

Nabataea – Final report – 1.0 – 30 April 2007



Thames Valley University
London Reading Slough

Project Nabataea: Final Report

Thames Valley University Shibboleth early adopter project

1st January 2006 – 31st March 2007

Author: Sue Wood, Nabataea Project Manager

With contributions from John Wolstenholme, Tiger Wang, Xiao Xu, Yiannis Seglias, and Dimitri Koveos

Table of contents

Acknowledgements	3
Executive summary	4
Background	5
Aims and objectives	6
Methodology	7
Implementation	7
Outputs and results	24
Outcomes	25
Conclusions	26
Implications	26
Recommendations	27
References	28
Appendices	29
Glossary	49

Acknowledgements

The Nabataea project was funded by The Joint Information Systems Committee (JISC) under the second round early adopters element of the Core Middleware Infrastructure Programme.

The project team wishes to acknowledge the funding from JISC and support from MATU (Middleware Assisted Take-up Service), in particular the learning opportunities provided by MATU workshops.

We also wish to thank the following individuals for their technical assistance :

John Paschoud and his team for talking to us about the project at LSE

Richard Annett from MATU for helping us install IdP

John Bond and James Westhoff from Eduserv Athens Local Authentication Support.

Ian Young from UK Access Federation for working with Xiao Xu of TVU in the process of identifying the Bugzilla Bug 620 – see http://bugzilla.internet2.edu/show_bug.cgi?id=620. Also for helping identify problems with Zetoc.

1 Executive summary

The main aim of the project was to provide all members of Thames Valley University with access to electronic information resources via Shibboleth as the next generation method of access management. The project initially set up a test implementation of Shibboleth integrated with a number of in-house test systems. This allowed us to understand the technology and how it integrates with our systems, whilst simultaneously testing federation access as a replacement for Athens. As part of this process we have designed and implemented a robust and flexible system to provide and update the necessary attributes to comply with our electronic resource licences.

We launched trial access to approximately 930 users in November 2006.

Following the initial trial phase, we extended the testing to a pre-production environment and we now have a successful implementation of Shibboleth integrated with live in-house systems running on two pre-production servers. The pre-production service providing access to resources using the Shibboleth/Athens gateway, and direct authentication to Shibbolised resources was launched for all students under the name of TVU e-Direct on 8/3/07. Through this service students have access via Shibboleth to 29 suppliers and 67 individual resources. A technical solution to allow staff access to TVU e-Direct is now in place and will be rolled out shortly.

Adjustments are still being made to the Shibboleth configuration, and access via Athens will continue until this process has stabilised. We are now at the stage where we are starting to consider the steps necessary for a smooth migration over from Athens to exclusive use of Shibboleth. We will be setting up the Shibboleth production servers during the summer of 2007. We anticipate that TVU will be ready to replace Athens authentication with Shibboleth technology as from autumn 2007. As part of this process we are setting up load balancing to ensure high availability and fast performance. The project demonstrates that Shibboleth can be implemented successfully at a very large institution with over 40,000 students, including provision for FE, HE and distance learners, and with a starting point of a number of separate legacy databases.

2 Background

Thames Valley University (TVU) is a very large educational institution based at three main sites: Ealing, Slough and Reading. TVU has over 40,000 students, including many distance and part-time students. Both further and higher education programmes are offered and considerable emphasis is placed upon widening participation and promoting progression from further to higher education. The University merged with Reading College and School of Arts and Design on 1st January 2004.

The university has a converged IT and Library service under the umbrella of Learning and Information Services (LIS). Two of the major challenges that faced LIS-IT following the merger were the different systems used in the two institutions as well as the requirement to extend the availability of information systems to all three campuses. As with most UK universities, identity management at TVU was fragmented with loosely-connected systems in place that reflected the independence of academic units (faculties, schools or departments). As part of the drive to address the challenges, steps were taken to optimise and harmonise user accounts with the ultimate aim of achieving a Single-Sign-On infrastructure. Microsoft's Active Directory was chosen to be the single authentication source for all staff and students. This is significant in the context of the Nabataea project since the key to a successful Shibboleth implementation is a unified directory against which LDAP queries will be executed.

At the time of the JISC call for bids under the second round early adopters element of the Core Middleware Infrastructure Programme, SSO was becoming an increasingly high priority. Alongside the need to improve usage of information systems, there was simultaneously a drive from Learning and Research Support (LRS) to provide SSO in order to simplify access to electronic information resources. Since the merger, LRS have created and maintained personal Athens usernames and passwords for all students by carrying out regular bulk uploads of data taken from the student records database. The Athens login details are then emailed automatically to student accounts. However, many students do not access their TVU student email and therefore do not receive the Athens account details. There have been particular issues for distance learners, as their email accounts require initialisation before they can access the message from Athens. There was a need to simplify the system for distance learners in order to make the process

clearer for both students and their tutors. Students also frequently forget their Athens details, requiring an ongoing process of resetting passwords. Staff use the process of self-registration to create their own Athens accounts and therefore provision of access has been incomplete. Together all these aspects have given rise to a significant administrative workload. LRS recognised in Shibboleth technology a solution that would reduce the amount of administrative effort and the number of passwords in use whilst improving security and ease of access.

Project Nabataea was seen as an opportunity to provide the technology and development environment to bring both these strands together and carry them forward. The Nabataea project bid was submitted as an LIS initiative and the project was carried out within the department by Learning and Research Support (LRS) and Corporate Systems Group (CSG) working in collaboration.

3 Aims and objectives

The aims and objectives agreed at the start of the project were as follows:

1. To provide authenticated access to internal systems and Shibboleth Federations by setting up and using Shibboleth technology
2. By using Eduserv's Shibboleth-Athens Gateway, to provide access to Athens resources through the single sign-on process
3. To simplify and increase the usage of key systems such as the Blackboard VLE and the Personal Development Plan system
4. To identify other systems that could be accessed through the single sign-on capability
5. To extend the access of online resources (*through Shibboleth*) to the whole of the TVU student and staff population, while putting in place fine-grained controls to these resources through the use of user attributes.

4 Methodology

The project was planned at the outset by identifying the necessary stages in the high level plan and estimating the timeframes. The initial research phase was followed by a re-working of the original high level plan to take account of our increased understanding of requirements.

We used an approach that would allow us to research, understand and test one step at a time. We decided to implement Shibboleth by first setting up a test environment which would allow us to gain confidence in our technical abilities while giving us the opportunity to increase our knowledge base. It was also a good opportunity to finalise our thoughts around how the authentication and authorisation elements would be implemented and work. Only once we were happy with our knowledge did we set-up the trial environment.

The trial environment allowed us to test out access to Shibboleth-Athens Gateway and Shibbolised resources through user feedback and testing by the project team. Specific checks were made to ensure that the service functioned correctly in relation to all aspects, including control of access to appropriate users, account security, sessions behaviour, recording of statistics, and function of each resource. This environment could then be turned into a live pre-production set-up with minimum changes (e.g. by changing the LDAP settings to use a live Directory).

Throughout the project the team met on a frequent basis and all discussions and decisions were recorded to ensure good communication and commitment to agreed actions and responsibilities.

5 Implementation

Throughout the project we were operating in a test environment with three distinct phases:

- Phase 1 – Initial test environment with test users
- Phase 2 – Pilot launched to 930 users

- Phase 3 – Pre-production implementation launched to all students

At the same time development was undertaken to re-design and tailor TVU directory services to provide a Shibboleth compliant identity management environment. This is discussed below in section 5.4 .

5.1 Phase 1 Initial test environment

The project began with a learning phase during which we investigated work carried out by other early adopter projects, including a visit to LSE to speak to John Paschoud and the LSE Shibboleth project team. Various members of the Nabataea team went on introductory courses run by the Middleware Assisted Take-Up Service (MATU). We found that it was quite difficult to catch up with the technical discussions and other issues being raised on the JISC-SHIBBOLETH discussion list. The terminology could be quite impenetrable especially as the discussions often did not provide a context. It took us quite a while to understand the big picture and the general concepts, and to sort out various confusions about federations (e.g. whether we needed to join the Athens Federation as well as the SDSS Federation), Shibboleth-Athens versus Athens-Shibboleth gateways, EduPerson attributes etc.

The initial test phase began for real with the installation of Shibboleth Identity Provider software (IdP) on a Windows server using Shib IdP version 1.3, Apache 2.2.3 and Tomcat 5.5:

Dell server
Intel Xeon(TM) CPU 2 x 280 GHz.....4GB RAM
300GB hard drive.....sliced in 3
31meg....12 GB....262 GB
Microsoft windows server 2003 R2
standard edition
service pack 1

The installation of the IdP software went smoothly with no major problems, although during the set up phase we learned a number of important lessons. Some of the issues were obvious, but it is very easy to pay insufficient attention to details or rush with the set-up. For example, as part of the set up we configured idp.xml. This is the main Shibboleth configuration file. It configures the location of other configuration files, the ukfederation-metadata.xml file, the encryption key and certificate and the Tomcat

services. We found that it was essential to use a good XML editor and make sure that the layout was neat and easy to read. It is very easy to make a small mistake which impacts on the syntax of the XML file, thus rendering it unusable. It was very important to ensure that any edits were triple checked for correctness.

As the next step in the set-up process, we joined the InQueue test federation (set up by Internet2 to serve the Shibboleth community as a testbed and learning facility). We used InQueue to carry out the necessary checks on the IdP installation. As a preparatory step we purchased a Verisign Secure Sockets Layer (SSL) certificate Secure Site Pro ready to enable secure authentication and authorisation.

