ShibboLEAP Project

Final Report:

School of Oriental and African Studies (SOAS)

Colin Rennie

May 2006

Shibboleth Implementation at SOAS

Table of Contents

Chapter 1: Introduction

What this document contains.

This document contains an introduction to the Shibboleth software and architecture followed by some details on the installation of this software at SOAS.

Who writes the Shibboleth software ?

The Shibboleth software is written by MACE (Middleware Architecture Committee for Education) who are part of the Internet2 group. The home page for Shibboleth can be found at http://shibboleth.internet2.edu

Chapter 2: **Why Shibboleth?**

What does Shibboleth do ?

Shibboleth provides a system for asserting a users identity and stating some attributes about that user. Shibboleth does not provide authentication directly, rather it uses the institutions existing identity management infrastructure (in SOAS' case Novell). Shibboleth is highly configurable in who it will allow to connect to it and what attributes it will provide about a user. It is perfectly possible to use Shibboleth to protect a web site without the owners of the protected web site ever knowing the name of the people logging in (in this case Shibboleth would assert to the web site that the person is known to SOAS but not provide the persons name).

What does it replace ?

Shibboleth replaces any system that protects web site content such as Microsoft Passport or Athens. Its major advantage over a system such as Athens is that individual universities run their own user database rather than the current centralised database used in Athens.

Chapter 3: How does Shibboleth work?

Shibboleth is a fairly complex and highly configurable system and so this section merely contains a basic overview to get you going. A better document to read is the Shibboleth Technical Overview

SAML

Shibboleth is a SAML (Security Assertion Markup Language) application. For a more detailed introduction see the Security Assertion Markup Language (SAML) 2.0 Technical Overview

SAML is an XML standard that defines a framework for exchanging security information between online business partners (according to the technical overview). SAML messages (xml text) are used to assert information about a subject. The SAML communications have two ends the IDP (Identity Provider) and the SP (Service Provider), the IDP being the end that knows something about someone (the server we are installing here at SOAS) and the SP being a web site that wishes to grant access to its content to people known to a specific IDP.

Data passes from IDP to SP via SAML assertions, so for example an IDP might send an assertion to an SP telling it that the user logged on using a password based authentication system. This tells the SP that the IDP recognises the current user (it is then a matter of policy for the SP to decided whether the user may access its services). Further information can also be supplied via user attributes. So an IDP may also add attributes to the previous assertion stating that the users email address is joe@blogs.com or that they are a member of staff.

It is this that will probably be of the most use to UK universities. If a user wishes to use a resource on a web site then Shibboleth will arrange for a users IDP to send an assertion to the service with the role attribute (staff, student etc). An assertion of this type tells the SP that the user is a member of the university and what role they have there. The SP can then grant or deny access based on this. At no point does the web site (SP) need to know the users name, login name or password.

In order for this system to hang together the IDP and the SP must trust each other. This is arranged in the software configuration and by signing and encrypting the SAML messages using public/private key encryption methods.

The Shibboleth Exchange

The actual exchange that takes places when using Shibboleth is as follows:

1. The user requests a web pages from a protected web site (SP).

   If the user is already logged on and is allowed access to this web page then a valid security context will exist for this user. This will have been obtained previously as follows and have been cached on the server. A cookie for the web site tells the server what security context belongs to the user. In this case the system skips straight to step 8.

2. The web site redirects the user to the Single Sign On (SSO) service at the IDP (our shibboleth server).

   At this point the user has requested a web page but has not yet signed on. In order to sign on the web server redirects the user to the Shibboleth identity provider server at SOAS. In the redirect URL are details of the service the user is trying to use, the identity of the service provider and the URL of the Shibboleth software at the service provider.

3. The user requests the SSO web page given in the previous step.

   When the user request the page given in the redirect they are requesting a page from the Shibboleth software to give them a SAML assertion that will allow them access to the web site they are trying to get to. It is at this stage that they have to login. The SSO web page they are trying to get from the SOAS Shibboleth software is protected (using the usual Apache method) so that only people with a valid SOAS login can access it.

4. The SSO responds with an HTML form containing the SAML response.

   Assuming they provide a valid SOAS login in the previous step then the SOAS Shibboleth server returns a page with a hidden form containing the SAML response. The target of this form is the URL given in step 2 of the Shibboleth software at the target web site. The form also contains the URL of the service the user is trying to get to and the service provider identity (as also provided in step 2).

5. The user posts this form to the assertion consumer service on the SP (the web site he/she is trying to get access to).

   The form is automatically posted using a bit of javascript so once logged in the user only briefly sees a web page informing him/her that they are being redirected to the web site they were after in the first place.

