider package of a SAML federating software system such as Shibboleth**
If you intend to use Shibboleth, the see https://wiki.shibboleth.net for detailed installation, configuration and operation instructions.

Identity Provider: Identity Attribute Provisioning

Policy Steps

Many organization/data stakeholders will need to understand federating and its impact on the institution, the service portfolio, related issues, and risks. Governance is typically required for ensuring proper data use, and federated access is no exception. For example, if a new service provider asks for certain information on service consumers, how can those who want to take advantage of this service determine if this release of information is within organization policies?

*** Identify who governs the decision to release attributes**
Organizations need to have a way to decide which attributes (is this person a student? In what year of studies is this student?) are released to service providers and for what purposes. This function often oversees compliance issues for government and other policies.

Develop policy governing use of your attributes by service providers such as attribute retention, sharing, etc.
Organizations should proactively develop and publish policies for service providers on what they will do with identity attribute information once provided. In addition, many schools have developed standard contract language for this to ensure policy adherence.

Consider setting up tiers or groups of attribute release policies for different categories of service providers
Identifying groups of service providers (library content providers, for instance) and related attribute release constraints can help streamline the governance process for approval. Also consider taking advantage of InCommon categories of service providers, allowing release of a group of attributes to an entire category (see the wiki for more information, https://spaces.internet2.edu/x/fgVOAg)

Business Practice Steps

*** Identify who is responsible for editing/implementing the attribute release policies**
This process should reflect the policies above, and in particular specify how they are carried out. Institutional policies on separation of concerns and audit should be considered when this determination is made.

Define the process a service provider would use to request attributes and the process used to respond to the request
This will happen with new providers and can also happen with new services from existing providers. Who should the provider contact? Who reviews these requests? This process generally implements the policies above.

Define the process to follow when a service provider requests an attribute that is not currently available as defined by the policy above
This process should implement the policies in the 'Policy Steps' section above.

*** Define problem escalation procedure if identity information is released in conflict with organization policies**
For example, if the wrong attributes are sent to a service provider, when does your organization notify users? Does your institution make a request to the service provider of some kind?

Technical Steps

* **Extend directory and/or person registry schemas if needed to support eduPerson**
A federation requires a common data schema to facilitate the passing of identity-related information (attributes) from identity to service providers for access. InCommon requires the support of the eduPerson data schema (see http://middleware.internet2.edu/eduperson/).

You can choose to support these attributes by storing them in your directory or database. If you use Shibboleth, the software can be configured to look up a local attribute in your directory and send it as an eduPerson attribute. Each attribute in eduPerson does not have to be populated. The ones that are most commonly used at this point are `eduPersonScopedAffiliation`, `eduPersonAffiliation`, and `eduPersonPrincipalName`.

While these are the most common solutions, there are a number of ways to meet this requirement. Ultimately, it matters that you are able to pass data in the appropriately named attributes.

*** Configure the identity provider attribute resolver for the appropriate sources**
Ensure that your organization's identity provider software is providing attributes according to the policies defined above and as needed by the service providers. The attribute resolver in Shibboleth, for example, gets the attributes from your data source (such as a directory or database), and performs operations that you specify to ensure that the attribute conforms to your policies and the federation technical and data schema specifications.

*** Configure the identity provider to release the right attribute(s) to your service providers**
Newly defined attributes are not released to service providers until you define an attribute filter policy for them. Such policies describe which service providers, under which conditions, receive which attributes. See the Shibboleth wiki on this topic at
https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAddAttributeFilter

Service Provider Preparation

Policy Steps

*** Determine which services you would like to offer to the InCommon community. Who will be accessing your service for what purpose?**
Determine audience and risk for each offered service and related requirements. How will you decide whether they are eligible or not to use the service? What kind of assurance of the user's identity will you require from the accessing organizations?

Develop policy governing the use of attributes received by SPs such as attribute retention, sharing, etc.
Will you keep the identity attribute information that identity providers send to you and if so, for how long?

Ensure your policies are comply with the federation requirements
Check the InCommon site to ensure your policies comply with the current federation requirements. In particular, make sure that you understand and meet the Baseline Expectations for Trust in Federation (www.incommon.org/federation/baseline).

Business Practice Steps

Identify who is responsible for managing the federated access to your service(s)

*** Identify which attributes you will require from partnering identity providers for access to your service. Determine which services are eligible to receive which attributes.**
It's best to go with common practice as much as possible. You can review InCommon's attribute overview at http://www.incommon.org/federation/attributes.html

*** Ensure you have a defined problem resolution process for remote users**
If a user has a problem accessing your service, where will they get help? Including contact information in your metadata, as required by Baseline Expecations, is a first step.

