Shibboleth

Shibboleth is a standards based, open source software package for web single sign-on across or within organizational boundaries. Shibboleth began as an Internet2 project and is currently developed as open source software, released under the Apache Software License8. The Shibboleth software package consists of many components, some of which are described in other sections of this document. This section focuses on the components that implement the SAML Identity and Service provider, namely:

- Shibboleth Identity Provider
- Shibboleth Service Provider

- Features
- Supported standards
- User Interfaces and APIs
- Support for Virtual Organisations
- Dependencies on other technologies
- Operational overview
- Expected level of support

Features

The Shibboleth Identity Provider provides Single Sign-On services through authentication of users and securely providing appropriate data to requesting services. In addition to a simple yes/no response to an authentication request, the Shibboleth Identity Provider provides a rich set of user-related data to the Service Provider. The main features of the Shibboleth Identity Provider can be summarized as following:

- Out-of-the-box support for LDAP, Kerberos, web server- and Servlet Container-based authentication systems.
- Out-of-the-box support for reading user data from LDAP directories and relational databases (no special schemas required) and performing simple or complex transformations on the acquired data.
- Support for releasing only selected data and making sure it gets there securely.
- Excellent scaling - a single instance can handle millions of authentication requests per day and can communicate with thousands of service providers.
- Works with all other known SAML implementations.
- Documented APIs to allow the software to be extended to support custom services.

The Shibboleth Service Provider SSO-enables and Federation-enables web applications written with any programming language or framework, integrating natively with popular web servers such as Apache and IIS.

The key features of the Shibboleth Service Provider are summarized below:

- Support for Apache and IIS web servers and FastCGI authorizers on a wide range of platforms, including
- Windows, Linux, OS X, and Solaris.
- Excellent scalability in both user load and management of Identity Providers.
- Support for virtualization of web servers and applications.
- Works with all compliant SAML implementations.
- A variety of authorization and policy-oriented features.

The AARC requirements supported by the tool are:

- User and Service Provider friendliness
- Attribute aggregation / Account linking
- User groups and roles
- Step-up authentication
- Browser & non-browser based federated access
- Federation solutions based on open and standards-based technologies

Supported standards

- SAML 2.0
- X509
- Kerberos
- LDAP
- SQL

User Interfaces and APIs

- Web
- SAML endpoints

Support for Virtual Organisations

Group memberships can be retrieved by issuing SAML 2.0 AttributeQueries to an Attribute Authority configured to retrieve additional attributes from its database and releasing them inside the User Session together with other user attributes.

Dependencies on other technologies

- JAVA
- JRE Open
- SAML-JAVA
- Java Application Server/Container (Tomcat, Jetty)
- Apache mod_shib
- LDAP

Operational overview

The Shibboleth Identity Provider (IdP) is a Java application that runs on a Java web application server (e.g. Apache Tomcat, Jetty).

The Shibboleth Service Provider consists of a daemon running on all major operating systems and a web server module, mod_shib, which is natively supported in the Apache HTTP server and IIS.

Expected level of support

Shibboleth is funded by the Shibboleth consortium. There is no indication that this situation will change in the mid-term future. Support is provided by the user community via the mailing lists, and the project is very well documented in the project's wiki page.