# InCommon Federation Basics

A Summary of Resources

Updated October 6, 2010

# Table of Contents

TABLE OF CONTENTS 3

GETTING STARTED 4

FEDERATED IDENTITY MANAGEMENT CHECKLIST 5

INCOMMON FAQ 11

JOINING INCOMMON 13

GETTING HELP 15

ADDITIONAL RESOURCES 17

PARTICIPATING IN INCOMMON 18

INCOMMON POLICIES AND PRACTICES 19

INCOMMON PARTICIPANT OPERATIONAL PRACTICES 20

TECHNICAL REQUIREMENTS  AND INFORMATION 31

SPONSORING PARTNERS INTO INCOMMON 33

# Getting Started

# 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

## Identity Provider: Identity Management Preparation

### Policy Steps

*** Review InCommon Participant Operating Practices (POP) document to familiarize yourself with the policies your organization will need in joining a federation**

The POP is a document produced by an Identity Provider to help other InCommon members understand their business practices as they relate to Identity Management (IdM). The practices detailed in the POP will serve as a guide as other organizations decide if they are willing to federate with you. Because all InCommon members must maintain online versions of their operating practices, so it is easy to find samples that can help your organization (such as these: http://its.lafayette.edu/about/policies/InCommonPoP, http://www.cit.cornell.edu/identity/InCommon.html). Reviewing these sites first will help familiarize you with the policies you will need to address and demonstrate later.

**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 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 reduce the number of times he or she needs to log into and out of systems. This convenience requires some security tradeoffs. These policies are of interest to your service providers in the federation, but they also give good information for informing 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 (1 hour? Until a web browser is closed?)"? These policies are documented in the POP.

*** 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 information 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 accounts are removed—when a student graduates or leaves, is the student's account removed immediately? In 1 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. These policies are documented in the POP.

**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.cfm](http://www.incommon.org/join.cfm) 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 problem resolution process for when users forget or lose 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.

*** Post your InCommon Participant Operating Practice (POP).**
For more information, see the identity provider portion of http://www.incommon.org/docs/policies/incommonpop_20080208.html. Remember that the POP is a living document. It needs to be updated as organizational procedures change.

### 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://spaces.internet2.edu/display/SHIB2/Installation for detailed installation, configuration and operation instructions.

# Identity Provider: Identity Attribute Provisioning

### Policy Steps

Many organization/data stakeholders will need to understand federating and it's 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 emerges asking 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 are released to service providers and for what purposes. For instance, is this person a student? In what year of studies is this student? 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.

### 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 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 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, such as InCommon, require 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 eduPerson data schema. For this step, familiarize yourself with the eduPerson data schema at http://middleware.internet2.edu/eduperson/ .

You can choose to support these attributes by storing them in your directory or database. If using Shibboleth, the software can also look up a local attribute in your directory and send it as an eduPerson attribute, if you configure it that way. 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), 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 it. Such policies describe which service providers, under which conditions, receive which attributes. See the Shibboleth 2 documentation wiki on this topic at https://spaces.internet2.edu/display/SHIB2/IdPAddAttributeFilter for more information.

# Service Provider Preparation

## Policy Steps

*** Review InCommon Participant Operating Practices (POP) document to familiarize yourself with the policies your organization will need in joining a federation**
All InCommon members must maintain online versions of their operating practices. See
http://www.incommon.org/docs/policies/incommonpop_20080208.html
for more information.

*** 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 in compliance with the federation requirements**
Check the InCommon site to ensure your policies are in compliance with the current federation requirements.

## Business Practice Steps

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

*** Identify what 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/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?

*** Define problem escalation and support procedure 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 process IdPs would use to request services and the process used to respond to the request**

*** Post your InCommon Participant Operating Practice (POP).**
For more information, see the service provider portion of
http://www.incommon.org/docs/policies/incommonpop_20080208.html.

## 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.internet2.edu 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 of 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.

### 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.

### 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 http://shibboleth.internet2.edu/.

# 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. 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 (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. Post your Participant Operational Practices (POP) [WORD] on your organization's website. (After the registration process is complete, your Administrator will submit your POP URL to InCommon.)

4. 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 (http://shibboleth.internet2.edu) and detailed on the Shibboleth documentation wiki (https://spaces.internet2.edu/x/mgM).

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.

These programs include face-to-face workshops, regular web-based workshops and presentations, and education provided in other ways. For the current offerings, see www.incommon.org/educate.