We set up a test Active Directory containing a small number of test users and configured the file http.conf to set up the connection between Shibboleth IdP and our test Active Directory. We then tested to ensure that authentication against the directory using LDAP was working correctly. We experienced two problems during this stage:

- Problem with password protect encryption keys

When we first created our encryptions keys, we password protected them. Unfortunately we found out that Apache on Windows (at least the version we used at the time) did not support password protected keys. After spending some time researching the problem and looking at a number of “solutions” we found one which we used to bypass the problem. The full solution can be found at: http://www.expertsexchange.com/Web/Web_Servers/Apache/Q_20771112.html

Basically the problem is bypassed by placing the following in the ssl.conf file. Obviously the appropriate path and password should be used :

```
SSLPassPhraseDialog "exec:C:/Shib-  
Runtime/Idp/Apache2.2.3/conf/passphrase.bat" and  
passphrase.bat does the following: @echo ourpassword
```

- Problem with LDAP Apache combination:

We found it difficult to get the Apache LDAP combination working properly. This problem was made apparent by Apache complaining about the LDAP syntax in

httpd.conf file and then would not run. The problem was fixed by upgrading to Apache 2.2.3 and then adding the following in httpd.conf:

```
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
```

And

```
<Location /shibboleth-idp/SSO>
    AuthType Basic
    AuthName "Please Login"
    AuthBasicProvider ldap
    AuthLDAPURL
    "ldap://localhost:389/cn=USERS,dc=CSG,dc=TVU,dc=AC,dc=
    UK?sAMAccountName?sub?(objectClass=*)"
    AuthLDAPBindDN
    "CN=UserToConnect,CN=Users,DC=CSG,DC=TVU,DC=AC,DC=UK"
    AuthLDAPBindPassword "APassword"
    AuthzLDAPAuthoritative off
    require valid-user
    SSLRequireSSL
</Location>
```

As can be seen, it is important to use the right mod files, and get the Location exactly right. A side-effect of using Apache 2.2.3 was that we had to use mod_jk instead of mod_jk2 which means that the set-up and workers.properties is slightly different (see Appendix A).

We analysed the staff and student body at TVU in order to identify all the different categories of potential e-resource users at TVU that would be required in order to satisfy our e-resource licences. The LRS E-Strategy Steering Group comprising Subject Librarians, Systems Librarians and members of the Electronic Information team was consulted as part of this process. We observed that Active Directory must be able to supply the required data to establish which attributes should be assigned to each user. There also needs to be a mechanism to update the attributes as an ongoing process.

The next step was to set up a test attribute store to hold details of our pilot users' attributes or roles. We decided to create a separate database of attributes in order to allow for control of access rights by library staff, whilst protecting the security of Active Directory. This would also make it easier to migrate data or to rebuild. Although we tested against both an LDAP store as well as a SQL database, we finally settled for an

attribute stored based on MySQL5.0.16-nt. See Appendix B for details of the entry of a MySQL connector in mysql-resolver.xml to provide database connectivity and the query we use to get the correct attributes for users. The details of TVU's attribute store database, giving tables and fields, can be seen in Appendix C.

We found that there are four key files that are crucial to enable the system to function. These are ldap.xml, ukfederation-metadata.xml, mysql-resolver.xml and arp.site.xml. Once we had established the structure of both the test Active Directory and test Attribute Store it was then necessary to correctly configure these four key files:

Table 1 Shibboleth IdP Configuration files

ldap.xml	This is the main Shibboleth configuration file. It configures the location of other configuration files, the ukfederation-metadata.xml file, the encryption key and certificate and the Tomcat services. (see Appendix D for detail).
ukfederation-metadata.xml	This is the file that provides details of the Service Providers (SPs) in the federation. We obtained this file from the UK access management federation (http://www.ukfederation.org.uk/content/Documents/OperationalInfo). In addition, we have set up a scheduled job to run the command daily to keep the copy of the metadata up to date.
mysql-resolver.xml	This is the attribute resolve configuration. We use a MySQL database to store attributes and used a MySQL connector to provide database connectivity, see Appendix E for detail.
arp.site.xml	This file tells Shibboleth IdP which of the attributes about a user configured in MySQL-resolver.xml can be released to which SP. Each IdP's arp file will be unique, depending on the mix of resources – ours is included in Appendix F

By this stage we had carried out the following:

- Installed and tested IdP using InQueue
- Set up a test Active Directory

Nabataea – Final report – 1.0 – 30 April 2007

- Tested authentication against Active Directory
- Changed the necessary configuration files

We then needed to test SSL communication between the TVU IdP and a Service Provider by setting up and testing links to our electronic information resources. We created a table of all our resources detailing the name of each database, the service provider, whether Shibboleth or Gateway compliant and the current authentication method. Most of our resources were Shibboleth-Athens Gateway compliant therefore we decided to set up our first access via the Gateway.

We established that we would need to join the Athens Federation in order to access resources through the Shibboleth-Athens Gateway. (At this point the UK Access Federation was not in place, and the SDSS Federation only provided access to Shibboleth resources (i.e. resources accessed directly via Shibboleth technology). Athens assigned us with a provider ID, which we then used to construct the appropriate link for each resource. We used the list of short resource codes available in the bulk upload area of the Athens administration site. The links are in the form:

```
http://auth.athensams.net/?ath_dspid=ATHENS&ath_action=shaauth&id=[your origination's assigned provider ID]urn:mace:eduser.v.org.uk:athens:provider:tvu.ac.uk&ath_returnurl=http://auth.athensams.net/tr1/1.0/-/[RES SHORT CODE]
```

An example of the link syntax for Shibboleth-Athens Gateway resources is as follows – in this case for Ovid Online:

```
http://auth.athensams.net/?ath_dspid=ATHENS&ath_action=shaauth&id=urn:mace:eduser.v.org.uk:athens:provider:tvu.ac.uk&ath_returnurl=http://auth.athensams.net/tr1/1.0/-/OVID_ONLINE
```

However, we found that login to ScienceDirect failed despite using the correct URL. This was because ScienceDirect was still authorising our users via our Athens Prefix. This issue was resolved by asking ScienceDirect to authorise our users via our Athens organisationID instead of our prefix tvu.

Previously in Athens we had used permission sets to ensure that resources were restricted to appropriate users. Since permission sets were no longer available to us we

needed to set up an alternative control mechanism within the Shibboleth framework. Our Shibboleth IdP was initially set up to release a single value per attribute. In order to control user access to both default and restricted resources, we needed to be able to release multiple values for the eduPersonEntitle attribute. We changed the relationship between 'member' and 'entitlement' from one-to-one to one-to-many, in order to allow each user to have more than one entitlement. This meant that one user could now have two or more values of entitlement, for example tvu#default and tvu#staff.

A web page of links was created to enable testing by the small number of test users. We used the Athens Federation to test the attribute store setup with satisfactory results.

The initial test set-up allowed us to authenticate users against Active Directory through LDAP and to release appropriate attributes stored on the database. Overall the initial test phase enabled us to understand the technology and how it integrates with our systems, whilst simultaneously testing federation access as a replacement for Athens.

5.2 Phase 2 – Pilot launched to 930 users

Having successfully implemented the test set-up, we now needed a pilot to ensure that users were satisfied with the new service, and to understand performance issues. The University's Active Directory was still under development and not ready to provide authentication for the pilot phase. We therefore decided to select and import additional users into our test Active Directory. We planned to select students on particular courses by taking those with the highest ratio of active Athens users to total numbers of students on a course. This would have tested out the widest range of different subject resources and users. However, problems with availability of information forced us to rethink. We finally identified participants by looking at our top Athens usage statistics across all sites in order to ensure selection of active users of LRS electronic information resources, and from a variety of backgrounds. We selected 1000 users, including FE students and staff with access rights to a restricted access database (Film and Sound Online Medical Restrict), to allow for appropriate testing. We excluded distance learners at this point as there were too many potential support problems.

Nabataea – Final report – 1.0 – 30 April 2007

We set up a web site for the pilot at <http://shibboleth1.tvu.ac.uk/shib/index.htm> (see Appendix G) and the selected pilot users were given the appropriate attributes in the attributes store database. The resources were initially restricted to those available via the Shibboleth-Athens Gateway, i.e. they did not at this point include any resources with direct Shibboleth access. At this point we joined the SDSS Federation in readiness for the next step of setting up and testing direct access to Shibbolised resources, such as Film and Sound Online and Education Image Gallery.

The pilot resources were selected to allow testing of FE/HE/Medical restrict/ Staff only attributes, and the list on the website included separate sections for 'Resources available to FE students only', 'Resources available to staff only' and 'Restricted resources'. The pilot site included a list of frequently asked questions, general instructions, a feedback form and a list of resource links with access via the Shibboleth-Athens Gateway.

In November 2006 we launched our pilot with the students and staff included in the test Active Directory. We sent emails to over 930 of the 1000 selected users, having removed a number who were no longer at the University. The email advised users that they had been selected to take part in a pilot to test out 'easy access to electronic resources' (see Appendix H). We tried to encourage participation by offering £10 vouchers for the top 10 users.

The pilot was successful from a technical point of view in so far as users who tried out the service were pleased with it and no major problems were identified. Specific checks were made to ensure that the service functioned correctly in relation to all aspects, including control of access to appropriate users, account security, sessions behaviour, recording of statistics, and function of each resource. However the usage and level of feedback from users was low (see Appendix I). We were not able to test out the service to the desired extent because we found that students were not accessing their TVU student email accounts and therefore the message was not getting through. Out of 930 students emailed, only 384 opened the email. We received a total of 36 feedback emails generated by the feedback form during November and December 2006. There were 16 positive responses, with most of these arising from users whose original problems had been solved.

