

Shibboleth Deployment Checklist

The checklist below provides a list of the policy, process, and technical steps for each deployment stage. Use this list as a guide, not a requirement; you may need to work through only a subset of these actions.

Stage 1: Intra-campus Web Single Sign-on - Central Identity Provider

Policy Steps

- _____ Define who establishes various policies related to single sign-on (SSO) and authentication
- _____ Have basic identity management policies in place, including data and service stewardship responsibilities and use of the system
- _____ Have policy in place specifying whether NONE/SOME/ALL campus authenticated web sites are REQUIRED to use the central single sign-on system

Business Practice Steps

- _____ Create Help desk support for users encountering problems accessing **central** web sites protected by SSO
- _____ Reliably issue credentials to on-campus faculty/staff/students
- _____ Create Help desk support for users encountering problems accessing **department** web sites protected by SSO

Technical - Basic Identity and Access Management Steps

- _____ Provision/de-provision accounts for and authenticate on-campus faculty, staff, and students
- _____ Provision/de-provision accounts for and authenticate other constituencies (e.g. applicants, alums, affiliates)

Technical - Shibboleth Software Steps

- _____ Install/operate/manage Shibboleth identity provider software

Stage 1: Intra-campus Web Single Sign-on - Central and Department Service Provider

Policy Steps

- _____ Define how often department service providers should refresh their metadata
- _____ Promulgate policy describing process and constraints when the service provider is compromised
- _____ Define minimum operational and environmental requirements for the remote server/application
- _____ Define policies on log retention at service providers

Business Practice Steps

- _____ Create process to register a new service providers (e.g. site inspection requirements)
- _____ Create problem resolution process for when users cannot access department-supported service provider
- _____ Create process for service providers to report abuse of their site (e.g. such as by anonymous users)

Technical - Basic Identity and Access Management Steps

- _____ Provide tech support to department service provider sites, including documentation describing the web SSO service (description, process to participate, etc)

Technical - Shibboleth Software Steps

- _____ Manage the metadata describing department service providers and provide mechanism for distribution
- _____ Choose approach to PKI trust within the campus federation (rooted, self-signed)
- _____ Provide installation instructions, configuration files and other local files (e.g. error pages, logos) customized to the campus for the department sysadmins

Stage 2: Attribute Delivery - Central Identity Provider

Policy Steps

_____ Identify attribute source systems and define and describe the set of attributes that are available

_____ Identify who governs the decision to release attribute X to service provider Y

_____ Develop policy defining, in a general way, which services are eligible to receive which attributes

_____ Achieve buy in to attribute release process from Identity stakeholders

Business Practice Steps

_____ Define problem escalation procedure, such as when the wrong attributes are sent to a service provider

_____ Define process to follow when a service provider requests an attribute that is not currently available as defined by the policy above

Technical - Basic Identity and Access Management Steps

_____ Maintain a minimal set of attributes describing each user

_____ Populate eduPerson attributes for each user

_____ Manage entitlement values on user objects

_____ Provide support for groups in the local directory and configure Shibboleth to use them

Technical - Shibboleth Software Steps

_____ Configure the identity provider attribute resolver for the appropriate sources

_____ Identify who is responsible for editing/implementing the attribute release policies

Stage 2: Attribute Delivery - Central and Department Service Providers

Policy Steps

_____ Develop policy governing use of attributes by service providers such as attribute retention, sharing, etc.

Business Practice Steps

_____ Define process an service provider would use to request attributes and the process used to respond to the request

Technical - Shibboleth Software Steps

_____ Document how a service provider's web server could authorize users given the provided attributes

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

Stage 3: Inter-campus Federation - Central Identity Provider

Policy Steps

_____ Ensure compliance with federation policies

_____ Publish identity management and identification and authentication practice, if required

Business Practice Steps

_____ Define process for a) a department requesting an attribute release policy referring to a remote site, and b) central IT reviewing, creating, and managing the attribute release policy

_____ Define help desk process for when user encounters a problem accessing remote sites

Technical - Basic Identity and Access Management Steps

_____ Ensure compliance with federation attribute practice

Technical - Shibboleth Software and Federation Requirements Steps

_____ Follow technical steps to join the desired federation

_____ Configure identity provider software to use federation metadata and credentials and refresh when required

Stage 3: Inter-campus Federation - Central and Department Service Providers

Policy Steps

_____ Ensure SP is compliant with federation policies

Business Practice Steps

_____ Ensure service provider has defined problem resolution process for remote users

_____ Create process for department service provider to ask to be added to federation metadata

Technical - Shibboleth Software and Federation Requirements Steps

_____ Add service provider information to the federation metadata

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