6. The assertion consumer service processes the SAML assertion, creates a security context and redirects the user to the page they were originally trying to get to.

   Here the web site is processing the form given in the previous step. It reads the SAML response in the form (which will give an assertion that the user has a valid SOAS logon and optionally other information about the user). Based on this information the web site can decide whether the user is allowed to use this service. Assuming the user can then the Shibboleth software creates a security context for this session (identified by a cookie) and redirects the user to the page they were after in the first place.

7. Since a security context exists the server serves the page to the user.

   At this point the user is identified and allowed to see the web page.

Shibboleth Federations

In the previous section we assume that the SP being accessed trusts the IDP used to sign on and that the SP knows where the Shibboleth server is at the IDP so that it can redirect the user to the login page.

This one to one relationship type configuration will quickly become difficult to manage when many different universities are trying to access many different web sites. Because of this the concept of a federation has been created. A federation is a group of IDP's and SP's that trust each and have agreed what information they will give each other about users.

In order to manage a federation several things are needed. First is a managed metadata file that lists all the IDP's and SP's and gives their certificates. This allows all IDP's and SP's to communicate over SSL and so trust each other. Secondly is a WAYF (Where Are You From) service. In step 2 above the SP redirects the user to his/her IDP. But in the case where many different universities are using a site the SP does not know which Shibboleth IDP server to redirect the user to. Instead they are redirected to a WAYF site run by the federation, this site knows where all the institutional Shibboleth IDP servers are. It presents a list of these to the user who can select his/her own site. The WAYF then redirects the user to the IDP and the process continues.

Organisation of the metadata file and the WAYF service is done by the federation centrally. Joining a federation is a matter of agreeing to the federation rules and then being added to the metadata file and WAYF service.

It should be noted that being a member of a federation does not give you access to the web sites in a federation. It merely gives users an ability to login and present a web site with a SAML assertion of who they are. It is still up to the web site whether users from that university are allowed access.

Chapter 4. Shibboleth at SOAS

Background

SOAS is part of the SherpaLEAP project which aims to develop open access e-print repositories for seven University of London institutions. Although access to the e-prints themselves is free and open, authentication is required for staff who wish to deposit documents on the repository and for other maintenance work.

The project ShibboLEAP was funded to enable a Shibboleth Identity Provider service for staff authorised to access the repository for administrative purposes.

Benefits for SOAS

SOAS will become a Shibboleth Identity Provider. Not only will this be of substantial help to staff involved in administering the institutional repository, but it will have a lasting impact for students and staff who wish to access controlled electronic resources that SOAS subscribes to.

At the moment, students and staff have to obtain an Athens username and password to access the majority of controlled electronic resources. This is very labour intensive for library staff who perform bulk uploads of student data to Athens at the start of each academic year. Athens automatically assigns student username and passwords and sends the details to them by email. Not only do students and staff have to memorise an additional password, but also they receive the email at the start of the term at a busy time of the year when they are already experiencing information overload. Students often misplace or forget their passwords which means they have to queue up at the Enquiry Desk to request their details.

The use of individual institutional passwords to access electronic resources will be of great benefit to students and will be less time consuming for library staff.

Future Developments at SOAS

SOAS will continue to continue to utilise the Shibboleth Identity Provider and is in the process of joining the SDSS Federation and of registering with the Shibboleth-Athens gateway.

Now that the ShibboLEAP project has concluded, Richard Baker who was contracted to oversee the technical installation of the Shibboleth server will transfer responsibility to the SOAS IT Department. It is not envisaged that this will affect Shibboleth services at SOAS in the long term but there will obviously be a period of time where staff will have familiarise themselves with Shibboleth technology.

Shibboleth Server.

The server is a standard Fedora Core (3 currently) install. Unix was chosen as most of the School's current services are on Unix servers so in house expertise exists to provide support. In order to pursue this pilot an existing Intel desktop box was used rather than buying a new server system. Following the successful completion of this project the Shibboleth server will be moved to a more robust machine purchased for this service. Since Intel hardware was available the chosen Unix was Linux. The School does not currently have a policy concerning which 'flavour' of Linux to use so Fedora was chosen on the understanding that most existing Shibboleth installs are on Fedora and so any problems may be more easily be solved with help form the Shibboleth community.

The Shibboleth server is registered in the DNS as shibbo.soas.ac.uk.

Choice of Directory.

SOAS operates a Novell eDirectory installation for all its user management functions. The Novell directory also provides an LDAP interface so no extra work was required to provide LDAP access to the School's user data.

Configuration of Directory.