We decided that it was necessary to increase the level of feedback in order to test out the system sufficiently. We considered removing Athens access from the pilot group, but rejected this approach as the pilot excluded some Athens resources, and also the reliability was not fully tested. We also considered sending follow up emails, but again this approach was rejected as it was not likely to increase the participation in the pilot to an adequate extent. We decided that it would confuse other users and staff if we carried out a mass advertising campaign to draw attention to the pilot, since only a very small proportion of potential users would actually be able to use the service. We therefore decided to extend the pilot service to the entire student body in order to achieve a greater level of testing and feedback. This involved bringing forward by eight months the launch date of the full Active Directory on the production server, specifically for use with the Shibboleth project. The steps necessary to achieve a Shibboleth compliant directory service are discussed below under 5.4.

Towards the end of this phase the UK Access Federation was launched. We therefore changed our SDSS metadata accordingly. We then set up direct access to Shibbolised resources via the UK Access Federation by using the links provided on the relevant Service Providers sites. We then re-configured our Shibboleth IdP (see *Configuring a Shibboleth Identity Provider for the UK Federation at <http://www.ukfederation.org.uk/content/Documents/SetupIdP>*).

A script was written and run to populate the student domain of Active Directory on the production server with all students at Slough and Ealing. (Reading students were already on Active Directory). The MySQL attributes database was extended to include the entire student population.

5.3 Phase 3 – Pre-Production implementation launched to all students

In this phase we launched access to Shibboleth to the entire student body to enable thorough testing of both system performance, reliability and user satisfaction. Although provision of access via Shibboleth is not a discrete service as such, we decided to name it as a service in order to differentiate it from Athens. We decided on the name TVU e-

Nabataea – Final report – 1.0 – 30 April 2007

Direct, a name which would integrate well with the TVU On-line portal brand. The launch of TVU e-Direct was delayed for about two months because of the structure of Active Directory. Staff and students were on separate ADs. We were planning to implement a separate flat directory structure by adding staff to the student tree but there was a problem with synchronising staff password changes. The approach we used to solve this problem is discussed in 5.4 below.

Setting up direct access to Shibbolised resources at the end of phase 2 had appeared to be straightforward, however at this stage we experienced a whole series of problems (see Appendix J). By working closely with the UK Access Management Federation it gradually emerged that there were two bugs operating at the same time and therefore making it difficult to find out what was causing the problem. Xiao Xu on the TVU team is acknowledged on the Internet2 website for helping to identify the Bugzilla Bug 620 – see http://bugzilla.internet2.edu/show_bug.cgi?id=620.

We completed the process of joining the UK Access Management Federation in February 2007. Having by this time sorted out the problem with direct access to Shibbolised resources, we were ready to launch TVU e-Direct to all students as soon as the necessary changes had been made to Active Directory (see section 5.4 below).

We successfully launched the TVU e-Direct service to the entire student body on 8/3/07, providing access to 29 suppliers and 67 individual Shibbolised and Gateway resources via an upgraded website at <http://e-direct.tvu.ac.uk/ed/index.htm> (see Appendix K). We carried out a student awareness initiative comprising a poster campaign, emails to 32164 students, distribution of flyers, popup network announcements at all sites, and an announcement on the Blackboard VLE. Since that time use of the site has been steadily growing, with logins per day now in three figures (see Appendix L). We are about to extend our advertising campaign to direct it specifically at distance learners. Access via Athens will continue whilst configuration changes are still being made, and we aim to switch over entirely to access using Shibboleth technology in the autumn of 2007.

A technical solution to provide staff access to TVU e-Direct has been put in place and details of this are included in section 5.4 below. Because Shibboleth requires a single active directory it was decided to include staff in the student directory. A web based

application has been designed to solve the staff domain problems such as a missing link with HR records and Single Sign On problems. Staff can now complete a web based registration form which then automatically creates an account on active directory at the back end.

5.4 Creation of a Shibboleth compliant identity management environment

The successful implementation of Shibboleth technology at TVU required the following technical challenges to be addressed:

- Establishment of a single identity store
- Provision of dynamic updating of the attributes store
- Dynamic management of the identity life cycle

5.4.1 Establishment of a Single identity store

Since January 2004 when the University merged with Reading College and School of Arts and Design on 1st January 2004 TVU has had two separate network systems, with the Reading network system and student record system remaining independent of rest of the university. The Reading site currently uses a Microsoft Active Directory based network system whilst the other sites use a Novell E_Directory based network system. Students based at Reading use the Microsoft Exchange email system whilst students at the other sites use the Novell GroupWise email system. All TVU staff use the Microsoft Exchange email system. Therefore, there are four identity stores in TVU:

- E_Directory - holding Ealing and Slough staff and student identities
- Staff Exchange (AD) - holding all TVU staff identities
- Reading Student AD - holding Reading student identities
- Reading Staff AD - holding Reading staff identities

As yet there is no single identity store for all staff and students in TVU.

5.4.2 Dynamically updating the attributes store

Once a single identity store is setup, the next stage of a Shibboleth project is to identify which attributes to use for the service providers to make authorisation decisions. An institution (or Identity Provider) is responsible for providing attributes about each of its members. Dynamically maintaining the attributes for each student and member of staff based on their status in the TVU student records system and HR system is far from straightforward.

5.4.3 Identity life cycle

A simple identity life cycle is composed four main components:

- | | |
|---------------------|--|
| New users | - user ID creation , access rights |
| Account changes | - promotions, transfers, new privileges and attribute changes |
| Password management | - strong password, lost password, password reset and synchronisation |
| Retire users | - delete/freeze accounts, delete/freeze entitlements |

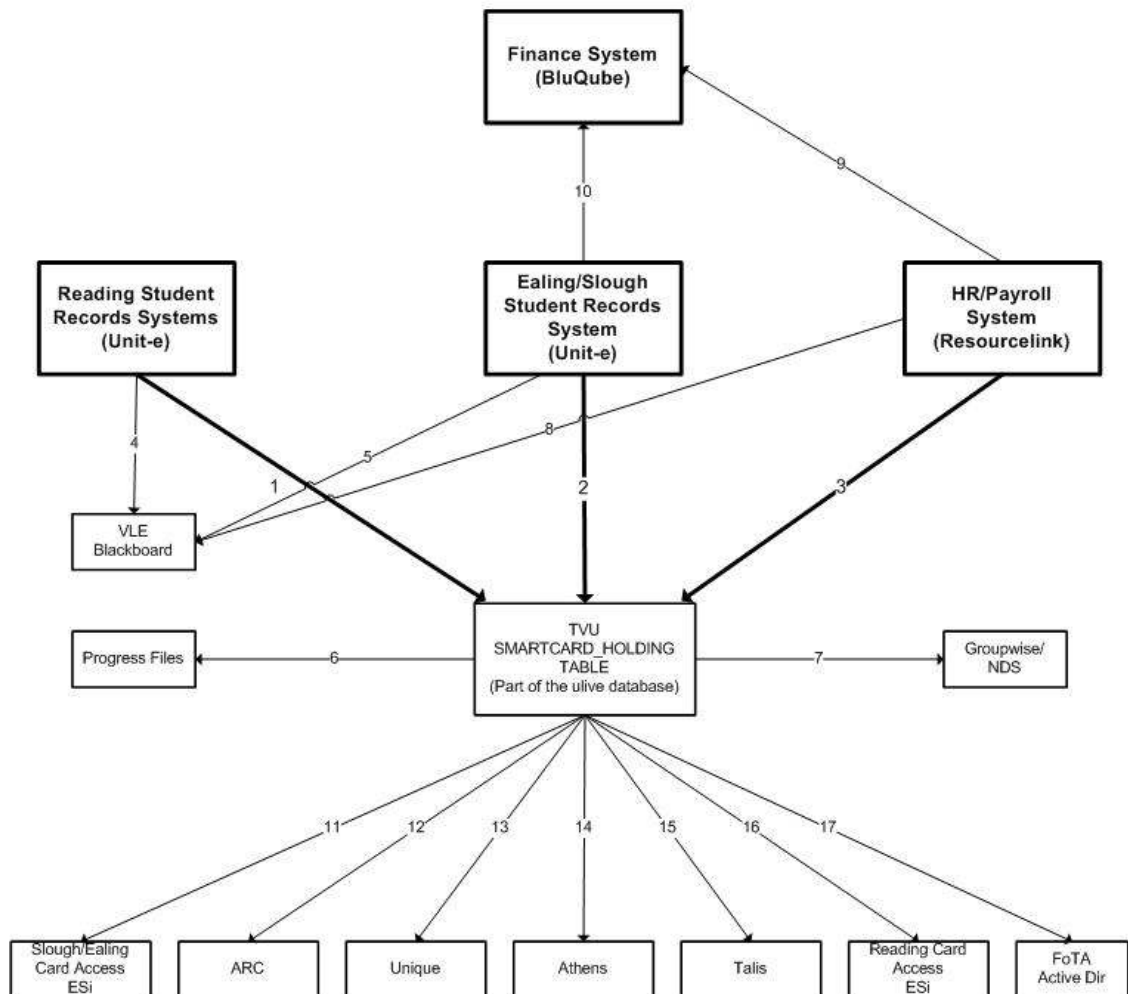
A dynamical identity management system is required by the Shibboleth project at TVU.

