The UK Access Management Federation
FOR EDUCATION AND RESEARCH

SWINDON COLLEGE

Table of Contents

These case studies, prepared by organisations who participated in the JANET Shibboleth on Windows project, are provided for information purposes only and reflect the particular arrangements and experience of those concerned. In each case, the configuration, installation and implementation of the Shibboleth on Windows software will vary according to the type of infrastructure and technical resources involved.

Executive Summary

Swindon College became a member of the Shibboleth on Windows[1] Installer group in 2008. This group was tasked with testing the Shibboleth for Windows installer software, which enables you easily to install a set of software and services to run an IdP service on a Windows platform.

This case study looks at the implementation of the Shibboleth IdP software for Windows at Swindon College, using the SDSS developed installer software. In addition to installing the software and documenting that procedure, research was undertaken in the area of using the Shibboleth IdP software as an alternate authentication method for accessing the Moodle VLE system.

The College uses the open source Moodle software for its virtual learning environment and has been using the software for approximately four years. It is run on a Microsoft Windows 2003 Server, utilising IIS6.

[1] http://www.ja.net/development/middleware/shibboleth-on-windows.html

Background Information

Swindon College is an FE College based in Swindon, Wiltshire. Its main emphasis is on vocational courses; however courses vary from general FE up to HE courses. The College in the main uses Microsoft Windows servers and Microsoft Windows operating systems on the desktop. The College deploys Microsoft's Active Directory services for LDAP and authentication services.

Resources for the Project

The College used a Dell PowerEdge 1950 server for the IdP installation. This had dual Xeon E5420 2.5Ghz processors, a 68Gb hardware RAID 1 disk configuration, 2Gb of RAM, and was running Windows 2003 Enterprise Server Edition with the latest service packs and hotfixes installed.

The server was positioned within the College's DMZ network, fronted by a Cisco ASA firewall, with the appropriate ports opened for external access to the IdP service.

The College has two Windows 2000 Domain Controllers on the internal network, offering LDAP and Windows authentication services. The College also has two internal DNS servers offering Windows DNS services and two Linux servers for external Internet DNS services.

The College has a JANET Primary Connection to the SWERN MAN. At the time of testing this was a 10Mbit/s connection.

Current Situation

Currently the IdP service has been installed and configured. Tests have been run against the testshibb.org site. Additional work is required to rework the IdP web pages with the College branding, and then further testing before attempting to integrate the IdP within the UK Federation.

In addition to this an additional server has been purchased to offer SP services for the College at some point in the future.

Access Management

There was no previous experience of any federated services before the commencement of this project, or of Shibboleth and its installation and configuration. Initial research was done to gain some background into what Shibboleth was and how it was being used. In addition to this an RSC South West event was attended on the UK Federation, identity services, and their impact within education.

The drivers behind deploying a FAM service were in the main the recent upheavals with Eduserv, with the need to ensure that the College could access the resources it wishes to offer its students. It was recognized that in the long run there was a possibility that some resource providers may move away from the Eduserv/ATHENS service, in which case the College wished to look into all the alternative solutions to gain access to any resources.

In addition to this the Shibboleth software also offered a more consistent way of accessing the resources and a more convenient way for students using only their AD

credentials and password, whether they were inside the College or accessing those resources from outside the College.

The College runs several Web sites, both for internal and external users. They are a mixture of Windows-based and Open Source PHP based solutions. Most of these Web services authenticate against the Windows AD LDAP service.

Some of the Web sites software are supplied from third parties and have their own internal authentication methods. In the long term we would wish that there was a single sign-on for all internal Web services; however we recognize that this may not be achievable without intervention by those third parties. We therefore fall back to multiple logins, but using the Windows AD LDAP supplied credentials whenever possible.

In addition to becoming familiar with the Shibboleth software and configuration, we also looked at the integration of our IdP and a test Moodle installation.

Aims and Objectives

Our main aim was the installation of an IdP service on a Windows platform. Our objectives were to gain experience with the technologies involved and from that grow the experience to support and troubleshoot the service for the benefit of the College.

Our second aim was to evaluate how easy it would be to integrate this with one of our internal services. For that we chose the Moodle VLE, as there was some indication from the documentation available that this could be achieved.

Methodology

Implementation

Looking at the various options available to us, we decided to try an in-house deployment. We wished to become more familiar with open, standards based identity management technology, and to evaluate it against our current Web site authentication methods.