## Corporate Consulting and Support

During 2010, InCommon is piloting an Affiliate Program, designed to connect InCommon participants with those providing federation-related products, services and consulting. Colleges and universities, for example, may be interested in help as they get started with InCommon or Shibboleth.

As the federation grows, InCommon has received an increased number of inquiries about services or consultants available to help with both the policy and technical implementation requirements. The Affiliate Program provides a bridge between the commercial or non-profit organizations that provide software, content, guidance, support, and implementation and integration services related to federation participation.

Proceeds from the program provide funding for the federation's ongoing programs, including outreach, collaboration activities, educational offerings, research and development, and technical operations.

Current InCommon Affiliates include:

- Unicon, Inc. – a leading provider of IT consulting services for the education market, including implementation support for Shibboleth. www.unicon.net

- AegisUSA – an identity management solution provider that has developed a Federated Identity Appliance for Education that provides turnkey infrastructure for joining and participating in InCommon. www.aegisusa.com

- Microsoft – a provider of software and identity management services and systems. www.microsoft.com

- Gluu – an identity management solution provider with a federated identity appliance deployed on-premise or in the cloud. www.gluu.org

Details on the services available from these companies are available at http://www.incommon.org/affilate.

## 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).

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

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

**InC-Cert:** An announcement-only email providing updates and information on the progress of the InCommon Certificate Service.

**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. To subscribe, send an e-mail to sympa@internet2.edu with the following message in the subject: subscribe ListName FirstName LastName (e.g.: subscribe shibboleth-announce Chris Jones)

- **Shibboleth-Announce**
  Used by the Shibboleth team to distribute news about Shibboleth and federations. This low-traffic list is also used by the Shibboleth team to distribute Security Advisories.
- **Shibboleth-Users**
  Used for discussion of Shibboleth deployment issues.
  NOTE: if you are new to Shibboleth, start with this list.
- **Shibboleth-Dev**
  Used for discussion of Shibboleth development issues.

# 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 shibboleth.internet2.edu. For information on development activities, refer to middleware.internet2.edu. 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 (http://www.incommon.org/policies.cfm) includes the InCommon participation agreement, fee schedule, POP template, Federation operating policies, information about attributes, and information about InCommon governance.

## Getting Started with Shibboleth

**The Shibboleth website** is the primary source for software, documentation, and deployment information.  Refer to the Info Centers for management-related and technical implementation information. http://shibboleth.internet2.edu

**Read These First:** If you are just getting started with Shibboleth, go to the "Get Started with Shibboleth page (http://shibboleth.internet2.edu/get-started.html) and also download the Shibboleth Deployment Checklist (http://shibboleth.internet2.edu/shib-checklist-final-website.pdf).

## 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.cfm). Documents are listed in the recommended order of reading. Policies and practices for InCommon are overseen by the InCommon Steering Committee.

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

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

**Participant Operational Practices**
http://www.incommon.org/docs/policies/incommonpop_20080208.html
Each participant's POP outlines its Identity Management and/or Service system(s). Service Providers will use the POP to determine their level of trust for assertions from each participant. Identity Providers will evaluate each Service's privacy policies and attribute collection and use policies. Participant POP statements must be publicly posted on a website. The URLs for participant POPs are available to all Administrators via the secure administrative interface. (See next section.)

**Federation Operating Policies and Practices**
http://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**
http://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) at:
http://www.incommon.org/docs/policies/ExampleExecLetter.doc

**InCommon Assurance Profiles**
http://www.incommon.org/assurance
InCommon is moving toward additional assurance profiles (including Silver), which will meet requirements for SPs with applications needing higher security, additional identity proofing, or other such needs.

**InCommon Attributes**
http://www.incommon.org/attributesummary.html.
InCommon supports eduPerson Schema attributes. For more information, see the InCommon Attribute overview page at http://www.incommon.org/attributes.html.

# InCommon Participant Operational Practices

Participation in the InCommon Federation (“Federation”) enables a federation participating organization ("Participant") to use Shibboleth identity attribute sharing technologies to manage access to on-line resources that can be made available to the InCommon community. One goal of the Federation is to develop, over time, community standards for such cooperating organizations to ensure that shared attribute assertions are sufficiently robust and trustworthy to manage access to important protected resources. As the community of trust evolves, the Federation expects that participants eventually should be able to trust each other's identity management systems and resource access management systems as they trust their own.