5.4.4 Solution

The solution for the technical challenges facing project Nabataea, as listed above, comprises two parts: a central Data Warehouse (DW) and a single Active Directory for the whole university. A central DW was built to provide a central resource for all student and staff information. Student and staff information is dynamically collected from the TVU's student record systems and the HR system. The DW enables dynamic transfer of

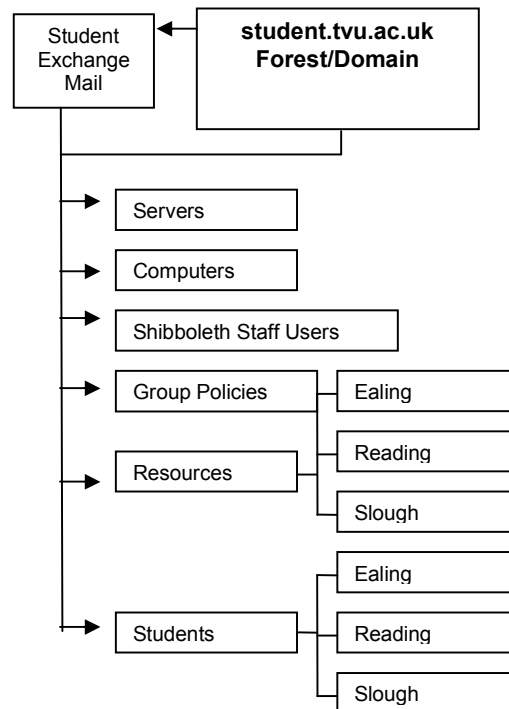
student information to related corporate systems, the library system, the security access system, the Blackboard E-Learning system and so on. The management of the identity store and attribute store of project Nabataea is based on the information from the DW.

Ealing/Slough and Reading Interfaces



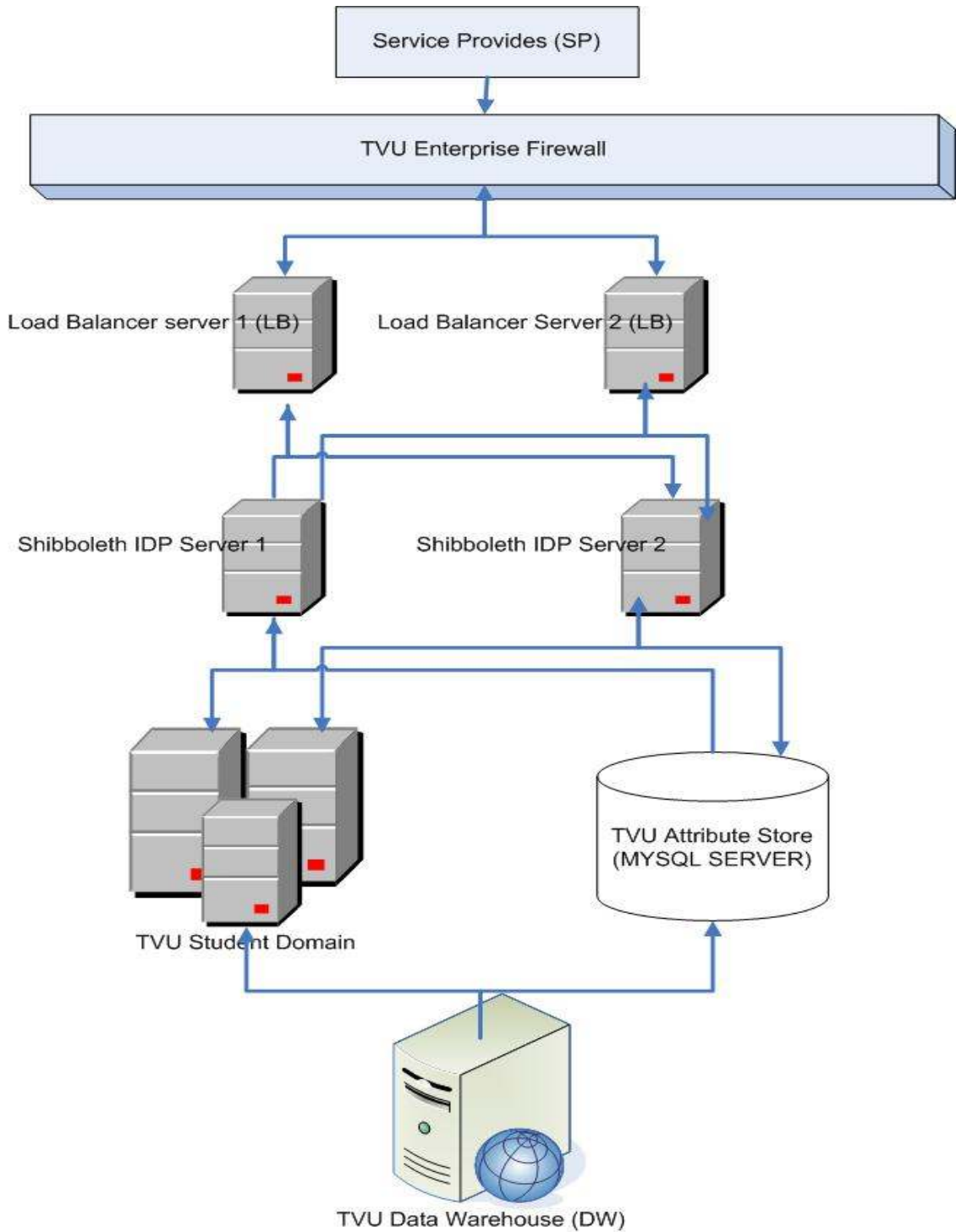
A single active directory built to provide the integrated identity for all students and staff in TVU.

TVU Active Directory Structure



5.4.5 Technical implementation details of project Nabataea

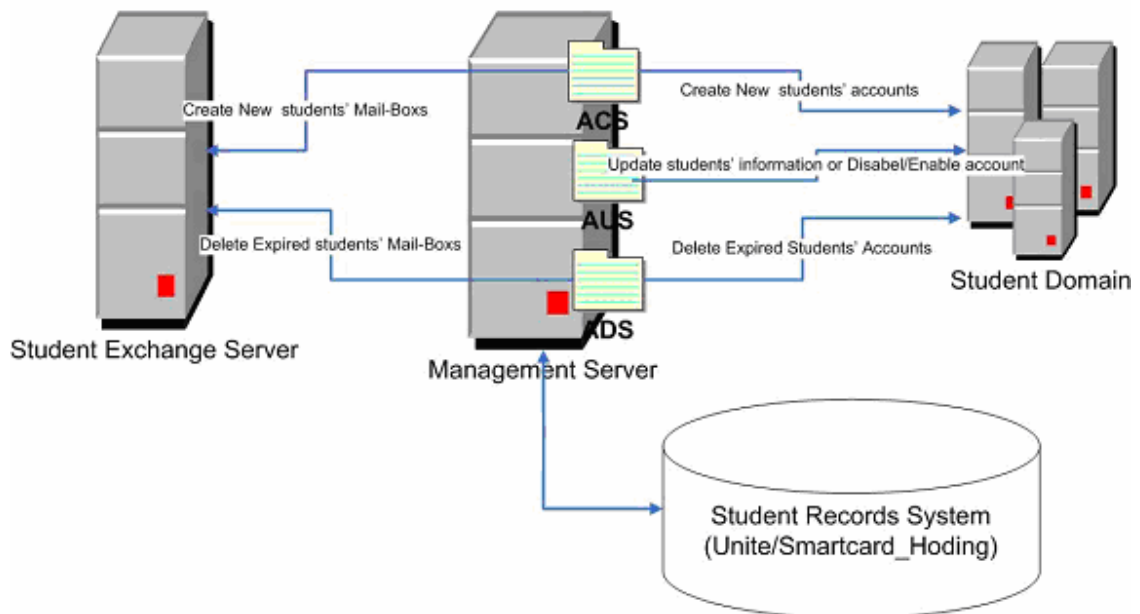
In the Shibboleth project, two IdP servers have been setup to provide the IdP services. Both IdP servers are sitting behind the enterprise firewall. Only SSL connection is allowed to connect both IdP Servers. Load balancer servers are being setup to provide high availability, secure and high performance IDP services in TVU. A set of integration processes in TVU DW is used to manage dynamically the identity life cycle and attribute store. Two additional servers, originally used for the pilot will be used for testing and development. Any changes to the live environment will be tested out first on the test and development servers to ensure that any problems are discovered and addressed before updating the live servers. Load balancer servers are being setup to provide high availability, secure and high performance IDP services in TVU.



5.4.6 Identity provisioning

Server Management scripts run on the management server (Edna) at scheduled times. It is composed of three scripts:

- Account Creation Script (ACS) used to create batch accounts when new students have been enrolled on the student record system (Unite).
- Account Updating Script (AUS) --- used to batch update existing student accounts status based on changes in student records system (Unite).
- Account Deleting Script (ADS) --- used to clean out the expired student accounts when each academic term ends.