Account management is done in-house so the Shibboleth IdP deployment was really seen as an extension of account management services. For example, the tailoring of access for particular groups within the identity provision infrastructure to particular resources would necessitate some intervention within our existing Windows AD LDAP service to enable this.

There are two people involved in the operational aspect of network services within the College, so both were involved in the installation and documentation process of the Shibboleth Windows Installer software.

Implementation Experiences

The initial installation with an early implementation of the Windows installer failed. We wanted to install the software to a separate non-system partition and unfortunately there was a bug within the software that would not allow this. A bug report was filed and a new version was quickly made available.

The second version of the software installed cleanly to the separate partition and we were able to proceed with the installation. We were also tasked, within the project group, with producing installation documentation; therefore the installation process was

run multiple times, testing each different form of installation type. We did not run into any problems during the installations with the second version of the installer software.

The next phase of the implementation was to ensure that the additional services were configured for operation with the IdP. DNS was set up. Research on the UK Federation indicated that a name like 'idp' is commonly used for the server providing the IdP service, so the internal and external DNS servers were configured with a CNAME entry to point to our IdP server.

The next service to configure was the firewall service. The ports used as part of the Shibboleth IdP service were 8442 and 8443. There was no reasonable method of testing that these were configured until we ran the testshibb tests. We did ensure that the ports were available on the server by using the Windows supplied netstat utility.

Once this was set up, we used the Shibboleth testing service (http://testshib.org/) to test the IdP implementation. This involved creating an account at the Openid.org Web pages, logging into the test service and setting up a configuration to test our IdP. A procedure for running the tests can be found in appendix A.

Once this was achieved, a test was run. This proved to be unsuccessful as we found that we couldn't login. Everything appeared to be fine with the configuration as far as we could tell, and we were getting the login page from our IdP server, but the login failed to authenticate.

To trace the problem we ran packet capture software to view what was happening during the login sequence. We found some authentication packets appeared to be going to an invalid LDAP address.

Internally we use Microsoft's DNS service running on a Windows 2003 Enterprise Server. We found some non-server accounts details under the domain, in the '_tcp' section which purported to point to LDAP servers, but these were old entries for devices that no longer existed. Once these entries were removed we re-ran the test. This time we logged in successfully and we got the corresponding Testshib results page.

We found that there doesn't seem to be a way to indicate to the Shibboleth service that it should use a particular LDAP/Authentication server; it takes information from your DNS entries and uses the first entry found. If this is incorrect then the software will then fail to authenticate.

Once a successful login was achieved we then moved on to try and integrate with the VLE. A fresh install was done of the Moodle VLE software on a test server. The version used was 1.9 and all defaults were accepted during the installation.

Research into the set-up for Shibboleth in Moodle extends to a readme file (see appendix B). Forums were searched on moodle.org but the information found was sparse.

After trying several times, with different configuration values, we could get no success in being able to login or even contact our IdP services. There also appears to be a fault with the configuration page as PHP code appears within the page itself, though this possibly has no effect on the operation of the configuration page or saved settings. See appendix C for some screen shots of the configuration settings page.

Given our time constraints we were not able to find the correct values to enter on the configuration page, or how to properly setup our particular VLE/IdP infrastructure. The documentation for the Shibboleth configuration of Moodle proved to be beyond our current understanding of the Shibboleth software infrastructure; there isn't a simple guide with some example values that we understood sufficiently to enable us to configure the Shibboleth authentication service on Moodle.

Current Moodle documentation also seems to imply a particular configuration which isn't stated. The Shibboleth Windows installer doesn't use a Web server as a base – it is self contained – whereas the readme.txt talks about IIS/Apache configurations. The xml configuration file it refers too doesn't appear to be available in the Windows Installer software. Again our unfamiliarity with the Shibboleth technology is probably at fault here.

Project Experience

The initial Shibboleth on Windows software set-up proceeded efficiently once the problems with the installer were resolved. In all we spent less than one working day setting up the server with Windows 2003, service packs and hotfixes, and installing the Shibboleth software.

The configuration of the shibbtest.org and the successful test took another day. In all if you don't run into any problems then an installation and the initial test could be completed in one working day. The issues we had added another two days to the process. However we estimate the extra research and reading we undertook took approximately two further days.

The amount of time indicated was spread over an extended period, and is adjusted to give a view of how long it would possibly take if you were starting from scratch and had no experience of the installation and configuration procedures. In addition to this time we estimate there will be an extra two to three days involved in finishing the configuration work for the current IdP service.

