BIRKENHEAD SIXTH·FORM·COLLEGE

High Quality Education For All

Computer Services Documentation

Shibboleth Implementation

{Initial Shibboleth 1.3 IdP and subsequent Shibboleth 2.1.2 IdP installation}

John Paul Szkudlapski

June 2009

Shibboleth Implementation
Birkenhead Sixth Form College
John Paul Szkudlapski - June 2009
johns@bsfc.ac.uk
Copyright (c) Birkenhead Sixth Form College 2009

Shibboleth Implementation
Birkenhead Sixth Form College
John Paul Szkudlapski - June 2009
johns@bsfc.ac.uk
Copyright (c) Birkenhead Sixth Form College 2009

Background Information

The college has been running a Shibboleth IdP since December 2008.

The move to Shibboleth was primarily seen as the best way to replace our Athens service and save the college the Athens yearly fee. The move was also proposed and supported by the Computer Services Manager, Colin Hawksworth, who is always looking to adopt new technologies that will benefit both staff and students. Personally Colin gives me a lot of encouragement and support when I propose projects to implement at the college.

We received a substantial amount of assistance from the SDSS team based in the University of Edinburgh. I mainly dealt with Rod Widdowson, but have equally received the same level of service, support and customer service from the other members of the SDSS team.

The SDSS team provide technical support to JANET(UK) in their operation of the UK Access Management Federation for Education and Research).Without the help of Rod and the fellow members of the SDSS team, I am convinced it would have taken far, far longer to implement Shibboleth at Birkenhead Sixth Form College.

After completion of our Shibboleth 1.3 IdP I received an e-mail from Rod:

"You were easily the fastest quick install that I have helped through to conclusion and I have to congratulate you on that."

So since January 2009 we have been contacting all of our E-Resources Providers to tell them that we are switching over to Shibboleth from 1st July 2009 and that the Athens service will be retired.

Shibboleth 1.3 Technical Brief

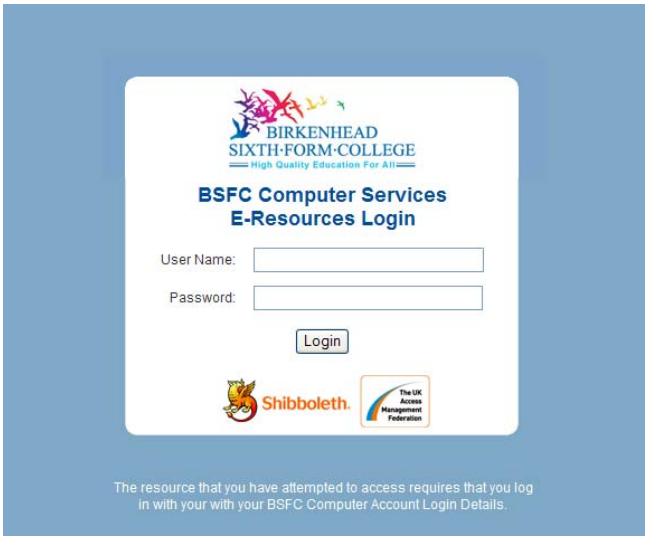
Our Shibboleth 1.3 IdP is based on the Windows Quick Installer developed at SDSS by Rod Widdowson under JISC funding and made available via Internet2.

We have configured our IdP to allow authentication to be performed via our Windows Active Directory Domain – this was a major plus point for the college, as it removed the need for a separate username and password (as per our Athens install).

The IdP configuration files were altered, so that they contained a read-only username to our domain – this allowed the IdP to do lookups based on our domain and authenticate the user if they are a member of our domain (bsfcdomain.bsfc.ac.uk).