5.4.7 Staff registration

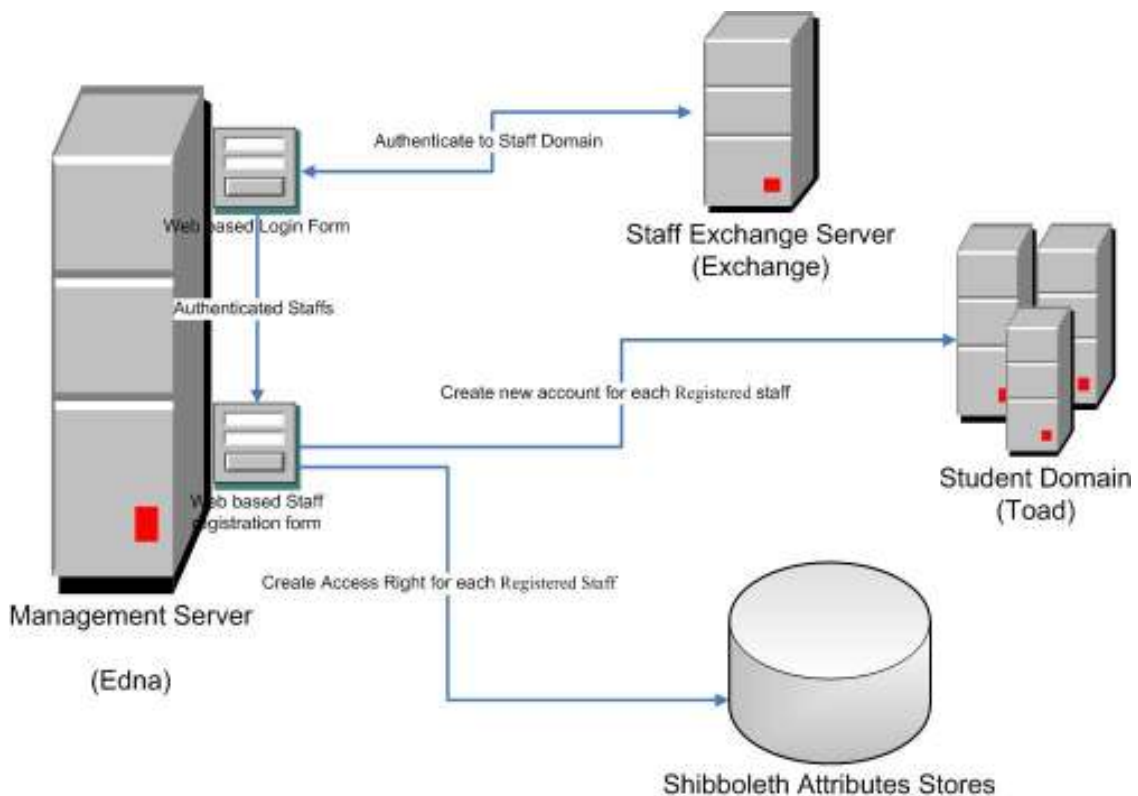
A staff registration form application has been developed. It focuses on two aspects:

- Linking staff email account with HR record.

As the current staff account on the staff exchange server cannot be linked to the appropriate HR record, each member of staff will be required to complete this online form with their staff ID. Registered staff information will be stored on the staff exchange server.

- Creating staff account on an OU of student domain for the Shibboleth project and the SSO solution.

The Shibboleth project requires a single directory with both staff and student accounts. We have chosen the student directory to be that single directory. Therefore, staff accounts need to be created on the student directory. The member of staff completes and submits the registration form, and this web based application then automatically creates a staff account on the student directory. Also, the access rights to electronic resources for the Shibboleth project will be automatically created in the Shibboleth attribute store.



Outputs and results

The most tangible output of the project is the TVU e-Direct website at <http://e-direct.tvu.ac.uk/ed/index.htm>, which provides access to all students to 29 suppliers and 67 individual Shibboleth and gateway resources. It provides a list of resources, support information, general instructions, frequently asked questions, an online feedback form, and further information. The list of resources includes separate sections for 'Resources available to FE students only', 'Resources available to staff only' and 'Restricted resources'. Once users have logged into one resource they are able to move freely from one resource to another without further authentication for the remainder of the browser session.

Outputs underlying the TVU e-Direct service site are:

- Authentication via a single identity store based on Active Directory
- A configuration of the Shibboleth IdP software appropriate for use in the TVU environment
- 2 operational pre-production servers
- 2 test and development servers
- A system capable of supporting all students and staff concurrently accessing electronic information resources both within and outside TVU
- A system for dynamic identity management that meets the requirements of the UK Access Management Federation
- A robust and flexible system to manage access control and update the attributes store

Temporary outputs produced in the course of the project include:

- Pilot access to Gateway compliant resources launched to 930 students via Pilot website and test Active Directory

Nabataea – Final report – 1.0 – 30 April 2007

- Launch to all students, with an awareness initiative comprising a poster campaign, emails to 32164 students, distribution of flyers, popup network announcements at all sites, and an announcement on the Blackboard VLE

Finally there is the Nabataea project website at <http://www.tvu.ac.uk/shibboleth> created to provide information about the project.

Outcomes

The outcomes of Project Nabataea will be of great value to TVU. For students and staff the new system represents a big improvement in terms of both ease of access and simplification of the whole process. Our students have always been very confused about Athens and how it relates to electronic information resources, and other internal authentication processes. Simplifying the process is of particular value to distance learners and their tutors. We are now in a position to be able to replace Athens in the autumn of 2007 and this will make the information skills induction process for new students much more straightforward. For LRS and IT helpdesk staff there will be a reduction in the administrative burden, allowing staff to focus on delivering and fulfilling our main aims and purpose.

As a result of the work carried out in the course of the project, we have

- Successfully implemented Shibboleth IdP on Windows platform
- Successfully designed and implemented a Shibboleth compliant directory service using a single Active Directory for authentication
- Set up a system for dynamic identity management that meets the requirements of the UK Access Management Federation.
- Designed and implemented a robust and flexible system to provide and update the attributes necessary for role based authentication
- Set up a system that allows access control to remain with Learning Resources staff. The attributes store is managed by the LRS electronic information team,

ensuring compliance with the access rights stipulated in individual electronic resource licences.

- Successfully launched the TVU e-Direct service to the entire student body, providing easy access to 29 suppliers and 67 individual Shibboleth and gateway resources through the UK Access Management Federation
- Achieved an implementation that will allow us to replace Athens in Autumn 2007
- Improved security – our implementation integrates directly with the mechanisms for adding/suspending/deleting standard network accounts
- Put in place a system that will reduce the administrative burden on LRC helpdesks
- Made substantial progress towards Single Sign On

Conclusions

The project has successfully implemented a Shibboleth environment for the University based on a good quality and centralised database. TVU is ready to replace Athens authentication in autumn 2007 with Shibboleth technology using the Shibboleth/Athens gateway, and direct authentication to Shibboleth resources. The project demonstrates that this can be done at a very large institution with over 40,000 students, including provision for FE, HE and distance learners, and with a starting point of a number of separate legacy databases.

Implications

Shibboleth will be an important element of the student experience, and unlike Athens where uptime was outsourced to an external provider, keeping Shibboleth running is now part of the Library/IT function. This will impact on IT and Library departments in terms of providing support, training, uptime, etc. We have previously had a number of authentication methods for the full range of electronic information resources. Once we

are entirely dependent on the Shibboleth-based service to provide access to all our electronic information resources, high availability will be of extreme importance. If the service goes down, we will lose access to all resources. We have therefore set up a robust system, based on two servers. If one server goes down, the service will continue to be provided by the other, and the same applies to downtime for maintenance. We are setting up load balancing to ensure high availability and fast performance.

It is important for libraries to remain in control of the management of access rights. Shibboleth projects should always include members of the library staff in the project team. At TVU the attributes store is managed by the LRS (Library) electronic information team, ensuring compliance with the access rights stipulated in individual electronic resource licences.

Shibboleth technology assumes a perfect world in which organisations/institutions will have a single directory of all users. So far, IdP can be set up only based on Apache Web Server. This will continue to be the case until either Apache or Shibboleth is expanded to support multiple directories. Therefore, a very significant implication for others is the importance of having a good quality and centralised database of staff and students and planning for the data management issues of dynamic updating of store and dynamic management of the identity life cycle at an early stage.

Recommendations

It would be useful to have a non-technical guide outlining the necessary steps in setting up access via Shibboleth, aimed at librarians, for example, how attributes are used to control access, how attributes are set up, how librarians can continue to manage and control access to resources, how usage statistics can be retrieved.

Institutions are recommended to ensure that their data management environment is in good shape at an early stage prior to commencing adoption of Shibboleth technology. Procedures and policies for maintaining up to date, accurate staff and student data need to be in place to ensure that institutions are able to comply with federation rules and resource licences.

References

Cantor, S. (No date) *Installing Shibboleth* [online]. Place, Michigan/Washington DC, Internet2. Available from:
<<https://spaces.internet2.edu/display/SHIB/InstallingShibboleth>> [Accessed May 2006].

Cantor, S. (No date) *Configuring Shibboleth* [online]. Place, Michigan/Washington DC, Internet2. Available from:
<<https://spaces.internet2.edu/display/SHIB/ConfiguringShibboleth>> [Accessed May 2006].

Young, Ian A. (2006) *Federation Technical Specifications* [online]. Place, UK Access Management Federation for Education and Research. Available from:
<<http://www.ukfederation.org.uk/library/uploads/Documents/Tech%20Federation%201.0%20final.pdf>> [Accessed 4 December 2006].

UK Access Management Federation for Education and Research. (2006) *Recommendations for use of personal data* [online]. Place, UK Access Management Federation for Education and Research. Available from:
< <http://www.ukfederation.org.uk/library/uploads/Documents/recommendations-for-use-of-personal-data.pdf>> [Accessed 12 December 2006].

UK Access Management Federation for Education and Research. (2006) *Configuring a Shibboleth Identity Provider for the UK Federation* [online]. Place, UK Access Management Federation for Education and Research. Available from:
< <http://www.ukfederation.org.uk/content/Documents/SetupIdP>> [Accessed 4 December 2006].