The main costs involved were the physical hardware and the software license for Windows 2003.

Our experience of the project was positive. We came from a position of having no knowledge of Shibboleth and its configuration to a point where we understand aspects of the technology and how it may benefit an organization. This has been invaluable, however we may proceed in the future, and we feel sure that this part of the project has been beneficial for the College.

The configuration and understanding of Shibboleth, and how to configure the Windows version we have, has been the toughest part of the experience. It has highlighted the fact that extra training is required to deepen our understanding so that troubleshooting is easier. This is important if we wish to offer and support the service in-house.

The extensive documentation covers a lot ground and is detailed, but it assumes a lot of background knowledge and seems to address issues around a Linux/UNIX installation rather than Windows-based installations.

Having said that the College now has the beginnings of an IdP service, which we are confident can meet our needs in respect of accessing resources as part of the UK Federation.

In regards to integration of the service internally with our current Web sites, that remains a much longer term project. Given that either Windows authentication is used for those Windows-based Web sites, or LDAP for the PHP-based Open Source Web sites, the need for Shibboleth services internally is somewhat diminished.

Conclusions and Implications

Shibboleth, and its software stack, is a complex subject which requires effort and time to get comfortable with. The Windows Installer software certainly makes it easy to get the IdP service up and running. Configuration is fairly simple but still requires manually editing text files; there are no easy user interfaces into this aspect of the software at the moment.

However, when it comes to troubleshooting any issues you may have, the documentation available on the Internet does not make it easy to ascertain where the problem may lie; especially as a lot of documentation and experience has gone into Linux/UNIX installations, and few Windows-based installs and configurations seem to be documented for the benefit of new or inexperienced, users.

Configuring access to your internal Web applications is another matter. Whilst it's possible, as it appears that others have been and are successful in this area, you must be confident of your understanding of Shibboleth before you attempt this. We are sure that if we had been able to devote more time to this it could have been achieved.

The Windows Installer project has been a pleasure to participate in, and worthwhile. The ability to discuss others' solutions to the issues faced during the project has proved invaluable.

References

Web Links

UK Federation

http://www.ukfederation.org.uk/

Internet2 Shibboleth

http://shibboleth.internet2.edu/

Moodle:

http://moodle.org/

Appendices

Appendix A Testshib procedure

- *Go to http://openidp.org/user/register. Enter a user name and an email address*
- *The initial password will be sent to you via email. You can use this or login to openidp.org and change it if you wish*
- *Now go to http://www.testshib.org/*
- *Click on the 'TestShib' icon*
- *Click on 'Policy' in the menu to review the site's policy and disclaimers*
- *Click on 'Login' from the menu*
- *Click on the 'Openidp' icon. You'll then be redirected to the OpenIDP site*
- *Login with your credentials that you obtained during steps 1 and 2*
- *You should be presented with the 'Metadata' options*
- *Click 'New Identity Provider'*
- *You'll be asked for the following items*
  - *domain name of the identity provider site*
  - *hostname for the idp server*
  - *a WAYF name for the site*
  - *a contact name, first name and last name*
- *Click 'continue' and you'll be taken to the next screen, where you can check the details entered*
- *Click 'submit' to create the identity*
- *You'll then get a page with the keys/certificate information, cut and past and save these to the filenames indicated*
- *Go back to the 'Metadata' menu option and this time click 'Edit'*
- *You'll see your newly created EntityID*
- *Click 'Edit XML'*
- *Select all the current text and remove*
- *You know need to get a file from your Shibboleth IdP installation. Use a text editor and open up the file C:\Program Files\Internet2\IdP\etc\metadata-segment.xml*
  - *Look for the tag <md:OrganisationName> and edit the value there*
  - *Look for the tag <md:GivenName> and edit the value there*
  - *Look for the tag <md:SurName> and edit the value there*
  - *Look for the tag <md:EmailAddress> and edit the value there*
- *Save the file*
- *Select all the text and paste into the testshib, XML text box. Click 'Continue'*
- *Click 'Submit' to save the file*
- *Make note of the Entity ID address. You'll need this for testing*
- *Copy the testshib.key and testshib.crt files to C:\Program Files\Internet2\IdP\etc*
- *Restart the tomcat service*
- *At the shibtest.org web site click on the 'Test' menu item*
- *Enter your Entity ID value and then press 'Go'*
- *You should be taken to your site's login page*
- *Login and you then should be re-directed back to the shibtest.org where there will be a page displaying the values obtained from your IdP and login*