Copyright (c) Birkenhead Sixth Form College 2009

We also created a customised login screen which looks like this:



Technically the IdP runs on a Windows 2003 RC2 server, which is actually a Virtual Server on our Virtualized Server Platform (MS Virtual Server 2005). The system specification for the "Virtual Server" is:

Dual Quad Core 2.49Ghz Xeon Processors
2GB RAM {Virtualization Server has 16GB Ram}
80GB Hard Drive {Virtualization Server has 1TB HDD (Raid1) }
1 x Virtual Network Card {LAN }
1 x Virtual Network Card { WAN }
{ Virtualization Server has 2 x 1GB NIC's }

Reporting / Progression

The only downside to moving from Athens over to Shibboleth is the reporting options. Athens has a lot of features enabling the production of stats and reports based on activity – Shibboleth only provides the information in a raw log file.

At the time of writing (June 2009) we (I & John Sparrow – our software developer) are currently discussing a project to create our own reporting system for Shibboleth.

What we intend to do is to either:

a) pull the Shibboleth Log files into Microsoft SQL Server and then produce pages, reports and queries based on the Shibboleth Log Files
b) get Tomcat to talk to SQL server so we can use the built in logging system

This is just in the discussion stage but it's something that we will accomplish.

Copyright (c) Birkenhead Sixth Form College 2009

Shibboleth 2 – Background Information

In March 2009, Rod Widdowson approached me to test out a new Windows IdP installer based on Shibboleth 2 IdP. At the time I was unable to proceed due to various factors, but had recently found the time (and the need) to get it up and running.

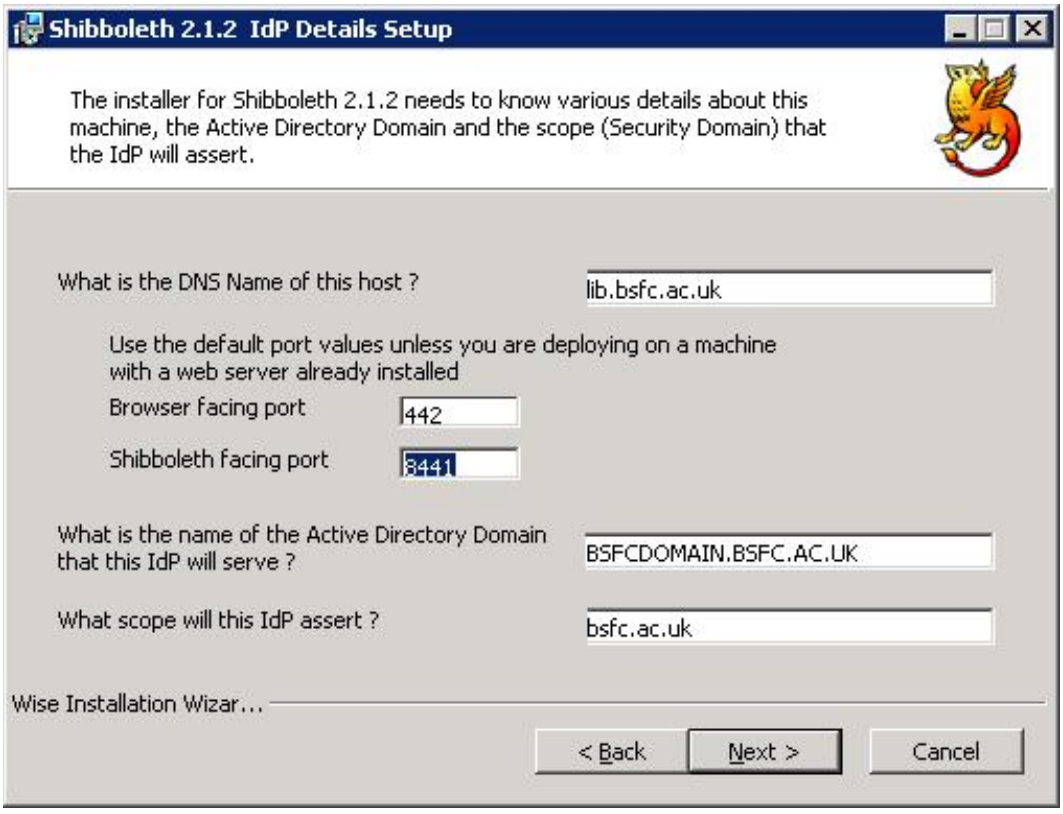
The college is looking at moving its student e-mail provision from being hosted in-house to being hosted on the Google Apps Service. Unfortunately the Google Apps service cannot sync passwords between Active Directory and Google Apps, so the only way around it is to use SSO. We were advised that Google Apps does not work with Shibboleth 1.3 and the only way to overcome our problem was to migrate to version 2.x of the Shibboleth IdP. { I have discussed Google Apps Integration near the end of this document }