Appendices

Appendix A

workers.properties

```
workers.tomcat_home=C:\Shib-Runtime\Idp\tomcat.5.5  
workers.java_home=C:\Shib-Runtime\java\jdk1.5.0  
ps=\
```

```
# Define worker 'ajp13worker1'  
worker.list=ajp13worker1,jkstatus
```

```
# Set properties for worker 'ajp13worker1' (ajp13)  
worker.ajp13worker1.type=ajp13  
worker.ajp13worker1.host=localhost  
worker.ajp13worker1.port=8009
```

```
#worker.ajp13worker1.lbfactor=1  
worker.ajp13worker1.cachesize=10  
worker.ajp13worker1.cache_timeout=600  
worker.ajp13worker1.socket_keepalive=1  
worker.ajp13worker1.recycle_timeout=300
```

```
worker.jkstatus.type=status
```

Appendix B

We use a separate MySQL database to store our users' attributes. Here are the entry of a MySQL connector in mysql-resolver.xml to provide database connectivity and the query we use to get the correct attributes for users:

```
<JDBCDataConnector id="mysql"
    dbURL="jdbc:mysql://localhost/institute?user=shibboleth&
password=shibbocsg1"
    dbDriver="com.mysql.jdbc.Driver"
    maxActive="10"
    maxIdle="5">
    <Query>SELECT distinct member.person_ref,
entitlement.entitlement, affiliation, affiliation.r_entitlement
FROM member, Entitlement, affiliation where
member.person_ref=entitlement.person_ref and
member.person_ref=affiliation.person_ref and member.person_ref =
?</Query>
</JDBCDataConnector>
```

Appendix C

TVU's attribute store database

TVU has three tables in the attribute store database:

- member table (holding users' personal information)
- entitlement table (holding the permission set for Shibboleth-to-Athens gateway resources)
- affiliation (holding the value of eduPersonEntitlement for medical restrict resources)

These tables comprise the following fields:

member

```
PERSON_REF (VARCHAR(55))
FORENAME (VARCHAR(60))
SURNAME (VARCHAR(60))
DEPARTMENT (VARCHAR(60))
COURSE_NAME (VARCHAR(100))
COURSE_REFERENCE_CS (VARCHAR(45))
FE_OR_HE (VARCHAR(2))
SITE (VARCHAR(45))
DEPARTMENT_2 (VARCHAR(45))
STUDENT (VARCHAR(1))
```

entitlement

```
PERSON_REF (VARCHAR(55))
ENTITLEMENT (VARCHAR(45))
```

affiliation

```
PERSON_REF (VARCHAR(55))
AFFILIATION (VARCHAR(45))
R_ENTITLEMENT (VARCHAR(255))
```

Appendix D

TVU Idp.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!-- Shibboleth Identity Provider configuration -->

    <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://shibboleth1.tvu.ac.uk:8443/shibboleth-idp/AA"
        resolverConfig="file:/c:/usr/local/shibboleth-idp/etc/mysql-
        resolver.xml"
        defaultRelyingParty="http://ukfederation.org.uk"
        providerId="urn:mace:eduserv.org.uk:athens:provider:tvu.ac.u
        k">

        <!-- This section contains configuration options that apply
        only to a site or group of sites
            This would normally be adjusted when a new federation
        or bilateral trust relationship is established -->

        <!-- InQueue example (the schemaHack is needed for 1.1/1.2
        SPs)-->

        <!-- <RelyingParty
        name="urn:mace:eduserv.org.uk:athens:provider:tvu.ac.uk"
        signingCredential="athens_creds"
            schemaHack="true">
            <NameID nameMapping="shm"/>
        </RelyingParty>-->

        <RelyingParty name="http://ukfederation.org.uk"
        signingCredential="ukfederationCred" schemaHack="true">
            <NameID nameMapping="shm"/>
        </RelyingParty>

        <!-- Configuration for the attribute release policy engine
            For most configurations this won't need adjustment -->
        <ReleasePolicyEngine>
            <ArpRepository
        implementation="edu.internet2.middleware.shibboleth.aa.arp.provid
        er.FileSystemArpRepository">
```

Nabataea – Final report – 1.0 – 30 April 2007

```
<Path>file:/C:/usr/local/shibboleth-
idp/etc/arps/</Path>
  </ArpRepository>
</ReleasePolicyEngine>

<!-- Logging Configuration
  The defaults work fine in this section, but it is
  sometimes helpful to use "DEBUG" as the level for
  the <ErrorLog/> when trying to diagnose problems -->
  <Logging>
    <ErrorLog level="DEBUG"
location="file:/C:/usr/local/shibboleth-idp/logs/shib-error.log"
/>
    <TransactionLog level="DEBUG"
location="file:/C:/usr/local/shibboleth-idp/logs/shib-access.log"
/>
  </Logging>
  <!-- Uncomment the configuration section below and comment
  out the one above if you would like to manually configure log4j -
  ->
  <!--
  <Logging>
    <Log4JConfig location="file:///tmp/log4j.properties"
/>
  </Logging> -->

  <!-- This configuration section determines how Shibboleth
  maps between SAML Subjects and local principals.
  The default mapping uses shibboleth handles, but other
  formats can be added.
  The mappings listed here are only active when they are
  referenced within a <RelyingParty/> element above -->
  <NameMapping
    xmlns="urn:mace:shibboleth:namemapper:1.0"
    id="shm"
    format="urn:mace:shibboleth:1.0:nameIdentifier"
    type="SharedMemoryShibHandle"
    handleTTL="28800"/>

  <!-- Determines how SAML artifacts are stored and retrieved
  The (sourceLocation) attribute must be specified when
  using type 2 artifacts -->
  <ArtifactMapper
implementation="edu.internet2.middleware.shibboleth.artifact.prov
ider.MemoryArtifactMapper" />

  <!-- This configuration section determines the keys/certs to
  be used when signing SAML assertions -->
```

Nabataea – Final report – 1.0 – 30 April 2007

```
<!-- The credentials listed here are used when referenced
within <RelyingParty/> elements above -->
<Credentials xmlns="urn:mace:shibboleth:credentials:1.0">
  <!-- Athens -->

  <FileResolver Id="ukfederationCred">
    <Key password="shibbol">
      <Path>file:/c:/shib-
runtime/idp/apache2.2.3/conf/ssl.key/shibbol.key</Path>
    </Key>
    <Certificate>
      <Path>file:/c:/shib-
runtime/idp/apache2.2.3/conf/ssl.crt/shibbolcert.crt</Path>
      <CAPath>file:/c:/shib-
runtime/idp/apache2.2.3/conf/ssl.crt/intermediate.crt</CAPath>
    </Certificate>
  </FileResolver>
</Credentials>

<!-- Protocol handlers specify what type of requests the IdP
can respond to. The default set listed here should work
for most configurations. Modifications to this
section may require modifications to the deployment descriptor --
>
  <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.
ShibbolethV1SSOHandler">
    <Location>https?://[^\:/]+(: (443|80))/?shibboleth-
idp/SSO</Location> <!-- regex works when using default protocol
ports -->
  </ProtocolHandler>
  <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.
SAMLv1_AttributeQueryHandler">
    <Location>.+ :8443/shibboleth-idp/AA</Location>
  </ProtocolHandler>
  <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.
SAMLv1_1ArtifactQueryHandler">
    <Location>.+ :8443/shibboleth-idp/Artifact</Location>
  </ProtocolHandler>
  <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.
Shibboleth_StatusHandler">
    <Location>https://[^\:/]+(:443)?/shibboleth-
idp/Status</Location>
  </ProtocolHandler>

<!-- This section configures the loading of SAML2 metadata,
which contains information about system entities and
```

Nabataea – Final report – 1.0 – 30 April 2007

how to authenticate them. The metadatatool utility can be used to keep federation metadata files in synch.

Metadata can also be placed directly within this these elements. -->

```
<!-- InQueue example (Deployments would need to get updated InQueue metadata) -->
```

```
<MetadataProvider
type="edu.internet2.middleware.shibboleth.metadata.provider.XMLMe
tadata"
```

```
    uri="file:/c:/usr/local/shibboleth-
idp/etc/ukfederation-metadata.xml"/>
```

```
</IdPConfig>
```

Appendix E

TVU's MySQL-resolver.xml

```
<AttributeResolver xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns="urn:mace:shibboleth:resolver:1.0"
xsi:schemaLocation="urn:mace:shibboleth:resolver:1.0 shibboleth-
resolver-1.0.xsd">

    <SimpleAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonScopedAffiliation" smartScope="tvu.ac.uk">
        <AttributeDependency requires="urn:mace:dir:attribute-
def:eduPersonAffiliation"/>
    </SimpleAttributeDefinition>

    <SimpleAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonAffiliation" sourceName="affiliation">
        <DataConnectorDependency requires="mysql"/>
    </SimpleAttributeDefinition>

    <SimpleAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonPrincipalName" smartScope="tvu.ac.uk"
sourceName="person_ref">
        <DataConnectorDependency requires="mysql"/>
    </SimpleAttributeDefinition>

    <SimpleAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonEntitle" sourceName="entitlement">
        <DataConnectorDependency requires="mysql"/>
    </SimpleAttributeDefinition>

    <SimpleAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonEntitlement" sourceName="r_entitlement">
        <DataConnectorDependency requires="mysql"/>
    </SimpleAttributeDefinition>

    <!-- MySql Connection to remote MySQLserver -->
    <JDBCDataConnector id="mysql"

        dbURL="jdbc:mysql://localhost/institute?user=shibboleth&
password=shibbocsg1"
        dbDriver="com.mysql.jdbc.Driver"
        maxActive="10"
        maxIdle="5">
        <Query>SELECT distinct member.person_ref,
entitlement.entitlement, affiliation, affiliation.r_entitlement
FROM member, Entitlement, affiliation where
member.person_ref=entitlement.person_ref and
member.person_ref=affiliation.person_ref and member.person_ref =
?</Query>
```

Nabataea – Final report – 1.0 – 30 April 2007

