Topics on Cutting-Edge Technology in LIS

Shri Yatrik Patel, Scientist C (CS) of the Centre is involved in the implementation of Shibboleth technology for the off-line access of e-resources available under the UGC-Infonet Digital Library Consortium. The technology is also being explored for the e-resources that will be available under the N-LIST (National Library and Information Services Infrastructure for Scholarly Content) Project to the Colleges of the Country. Shri Patel has explained the Shibboleth technology in this issue of the Newsletter under the article "Shibboleth Based Access Management for Consortia". Sh. Yatrik Patel can be contacted at yatrik@inflibnet.ac.in.

The INFLIBNET Centre provides access to scholarly e-resources to universities in India as one of its core mandates under the UGC –INFONET Digital Library Consortium. The Centre is keen to optimize the utilization of e-resources so as to ensure better returns on investment and greater benefits to the academic community. At present the access to e-resources in universities is IP-enabled and, as such, access is restricted within the confine of a given university campus. Although, usage of e-resources is satisfactory and access to e-resources are restricted to university campuses only due to lack of proper authentication mechanism. The Centre is working towards deploying appropriate access management tools for enabling users to access e-resources either from his / her campus, home or even from while traveling. Implementation of such a solution requires setting-up of proper user authentication and access control mechanism ensuring trust relationship between publisher, "identity providing" agency and the user institution. The Centre is keen on implementing Shibboleth access management system for its e-resources available for access under the consortium.

What is Shibboleth?

The Shibboleth System is an open source software package for web single sign-on across or within organizational boundaries based on open standards of access management. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. Using this technology, user can access designated electronic resources within institute as well as off campus.

The Shibboleth software implements widely used federated identity standards, principally OASIS' Security Assertion Markup Language (SAML), to provide a federated single sign-on and attribute exchange framework. Shibboleth also provides extended privacy functionality allowing the user and their home site to control the attributes released to each application. Using Shibboleth-enabled access simplifies management of identity and permissions for organizations supporting users and applications. Shibboleth is developed in an open and participatory environment and is freely available.

In addition to providing single sign-on functionality, Shibboleth can help control access to either campus-based or licensed resources. Working with identity management systems, Shibboleth releases the information for which service partners need to authorize actions or customize the user's experience. This reduces the need for developers to have access to the directory and instead provides fresh data, just-in-time. This can be implemented on- and off-campus. Shibboleth provides effective and efficient answer to the following challenges:

- multiple passwords required for multiple applications: Shibboleth supports single-sign on functionality
- scaling the account management of multiple applications: Most e-resources are Shibboleth compliant
- security issues associated with accessing third-party services privacy: Shibboleth uses Security Assertion Markup Language (SAML) and encrypted digital certificates for transfer of user attributes
- interoperability within and across organizational boundaries: Shibboleth uses open standards and is based on open source software
- enabling institutions to choose their authentication technology: Shibboleth can adopt already existing authentication mechanism (e.g. LDAP or Database) in an organization
- enabling service providers to control access to their resources: Shibboleth's Service Provider's interface at the publisher's end can be configured to allow access based on attribute provided by Shibboleth's Identity Provider.

An individual users can access resources offered by the institution and provider organizations through his / her campus login and password and they can also use authentication technology as per his / her choice as Shibboleth sits on top and provides the web single sign-on functionality.

There are two primary components to the Shibboleth system:

1. Identity Provider - the software run by an organization with users wishing to access a restricted service;

2. Service Provider - the software run by the provider managing the restricted service.

Shibboleth leverages the organization's identity and access management system, so that the individual's relationship with the institution determines access rights to services that are hosted both on- and off-campus.

To understand working of Shibboleth we need to clear some of the common terms in context of Shibboleth, those are described below:

Single sign-on

Many web-based applications have their own authentication system and each user of that application is issued with a username specifically for access to that system. Similarly owners of protected web sites issue usernames and passwords for access to their protected or subscribed resources. So, a typical user is likely to have various usernames; for access to the Library Catalogue, local PCs, Virtual Learning Environment, and for access to academic research material.

This proliferation of usernames causes management problems to the organizations, confusion to users and customer service providers. The purpose of a single sign-on system is twofold:

☞ to allow a user to use a single identity for access multiple online resources; and

☞ to allow a user to navigate from one resource to another without having to re-type the username and password.

The principal objective of Shibboleth is to allow an organization to have a single set of username and password for accessing multiple online resources either local or external available to members of the organization. The organization takes responsibility for authenticating the users by whatever means, Shibboleth does not pre-ordain the method that can be used for web server based authentication.

Attributes

The organization is responsible for providing attributes to each of its members such as member of department, role of student or faculty, entitlement to restricted resources. The organization also provides an Attribute Release Policy (ARP), accordingly, administrators choose appropriate attributes for online resources. The reference software provides an Attribute Authority (AA) which can be used to retrieve attributes from various sources, such as LDAP Directories, databases and files.