A fundamental expectation of Participants is that they provide authoritative and accurate attribute assertions to other Participants, and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the Federation or the source of that information. In furtherance of this goal, InCommon requires that each Participant make available to other Participants certain basic information about any identity management system, including the identity attributes that are supported, or resource access management system registered for use within the Federation.

Two criteria for trustworthy attribute assertions by Identity Providers are: (1) that the identity management system fall under the purview of the organization’s executive or business management, and (2) the system for issuing end-user credentials (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) specifically have in place appropriate risk management measures (e.g., authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.).

InCommon expects that Service Providers, who receive attribute assertions from another Participant, respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Furthermore, such information should be used only for the purposes for which it was provided. InCommon strongly discourages the sharing of that data with third parties, or aggregation of it for marketing purposes without the explicit permission1 of the identity information providing Participant.

InCommon requires Participants to make available to all other Participants answers to the questions below.2 Additional information to help answer each question is available in the next section of this document. There is also a glossary at the end of this document that defines terms shown in italics.

[1] Such permission already might be implied by existing contractual agreements.

[2] Your responses to these questions should be posted in a readily accessible place on your web site, and the URL submitted to InCommon. If not posted, you should post contact information for an office that can discuss it privately with other InCommon Participants as needed. If any of the information changes, you must update your on-line statement as soon as possible.

## 1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name ________________________________

The information below is accurate as of this date __________________________

1.2 Identity Management and/or Privacy information

Additional information about the Participant's identity management practices and/or privacy policy regarding personal information can be found on-line at the following location(s).

URL(s) ________________________________________________________

1.3 Contact information

The following person or office can answer questions about the Participant's identity management system or resource access management policy or practice.

Name ________________________________________________________

Title or role __________________________________________________

Email address _________________________________________________

Phone ____________________________ FAX ________________________

## 2. Identity Provider Information

The most critical responsibility that an Identity Provider Participant has to the Federation is to provide trustworthy and accurate identity assertions.[3] It is important for a Service Provider to know how your *electronic identity credentials* are issued and how reliable the information associated with a given credential (or person) is.

[3] A general note regarding attributes and recommendations within the Federation is available here: http://www.incommonfederation.org/attributes.html

### Community

2.1 If you are an Identity Provider, how do you define the set of people who are eligible to receive an electronic identity? If exceptions to this definition are allowed, who must approve such an exception?

2.2 "Member of Community"[4] is an assertion that might be offered to enable access to resources made available to individuals who participate in the primary mission of the university or organization. For example, this assertion might apply to anyone whose affiliation is "current student, faculty, or staff."

What subset of persons registered in your identity management system would you identify as a "Member of Community" in Shibboleth identity assertions to other InCommon Participants?

### Electronic Identity Credentials

2.3 Please describe in general terms the administrative process used to establish an electronic identity that results in a record for that person being created in your electronic identity database? Please identify the office(s) of record for this purpose. For example, "Registrar's Office for students; HR for faculty and staff."

2.4 What technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

2.5 If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across a network without being protected by encryption (i.e., "clear text passwords" are used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

2.6 If you support a "single sign-on" (SSO) or similar campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for InCommon Service Providers, please describe the key security aspects of your SSO system including whether session timeouts are enforced by the system, whether user-initiated session termination is supported, and how use with "public access sites" is protected.

2.7 Are your primary electronic identifiers for people, such as "net ID," eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and is there a hiatus between such reuse?

[4] "Member" is one possible value for eduPersonAffiliation as defined in the eduPerson schema. It is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., library privileges). "Member of Community" could be derived from other values in eduPersonAffiliation or assigned explicitly as "Member" in the electronic identity database. See http://www.educause.edu/eduperson/

### Electronic Identity Database

2.8 How is information in your electronic identity database acquired and updated? Are specific offices designated by your administration to perform this function? Are individuals allowed to update their own information on-line?

2.9 What information in this database is considered “public information” and would be provided to any interested party?

### Uses of Your Electronic Identity Credential System

2.10 Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

### Attribute Assertions

*Attributes* are the information data elements in an attribute assertion you might make to another Federation participant concerning the identity of a person in your identity management system.

2.11 Would you consider your attribute assertions to be reliable enough to:

[ ] control access to on-line information databases licensed to your organization?

[ ] be used to purchase goods or services for your organization?