Appendix B Moodle shibboleth readme.txt

```
Shibboleth Authentication for Moodle
-------------------------------------------------------------------------------
Requirements:
- Shibboleth target 1.1 or later. See documentation for your Shibboleth
  federation on how to set up Shibboleth.
Changes:
- 11. 2004: Created by Markus Hagman
- 05. 2005: Modifications to login process by Martin Dougiamas
- 05. 2005: Various extensions and fixes by Lukas Haemmerle
- 06. 2005: Adaptions to new field locks and plugin config structures by Martin Langhoff
and Lukas Haemmerle
- 10. 2005: Added better error messages and moved text to language directories
- 02. 2006: Simplified authentication so that authorization works properly Added
instructions for IIS
- 11. 2006: User capabilities are now loaded properly as of Moodle 1.7+
- 03. 2007: Adapted authentication method to Moodle 1.8
- 07. 2007: Fixed a but that caused problems with uppercase usernames
- 10. 2007: Removed the requirement for email address, surname and given name
attributes on request of Markus Hagman
- 11. 2007: Integrated WAYF Service in Moodle

Moodle Configuration with Dual login
-------------------------------------------------------------------------------
1. Protect the directory moodle/auth/shibboleth/index.php with Shibboleth.
   The page index.php in that directory actually logs in a Shibboleth user.
   For Apache you have to define a rule like the following in the Apache config:
--
<Location ~  "/auth/shibboleth/index.php">
       AuthType shibboleth
       ShibRequireSession On
       require valid-user
</Location>
--
   To restrict access to Moodle, replace the access rule 'require valid-user'
   with something that fits your needs, e.g. 'require affiliation student'.
   For IIS you have protect the auth/shibboleth directory directly in the
   RequestMap of the Shibboleth configuration file (shibboleth.xml). See
   https://spaces.internet2.edu/display/SHIB/xmlaccesscontrol?topic=XMLAccessControl
2. As Moodle admin, go to the 'Administrations >> Users >> Authentication
   Options' and click on the the 'Shibboleth' settings.
3. Fill in the fields of the form. The fields 'Username', 'First name',
   'Surname', etc. should contain the name of the environment variables of the
   Shibboleth attributes that you want to map onto the corresponding Moodle
   variable (e.g. 'HTTP_SHIB_PERSON_SURNAME' for the person's last name, refer
   the Shibboleth documentation or the documentation of your Shibboleth
   federation for information on which attributes are available).
   Especially the 'Username' field is of great importance because
   this attribute is used for the Moodle authentication of Shibboleth users.
```

```
##################################################################
######################
  Shibboleth Attributes needed by Moodle:
 For Moodle to work properly Shibboleth should at least provide the attribute
 that is used as username in Moodle. It has to be unique for all Shibboleth
  Be aware that Moodle converts the username to lowercase. So, the overall
  behaviour of the username will be case-insensitive.
  All attributes used for moodle must obey a certain length, otherwise Moodle
  cuts off the ends. Consult the Moodle documentation for further information
  on the maximum lengths for each field in the user profile.

##################################################################
######################
4.a  If you want Shibboleth as your only authentication method with an external
     Where Are You From (WAYF) Service , set the 'Alternate Login URL' in the
     'Common settings' in 'Administrations >> Users >> Authentication Options'
     to the the URL of the file 'moodle/auth/shibboleth/index.php'.
     This will enforce Shibboleth login.
4.b If you want to use the Moodle internal WAYF service, you have to activate it
    in the Moodle Shibboleth authentication settings by checking the
    'Moodle WAYF Service' checkbox and providing a list of entity IDs in the
    'Identity Providers' textarea together with a name and an optional
    SessionInitiator URL, which usually is an absolute or relative URL pointing
    to the same host. If no SessionInitiator URL is given, the default one
    '/Shibboleth.sso' will be used.
    Also see https://spaces.internet2.edu/display/SHIB/SessionInitiator
    Important Note: If you upgraded from a previous version of Moodle and now
                    want to use the integrated WAYF, you have to make sure that
                    in step 1 only the index.php script in
                    moodle/auth/shibboleth/ is protected but *not* the other
                    scripts and especially not the login.php script.
5.  Save the changes for the 'Shibboleth settings'. T
    Important Note: If you went for 4.b (integrated WAYF service), saving the
                    settings will overwrite the Moodle Alternate Login URL
                    using the Moodle web root URL.
6.  If you want to use Shibboleth in addition to another authentication method
    not using the integrated WAYF service from 4.b, change the 'Instructions' in
    'Administrations >> Users >> Manage authentication' to contain a link to the
     moodle/auth/shibboleth/index.php file which is protected by
     Shibboleth (see step 1.) and causes the Shibboleth login procedure to start.
     You can also use HTML code in that field, e.g. to include an image as a
     Shibboleth login button.
     Note: As of now you cannot use dual login together with the integrated
          WAYF service provided by Moodle (4.b).
7. Save the authentication changes.
How the Shibboleth authentication works
--------------------------------------------------------------------------------
To get Shibboleth authenticated in Moodle a user basically must access the
Shibboleth-protected page /auth/shibboleth/index.php. If Shibboleth is the only
```

