
# SWANSEA COLLEGE

*Christopher Simpson*

## 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

This case study describes the experiences at Swansea College of deploying Shibboleth on Windows. The work was undertaken as part of JANET(UK)'s Shibboleth on Windows[1] project.

## College Background

*Swansea College is one of the largest colleges in the region of South West Wales. It places the concepts of widening participation, lifelong learning and equal opportunities at the forefront of its operations, and continues to strive for excellence and quality in the development and delivery of its complete portfolio.*

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

*The college runs with 2000 full time and 16,000 part time students and 900 staff (approx).*

## Current Access Management Implementation

*Before implementing AthensDA*[2] *the college used the simplest form of access management where resources were only available from within the college (access restricted by IP address).*

*In early 2003 we looked into using ATHENS to authenticate at user level, where we trialled uploading bulk student and staff details onto the ATHENS online management system. However, we soon realised that due to the quantities this task was going to become very difficult, time consuming and not cost effective in terms of staff support time.*

AthensDA was released during the summer of 2003 and we implemented it. We developed an XAP page using ASP (2004) and then ASP.NET (2005). It has worked efficiently since being installed.

There was very limited documentation on release and what was available was difficult to follow.

The only problem we have encountered with AthensDA is our server clock becomes out of sync with those of ATHENS and sometimes failure occurs.

AthensDA is seamlessly integrated into our systems, and no further logins were required after the user logged onto the Windows system.

We currently use AthensDA to access online collections such as:

- Education Image Gallery
- Infotrac
- Film and Sound Online
- Gale Virtual Reference Library

## Aims and Objectives

*Factors leading to Project Participation*
We currently use AthensDA to authenticate college users (staff and students) to licensed online resources, subscribed to by our LRC as described above.

AthensDA has been available free of charge since its release, but this is changing during the summer of 2008. The cost of AthensDA may be relatively cheap per user, but it is a substantial payout if you wish all college members to be able to access the services.

[2] *http://www.athensams.net/local_auth/athensda*

Shibboleth is to replace AthensDA as the authentication methodology across the education sector, and using the UK Access Management Federation we will be able to access most of the resources we currently subscribe to.

*Our objectives from the project*
We are actually in a more fortunate position than other colleges in that we do have previous experience with Shibboleth. However, what was learnt was at a highly technical level using technologies that are not generally used by the FE educational sector in the UK, i.e. JAVA and Tomcat.

This project was of particular interest because, if successful, we could bypass the need for JAVA and Tomcat experience as the installer would automatically configure and install 80% of the Shibboleth framework. This was particularly interesting with the release of Shibboleth 2 approaching and would reduce a further steep learning curve at implementation.

The documentation produced to support the process would fill in the missing gaps. This along with the Windows installer should allow an IT Technical Support Officer to configure and get Shibboleth up and running without in-depth specialist knowledge.

## Current Shibboleth Situation

We have been using Shibboleth 1.3 for the last 24 months. We use Shibboleth as the authentication methodology to share resources between 2 local FE colleges plus all the Swansea Post 16 Schools.

We installed 3 IdP servers plus 3 SP servers to create our own federation. An IdP server was held at each of the colleges; the local education authority that centrally controlled all the Schools Active Directories also had an IdP server.

All the organisations used Windows 2003 servers but as an added complication IIS was selected as the web server of choice. IIS was used due to lack of experience in Apache support within the technical teams. This made the installation process far more complex. It came to light that we were possibly the first people (2005/6) to implement Shibboleth on this platform and there was no evidence that it could even be done.


**Figure 1. Customised IdP Login Page**

Lack of documentation available to complete this simple task in 2005/6.

The IdP installation documentation available was very patchy at best and we had to make a great deal of amendments for IIS instead of the suggested and tested Apache.

Fortunately MATU was set up during this period, and between both teams we managed to get Shibboleth up and running.

The SP installation was far easier as it was released as a Windows installer package (MSI), which just required configuring.

We ended up with a central Moodle server which could be used by staff/students from any of the organisations. We also used uPortal as a front end to access the resources. Some tools developed in-house were re-configured to use Shibboleth member attributes so that individual users could configure different views of applications and display relative personalised content.

## Implementation

*Network Deployment*
We have approximately 1000 PCs and a number of Apple Macs which are based at a number of different sites within the organisation. All of these are networked. All the PCs are at least Pentium 4 with the majority now being Dual Core, running Windows XP Service Pack 2 with Internet Explorer 6 as the standard browser.