Individual privacy

The architecture of Shibboleth enforces the concept of individual privacy, allowing users to have a one-time session identifier and no persistent identity visible outside the organization.

Individual privacy is also enforced by the concept of ARP which is designed to allow the user to restrict the release of attributes to third parties. Management interfaces to enforce the ARP are not yet available.

Federation

This is a set of organizations and resources which agree to work together within a given set of policies, governance and legal agreements. The federation provides a list of participating organizations, with details of the registered Shibboleth components for that organization. This is made available to users wishing to access resources registered with the federation, to allow them to navigate to their home organization for authentication and the provision of authorization information. This list is known as the Where Are You From (WAYF) service.

Service Provider

The online resource is responsible for determining whether a user is entitled to access the resource, using attribute information supplied by the user's home organization. The Service Provider is also responsible for publicizing details of attributes required for access to each resources, enabling users to prepare themselves in order to access resources.

Identity Provider

The organization is known as the Identity Provider and provides:

Its own authentication and single sign-on system. An Attribute Authority linked to user attribute information (also part of the reference software)

The Shibboleth authentication and authorization process

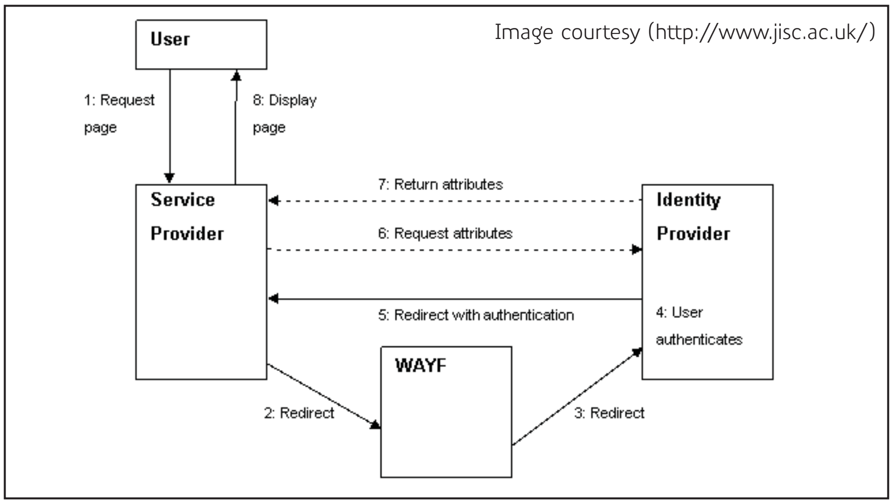

Image courtesy (http://www.jisc.ac.uk/)

1. First of all, the user accesses a protected resources.
2. The resource redirects the user to the WAYF, so that he/she can select his home organization. Depending on the policy of the federation, the user may be able to record this preference, perhaps in a cookie, for future use.
3. The user is then directed to his home organization, which sends him to the authentication system at his organization.
4. The user authenticates himself, by whatever means his organization deems appropriate for this federation.
5. After successful authentication, a one-time handle or session identifier is generated for this user session, and the user is returned to the resource
6. The resource uses the handle to request attribute information from the Identity Provider for this user.
7. The organization allows or denies the attribute information to be made available to this resource using the ARP.
8. Based on the attribute information made available, the resource then allows or denies the user access to the resource.

Shibboleth @ INFLIBNET

The Shibboleth working architecture described above requires each participating institutions to set-up their own "identity provider" services. Looking at the present scenario, universities and colleges do not have requisite technical know-how and ICT infrastructure, as such, INFLIBNET has decided to act as IDP (Identity Provider) for all the institutions, including universities and colleges under its umbrella. As such, the working scenario at INFLIBNET will change as per the Shibboleth implementation:

1. The service provider (publisher) will recognize INFLIBNET Centre as a trusted organization for authenticating user and will give an option on their Web site to select INFLIBNET as an "Identity provider" (IDP).
2. Since INFLIBNET will serve as an IDP for all its member institutions, individual institutions would not be required to set-up their separate IDP and publisher would not be required to maintain separate link for each institution
3. When a user chooses INFLIBNET Consortia, he / she may be re-directed to IDP link at INFLIBNET Server
4. After verifying user's credentials, IDP at INFLIBNET will pass "user attributes" which may also contain his / her credentials (such as institute, department, role as faculty/student/researcher) and if agreed, whether he / she is having access to particular journal of publisher or not and / or other attributes which are mutually agreed.
5. If allowed (based on attributes) user will be able to access journals.

References

http://shibboleth.internet2.edu/
http://www.jisc.ac.uk/