authentication method (see 4.a), this happens automatically when a user selects his home organization in the Moodle WAYF service or if the alternate login URL is configured to be the protected /auth/shibboleth/index.php
Otherwise, the user has to click on the link on the dual login page you provided in step 5.b.

Moodle basically checks whether the Shibboleth attribute that you mapped as the username is present. This attribute should only be present if a user is Shibboleth authenticated.

If the user's Moodle account has not existed yet, it gets automatically created.

To prevent that every Shibboleth user can access your Moodle site you have to adapt the 'require valid-user' line in your webserver's config (see step 1) to allow only specific users. If you defined some authorization rules in step 1, these are checked by Shibboleth itself. Only users who met these rules actually can access /auth/shibboleth/index.php and get logged in.

You can use Shibboleth AND another authentication method (it was tested with manual login). So, if there are a few users that don't have a Shibboleth login, you could create manual accounts for them and they could use the manual login. For other authentication methods you first have to configure them and then set Shibboleth as your authentication method. Users can log in only via one authentication method unless they have two accounts in Moodle.

Shibboleth dual login with custom login page

You can create a dual login page that better fits your needs. For this to work, you have to set up the two authentication methods (e.g. 'Manual Accounts' and 'Shibboleth') and specify an alternate login link to your own dual login page. On that page you basically need a link to the Shibboleth-protected page ('/auth/shibboleth/index.php') for the Shibboleth login and a form that sends 'username' and 'password' to moodle/login/index.php. Set this web page then als alternate login page.
Consult the Moodle documentation for further instructions and requirements.

How to customize the way the Shibboleth user data is used in Moodle
---
Among the Shibboleth settings in Moodle there is a field that should contain a path to a php file that can be used as data manipulation hook.
You can use this if you want to further process the way your Shibboleth attributes are used in Moodle.

Example 1: Your Shibboleth federation uses an attribute that specifies the user's preferred language, but the content of this attribute is not compatible with the Moodle data representation, e.g. the Shibboleth attribute contains 'German' but Moodle needs a two letter value like 'de'.
Example 2: The country, city and street are provided in one Shibboleth attribute and you want these values to be used in the Moodle user profile. So

You have to parse the corresponding attribute to fill the user fields.

If you want to use this hook you have to be a skilled PHP programmer. It is strongly recommended that you take a look at the file moodle/auth/shibboleth/auth.php, especially the function 'get_userinfo' where this file is included.
The context of the file is the same as within this login function. So you can directly edit the object $result.

Example file:

```
--
<?PHP
   // Set the zip code and the adress
   if ($_SERVER[$this->config->field_map_address] != '')
   {
      // $address contains something like 'SWITCH$Limmatquai 138$CH-8021 Zurich'
      // We want to split this up to get:
      // institution, street, zipcode, city and country
      $address = $_SERVER[$this->config->field_map_address];
      list($institution, $street, $zip_city) = split('\$', $address);
      ereg(' (.+)',$zip_city, $regs);
      $city = $regs[1];

      ereg('(.+)-',$zip_city, $regs);
      $country = $regs[1];

      $result["address"] = $street;
      $result["city"] = $city;
      $result["country"] = $country;
      $result["department"] = $institution;
      $result["description"] = "I am a Shibboleth user";

   }

?>
--
```

In case of problems and questions with Shibboleth authentication, contact Lukas Haemmerle <lukas.haemmerle@switch.ch> or Markus Hagman <hagman@hytti.uku.fi>

Appendix C Moodle Shibboleth Configuration Page
These are screenshots of the configuration pages with the Moodle VLE for Shibboleth.