Shibboleth 2 – Implementation

I contacted Rod Widdowson to ascertain the status of the vsn 2.x IdP installer and if I could implement it at Birkenhead Sixth Form College and continue to test and provide feedback for him.

Rod advised that I should download the latest version (version alpha-5) and install it alongside our existing 1.3 IdP. This installer uses version 2.1.2 of the Shibboleth IdP with a security patch added.

Because the server we were going to use is already running our 1.3 IdP and Microsoft IIS we ran our 2.x Shibboleth using the following ports & settings;



Copyright (c) Birkenhead Sixth Form College 2009

Again, as we already have a Shibboleth installation I wanted to be able to distinguish between the two Tomcat installations, so I created 2 shortcuts inside a Shibboleth folder off the start menu:

Manage 1.3 Tomcat 5 (C:\fam\Internet2\CaptiveTomcat5.5\bin\tomcat5w.exe)
Manage 2.x Tomcat 6 (C:\fam\Internet2\CaptiveTomcat 6.0\bin\tomcat6w.exe)

Also, following Rod's advice I limited the memory on our new 2.1.2 IdP to be 512mb.

Shibboleth 2.1.2 Technical Brief

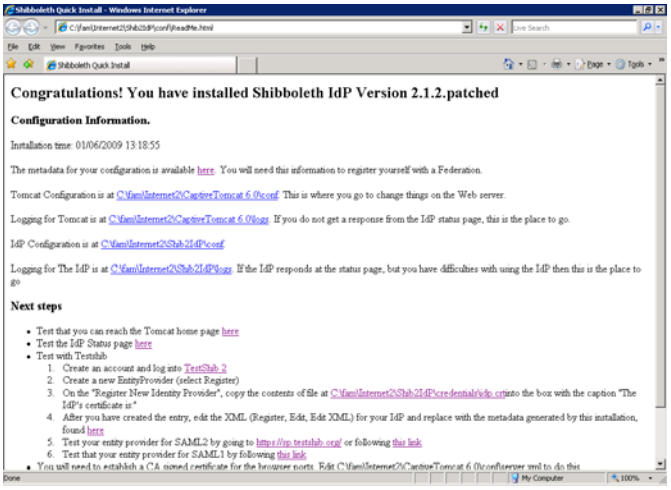
Again our Shibboleth 2.1.2 IdP is based on the Windows Quick Installer developed at SDSS by Rod Widdowson under JISC funding and made available via Internet2.

As with our existing Shibboleth 1.3 IdP it will be configured to allow authentication to be performed via our Windows Active Directory Domain

With this Shibboleth 2.1.2 installer you no longer have to edit the configuration to set the %ldapuser% because it asks you for the username and password during installation, so I entered the same username and password for our existing 1.3 IdP, which is a read-only username on our domain – this allowed the IdP to do lookups based on our domain and authenticate the user if they are a member of our domain (bsfcdomain.bsfc.ac.uk).

Getting Shibboleth 2.1.2 to Run @ BSFC

After the installer completed I was rewarded with this page;

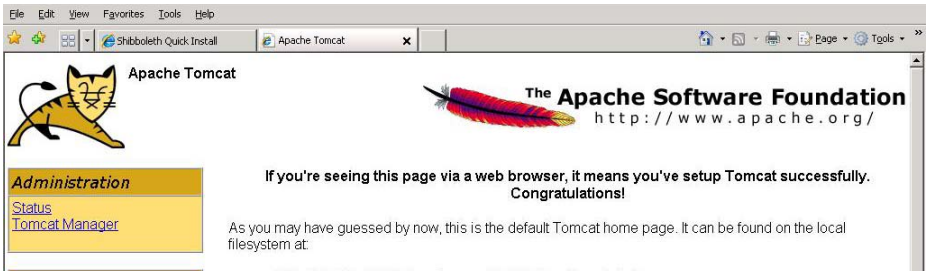


Detailing what had to be accomplished next;

- **Test that you can reach the Tomcat home page here**

I could successfully reach the Tomcat home page

Copyright (c) Birkenhead Sixth Form College 2009



- **Test the IdP Status page here**

  I could successfully test the IdP Status Page – it displayed "ok" in a web page.