All servers are based at the main campus, Tycoch. Most of the servers are now Dual Core Xeon at minimum and rack mounted.

All servers run Windows 2003, except for 2 which are still operating with Windows 2000.

*Resources*

**Server**

- Rack mounted
- 3.0Ghz Intel Xeon Processor
- 4 Gigabytes RAM
- 500Gb Hard Disk Space
- Dual network card

**Operating System**

- Windows 2003 Server (fully updated using Windows Update)

**Software Installed**

- Microsoft Firewall client for ISA Server 2004

**Authentication Database**

- Windows 2003 Active Directory

*Server Connection Configuration*

**Connections to server**

- 1Gb connection via SWANCOLL domain
- 1Gb connection via DMZ

**Firewalls**

- Sonic Firewall

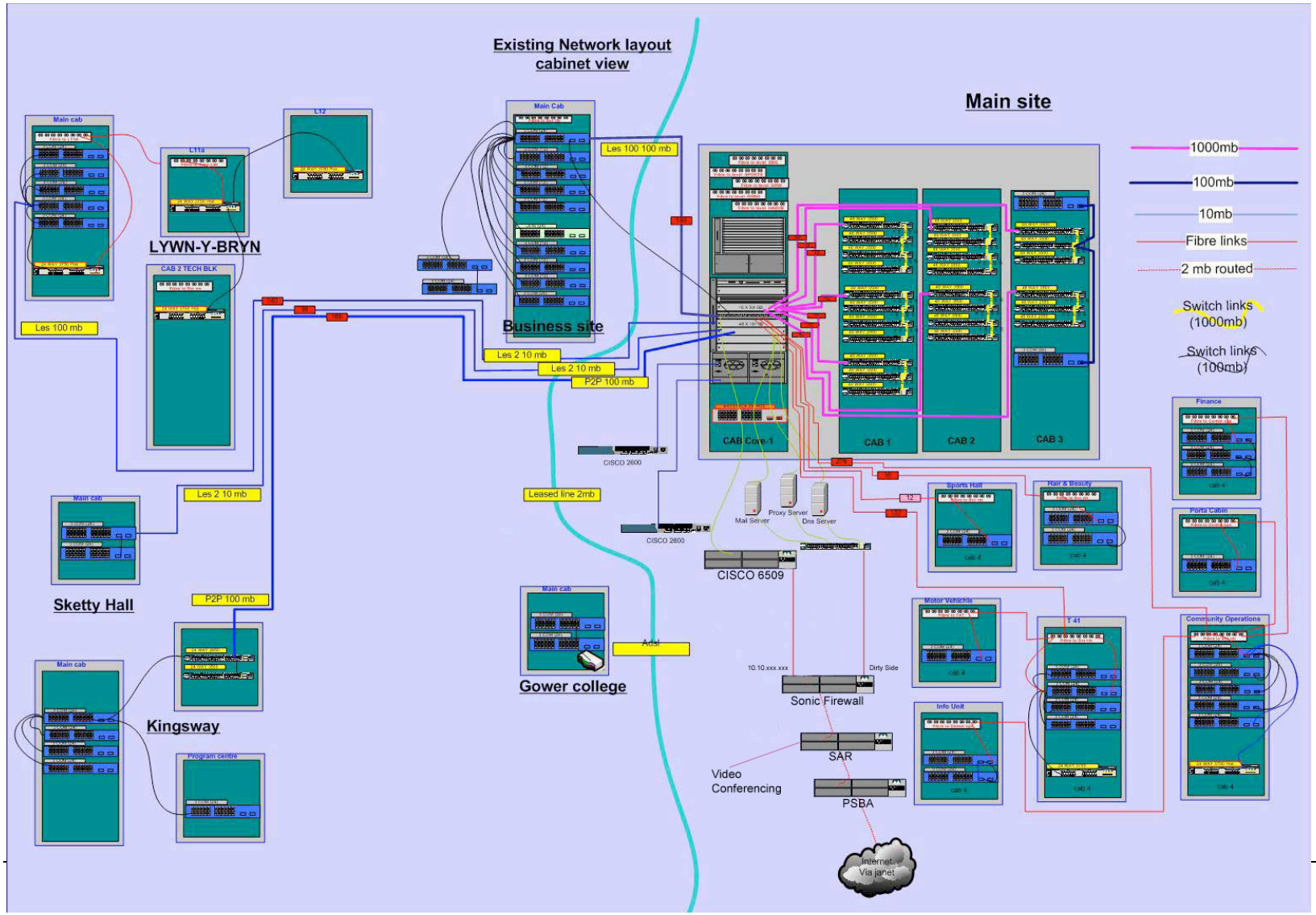
**Ports opened and traffic direction**

- 80 Inward / Outward
- 443 Inward / Outward
- 8443 Inward / Outward

We currently do not use VLAN technology but the college is looking to implement this over the next 12 months. Our implementation is expected to have no bearing on this install of Shibboleth.

