QMShibb - Shibboleth enabling Questionmark Perception

If you are interested in Shibboleth, then you are probably aware of the complex shuttling between the Service Provider (SP) and the Identity Provider (IdP) ultimately leading to a set of attributes emerging from the Service Provider and being presented to the Shibboleth-protected resource. (If this is all new to you, read the excellent introduction in the Educause Quarterly.)

Let's assume that the user has tried to access a Shibboleth-protected resource. She has been intercepted by the SP and sent off to the WAYF which in turn sends her on to the IdP. She authenticates to the the IdP which then sends an authentication assertion to the SP. The SP responds by requesting the user's attributes from the IdP. But what happens when they arrive? Many diagrams of the Shibboleth authentication process simply end at this point with 'access to resource granted'. This may be the case if all that is necessary for access is for certain Shibboleth attributes to be present in the HTTP request. In this case the protected resource doesn't use the values of the attributes. It is enough to know for example that there is an attribute present that indicates that the user is a member of an organization that has paid a subscription for access to the resource.

Shibboleth and e-Learning

Shibboleth as originally developed has a very strong emphasis on protecting the user's privacy and not releasing more information than absolutely necessary. For example, as long as the user or her organization has paid a subscription, there is no need to release her identity to a publisher's website. However, this does not work in the world of e-learning where the protected resource might be a bulletin board or an online assessment system such as Questionmark Perception. Students need to be assessed. How can you assess a student if you don't know who she is? If you are accessing systems such as Questionmark Perception, then the minimum user attributes necessary will be some sort of system-specific identifier (e.g. a username), probably the student's real name and possibly an indication of the groups to which she belongs.

Shibboleth and Questionmark Perception

This means that you can't just put Perception behind a Shibboleth SP and expect it to work. You need another software component, a Resource Manager, that can extract the information from the Shibboleth attributes and pass it on to Perception in a form that it can use. Perception has web service called Questionmark Web Integration Services environment (QMWISe). This allows password-free access to much of Perception's functionality, including account and group creation, presentation of assessments and other administrative functions. As part of the SOCKET JISC eLF project, we have developed a resource manager that will allow Shibboleth attributes to be passed to QMWISe. The resource manager is called QMShibb.

QMShibb

Questionmark Perception is a Windows web application running within Microsoft Internet Information Server (IIS). We are primarily interested in interfacing Perception to our VLE, which uses the Bodington software written in Java. Bodington has the advantage that it has both Shibboleth IdP and Shibboleth SP functionality built-in. QMShibb is a set of Java servlets which run in a servlet container that implements the Java Servlet Specification version 2.3 or above. It can be deployed on the same server as the VLE, the same server as Perception or on a third server. There is no restriction on the domains in which the servers reside, but they should not use HTTP proxies.

The preferred servlet container for QMShibb is Apache Tomcat. This can be installed as a standalone application, or it can be installed within Apache or IIS. In the latter case, it can be installed within the same installation of IIS as that running Perception.

When QMShibb is installed behind a Shibboleth SP, it expects to find the following attributes in the HTTP request headers:

> An attribute containing the user's principalName. This will usually take the form of a site-qualified username e.g. username@mysite.myuni.ac.uk This attribute is required and QMShibb will report an error if it is not present.
>
> A single attribute containing the user's real name or a pair of attributes containing the first and last names. If there is no name attribute, the user will be given the default name 'Anonymous User'
>
> An optional attribute containing a list of the names of groups to which the user belongs. The list separator character can be set in QMShibb's configuration file.

The names of the HTTP headers containing these attributes can be set in the configuration file. The configuration file also contains entries for setting the SOAP security header required by QMWISe. Other entries allow optional automatic participant account creation, automatic addition of the participant to existing groups within Perception, or the automatic creation of groups (with the same names as those in the Shibboleth attribute) and the addition of the participant to them.