- **Test with Testshib**
  - **Create an account and log into *TestShib 2***
  - **Create a new Entity Provider (select Register)**
  - **On the "Register New Identity Provider", copy the contents of file at *C:\fam\Internet2\Shib2IdP\credentials\idp*.crt into the box with the caption "The IdP's certificate is:"**
  - **After you have created the entry, edit the XML (Register, Edit, Edit XML) for your IdP and replace with the metadata generated by this installation.**
  - **Test your entity provider for SAML2 by going to *https://sp.testshib.org/***
  - **Test your entity provider for SAML1 by following**

  I could successfully test the IdP against TestShib after I had made the required changes to the XML file.

- **You will need to establish a CA signed certificate for the browser ports. Edit C:\fam\Internet2\CaptiveTomcat 6.0\conf\server.xml to do this**

  Rod's advice was to copy the existing certificate from our 1.3 IdP. I done this, but found that Tomcat failed to restart properly.

  After a conversation with Rod, I had a closer look at the 2.1.2 server.xml file compared to the 1.3 server.xml file

  I decided not to paste the information directly in but manually copy in the settings from our existing 1.3 IdP. I noticed some differences between the 1.3 version and the 2.1.2 version;

The 1.3 IdP server.xml file contained

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8442"
maxHttpHeaderSize="8192"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
disableUploadTimeout="true"
acceptCount="100"
scheme="https"
```


Copyright (c) Birkenhead Sixth Form College 2009

```
secure="true"
clientAuth="false"
sslProtocol="TLS"
keystoreFile="C:\fam\Internet2\\Idp\etc\apps.pfx"
keystorePass="%PASSWORD%"
keystoreType="PKCS12" />

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

The 2.1.2 default IdP server.xml file contained

```
<Connector port="442"
protocol="org.apache.coyote.http11.Http11Protocol"
maxHttpHeaderSize="8192"
maxSpareThreads="75"
scheme="https"
secure="true"
SSLEnabled="true"
sslProtocol="TLS"
keystoreFile="C:/fam/Internet2/Shib2IdP/credentials/idp.jks"
keystorePass="SeCrEt" />

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Once I had seen the differences between the two files, I amended the 2.1.2 server.xml file by replacing the last two lines above with the following three lines:

```
keystoreFile="C:\fam\Internet2\Shib2Idp\Credentials\apps.pfx"
keystorePass="%PASSWORD%"
keystoreType="PKCS12" />
```

Thus the following lines from the 1.3 server.xml file are omitted from the 2.1.2 server xml file:

```
port="8442"
maxThreads="150"
minSpareThreads="25"
enableLookups="false"
disableUploadTimeout="true"
acceptCount="100"
clientAuth="false"
```

But add this line;

```
SSLEnabled="true"
```

Tomcat started normally and I was able to test out testshib from our new 2.1.2 IdP

Authentication via our Active Directory Domain

During testing I noticed that I could not authenticate users outside of the organisational unit which contained our %ldapuser%, after a quick e-mail conversation with Rod, he suggested:

```
Assuming that you are not running a forest, that' correct - the files
you want to look at are

      C:\fam\internet2\shib2idp\config\login.config
      C:\fam\internet2\shib2idp\config\atribute-resolver.xml
```


Copyright (c) Birkenhead Sixth Form College 2009

I altered the “base” statement in the files from:

```
base="CN=Users,DC=bsfcdomain,DC=bsfc,DC=ac,DC=uk"
```

to:

```
base="DC=bsfcdomain,DC=bsfc,DC=ac,DC=uk"
```

but this did not solve the problem, it still only allowed me to authenticate with users that were in the same Organisational Unit as %ldapuser%.

I knew that the %ldapuser% and password were correct as we were using it for our existing 1.3 IdP, even so I ran a few LDAP tests to see if anything came up – the test passed, so after a conversation with Rod he said:

“
Good (ish) news. I have got your issue reproduced in the lab. This is not a quick installer issue - it is something to do with the login connector from VT.

Having said that - I just tried one last thing. Can you give it a whirl (it seems to be OK for me) in login.conf, set the port to be 3268.
”

So in the login.conf file I changed the LDAP port from 389 (the standard LDAP port) to port 3268 (Global Catalog Queries Port)

Copyright (c) Birkenhead Sixth Form College 2009

```
ShibUserPassAuth {
   edu.vt.middleware.ldap.jaas.LdapLoginModule required
      host="BSFCDOMAIN.BSFC.AC.UK"
      port="3268"
      base="DC=bsfcdomain,DC=bsfc,DC=ac,DC=uk"
      serviceCredential="%PASSWORD%"
      userRoleAttribute="samAccountName"
      serviceUser="%ldapuser%@bsfcdomain.bsfc.ac.uk"
      subtreeSearch = "true"
      userField="samAccountName";
```

I also made sure that my attribute-resolver file was still set to use the 389 ldap port

```
      <resolver:DataConnector id="myLDAP" xsi:type="LDAPDirectory"
            xmlns="urn:mace:shibboleth:2.0:resolver:dc"
            ldapURL="ldap://BSFCDOMAIN.BSFC.AC.UK:389"
            baseDN="DC=bsfcdomain,DC=bsfc,DC=ac,DC=uk"
            principal="%LDAPUSER%@bsfcdomain.bsfc.ac.uk"
            principalCredential="%PASSWORD">
      <FilterTemplate>
          <![CDATA[
              (sAMAccountName=$requestContext.principalName)
          ]]>
      </FilterTemplate>

<!–
      We rely on the uniqueness of the objectSid.  But it is binary so we
      must* make it so
-->
       <LDAPProperty name="java.naming.ldap.attributes.binary"
       value="objectSid"/>
<!–
      If we are following from the GC we need thus on
-->
       <LDAPProperty name="java.naming.referral" value="follow"/>

    </resolver:DataConnector>
```

I then stopped Tomact

net stop tomcat6

cleared out the log files from C:\fam\Internet2\Shib2IdP\logs

and restarted Tomat

net start tomcat6

and tried to authenticate via testshib using domain accounts that were not in the same OU (Organisational Unit), which had previously failed – **they worked**

Authentication via our Active Directory Domain

I was now ready to register the IdP in the UK Federation (`http://www.ukfederation.org.uk/content/Documents/Register2IdP`)

I read over the document and prepared an e-mail to the UK Federation Helpdesk (service@ukfederation.org.uk) which contained the information they asked for:

Copyright (c) Birkenhead Sixth Form College 2009

```
##############################
Administrative contact:
Colin Hawksworth
colh@bsfc.ac.uk

Technical contact:
John Paul Szkudlapski
johns@bsfc.ac.uk

Support contact:
Computer Services
Compserv@bsfc.ac.uk

User accountability:
Yes

Security domains:
bsfc.ac.uk

Entity ID:
https://lib.bsfc.ac.uk/idp/shibboleth

Organization display name:
Birkenhead Sixth Form College

Organization URL:
http://www.bsfc.ac.uk

Software:
Shibboleth IdP 2.1.2 - Quickinstall-Alpha5

Visibility:
No
```

With regards to the metadata template, The UK federation help page (`http://www.ukfederation.org.uk/content/Documents/Register2IdP`) suggests that you might need to make changes to the metadata template '*C:\fam\Internet2\Shib2IdP\metadata\idp-metadata.xml* '.

The installer makes these changes for you so long as you so as long as you do not seek to change the entityID or the certificates, you can attach the default.

I submitted the information and then received an e-mail from John Murison @ SDSS:

```
"
Hello John Paul,

I am a member of the SDSS team based in the University of Edinburgh (and a
colleague of Rod's). We provide technical support to JANET(UK) in their
operation of the UK federation, and your IdP registration request was passed
to us.