## Swansea College Network Diagram (Figure 2)



*Active Directory Structure*

The Active Directory structure is relatively simple at Swansea College. However because of its structure there are some users which will not/cannot be authenticated by a single Shibboleth 1.3 install.

To remotely view an Active Directory, you can use JExplorer which is a JAVA based tool (see references for link).

Figure 3 shows a screen capture of the Swansea College Active Directory from JExplorer.

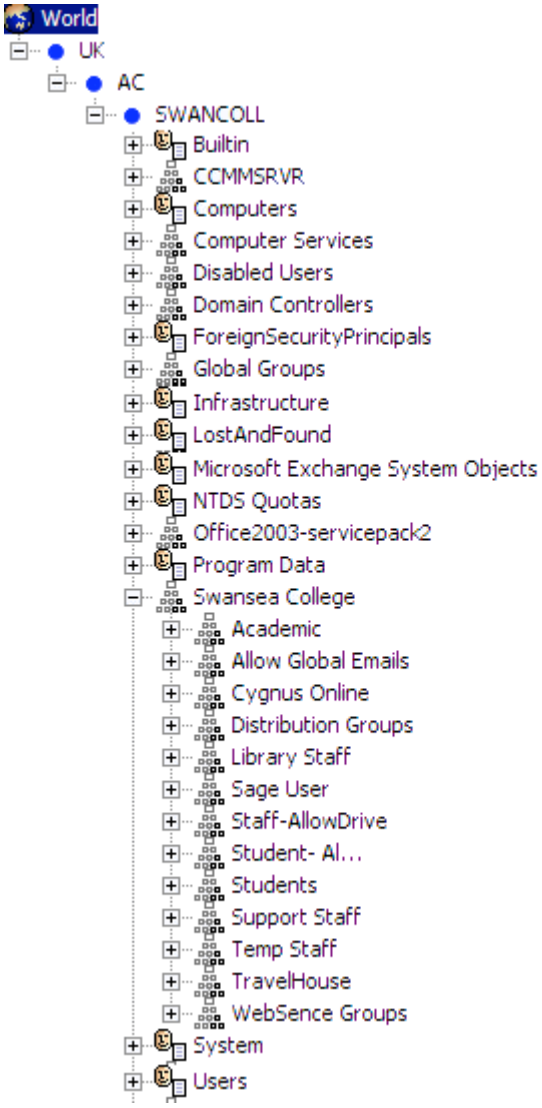



**Figure 3. Swansea College Active Directory.**

An Active Directory is a tree structure, made up of containers and sub containers.

Swansea College stores all user information in a number of these containers or OU (Organisational Unit) for short. 99% of the users are held in the Swansea College OU. Within it are a number of sub OUs, i.e. Academic, Library Staff and Students.

At Swansea College there is a small amount of user information also held in the Computer Services OU.

Shibboleth can currently only point to a single OU to start its authentication and attribute search. It will traverse down the tree structure from this point.

Therefore if we set Swansea College as our search start point, any users in the Computer Services OU will not be found.

If we look at the resolver.xml, you will see the following tag which determines the provider information (OU to search from)

```
<Property name="java.naming.provider.url"
value="ldap://10.10.1.100:389/ou=Swansea%20College,dc=SWANCOLL,dc=AC,dc=UK" />
```

You will also find the following setting in the same file:

```
<Controls searchScope="SUBTREE_SCOPE"
```

This setting informs Shibboleth to allow searching through the sub tree elements as described above.

*Active Directory Suggestions*
As explained above, users should (if possible) all be contained within a single OU, and then broken down into sub OUs within an Active Directory Structure.

OU Structure change is possible but this can cause problems with Group Based Policy set by your IT Administrators.

You should password protect your Active Directory allowing Read Only permissions to the users defined in the resolver.xml file.

*Configuration Settings for UK Access Management Federation*
The appendix shows settings contained in the following files which are used by our Shibboleth installation to work with the UK Access Management Federation

- idp.xml
- resolver.xml
- metadata.xml

*Experience with the Installer*
The Windows Installer has been run on multiple occasions and it has been found to be very reliable. It is very simple to use and it is very quick.