Currently, three servlets are provided with QMShibb. These are:

> *getaccessassessment*
> This servlet receives the Shibboleth attributes, carries out optional account/group creation and then redirects to a Perception assessment whose id is specified as a parameter in the request's query string. This servlet is accessed via a URL of the form:
> http://path.to.tomcat/QMShibb/getaccessassessment?assessment=1234567890
> The user is presented with the assessment as if she had logged into the perception.dll
>
> *getaccessassessmentlist*
> This servlet receives the Shibboleth attributes, carries out optional account/group creation and then redirects to the user's list of available Perception assessments. This servlet is accessed via a URL of the form: http://path.to.tomcat/QMShibb/getaccessassessmentlist
> The user is presented with the assessment list as if she had logged into the perception.dll
>
> *getaccessadministrator*
> This servlet receives the Shibboleth attributes of an existing Perception administrator, and redirects to the Perception Enterprise Manager without account or group creation. This servlet is accessed via a URL of the form: http://path.to.tomcat/QMShibb/getaccessadministrator
> The user is presented with the Enterprise Manager as if she had logged into it directly.

Following a conversation with John Kleeman, the Questionmark chairman, we modified the behaviour of the *getaccessassessment* and *getaccessassessmentlist* servlets. Both of these now ensure that the participant is added to the group 'external_shibboleth_users'. In addition, the *getaccessasssesment* servlet checks to see if a schedule exists that links the user to the assessment. If not, then it creates a schedule that allows the user a single attempt at the assessment. For any further use of the assessment by that user a new schedule must be created.

Installing Tomcat with IIS 6.0

Although QMShibb will work on any server running a servlet container, it is convenient to install it into IIS on the same server as that running QuestionMark Perception. Unfortunately, IIS is not a servlet container, so you must install Java and Tomcat, and then optionally install the Jakarta Tomcat Connector. Here's how to do it. We are assuming that you are running Windows Server 2003 and IIS 6.0.

Install Java

Download the Java JDK 1.5 from http://java.sun.com/j2se/1.5.0/download.jsp

Choose a custom installation so that you can specify the installation location. I chose to install in c:\Program Files\Java

When the Java JDK has installed, you need to set a couple of environment variables to ensure that Tomcat will work correctly. Click on the Windows Start button at the bottom left of your screen. Select Control Panel. In the Control panel, select System. This will bring up the System Properties dialog. Click on the Advanced tab and then on the Environment Variables button. Create a variable called JAVA_HOME and give it the value of the directory where you installed Java - in my case this is c:\Program Files\Java. Create another environment variable called CATALINA_HOME and give it the value c:\Program Files\Tomcat 5.5 then close the environment variables dialog. Back in Control Panel, select the Java item. This will launch the Java Control Panel. Select the Update tab. Make sure that the Check for Updates Automatically box is unchecked. Close the Java Control Panel and the Windows Control Panel.

Install Apache Tomcat

Download the Windows Excutable from http://tomcat.apache.org/download-55.cgi. At the time of writing the current version is 5.5.17.

Run the installer and select a Full Installation.

At the Choose Install Location dialog, enter c:\Program Files\Tomcat 5.5

At the Configuration Options, leave the port as 8080 (assuming you have nothing else running on that port) and change the password to a strong one that you can remember.

At the Java Virtual Machine dialog, enter the path to your Java setup - in my case c:\Program Files\Java

At the final dialog, click on the Finish button. Tomcat is now installed as service that will start automatically.

Install the Jakarta Tomcat Connector

It is not essential to install the Connector as Tomcat and IIS will coexist happily, each serving pages on their respective ports, 8080 and 80. However, it is convenient to arrange for IIS to receive all requests and to pass those for servlets to Tomcat while dealing with all other requests itself. In this case, all requests can address IIS and the users can ignore the issue of ports.

The Apache Tomcat website has a complicated protocol for installing the connector, involving dangerous operations such as editing the registry. Mercifully, this is not necessary as there is a program you can download that handles most of the installation process. Download isapi_redirect.msi from http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/jk-1.2.15/. Run the installer and install the redirector to c:\Program Files\Tomcat 5.5.

Open IIS manager and check that there is a virtual directory called jakarta in the default web site. The virtual directory should point to c:\Program Files\Tomcat 5.5\bin and it should contain the files isapi_redirect.dll and isapi_redirect.properties as well as some others. Check that there is a Web Service Extension called jakarta whose status is Allowed.