The only remaing work to perform on the LDAP directory was to install the eduPerson object type, thankfully a schema for Novell eDirectory is provided. Steps taken to install this schema are as follows:

Downloaded eduPerson LDIF from http://middleware.internet2.edu/dir/schema/ (Novell eDirectory eduPerson (200312) version).

Use the Import Convert Export utility (ICE) from the server console to import the schema modification. The command line was:

ice -l<path/to/logfile.log> -SLDIF -f/path/to/ldif/novellEDIReduperson-schema1.6-200210.ldif -a -DLDAP -s<ip address of ldap server> -p636 -d<fqdn of admin user> -w<admin password> -L/<path to Trusted Root certificate in .der format>

Once the schema was updated the attributes were populated from the existing directory entries. Populating any one of the attributes for a user automatically associates the eduPerson Class with the user object.

Since SOAS is a small institution it was possible to liase directly with the directory adminstrator and perform this action on the live server quickly with out any requirement for approval from any committee.

Software Location

The Shibboleth IDP software is a Java based web application. It uses the Tomcat servlet container. The software is installed at:

Table 4.1. Software Locations

Tomcat 5	/usr/jakarta-tomcat
Shibboleth	/opt/shibboleth-idp
Apache	Usual Fedora Apache install

Apache Configuration

Apache has two SSL virtual hosts configured using the name https://shibbo.soas.ac.uk on ports 443 and 8443. Both these hosts have Tomcat mounted on the /shibboleth-idp directory. So that any request for https://shibbo.soas.ac.uk/shibboleth-idp/whatever is forwarded to the Tomcat server.

A certificate was purchaed from GlobalSign in order to provide secure access to the Shibboleth server (user sign on actually occurs on the Intranet server which is also protected using a GlobalSign certificate).

SOAS Single Sign On integration

The Single Sign On (SSO) Shibboleth page (https://shibbo.soas.ac.uk/shibboleth-idp/SSO) is protected by a Perl access handler written in house for the School's intranet site. The Perl access handler on shibbo.soas.ac.uk uses the same database as the intranet server so that if a user is logged in to the intranet then they are already logged into shibbo.soas.ac.uk. If the user is not logged in then they are redirected to the login page on the inranet server and then back to shibbo.soas.ac.uk upon successful log in.

Shibboleth Configuration files

The following configuration files for the Shibboleth software were altered:

Table 4.2. Shibboleth Config files

idp.xml	This is the main Shibboleth config file. It configures the position of other config files, the metadata.xml file , the encryption key and certificate and where the Tomcat services are.
metadata.xml	This is the file that provides details of the SP's we accept connections from. This file is obtained from the federation.
resolver.ldap.xml	This is the attribute resolver configuration. This file names the attributes that we know about users and how to query them (the Novell LDAP server in our case)
arps/arp.site.xml	This file tells Shibboleth which of the attributes about a person configured in resolver.ldap.xml can be released to which SP's.

Shibboleth access to the LDAP server.

The entry in resolver.ldap.xml to allow access to our LDAP server is as follows:

```
<JNDIDirectoryDataConnector id="directory">
  <Search filter="(commonName=%PRINCIPAL%)">
    <Controls searchScope="SUBTREE_SCOPE" returningObjects="false" />
  </Search>
  <Property name="java.naming.factory.initial" value="com.sun.jndi.ldap.LdapCtxFactory" />
  <Property name="java.naming.provider.url" value="ldap://tuckbox.soas.ac.uk/ou=soas,o=ac,c=uk"/>
</JNDIDirectoryDataConnector>
```

Where tuckbox.soas.ac.uk is the LDAP server and 'ou=soas,o=ac,c=uk' the top level of the LDAP directory structure at SOAS.

Future Plans.

As already mentioned above SOAS will migrate the current Shibboleth setup from the development server it is currently installed on to a rack mount server purchased specifically to be the School's Shibboleth Server.

Internal documentation and some training will be provided to enable the Network Services team to manage the Shibboleth service.

Appendix 1.

ShibboLEAP Identity Provider Installation.

Partner: School of Oriental and African Studies.
*Contact Name and Email: P*roject co-ordinator**: Colin Rennie: cr22@soas.ac.uk**
Technical Officer **Richard Baker: rich@mondaymorning.org**

Planning (what you intended to do)

Institutional directory type:	Novell Netware 6.5 with eDirectory 8.73.
Institutional directory administrative contact:	Mark Douglas (md11@soas.ac.uk).
Authentication method:	SOAS in house cookie authentication system.
Type of server used :	Fedora Core Release 3
Version of apache/tomcat:	2.0.52/5.5.9
Version of Java:	Sun 1.5.0_04
Certificate CA:	GlobalSign