The installer has been tried on both Apache and IIS web servers and it seems to be reliable running on either.

It basically does what it says on the box!

*Time to complete install*
Using the documentation on the wiki, the install was completed within 3 hours, i.e. it was up and running; connected to Shibtest and authenticating against our live Active Directory.

*Problems and Suggestions*
The only problem discovered was that the 'incorrect username and password' file did not work and a blank page was displayed instead. This can be easily repaired but it is suggested that this is fixed prior to release.

Another suggestion; why not include the LDAP .jar file and an example Active Directory Connector in the Tomcat configuration on installation? This would save much time and reduce the amount of understanding needed to complete an install. Most people who will use this installer will most likely use an Active Directory connector for authentication.

*Shibboleth Technical Difficulties*
Getting port 8442 opened on our Windows ISA server was not a feasible option. There were both technical plus security issues that were raised.

By default, you get an error if using https:// through any port other than 443 and 8443 using ISA server.

Our technical support team suggested that it was better to use port 443 instead of 8442 for the SSL traffic and therefore reducing the number of ports we needed to open up.

To get round this problem all references to port 8442 were removed in the Shibboleth configuration files.

This does seem to be a route which many organisations have taken and is worth looking at if you have problems with getting the default 8442 port opened.

*Service Providers*
The switchover from ATHENS to Shibboleth does seem to be successful and many organisations have implemented Shibboleth IdP servers.

However, on the other side of the coin many of the Service providers seem to be struggling to implement the Shibboleth SP services.

## Recommendations

The installer massively reduces the amount of time effort and knowledge that is needed to install the Shibboleth IdP service.

However, the actual installation process is probably at best 80% of the complete task for most organisations.

*Security*
Security is a major consideration for each organisation and each will have different issues and nuances.

There will be firewalls that require holes allowed for Shibboleth to work. Proxy servers (ISA) need configuring to allow access to port 8442 in particular. ***Please read Shibboleth Technical Difficulties for more information.***

Restrict access to the Active Directory. Consider restricting access to the Tomcat manager.

*Active Directory Structure*
Shibboleth needs to start searching from a single OU in the Active Directory. Some organisations may have users in a structure that will not allow for nested searching ***(please see Active Directory Section above for more detail)***

Multiple shibboleth installations or Active Directory restructuring may be required to solve some of these issues.

*SSL Certificates*
One of the most notable difficulties with previous installs of Shibboleth IdP (prior to the Shibboleth installer) was the use of SSL certificates. MATU suggested that we used IIS to secure Shibboleth and used the IIS certificate creation wizard to create a certificate request.

However, a great deal of effort was consequently spent getting all the Windows 2003 servers within the federation to trust the certificates for each server. OPENSSL had to be used to create a suitable certificate and key from the exported IIS SSL Certificate.

The Shibboleth installer takes much of the pain out of this process.

*SSO (Single Sign On) and the User Experience*
Although far more technically advanced, from a user's perspective Shibboleth 1.3 may be a step backward from AthensDA. With AthensDA the user was seamlessly authenticated via IWA (Integrated Windows Authentication) from within the college network and forwarded onto the resources.

With Shibboleth 1.3 the user will be required to login for a second time (firstly with a Windows user logon) and also select the organisation via a WAYF.

The process therefore creates two extra steps to get to a resource which is detrimental to the user experience.

It is possible to default the WAYF to the selected organisation within the college which will help.

It is also hoped that Shibboleth 2.0 will as expected allow us to bypass the login screen for users already known and authenticated to the network.

## References

Swansea College
http://www.swancoll.ac.uk

JANET
http://www.ja.net

JISC UK Federated Access Management
http://www.jisc.ac.uk/federation/

Internet2
http://shibboleth.internet2.edu/

The UK Access Management Federation for Education and Research
http://www.ukfederation.org.uk

JISCmail – Shibboleth
http://www.jiscmail.ac.uk/cgi-bin/webadmin?A0=JISC-SHIBBOLETH

SWITCH AAI
http://www.switch.ch/aai/

TestShib
http://www.testshib.org/

JXPlorer
http://www.jxplorer.org/

## Appendix 1: Configuration Settings for UK Access Management

### Idp.xml

This is the generic configuration file for the Shibboleth IDP service. If you use the quick installer then there are not many / any changes you will need to make here.