Right-click on Default Web Site in the left pane. Select Properties. In the Default Web Site Properties dialog, click on the ISAPI Filters tab. There should be a filter called jakarta, but this step of the installation often fails. If it's not there, click on the Add... button. Give the filter the name jakarta, set the executable as c:\Program Files\Tomcat 5.5\bin\isapi_redirect.dll and then click on OK.

Go to the directory c:\Program Files\Tomcat 5.5\conf and open the file server.xml in a text editor. Locate the line:

```
<Connector port="8009" enableLookups="false" redirectPort="8443" protocol="AJP/1.3"
```

Make sure that this entry is not commented out. Save the file.

Open the file workers.properties in a text editor and edit its contents to the following:

```
worker.list=wlb,jkstatus

worker.ajp13w.type=ajp13
worker.ajp13w.host=localhost
worker.ajp13w.port=8009

worker.wlb.type=lb
worker.wlb.balance_workers=ajp13w

worker.jkstatus.type=status
```

Save the file.

Open the file uriworkers.properties in a text editor and edit its contents to the following:

```
/admin/*=wlb
/manager/*=wlb
/jsp-examples/*=wlb
/servlets-examples/*=wlb
/QMShibb/*=wlb

/jkmanager=jkstatus


Save the file.
```

Now restart Tomcat and IIS. All requests for URLs containing the directories admin, manager, jsp-examples, servlets-examples and QMShibb will now be passed from IIS to Tomcat.

To reiterate: these instructions show how to install Tomcat into the IIS server running Perception, but QMShibb can be installed into Tomcat running on any server - the server running Perception, the server running a Java-based VLE such as Bodington, or an entirely separate server.

Installing, configuring and testing QMShibb

QMShibb is a web application that can be installed and tested in Apache Tomcat. Here's how to do it. I assume that the Questionmark Web Integrated Services environment (QMWISE) is installed on the IIS server running Perception and that Tomcat has been installed.

Setting up Perception and QMWISe for QMShibb

Go to the directory that contains the configuration file for Perception, probably Perception\server, and open the file Perception.ini (or Perceptionv4.ini). Look for these entries in the Enterprise Manager section:

```
Enable exlogin=0

Allow external EM entry =0

Simple EM checksum =0
```

Edit these to:

```
Enable exlogin=1

Allow external EM entry =1

Simple EM checksum =1
```

There may be a section in this file that refers to QMWISe. If so, look for the following entries in that section:

```
SecurityRequire=0
TrustRequire=0
```

Edit these to:

```
SecurityRequire=1
TrustRequire=0
```

Now go to the directory that contains QMWISE, probably Perception\server\qmwise, and open the file Web.config in a text editor. Look for the entries:

```
<add key="SecurityRequire" value="0" />
<add key="TrustRequire" value="0" />
```

Edit these to:

```
<add key="SecurityRequire" value="1" />
<add key="TrustRequire" value="0" />
```

Save the file and use the Enterprise Manager to reset the Perception dlls.

Installing and configuring QMShibb

Download the file QMShibb.war from the SOCKET Sourceforge site.

Put this file in the webapps directory of Tomcat (e.g. c:\Program Files\Tomcat 5.5\webapps). It will be automatically expanded with all of the directory structures and files needed.

Go to the QMShibb WEB-INF directory (e.g. c:\Program Files\Tomcat 5.5\webapps\QMShibb\WEB-INF) and open the file web.xml in a text editor. This file contains the configuration settings for QMShibb. Here is a description of the settings:

```
<context-param>
<param-name>
    security
</param-name>
<param-value>
    1
</param-value>
</context-param>
```

This parameter controls whether or not the QMWISe security header is sent in the SOAP request. You should set this to 1 if the header is to be sent or 0 if not. The recommended setting is 1. This is a required parameter.

```
<context-param>
<param-name>
    ClientID
</param-name>
<param-value>
    Manager
</param-value>
</context-param>
```

This parameter contains the username of a Perception administrator who has at least sufficient privilege to manage the server dlls and configure the server. This parameter is ignored if the security parameter is set to 0.

```
<context-param>
<param-name>
    checksum
</param-name>
<param-value>
    xxxxxx
</param-value>
</context-param>
```