[ ] enable access to personal information such as student loan status?

### Privacy Policy

Federation Participants must respect the legal and organizational privacy constraints on attribute information provided by other Participants and use it only for its intended purposes.

2.12 What restrictions do you place on the use of attribute information that you might provide to other Federation participants?

2.13 What policies govern the use of attribute information that you might release to other Federation participants? For example, is some information subject to FERPA or HIPAA restrictions?

## 3. Service Provider Information

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

3.1 What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service ProviderID that you have registered.

3.2 What use do you make of attribute information that you receive in addition to basic access control decisions? For example, do you aggregate session access records or records of specific information accessed based on attribute information, or make attribute information available to partner organizations, etc.?

3.3 What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted?

3.4 Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

3.5 If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

## 4. Other Information

4.1 Technical Standards, Versions and Interoperability
Identify the version of Internet2 Shibboleth code release that you are using or, if not using the standard Shibboleth code, what version(s) of the SAML and SOAP and any other relevant standards you have implemented for this purpose.

4.2 Other Considerations
Are there any other considerations or information that you wish to make known to other Federation participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

## Additional Notes and Details on the Operational Practices Questions

As a community of organizations willing to manage access to on-line resources cooperatively, and often without formal contracts in the case of non-commercial resources, it is essential that each Participant have a good understanding of the *identity* and resource management practices implemented by other Participants. The purpose of the questions above is to establish a base level of common understanding by making this information available for other Participants to evaluate.

In answering these questions, please consider what you would want to know about your own operations if you were another Participant deciding what level of trust to place in interactions with your on-line systems. For example:

- What would you need to know about an *Identity Provider* in order to make an informed decision whether to accept its *assertions* to manage access to your on-line resources or applications?
- What would you need to know about a *Service Provider* in order to feel confident providing it information that it might not otherwise be able to have?

  It also might help to consider how *identity management systems* within a single institution could be used.
- What might your central campus IT organization, as a *Service Provider*, ask of a peer campus *Identity Provider* (e.g., Computer Science Department, central Library, or Medical Center) in order to decide whether to accept its *identity assertions* for access to resources that the IT organization controls?
- What might a campus department ask about the central campus *identity management system* if the department wanted to leverage it for use with its own applications?

The numbered paragraphs below provide additional background to the numbered questions in the main part of this document.

[1.2] InCommon Participants who manage Identity Providers are strongly encouraged to post on their website the privacy and information security policies that govern their *identity management system*. Participants who manage Service Providers are strongly encouraged to post their policies with respect to use of personally identifying information.

[1.3] Other InCommon Participants may wish to contact this person or office with further questions about the information you have provided or if they wish to establish a more formal relationship with your organization regarding resource sharing.

[2] Many organizations have very informal processes for issuing electronic credentials. For example, one campus does this through its student bookstore. A *Service Provider* may be more willing to accept your *assertions* to the extent that this process can be seen as authoritative.

[2.1] It is important for a *Service Provider* to have some idea of the community whose identities you may represent. This is particularly true for *assertions* such as the eduPerson “Member of Community.”. A typical definition might be “Faculty, staff, and active students” but it might also include alumni, prospective students, temporary employees, visiting scholars, etc. In addition, there may be formal or informal mechanisms for making exceptions to this definition, e.g., to accommodate a former student still finishing a thesis or an unpaid volunteer.

This question asks to whom you, as an *Identity Provider*, will provide electronic credentials. This is typically broadly defined so that the organization can accommodate a wide variety of applications locally. The reason this question is important is to distinguish between the set of people who might have a credential that you issue and the subset of those people who fall within your definition of "Member of Community" for the purpose of InCommon *attribute assertions*.

[2.2] The *assertion* of "Member of Community" is often good enough for deciding whether to grant access to basic on-line resources such as library-like materials or websites. InCommon encourages participants to use this *assertion* only for "Faculty, Staff, and active Students" but some organizations may have the need to define this differently. InCommon *Service Providers* need to know if this has been defined differently.

[2.3] For example, if there is a campus recognized office of record that issues such electronic credentials and that office makes use of strong, reliable technology and good database management practices, those factors might indicate highly reliable credentials and hence trustworthy *identity assertions*.