*** Define problem escalation and support procedures for IdP users of your service(s)**
If you have a break in service, how will you let your partners know? If you find one or more users abusing your service, how will you contact their home organization?

*** Define the process IdPs would use to request services and the process used to respond to the request**

Technical Steps

*** Install/operate/manage SAML Service Provider federating software such as Shibboleth**

*** Connect services to be federated to the federating software and enable them to use the incoming attributes to control access**
If the application that you are federating doesn't support the federating software, you will have to do some programming work to enable it to use the sent attributes. A growing number of applications, though, support Shibboleth so check shibboleth.net or send a note to the Shibboleth Users list to find out about integrated versions.

*** Add service provider information to the federation metadata**

*** Configure service provider software to use federation metadata and credentials and refresh when required**

Document how your SP could authorize users given the provided attributes

Document how your application could use the supplied attributes in alternative ways, such as for customization or form completion

InCommon FAQ

About InCommon

The mission of the InCommon Federation is to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States. To achieve its mission, InCommon will facilitate development of a community-based common trust fabric sufficient to enable participants to make appropriate decisions about the release of identity information and the control of access to protected online resources. InCommon is intended to enable production-level end-user access to a wide variety of protected resources.

What is InCommon?

InCommon is a formal federation of organizations focused on creating a common framework for collaborative trust in support of research and education. InCommon makes sharing protected online resources easier, safer, and more scalable in our age of digital resources and services. Leveraging SAML-based authentication and authorization systems, InCommon enables cost-effective, privacy-preserving collaboration among InCommon participants. InCommon eliminates the need for researchers, students, and educators to maintain multiple, password-protected accounts. The InCommon federation supports user access to protected resources by allowing organizations to make access decisions to resources based on a user's status and privileges as presented by the user's home organization.

What are the benefits of joining InCommon?

InCommon supports web-based distributed authentication and authorization services, an example of which is controlled access to protected library resources. Participation in InCommon means that trust decisions regarding access to resources can be managed by exchanging information in a standardized format. Using a standard mechanism for exchanging information provides economies of scale by reducing or removing the need to repeat integration work for each new resource.

Since access is driven by policies set by the resource being accessed, higher security and more granular control to resources can be supported. Reduced account management overhead is another benefit, since users can be authenticated and access resources from the home institution and no longer need separate accounts to access particular resources. InCommon is operated by Internet2 to provide consistency and participant support.

InCommon and User Identity

InCommon also preserves privacy since the home institution controls when identity is disclosed. Information can be exchanged about authorized user access, without having to disclose the identity of the user unless both sides agree it's needed.

What is a federation?

A federation is an association of organizations that use a common set of attributes, practices and policies to exchange information about their users and resources in order to enable collaborations and transactions.

Who can currently join InCommon?

There are two primary categories of federation participation in InCommon: Higher Education Institutions and their Sponsored Partners. To learn more about the eligibility criteria and the processes for joining, visit our join page (http://www.incommon.org/join.html).

What is required to join InCommon?

Organizations applying to join InCommon must agree at an executive level of their organization to the terms and conditions of federation participation (legal framework and federation policies), which

include documenting an organization's practices and procedures used to grant and manage user accounts. Contacts for the organization must be official representatives and will be verified as such. There are also technical requirements to support InCommon's federated authentication model. For more details on the Shibboleth software, please see the question on Shibboleth below.

Being accepted into InCommon is a two-step process. The first step is to complete the InCommon agreement, identifying the person who will act as the Executive Liaison to InCommon. After the participation agreement has been signed by both parties, a registration process will verify the designated Executive and Administrators for the organization, after which the organization will be able to register its systems in the federation. For more information on this process, see the join page (www.incommon.org/join.html).

How do I prepare for InCommon?

Organizations that are eligible to join InCommon may consider testing with Shibboleth to gain familiarity with federation technology, concepts, and requirements. As described on the join page, the first step in participation is to review and submit a signed participation agreement. The NMI-EDIT Consortium has some excellent resources available on planning, which among other resources includes two excellent roadmaps: The Enterprise Directory Implementation Roadmap and The Enterprise Authentication Implementation Roadmap (www.nmi-edit.org).

What is Shibboleth?

Shibboleth software enables the sharing of Web resources that are subject to access controls such as user IDs and passwords. Shibboleth leverages institutional sign-on and directory systems to work among organizations by locally authenticating users and then passing information about them to the resource site to enable that site to make an informed authorization decision. The Shibboleth architecture protects privacy by letting institutions and individuals set policies to control what type of user information can be released to each destination. For more information on Shibboleth please visit https://shibboleth.net

Joining InCommon

1. Are You Eligible?

Participation in InCommon is open to:

Higher Education – Two- and four-year, degree-granting academic institutions that are accredited by a U.S. Department of Education Regional Institutional Accrediting Agency, or a national or state accrediting agency. See www.incommon.org/accrediting.html for a list of agencies.