This parameter contains the security checksum. It is an MD5 digest of the concatenation of the username and encrypted password of the administrator whose username is present in the ClientID parameter. See below for a description of how the checksum is obtained. This parameter is ignored if the security parameter is set to 0.

```
<context-param>
<param-name>
    QMWISe-url
</param-name>
<param-value>
  http://.../QMWISe/QMWISe.asmx
</param-value>
</context-param>
```

This parameter contains the URL of the QMWISe web service. This is a required parameter. The value can be obtained by running IIS Manager and then looking for the actual path of the virtual directory qmwise.

```
<context-param>
<param-name>
    test-mode
</param-name>
<param-value>
    1
</param-value>
</context-param>
```

This parameter allows you to put QMShibb into test mode. This allows you to test QMShibb without having to put it behind a Shibboleth Service Provider. When this parameter is set to 1, QMShibb will generate Shibboleth attributes using the information in the following parameters. This parameter should be set to 0 for a production deployment. This is a required parameter.

```
<context-param>
```

```
<param-name>
    test-user
</param-name>
<param-value>
    ADent
</param-value>
</context-param>
```

The username of the fictional user in the Shibboleth attribute to be used in test mode. This parameter is ignored if the test-mode parameter is set to zero.

```
<context-param>
<param-name>
   test-firstname
</param-name>
<param-value>
    Arthur
</param-value>
</context-param>
```

The first name of the fictional user in the Shibboleth attribute to be used in test mode. This parameter is ignored if the test-mode parameter is set to zero.

```
<context-param>
<param-name>
    test-lastname
</param-name>
<param-value>
    Dent
</param-value>
</context-param>
```

The last name of the fictional user in the Shibboleth attribute to be used in test mode. This parameter is ignored if the test-mode parameter is set to zero.

```
<context-param>
<param-name>
    test-groups
</param-name>
<param-value>
  test_group1;test_group2
</param-value>
</context-param>
```

The names of the fictional groups in the Shibboleth attribute used in test mode. This parameter is ignored if the test-mode parameter is set to zero.

```
<context-param>
<param-name>
    create-account
</param-name>
<param-value>
    1
</param-value>
</context-param>
```

When this parameter is set to 1, QMShibb will create a new Perception participant account for the user whose username is present in the Shibboleth header defined below. If the parameter is set to 0, no automatic account creation will occur. This is a required parameter.

```
<context-param>
<param-name>
    join-existing-groups
</param-name>
<param-value>
    1
</param-value>
</context-param>
```

When this parameter is set to 1, QMShibb will add the user whose username is present in the Shibboleth header defined below to any existing Perception group whose name matches one of the group names present in the Shibboleth header defined below. This parameter is ignored if the create-account parameter is set to 0.

```
<context-param>
<param-name>
    create-groups
</param-name>
<param-value>
    0
</param-value>
</context-param>
```

When this parameter is set to 1, QMShibb will create a Perception group if its name matches one of the group names present in the Shibboleth header defined below and the group does not already exist. It will then add the user whose username is present in the Shibboleth header defined below to the newly-created or existing group. This parameter is ignored if the create-account parameter is set to 0 or the join-existing-group parameter is set to 1.

```
<context-param>
<param-name>
    username-attribute
</param-name>
<param-value>
 HTTP_..._eduPersonPrincipalName
</param-value>
</context-param>
```

The name of the Shibboleth attribute carrying the site-qualified username of the user. This is a required parameter. QMShibb will report an error if this Shibboleth header is not present in the HTTP request.

```
<context-param>
<param-name>
    fullname-attribute
</param-name>
<param-value>
   HTTP_..._eduPersonNickname
</param-value>
</context-param>
```

The name of the Shibboleth attribute carrying the full name of the user. This parameter is ignored if the firstname-attribute and lastname-attribute Shibboleth headers described below are both present in the HTTP request. If no Shibboleth header containing name information is present in the HTTP request, QMShibb will give the user the default name Anonymous User.

```
<context-param>
<param-name>
    firstname-attribute
</param-name>
<param-value>
    HTTP_givenName
</param-value>
</context-param>
```

The name of the Shibboleth attribute carrying the first name of the user. This parameter is not required if the full name of the user is delivered in the Shibboleth attribute defined in the fullname-attribute above. If no Shibboleth header containing name information is present in the HTTP request, QMShibb will give the user the default name Anonymous User.

```
<context-param>
<param-name>
    lastname-attribute
</param-name>
<param-value>
    HTTP_sn
</param-value>
</context-param>
```