[2.4] Different technologies carry different inherent risks. For example, a userID and password can be shared or "stolen" rather easily. A PKI credential or SecureID card is much harder to share or steal. For practical reasons, some campuses use one technology for student credentials and another for faculty and staff. In some cases, sensitive applications will warrant stronger and/or secondary credentials.

[2.5] Sending passwords in "clear text" is a significant risk, and all InCommon Participants are strongly encouraged to eliminate any such practice. Unfortunately this may be difficult, particularly with legacy applications. For example, gaining access to a centralized calendar application via a wireless data connection while you are attending a conference might reveal your password to many others at that conference. If this is also your campus credential password, it could be used by another person to impersonate you to InCommon Participants.

[2.6] "Single sign-on" (SSO) is a method that allows a user to unlock his or her *electronic identity credential* once and then use it for access to a variety of resources and applications for some period of time. This avoids people having to remember many different identifiers and passwords or to continually log into and out of systems. However, it also may weaken the link between an *electronic identity* and the actual person to whom it refers if someone else might be able to use the same computer and assume the former user's *identity*. If there is no limit on the duration of a SSO session, a Federation *Service Provider* may be concerned about the validity of any *identity assertions* you might make. Therefore it is important to ask about your use of SSO technologies.

[2.7] In some *identity management systems*, primary identifiers for people might be reused, particularly if they contain common names, e.g. Jim Smith@MYU.edu. This can create ambiguity if a *Service Provider* requires this primary identifier to manage access to resources for that person.

[2.8] Security of the database that holds information about a person is at least as critical as the *electronic identity credentials* that provide the links to records in that database. Appropriate security for the database, as well as management and audit trails of changes made to that database, and management of access to that database information are important.

[2.9] Many organizations will make available to anyone certain, limited "public information." Other information may be given only to internal organization users or applications, or may require permission from the subject under FERPA or HIPAA rules. A *Service Provider* may need to know what information you are willing to make available as "public information" and what rules might apply to other information that you might release.

[2.10] In order to help a *Service Provider* assess how reliable your *identity assertions* may be, it is helpful to know how your organization uses those same assertions. The assumption here is that you are or will use the same *identity management system* for your own applications as you are using for federated purposes.

[2.11] Your answer to this question indicates the degree of confidence you have in the accuracy of your *identity assertions*.

[2.12] Even "public information" may be constrained in how it can be used. For example, creating a marketing email list by "harvesting" email addresses from a campus directory web site may be considered illicit use of that information. Please indicate what restrictions you place on information you make available to others.

[2.13] Please indicate what legal or other external constraints there may be on information you make available to others.

[3.1] Please identify your access management requirements to help other Participants understand and plan for use of your resource(s). You might also or instead provide contact information for an office or person who could answer inquiries.

[3.2] As a *Service Provider*, please declare what use(s) you would make of attribute information you receive.

[3.3] Personally identifying information can be a wide variety of things, not merely a name or credit card number. All information other than large group identity, e.g., "member of community," should be protected while resident on your systems.

[3.4] Certain functional positions can have extraordinary privileges with respect to information on your systems. What oversight means are in place to ensure incumbents do not misuse such privileges?

[3.5] Occasionally protections break down and information is compromised. Some states have laws requiring notification of affected individuals. What legal and/or institutional policies govern notification of individuals if information you hold is compromised?

[4.1] Most InCommon Participants will use Internet2 Shibboleth technology, but this is not required. It may be important for other participants to understand whether you are using other implementations of the technology standards.

[4.2] As an *Identity Provider*, you may wish to place constraints on the kinds of applications that may make use of your *assertions.* As a *Service Provider*, you may wish to make a statement about how User credentials must be managed. This question is completely open ended and for your use.

## 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:
http://www.incommon.org/ops/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/InCCollaborate/Technical+Guide.

Shibboleth installation guides and general support:
http://shibboleth.internet2.edu/support.html.

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 and supports SAML 1.1 and SAML 2.0. 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.

## Testing the Service Provider

There are at least two ways to test your Service Provider. They are documented at http://www.incommon.org/test_SP.html.

## Participant Operating Practices

Federation participants must provide InCommon with a link to their practices as described in the Participant Operating Practices (POP).

## Your EntityID

Getting ready to start the federating process? The technical guide on the InCommon-Collaborate wiki provides important information about things to consider concerning your EntityID:
https://spaces.internet2.edu/display/InCCollaborate/Technical+Guide.

## 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 http://www.incommon.org/metadata.html.

### Identity Attributes

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