The content of your IdP registration request appears to be fine.
However, since you are planning to use a long life self-signed certificate, I
need to carry out our 'due diligence' procedure to ensure that the
certificate is really coming from Birkenhead Sixth Form College.
```


Copyright (c) Birkenhead Sixth Form College 2009

I would therefore like to telephone you and ask you to supply the SHA1 fingerprint of the certificate embedded in the metadata which you have supplied. When may I do this?
John
”

I replied to John with a convenient time and prepared the information for when he arrived.

To get the SHA1 fingerprint of the certificate I put the certificate onto my Desktop, then double clicked it (making sure the extension was .crt)

The certificate appeared, click on the Details tab, then I went down to the bottom of the menu and click ‘Thumbprint’ (Microsoft’s name for a fingerprint) and found the list of hexadecimal digits which appear in the lower pane.

After successfully confirming the fingerprint of our certificate, John advised that the IdP would be added to the UK Federation and he would e-mail when complete.

I received an e-mail off John the next day:

”
Hello John Paul,

Your IdP registration update has been accepted and the UK federation metadata was modified accordingly at about 6pm yesterday.

'Birkenhead Sixth Form College (Shib2 - test only)' does not appear in the federation WAYF drop-down menu, because you asked for it to be hidden.

But it does appear in the unfiltered WAYF used, for example, by the first test page references on the federation website at

http://www.ukfederation.org.uk/content/Documents/OperationalInfo

Please get back to the sdss-support@lists.ed.ac.uk if you have any comments or queries.

Regards,

John
”

Google Apps

I now moved onto setting up Google Apps for our students.

I will not document the process of setting up the main Google Apps account and getting it to sync via Active Directory (contact me if you would like to know more on this). I will only document the process of getting Google Apps to authenticate our Users via our 2.1.2 Shibboleth IdP.

Copyright (c) Birkenhead Sixth Form College 2009

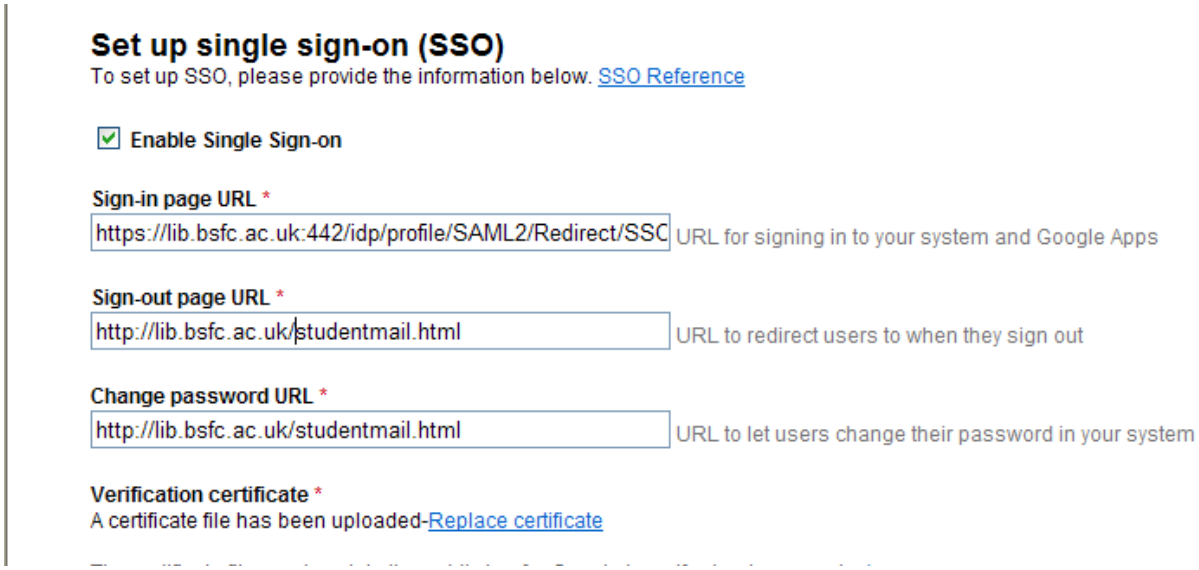
But what I will say is that the reason I am authenticating our students via our Shibboleth IdP is that Google Apps cannot sync the passwords via the Google DirectorySync Utility & Active Directory so you must use a SSO mechanism, in this case I'm using our new 2.1.2 IdP.

Google Apps & Shibboleth Authentication

There is a document on Google's site about setting up SSO & Google Apps, written by:

Will Norris, University of Southern California
(`http://code.google.com/apis/apps/articles/shibboleth2.0.html`)

Following the document I logged into the control panel for our student e-mail at Google Apps and inputted the following information



Sign-in page URL :

`https://lib.bsfc.ac.uk:442/idp/profile/SAML2/Redirect/SSO`

Sign-out page URL :

`http://lib.bsfc.ac.uk/studentmail.html`

A temporary page until the service is live

Change password URL :

`http://lib.bsfc.ac.uk/studentmail.html`

A temporary page until the service is live

Verification Certificate :

I uploaded the .crt file from my C:\fam\Internet2\Shib2IdP\credentials

Then I had to make some changes to files within my IdP. I took backups of the files before hand:

Copyright (c) Birkenhead Sixth Form College 2009

I had to create a new .xml file in the C:\fam\Internet2\Shib2IdP\metadata folder called google-metadata.xml. This contained:

google-metadata.xml