The name of the Shibboleth attribute carrying the last name of the user. This parameter is not required if the full name of the user is delivered in the Shibboleth attribute defined in the fullname-attribute above. If no Shibboleth header containing name information is present in the HTTP request, QMShibb will give the user the default name Anonymous User.

```
<context-param>
<param-name>
    groups-separator
</param-name>
<param-value>
    ;
</param-value>
</context-param>
```

The names of the groups to which the user belongs are delivered as a list in a single Shibboleth attribute. This parameter is used to define the list separator (e.g. a comma, colon or semicolon).

```
<context-param>
<param-name>
    groups-attribute
</param-name>
<param-value>
  HTTP_urn:bodington:member
</param-value>
</context-param>
```

The name of the Shibboleth attribute carrying the list of groups to which the user belongs. This list will be used to create equivalent groups in Perception if the appropriate parameters are set above.

You need to provide the username of a Perception administrator who has at least sufficient privilege to manage the server dlls and configure the server. Edit the ClientID parameter to that username. You also need to edit the checksum parameter. QMWISe comes with a test harness program that is designed to generate the checksum from the administrator's username and password. At the time of writing, the checksums generated by this program are incorrect. You can contact Questionmark for help with

generating checksums. In the US you can email support@questionmark.com and in the UK you should contact helpdesk@questionmark.co.uk. If you have access to the installation of Microsoft SQL Server that hosts the Perception database, you can generate your own checksum as follows:

Open the SQL Server management application and connect to the server. Select the Perception database and open the Tables item. Select the table whose name ends in User (e.g. dbo.G_User). Right-click on this item and select Open Table. You should be able to locate the username of your chosen administrator in the User Name column. Next to it is the Password column. This contains 16-digit numbers that are the encrypted form of the password. Note the number corresponding to your chosen administrator. Close the SQL Server Management application. Open a web browser and go to http://pajhome.org.uk/crypt/md5/. In the input box type the username of the administrator followed immediately by the encrypted password. If you administrator's username is Admin and the encrypted password is 1234567887654321, then you should type Admin1234567887654321. The input is case-sensitive so make sure that the Caps Lock key on your keyboard is not on and make sure that there is no space between the username and the encrypted password. Now click on the MD5 button. The result is the checksum that you should enter in the checksum parameter in your web.xml file.

Go back to your web.xml file and make sure that the QMWISe-url parameter is correct for your setup. Set the test-mode parameter to 1 and save the web.xml file. Then restart Tomcat.

Testing QMShibb

Open a browser.

If your Tomcat is a standalone installation, go to the URL:

http://path_to_Tomcat:8080/QMShibb/getaccessassessmentlist

If you have installed Tomcat into IIS, go to the URL:

http://path_to_IIS/QMShibb/getaccessassessmentlist

There will be a slight delay while the servlet is instantiated, but then you should be directed to the Perception list of assessments for Arthur Dent. This will probably be empty.

Open the Questionmark Enterprise Manager and look at the lists of Participants and Groups. Arthur Dent should now be one of your Participants and he should be the only member of a group called external_shibboleth_users. You can delete the Participant and the Group if you want to. Close the Enterprise Manager and go back to the directory containing the QMShibb web.xml file. Change the test-mode parameter to 0. Decide on a policy regarding automatic account and group creation and set the parameters appropriately. Save the web.xml file and restart Tomcat.

Shibboleth and QMShibb

Having established that QMShibb is working correctly, you must protect the servlets in the QMShibb directory. The easiest way to do this is to put the QMShibb servlets behind a Guanxi Service Provider Guard. This approach has the advantage that it will work irrespective of the location of Tomcat - on the Perception server, a VLE server or a third server. Alternatively, if you have installed Tomcat into the IIS server running Perception, you can install the Internet2 Service Provider and configure it to protect the QMShibb directory. Whichever method you choose, you will have to make sure that before you try

using QMShibb, your Service Provider has exchanged the appropriate metadata and certificates with the Shibboleth Identity Provider(s) that you are going to use.