Wisconsin Federation Integration Standards and Guidelines

Draft – Last Updated 2/13/2014

# Introduction

The purpose of the following guidelines is to inform application owners and service providers about the IAM-related functions that must be addressed when planning the implementation of a campus or UW System service that will make use of federated authentication. These guidelines assist application owners in identifying integration activities and issues and planning and executing their federated application implementations.

# Definitions

**Identity Federation –** a model of supporting authentication and authorization to IT systems that enables different campuses to use local campus credentials to authenticate to System-wide applications. The Wisconsin Federation is a Federated Identity Management System based on SAML2 technologies.

**Identity Provider (IdP) -** An authentication and attribute provider operated by a campus (or by the IAM Support Team on behalf of a campus) that provides authentication or authorization services for one or more federated applications.

**Service Provider (SP) –** A service operated by a campus, UW System or external service provider that makes use of an IdP to perform authentication or authorization to the service.

**Sponsor –** The campus or UW System department seeking to purchase or implement the service.

**SAML –** An open, standards-based technology for exchanging authentication and authorization data between an IdP and a SP. The Wisconsin Federation uses the SAML standard to relay authentication and authorization information between parties.

**Metadata –** Information regarding the IdP and SP participants in an Identity Federation. Wisconsin Federation metadata defines the IdPs and SPs within the federation and is distributed automatically to all federation members.

**Shibboleth –** A specific implementation of the SAML2 protocol developed and supported by the Internet2 community and used by the Wisconsin Federation.

**Provisioning and Deprovisioning –** The process of creating or deleting user accounts, or granting or removing access to applications or services for preexisting accounts.

**Attributes –** Specific data about an individual that may be delivered through the authentication process. Examples could include name, email address, major, department, etc.

**Attribute delivery** – The process by which attribute information (such as demographic data) is conveyed from the Identity Provider to the application.

# Integration Process

There are four distinct stages involved in integrating an application or service into the Wisconsin Federation:

**Ideation / Exploration –** At this stage, an application need is identified. During ideation / exploration, sponsors should engage the IAM Support Team to describe the application and intended audience, and to discuss possible integration strategies and issues. Exploration may include definition of a Proof of Concept (POC) project to ensure that the integration will meet the desired needs.

**Acquisition / Analysis –** At this stage, detailed specifications are defined for use in the contracting or procurement process. The IAM Support Team will engage in the procurement or evaluation process to assist in interpretation of vendor technical information and to ensure that the proposed application can be successfully integrated into the Wisconsin Federation.

*NOTE: It is important to note that free or inexpensive services that do not require a formal procurement or acquisition cycle must still go through the analysis phase, as there are likely to be integration costs and activities regardless of the application’s purchase cost.*

**Pilot –** During pilot, the application will be deployed to a subset of users and tested. If the purpose of the pilot is to explore functionality only, there may not be an integration with the Wisconsin Federation during the pilot phase. If the initial pilot phase does not include integration analysis and testing, these steps must be performed before a larger acquisition or deployment is planned.

Some projects may proceed to the pilot stage without evaluation. Examples include projects intended solely to explore whether or not the software can meet a defined business need. These projects should be clearly scoped so that an additional phase is added to explore integration issues.

**Implementation –**During implementation, the application will be deployed to the full subset of users and support and documentation processes will be put in place. The application will then transition to lifecycle maintenance.

# Resource Allocation for Wisconsin Federation Integration

1. The Sponsor should contact the IAM Support Team during the Ideation / Exploration phase to establish the parameters of the project. The IAM Support Team will then work with the sponsor to determine resource allocation and to define project roles during acquisition and later stages.
2. The Sponsor’s implementation plan should include regular checkpoints with the IAM Support Team, encompassing the above phases as minimum checkpoints during the project.
3. The sponsor should submit a request for integration to the IAM Steering Committee for review and approval. This approval is required for integration of a new application or service, or for changes to the data provided to an existing service. The IAM Steering Committee meets monthly to review requests, so sponsors should allow adequate time for the review and approval process.
4. Roles and responsibilities of all parties supporting the services should be understood and documented prior to implementation and ongoing support of the service. It is expected that the following groups are likely to be involved in supporting any federated service:
	1. Application / Service Provider support staff
	2. IAM Support Team
	3. DoIT / UW Madison Helpdesk
	4. Campus Helpdesks
	5. Campus Identity and Access Management (IAM) support staff
5. The Sponsor should request that the Service Provider identify and provide a dedicated technical contact that is knowledgeable about Identity Federation and SAML integration concepts.

# Implementation Guidelines for Wisconsin Federation Applications

1. The Sponsor should evaluate services that are already in use to determine if the need can be met through use or expansion of a service that has already been successfully integrated.
2. The Sponsor should contact the IAM Support Team to engage in assessing the Service Provider’s ability to integrate with the Wisconsin Federation to determine the following items:
	1. The costs and activities associated with integrating the application to the Wisconsin Federation,
	2. The data needed to achieve the integration, and
	3. How the data will be conveyed to the Service Provider.
3. The Sponsor should work with the IAM Support Team to submit the request to the IAM Steering Committee for review and approval.
4. The Sponsor should determine whether or not it is necessary to devise a data extract or load to the service provider other than what is provided via the Wisconsin Federation during authentication.
5. The Sponsor should review and understand the implications of single-signon implied by use of the Wisconsin Federation to understand the features and limitations of the Wisconsin Federation’s SAML IdP service as they apply to login and logout.
6. The Sponsor should work with the IAM Support Team to verify that the Service Provider can perform appropriate authorization checks based on the data provided. Service Providers should not assume authorization based on a successful authentication from a Wisconsin Federation IdP.
7. The Sponsor should work with the IAM Support Team to verify that the Service Provider can send, receive and process automatic refreshes of the Wisconsin Federation SAML metadata to ensure that the information about Federation endpoints is up to date and accurate.
8. The Sponsor should work with the Service Provider and IAM Support Team to understand and document how users will be provisioned and deprovisioned. The Service Provider should document any special procedures or negative impacts resulting from changes to user identifiers such as login name, email address or other unique identifier.
9. The sponsor should work with the Service Provider and IAM Support Team to understand and document the unique identifiers that should be used to represent users in the service, and the processes that should be followed if unique identifiers must be changed.
10. The Sponsor’s testing and implementation plan should include testing authentication and authorization components of the system as well as user provisioning and deprovisioning. The Sponsor should engage the IAM Support Team in the test planning process to ensure appropriate resources are available for testing.
11. Service Providers are generally encouraged not to store attributes received during SAML assertions. Recognizing that there may be an operational need, Service Providers that store attributes received during a SAML assertion should update these attributes after every assertion to ensure that the attributes are current. The IAM Support Team generally discourages applications from providing the ability to manually update attributes that are asserted by a Wisconsin Federation SAML IdP.

# Support Guidelines for Wisconsin Federation Service Providers

1. Wisconsin Federation Service Providers should develop and distribute a set of service documentation that identifies the following attributes at a minimum:
	1. A description of the service
	2. The authorized users of the service
	3. The data attributes required for the service to operate properly
	4. Commonly expected failure modes in the authentication and authorization including error messages
	5. Common troubleshooting steps expected of campus helpdesk staff, campus IAM support staff, the IAM Support Team and others.
2. Wisconsin Federation Service Providers should develop a landing page for the service that is not SAML protected that users can bookmark and that should be advertised as the login page for the service. Without this page, users may bookmark the IdP authentication page and will receive an error the next time they use the bookmarked page.