```
</JDBCDataConnector>

<!-- If other AttributeDefinitions want information out of
this database, might want to use SQL:
    select membertype from members where username = ?
-->

<!-- Need to get the following working on a locally
installed MySQL server
    <JDBCDataConnector id="mysql"

        dbURL="jdbc:mysql://localhost/institute?user=root&passwo
rd=mysql_password"
            dbDriver="com.mysql.jdbc.Driver"
            maxActive="10"
            maxIdle="5">
            <Query>select person_ref, entitlement, entitlement2
from members where person_ref = ?</Query>
        </JDBCDataConnector>
-->

</AttributeResolver>
```

Appendix F

TVU arp site xml

```
<?xml version="1.0" encoding="UTF-8"?>
<AttributeReleasePolicy
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:mace:shibboleth:arp:1.0"
xsi:schemaLocation="urn:mace:shibboleth:arp:1.0 shibboleth-arp-
1.0.xsd" >
  <Description>Simplest possible ARP.</Description>
  <Rule>
    <Target>
      <AnyTarget/>
    </Target>

    <Attribute name="urn:mace:dir:attribute-
def:eduPersonScopedAffiliation">
      <AnyValue release="permit"/>
    </Attribute>

    <Attribute name="urn:mace:dir:attribute-
def:eduPersonPrincipalName">
      <AnyValue release="permit"/>
    </Attribute>

    <Attribute name="urn:mace:dir:attribute-
def:eduPersonEntitle">
      <AnyValue release="permit"/>
    </Attribute>
  </Rule>
  <Rule>
    <Description>"Film and Sound"</Description>
    <Target>

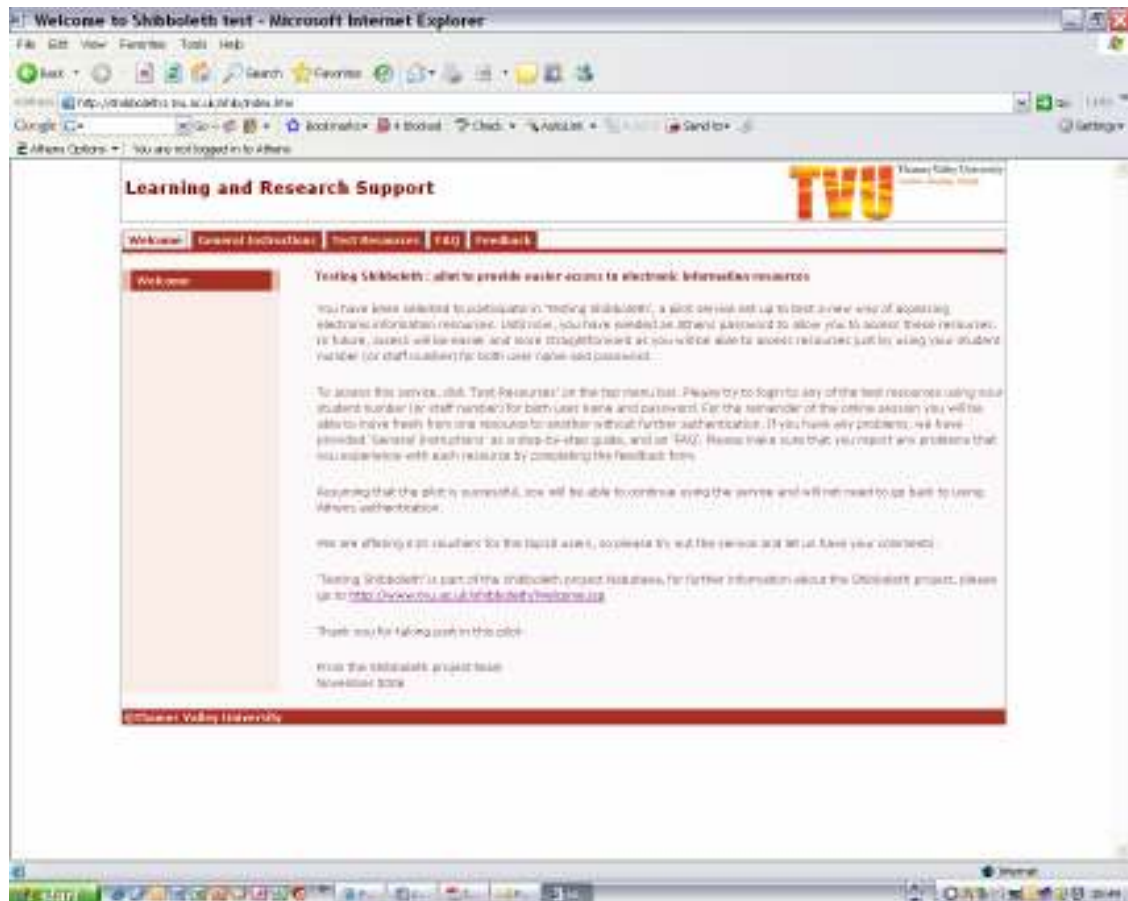
<Requester>urn:mace:ac.uk:sdss.ac.uk:provider:service:emol.sdss.a
c.uk</Requester>
      </Target>
      <Attribute name="urn:mace:dir:attribute-
def:eduPersonEntitlement">
        <Value
release="permit">urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.
ac.uk:restricted</Value>
      </Attribute>
    </Rule>
  <Rule>
    <Description>ZETCO Search</Description>
    <Target>
```

Nabataea – Final report – 1.0 – 30 April 2007