#### IdPConfig

```
<IdPConfig

        xmlns="urn:mace:shibboleth:idp:config:1.0"
        xmlns:cred="urn:mace:shibboleth:credentials:1.0"
        xmlns:name="urn:mace:shibboleth:namemapper:1.0"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:mace:shibboleth:idp:config:1.0 ../schemas/shibboleth-idpconfig-1.0.xsd"
        AAUrl="https://$IDP_ADDR:8443/shibboleth-idp/AA"
        resolverConfig="file:/C:/Program%20Files/Internet2/idp//etc/resolver.xml"
        defaultRelyingParty="urn:mace:shibboleth:examples"
        providerId="https://shib.swancoll.ac.uk/shibboleth">
```

The only tag you are likely to amend here is the tag that defines the location and name of the resolver file:

```
        resolverConfig="file:/C:/Program%20Files/Internet2/idp//etc/resolver.xml"
```

#### Logging

```
<Logging>
        <ErrorLog level="DEBUG" location=" file:/C:/Program%20Files/Internet2/idp//logs/shib-error.log" />
        <TransactionLog level="DEBUG" location="file:/C:/Program%20Files/Internet2/idp//logs/shib-
access.log/>
</Logging>
```

The logging tag defines the level and location of the logs. The suggested level whilst in the testing phase is DEBUG, but INFO is sufficient after test phase complete. The DEBUG option does create very detailed information regarding the process and consequently large log files can be created.

**Credentials**

```
<Credentials xmlns="urn:mace:shibboleth:credentials:1.0">
        <FileResolver Id="example_cred">
                <Key>
                <Path>file:/C:/Program%20Files/Internet2/idp/etc/shib.swancoll.ac.uk.key</Path>
                </Key>
                <Certificate>
                <Path>file:/C:/Program%20Files/Internet2/idp/etc/shib.swancoll.ac.uk.crt</Path>
        </Certificate>
        </FileResolver>
</Credentials>
```

The credential tag defines the location of the certificates to be used to encrypt data being sent between the IdP and SP servers.

**MetadataProvider**

```
        <MetadataProvider type="edu.internet2.middleware.shibboleth.metadata.provider.XMLMetadata"
          uri="file:/C:/Program%20Files/Internet2/idp/etc/UKmetadata.xml"/>
```

The metadata tag determines the metadata file to be used. The uri is the setting that you are most likely to change. The full path should be entered here. Details of the metadata file can be found further into this document.

## Resolver.xml

This file determines where attributes are located and which attributes can be retrieved. It is possible to use multiple sources, i.e. Databases and LDAP Implementations.

The example below is a LDAP connection example. This connects to our sample Active Directory (Microsoft's implementation of LDAP)

```
<JNDIDirectoryDataConnector id="directory">
                <Search filter="sAMAccountName=%PRINCIPAL%">
                        <Controls searchScope="SUBTREE_SCOPE" returningObjects="true" />
                </Search>
                <Property name="java.naming.factory.initial" value="com.sun.jndi.ldap.LdapCtxFactory" />
                <Property name="java.naming.provider.url"
value="ldap://10.10.1.99:389/ou=Swansea%20College,dc=SWANCOLL,dc=AC,dc=UK" />
                <Property name="java.naming.security.principal"
value="cn=ouruser,cn=Users,dc=SWANCOLL,dc=AC,dc=UK" />
                <Property name="java.naming.security.credentials" value="ourpassword" />
</JNDIDirectoryDataConnector>
```

Key elements are:

**<Search filter="sAMAccountName" …..**

sAMAccountName is used by Microsoft's implementation of LDAP to store the username. Other implementations may use different elements.

**<Controls searchScope="SUBTREE_SCOPE" />**

By selecting SUBTREE_SCOPE all accounts in sub containers will be included in the search, i.e. for example if you had nested containers Staff and Students within a container CollegeUsers, you could point the provider.url at CollegeUsers and entries in CollegeUsers, Staff and Students would all be searched. This can be very useful!

**<Property name="java.naming.provider.url" ……**
This is the provider address. This is the IP address of the server that holds your Active Directory. Usually port 389 is used. The full address of the root OU follows. Please note %20 is used instead of a space.

**<Property name="java.naming.security.principal" ……**
This contains the location of the user with permissions to query the Active Directory. Remember that you must give this user the adequate permissions. This is the full name as can be seen from the example above.

