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 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