Sponsored Partners – Business, education, and research organizations who partner with higher education may join the federation as Sponsored Partners. Sponsored Partners must be sponsored by the designated Executive of a current InCommon Higher Education Institution or Research Organization. Information on sponsoring is at www.incommon.org/sponsor.html.

2. Review the Fee Schedule (www.incommon.org/fees.html)

3. Send Us the Agreement (and Sponsor Letter)

If you are eligible, send us a signed copy of the InCommon Participation Agreement by postal mail, email or fax. This agreement also designates your trusted Executive (we will identity-proof this person for security), and is signed by an authorized representative of your organization.

If you are applying as a Sponsored Participant, InCommon must receive a sponsorship letter from a current InCommon higher education institution.

4. InCommon Countersigns the Agreement and Sends a Registration Link

5. Payment of Annual Fee

InCommon emails an invoice for the first year's annual fee (which is prorated depending on the quarter in which you join). This fee is based on Carnegie classifications for higher ed and annual revenue for companies. See the fee schedule for details (http://www.incommon.org/fees.html).

6. Register for Your Executive and Administrator for Identity Verification

After your Agreement has been executed and you are in our system:

1. Pay the one-time registration fee ($700)
2. Designate individuals to fill InCommon-related roles and submit their names during registration.
    - Administrator (we will identity-proof this person for security)
    - Billing Contact (recorded but not identity-proofed)
    - Executive: You will have already appointed your Executive in the agreement.
3. Review InCommon policies and practices.

7. Identity Proofing via Telephone

Our Registration Authority will identity-proof your Executive and Administrator via telephone appointment.

8. Manage your system via the site administration interface

Following identity proofing, your InCommon Administrator can gain access to the site administration interface for registering and managing your systems for interoperability.

9. Planning and Implementing Identity and Access Management

The NMI-EDIT Consortium provides excellent resources available on planning which, among other resources, includes two detailed roadmaps: The Enterprise Directory Implementation Roadmap (http://www.nmi-edit.org/roadmap/dir-roadmap_200510/index-set.html) and the Enterprise Authentication Implementation Roadmap (http://www.nmi-edit.org/roadmap/draft-authn-roadmap-03/).

The Shibboleth system is addressed on the Shibboleth website (https://shibboleth.net) and detailed on the Shibboleth documentation wiki (https://wiki.shibboleth.net).

For library resources, the InC-Library Collaboration has published a set of best practices on their wiki (https://spaces.internet2.edu/display/inclibrary/Best+Practices).

Getting Help

InCommon Education and Outreach

InCommon offers a number of education and training programs to help participants get started in the federation, to better make use of their federated identity management system, and to install and configure Shibboleth Federated Single Sign-on Software. The best way to stay up-to-date on these opportunities is to subscribe to the email list participants@incommon.org (send email to sympa@incommon.org with the subject: subscribe participants.

Community Support: Email Lists

InCommon operates a number of email lists, both for general information and help, as well as lists for specific topics and collaboration groups. A list of available email lists is at https://lists.incommon.org/sympa/lists. To subscribe to a list, send email to sympa@incommon.org with this message in the subject line: subscribe ListName FirstName LastName (e.g. subscribe inc-cert Joe Doaks).

Announce: An announcement-only email list with news and informational items about InCommon, as well as the means to distribute a monthly email newsletter.

Participants: A list to discuss collaboration and implementation issues related to InCommon.

InC-Ops-Notifications: This email list is used by InCommon Operations to send important notifications about modifications to the metadata generation system, service interruptions, and any other important technical announcements as they occur. All official InCommon Site Administrators are automatically subscribed to this list as a requirement to participation in InCommon services.

There are other lists related to the InCommon collaboration groups, including InC-Student, InC-Library, the U.S. Federations group, and others. For information, see https://lists.incommon.org/sympa/lists

Shibboleth Email Lists provide forums for discussing development and user topics, as well as learning about the latest news. See the Shibboleth website (https://shibboleth.net/community/lists.html) for information on subscribing to the Shib announcements, user, and development lists.

Additional Resources

Links to many of the documents below can be found on the InCommon website at www.incommon.org and the Shibboleth website at https://shibboleth.net. For information on development activities, refer to www.internet2.edu/middleware. For more information on identity management, refer to www.nmi-edit.org.