**<Property name="java.naming.security.credentials" …….**
This contains the password of the user defined above.

Attributes that are allowed to be released are also defined in the resolver:

```
<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:sAMAccountName">
        <DataConnectorDependency requires="directory"/>
</SimpleAttributeDefinition>
```

The above example allows the sAMAccountName to be used in conjunction with the ARP file in making this information available to the service providers (SPs).

Also note that the above states that this information should come from "directory" which is the Active Directory definition above.

We could have multiple sources of data, i.e. the username coming from LDAP and other information coming from a Database (i.e. course enrolments).

The resolver can be as simple or complex as you like.

Note that the ARP restricts which Services (SPs) can access the different information sources.

## Metadata.xml

*The metadata file contains details of all the other service provider and identity providers within the federation.*

*These are usually supplied to you when you join a federation, i.e. testshib so you shouldn't need to amend anything in here.*

*The metadata.xml file is generally made up of EntityDescriptors. There is one format for each IdP and a slightly differing format for the SPs.*

*Here is the entry for the Swansea College IdP server within the UK Access Management Federation:*

```
<EntityDescriptor ID="uk000366" entityID="https://shib-idp.swancoll.ac.uk/shibboleth">
   <!--
      This is an IdP for Swansea College.
   -->
   <Extensions>
```

```
      <shibmeta:Scope xmlns:shibmeta="urn:mace:shibboleth:metadata:1.0"
regexp="false">swancoll.ac.uk</shibmeta:Scope>
      <AccountableUsers xmlns="http://ukfederation.org.uk/2006/11/label"></AccountableUsers>
      <UKFederationMember xmlns="http://ukfederation.org.uk/2006/11/label"></UKFederationMember>
   </Extensions>
   <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
urn:mace:shibboleth:1.0">
      <Extensions>
         <shibmeta:Scope xmlns:shibmeta="urn:mace:shibboleth:metadata:1.0"
regexp="false">swancoll.ac.uk</shibmeta:Scope>
      </Extensions>
      <KeyDescriptor use="signing">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:KeyName>shib-idp.swancoll.ac.uk</ds:KeyName>
         </ds:KeyInfo>
      </KeyDescriptor>
      <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
Location="https://shib-idp.swancoll.ac.uk/shibboleth-idp/Artifact" index="1"></ArtifactResolutionService>
      <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
      <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="https://shib-
idp.swancoll.ac.uk/shibboleth-idp/SSO"></SingleSignOnService>
   </IDPSSODescriptor>
   <AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
      <Extensions>
         <shibmeta:Scope xmlns:shibmeta="urn:mace:shibboleth:metadata:1.0"
regexp="false">swancoll.ac.uk</shibmeta:Scope>
      </Extensions>
      <KeyDescriptor use="signing">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:KeyName>shib-idp.swancoll.ac.uk</ds:KeyName>
         </ds:KeyInfo>
      </KeyDescriptor>
      <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
Location="https://shib-idp.swancoll.ac.uk/shibboleth-idp/AA"></AttributeService>
      <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
   </AttributeAuthorityDescriptor>
   <Organization>
      <OrganizationName xml:lang="en">Swansea College</OrganizationName>
      <OrganizationDisplayName xml:lang="en">Swansea College</OrganizationDisplayName>
      <OrganizationURL xml:lang="en">http://www.swancoll.ac.uk/</OrganizationURL>
   </Organization>
   <ContactPerson contactType="support">
      <GivenName>IT Helpdesk</GivenName>
      <EmailAddress>mailto:helpdesk@swancoll.ac.uk</EmailAddress>
   </ContactPerson>
</EntityDescriptor>
```

*The completed document contains hundreds of such entries and is approximately 1.8Mbytes in size. The metadata file is supplied by the federation upon being accepted into it.*

*The XML entry above contains identification information of the specific IdP server and also includes contact details for the organisation.*

## Appendix 2: Project Team

***Christopher Simpson (Project Manager)***
*Integrated Systems Manager*
*Relatively experienced with Shibboleth prior to the project. Successfully set up a federation for the SALIERI project 2005-2007, consisting of 3 IdP servers plus 3 SP servers on an IIS/Windows 2003 platform to share resources between the 2 colleges plus all the sixth form schools across Swansea.* Email: c.simpson@swancoll.ac.uk

***Ian Stewart***
*Computer Services Manager*
*Little direct experience of Shibboleth before the project started other than understanding of the Active Directory, Security and Certificate requirements gained through the SALIERI project.*

***Henry Ablade***
*IT Technical Support Team Member*
*No experience of Shibboleth before the project started. Background includes specific experience of the Apache web server on Linux and also general IT.*