IdP Strategy - Shibboleth (local)

Description

The Shibboleth Identity Provider software integrated with the local IdMS and operated locally is presented as a baseline for comparison of all proposed alternative solutions which are not set up, run, and maintained locally by a campus .

Fact Finder

Janemarie Duh and David Walker

Example Deployments

Shibboleth is the primary IdP software used in R&E federations.

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata

The Shibboleth IdP can be configured to support all recommended technical basics.

Support for Attribute Release

Shibboleth can be configured to release any attributes supported by the IdMS. Attribute filter policies are set on the IdP to release attribute values and done so in a privacy-preserving way.

Support for Entity Attributes/categories (e.g., R&S)

The IdP software supports the release of entity attribute bundles in fixed or dynamic subsets to all SPs or R&S SPs.The benefit of supporting attribute bundles is the decreased administrative overhead. An attribute is configured for the entity category.

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

Identity assurance. The Multi-Context Broker, an extension to the Shibboleth IdP, supports multiple assurance profiles.

https://spaces.at.internet2.edu/display/InCAssurance/Multi-Context+Broker

Support for ECP (Enhanced Client or Proxy)

ECP is a SAML authentication profile for non-browser clients. There is a Java client which is a wrapper around the Apache HTTPClient that provides Shibboleth support.

https://github.com/reckart/shib-http-client

Support for User Consent

User attribute release consent. Technology exists via an extension for Shibboleth IdPs, uApprove, to implement attribute release consent. It also handles Terms of Use.

https://www.switch.ch/aai/support/tools/uApprove.html

There is also current work on a privacy manager through the NSTIC-sponsored Scalable Privacy Project.

Expertise Required

Shibboleth requires expertise in the operation of Java-based services and XML, in addition to general knowledge of federation architecture.

Resources Required

Shibboleth requires a Java servlet container, such as Apache Tomcat. Hardware resources that must be allocated are dependent on load, but are generally low.

Upkeep and Feeding Required

Maintaining an IdP requires keeping up on security patches and advisories for the underlying resources as well as keeping current on the IdP software itself. Site administrators are tasked with maintaining the IdP metadata and monitoring the InCommon NOTICE list in case technical changes are made that require them to take corrective action regarding their IdP and how it operates in a federated context.

Applicable Environments

Shibboleth is highly adaptable to arbitrary environments.

Pros / Benefits

Shibboleth is the mainstream SAML implementation. It is used in the vast majority of federation deployments, and new developments in the use of SAML are usually built for Shibboleth first.

Cons / Risks

Shibboleth requires specialized expertise to operate. This expertise may not already be available in an environment that does not already support Java.