Getting Started with InCommon

The InCommon website (www.incommon.org) is your primary resource for background, as well as policy documents, education and outreach activities, collaboration groups and technical information.

Policies and Practices: The policies and practices page (www.incommon.org/policies.html) includes the InCommon participation agreement, fee schedule, Federation operating policies, information about attributes, and information about InCommon governance.

Getting Started with Shibboleth

The Shibboleth website (https://shibboleth.net) is the primary source for software, documentation, and deployment information.

Getting Started with Identity Management

- **Enterprise Directory Implementation Roadmap** describes a process campuses can use to work through the technology, business practice, and policy issues associated with deploying an enterprise directory and initial identity management services. http://www.nmi-edit.org/roadmap/directories.html
- **Enterprise Authentication Implementation Roadmap (Draft)** offers a project framework and related resources for deploying authentication services, including technical, management, and policy concepts. http://www.nmi-edit.org/roadmap/authentication.html
- **EDUCAUSE Identity Management Working Group** offers ongoing discussion and networking with peers via email along with related resources. http://www.educause.edu/cg/idm

Participating in InCommon

InCommon Policies and Practices

The documents listed below comprise the polices and practices under which the InCommon Federation and Participants operate. These documents should be reviewed prior to submitting an application. For eligibility questions, please refer to the join InCommon page (http://www.incommon.org/join.html). Documents are listed in the recommended order of reading. Policies and practices for InCommon are overseen by the InCommon Steering Committee.

Participation Agreement:
www.incommon.org/docs/policies/participationagreement.pdf

Fee Schedule (also in the participation agreement):
www.incommon.org/fees.html

Federation Operating Policies and Practices
www.incommon.org/docs/policies/incommonfopp.html
The FOPP describes the activities and systems of the InCommon Federation. A paper on further risk assessment is also available at http://www.incommon.org/docs/policies/risk_assessment.html.

Changing Your Site Administrator or InCommon Executive
www.incommon.org/roles.html
When you change your executive contact for InCommon, we need information in writing (this can be emailed). There is a template for a letter (which must be on your institution's letterhead) on the roles page, as well.

InCommon Attributes
InCommon supports eduPerson Schema attributes. www.incommon.org/federation/attributes.html.

Glossary

access management system	The collection of systems and or services associated with specific on-line resources and/or services that together derive the decision about whether to allow a given individual to gain access to those resources or make use of those services.
assertion	The *identity* information provided by an *Identity Provider* to a *Service Provider*.
attribute	A single piece of information associated with an *electronic identity database* record. Some *attributes* are general; others are personal. Some subset of all *attributes* defines a unique individual.
authentication	The process by which a person verifies or confirms their association with an *electronic identifier*. For example, entering a password that is associated with an UserID or account name is assumed to verify that the user is the person to whom the UserID was issued.
authorization	The process of determining whether a specific person should be allowed to gain access to an application or function, or to make use of a resource. The resource manager then makes the access control decision, which also may take into account other factors such as time of day, location of the user, and/or load on the resource system.
electronic identifier	A string of characters or structured data that may be used to reference an *electronic identity*. Examples include an email address, a user account name, a Kerberos principal name, a UC or campus *NetID*, an employee or student ID, or a PKI certificate.
electronic identity	A set of information that is maintained about an individual, typically in campus *electronic identity databases*. May include roles and privileges as well as personal information. The information must be authoritative to the applications for which it will be used.
electronic identity credential	An *electronic identifier* and corresponding *personal secret* associated with an *electronic identity*. An *electronic identity credential* typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access.
electronic identity database	A structured collection of information pertaining to a given individual. Sometimes referred to as an "enterprise directory." Typically includes name, address, email address, affiliation, and *electronic identifier(s)*. Many technologies can be used to create an *identity database,* for example LDAP or a set of linked relational databases.

identity	*Identity* is the set of information associated with a specific physical person or other entity. Typically an Identity Provider will be authoritative for only a subset of a person's *identity* information. What *identity attributes* might be relevant in any situation depend on the context in which it is being questioned.
identity management system	A set of standards, procedures and technologies that provide electronic credentials to individuals and maintain authoritative information about the holders of those credentials.
Identity Provider	A campus or other organization that manages and operates an *identity management system* and offers information about members of its community to other InCommon participants.
NetID	An *electronic identifier* created specifically for use with on-line applications. It is often an integer and typically has no other meaning.
personal secret (also verification token)	Used in the context of this document, is synonymous with password, pass phrase or PIN. It enables the holder of an *electronic identifier* to confirm that s/he is the person to whom the identifier was issued.
Service Provider	A campus or other organization that makes on-line resources available to users based in part on information about them that it receives from other InCommon participants.