```
      <EntityDescriptor entityID="google.com"
            xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
            format:unspecified</NameIDFormat>
      <AssertionConsumerService index="1"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://www.google.com/a/students.bsfc.ac.uk/acs" />
</SPSSODescriptor>
      </EntityDescriptor>
```

I then made changes to C:\fam\Internet2\Shib2IdP\conf\relying-party.xml, underneath the </DefaultRelyingParty> which were

relying-party.xml

```
<RelyingParty id="google.com"
      provider=https://lib.bsfc.ac.uk/idp/shibboleth
      defaultSigningCredentialRef="IdPCredential">
      <ProfileConfiguration xsi:type="saml:SAML2SSOProfile"
      encryptAssertions="never" encryptNameIds="never" />
</RelyingParty>
```

I then made changes to C:\fam\Internet2\Shib2IdP\conf\attribute-resolver.xml

attribute-resolver.xml

```
<resolver:AttributeDefinition id="principal" xsi:type="PrincipalName"
      xmlns="urn:mace:shibboleth:2.0:resolver:ad">
      <resolver:AttributeEncoder xsi:type="SAML2StringNameID"
      xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
      nameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" />
</resolver:AttributeDefinition>
```

I then made changes to C:\fam\Internet2\Shib2IdP\conf\attribute-filter.xml

Attribute-filter.xml

```
<AttributeFilterPolicy>
      <PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
      value="google.com" />
      <AttributeRule attributeID="principal">
      <PermitValueRule xsi:type="basic:ANY" />
      </AttributeRule>
</AttributeFilterPolicy>
```

I then stopped Tomcat, cleared out the logs and restarted Tomcat.

I then browsed to http://mail.students.bsfc.ac.uk which now redirects to our Shibboleth IdP instead of the Google Login page.

I was able to login successfully as a test user.

Conclusion

Copyright (c) Birkenhead Sixth Form College 2009

We received a substantial amount of assistance from the SDSS team based in the University of Edinburgh. I mainly dealt with Rod Widdowson, but have equally received the same level of service, support and customer service from the other members of the SDSS team. So I would like to offer thanks to the members of the SDSS team – they do a fantastic job.

Also thanks to my boss Colin, for the continued support and encouragement.

We are now going to look at doing a rolling upgrade of our IdP

(http://www.ukfederation.org.uk/content/Documents/RollingIdPUpgrade)

Copyright (c) Birkenhead Sixth Form College 2009