Technical Requirements and Information

Supported Software

Organizations participating in InCommon must install and operate software systems that can interoperate with other participants. See the software guidelines for information on recommended software: www.incommon.org/federation/softguide.html

InCommon Deployment

The bulk of the work of configuring a Shibboleth IdP or SP is not specific to the federation(s) you are participating in, but there are various steps involved in making your deployment "InCommon-aware" once it's up and running. To get started, visit the Technical Guide on the InCommon Collaboration wiki:
https://spaces.internet2.edu/display/InCFederation/Federation+Technical+Guide

Shibboleth installation guides and general support: https://wiki.shibboleth.net

Shibboleth Deployment Guide for The Ohio State University:
https://webauth.service.ohio-state.edu/%7Eshibboleth/.

Testing the Identity Provider

The best way to test the installation of your IdP is to also install the SP and run it yourself, using it to verify your system. If you want to run an IdP, you need to be able to control the SP and view the logs for troubleshooting purposes. Testing with Remote SPs is never a viable substitute.

You can even register such SPs in InCommon, if you like, and essentially use the exact same approaches as you will with outside SPs. Once installed, you can test your Identity Provider configuration by visiting the InCommon Test Service web page (https://service1.internet2.edu/test/), which runs the Shibboleth 2.x SP. If you want to test with an external site, you can go to the Internet2 spaces wiki (http://spaces.internet2.edu), find your IdP on the WAYF and log in.

Your EntityID

Getting ready to start the federating process? The technical guide on the InCommon Federation wiki provides important information about things to consider concerning your EntityID:
https://spaces.internet2.edu/display/InCFederation/Entity+IDs

Registering Your Systems in Federation: Metadata

It's fairly simple to activate a resource (SP) or identity management system (IdP) in the federation. All Participants' Administrators (as designated by your Executive) have access to the site admin management interface: https://service1.internet2.edu/siteadmin/manage.

Self-Signed Certificates: InCommon accepts self-signed certifications. For more information, see the wiki page on X.509 certificates:
https://spaces.internet2.edu/display/InCCollaborate/X.509+Certificates+in+Metadata.

Data for SPs: Entity ID, Assertion Consumer Service Endpoints: Type (post/artifact) and URL; KeyName; and Contacts (support, technical, administrative).

Data for IdPs: Error URL; URL and KeyName for Single Sign On Service; URL and KeyName for Attribute Service; and Contacts (support, technical, administrative)
For detailed information on InCommon metadata and the InCommon WAYF ("Where Are You From?") service, please see the Metadata page at www.incommon.org/federation/metadata.html

Identity Attributes
For information regarding the attributes InCommon recommends, please visit the Attributes page: www.incommon.org/federation/attributes.html.

Sponsoring Partners into InCommon

If you are a partner of a higher-education institution, you must have a current InCommon higher education participant sponsor your participation. The sponsoring institution's designated InCommon Executive must send to InCommon, via email or postal mail, a sponsorship letter as suggested below, including the Sponsored Partner's homepage URL and the name of their Executive-level contact. We use this information to cross-reference the Partner's application and to begin the identification and authentication steps necessary to validate the organization and its trusted officers. If you need assistance finding a sponsor, contact us.

Template for Minimal Sponsorship Letter
To: incommon-admin@incommon.org
[InCommon, c/o Internet2, 1000 Oakbrook Dr, Suite 300, Ann Arbor, MI 48104]

Dear InCommon,

[Sponsored Partner] is currently involved in providing resources to the higher education, research and education community. I believe this service provider will be an InCommon Federation participant in good standing and submit their name and URL below.

PARTNER EXECUTIVE CONTACT NAME
HTTP://SPONSORED_PARTNER'S_URL

Sincerely,
[InCommon Executive Liaison]

Sample Sponsorship Letter
Dear InCommon,

SAMPLE University entered into a business relationship with PARTNER in 2007 to use their web-based resource to support individualized instruction in IT topics to faculty, staff, and students. We want to use our identity management system to leverage their product. In addition, we are currently engaged in a project with PARTNER that will allow our students to access digital versions of textbooks published by PARTNER in a way that leverages our identity management system. For both of these products we want to be able to provide access either directly by end users or via our course management systems. In order to accomplish our goals with both of these services, we would like to sponsor PARTNER to join InCommon.

Our PARTNER:
Ms. JANE EXECUTIVE
PARTNER INC.
HTTP://URL_OF_PARTNER

Sincerely,
Dr. Executive
Vice Provost, Information Technology
SAMPLE University