```
        <Requester>http://zetoc.mimas.ac.uk:8000/cgi-  
bin/wzshib</Requester>  
      </Target>  
    <Attribute name="urn:mace:dir:attribute-  
def:eduPersonScopedAffiliation">  
      <AnyValue release="permit" />  
    </Attribute>  
  </Rule>  
</AttributeReleasePolicy>
```

Appendix G

Pilot site



Appendix H

Pilot to provide easier access to electronic information resources

Dear student

You have been selected to participate in 'Testing Shibboleth', a pilot service set up to test a new way of accessing electronic information resources. Until now, you have needed an Athens password to allow you to access these resources. In future, access will be easier and more straightforward as you will be able to access resources just by using your normal network login.

In order to access this service you should go to the 'Testing Shibboleth' site at <http://shibboleth1.tvu.ac.uk/shib/index.htm> where you will find a list of test resources, an online feedback form, frequently asked questions, general instructions and further information. Login to any of the test resources using your student number and normal network password and for the remainder of the online session you will be able to move freely from one resource to another without further authentication. Please make sure that you report any problems that you experience with each resource by completing the feedback form.

Assuming that the pilot is successful, you will be able to continue using the service and will not need to go back to using Athens authentication.

We are offering £10 vouchers for the top10 users, so please try out the service and let us know of any problems you have using the feedback form .

For further information about the Shibboleth project, please go to <http://www.tvu.ac.uk/shibboleth/Welcome.jsp>

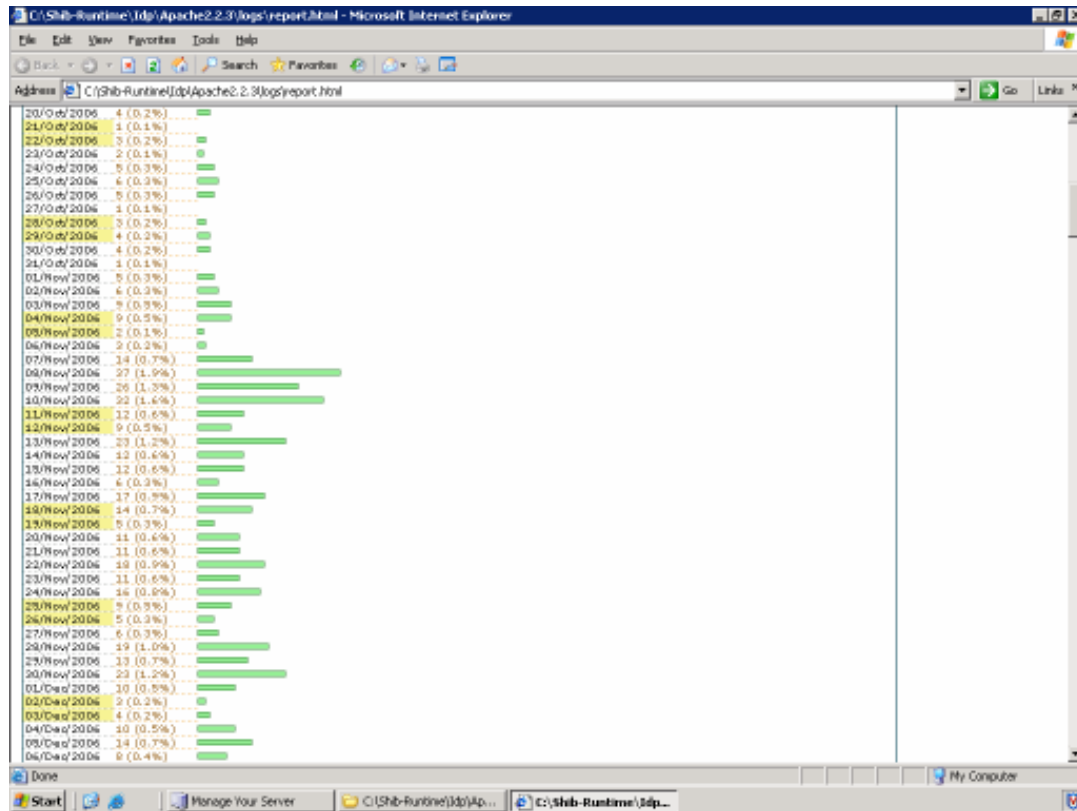
Thank you for taking part in this pilot.

From the Shibboleth project team

Appendix I

Statistics showing low usage during the pilot phase

Statistics generated with [VISITORS Web Log Analyzer](#) version 0.7



Appendix J

We experienced a problem with setting up the access to the Shibbolised resources and helped identify a bug in the SP software and another bug in the IdP software.

A warning message appeared at the SP server end each time we accessed Film and Sound that indicated something was not set up properly in the IdP. We were advised by UK Federation to add smartScope="tvu.ac.uk" to the attribute EPPN (eduPersonPrincipalName). This was because our ARP file included reference to EPPN.

We altered this so that ARP.xml is customised for each database separately, following the examples at <http://ukfederation.org.uk/content/Documents/AttributeUsage> .

Once the change had been made to mysql-resolver.xml we experienced 'Session creation failure' message. We were then unable to access the Shibbolised resource Film and Sound despite confirming that the details added to resolver.xml had been correct. The mysql-resolver.xml file was then changed back to omit the smartScope details, but the problem persisted.

After this every time we tried to access Film and Sound the SP server went down. Testing was done to identify the configuration that was causing the problem. A bug was detected in the SP code that was being triggered by our resolver file containing smartScope. UK Federation suspected that this bug had not emerged previously because the service providers we had tested against did not require eduPersonPrincipalName. They would see an invalid ePPN value coming in from our IdP, discard it because it was invalid, then proceed to allow us access on the basis of the other attributes such as eduPersonScopedAffiliation. Relatively few services require ePPN, so we could be releasing invalid ePPN values for some time before noticing it. (UK Federation recommend that in order to protect the privacy of users that ePPN values should be released only to those services that have a real need for ePPN. See Technical Recommendations for Participants and the Recommendations for use of Personal Data published by the UK Federation at <http://ukfederation.org.uk/content/Documents/FedDocs>

Nabataea – Final report – 1.0 – 30 April 2007

UK Federation isolated the line in the SP code that contained the bug and coded a patch to correct it.

We then needed to solve the original problem with the session creation failure message.. It emerged that the local user identification name in the TVU attribute store in the MySQL database was stored as integer type. This was perfectly legal, but was causing a problem because we were using Shibboleth 1.3c which normally communicates with data stores where everything is essentially a string. The code that handles scoped attributes refused to handle the integer typed value and caused an exception. This would be fixed in the upcoming 1.3.2 release. In the short term we fixed this by changing the data type of our person_ref field from INT(11) to VARCHAR(11).

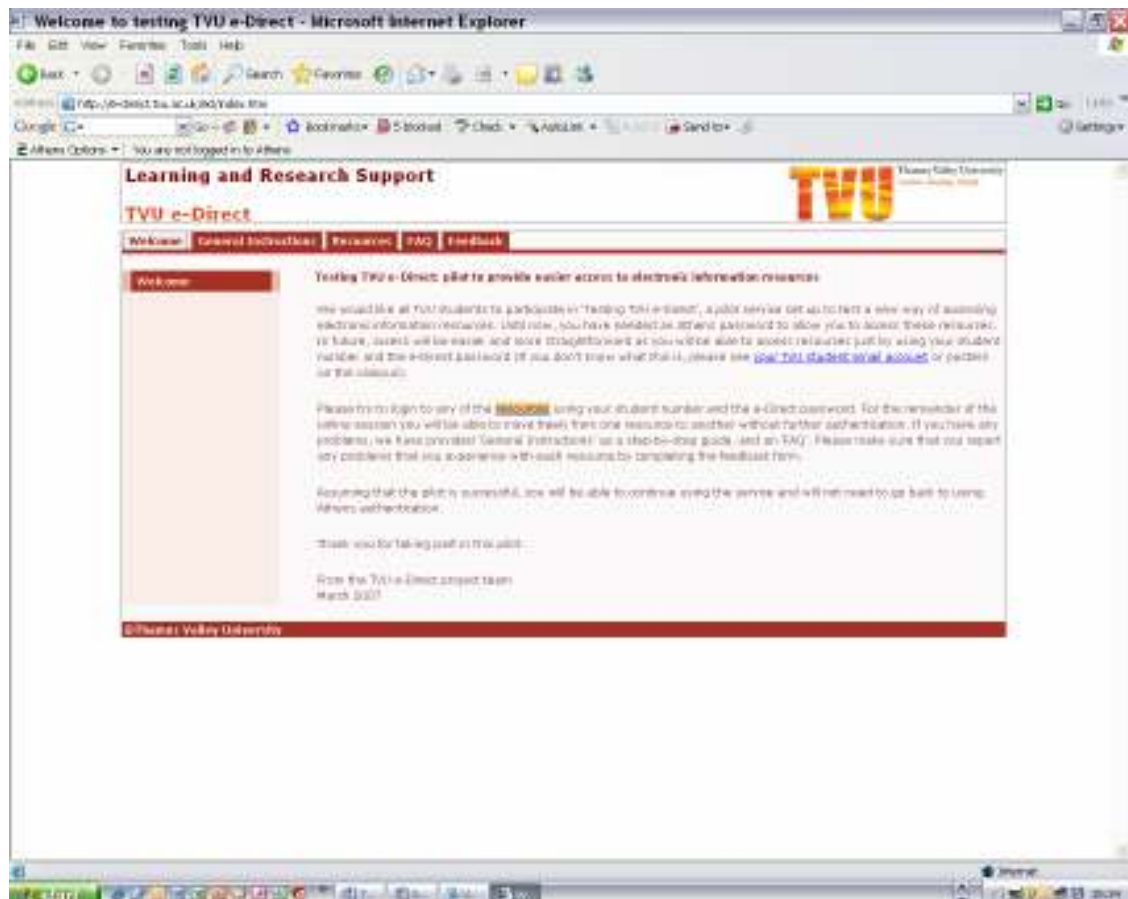
For the full technical details see Internet 2 Bugzilla Bug 620

http://bugzilla.internet2.edu/show_bug.cgi?id=620

Appendix K

TVU e-Direct site

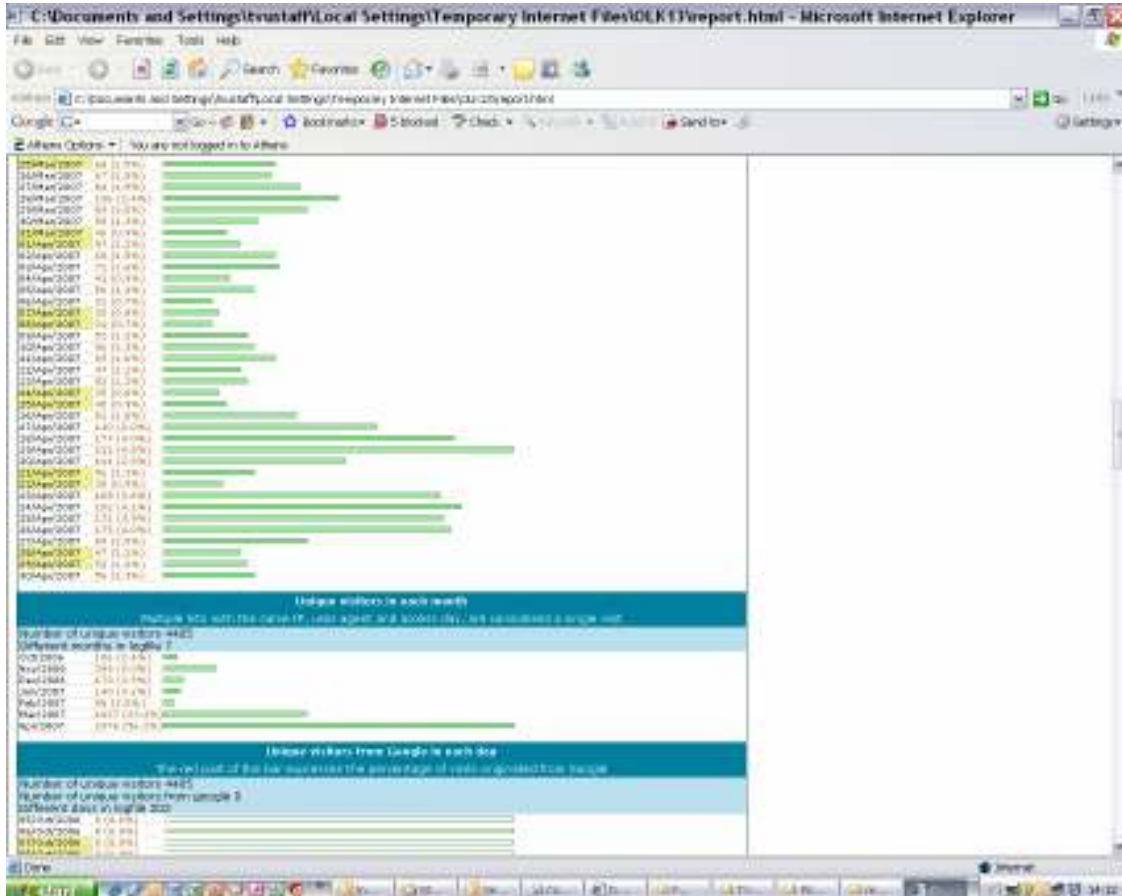
<http://e-direct.tvu.ac.uk/ed/index.htm>



Appendix L

Statistics generated with [VISITORS Web Log Analyzer](#) version 0.7

Statistics showing the increase in usage after the launch of TVU e-Direct



Appendix M

Glossary

AD - Active Directory, an implementation of LDAP directory services by Microsoft for use primarily in Windows environments

Apache - Web server software

Athens - Athens is an Access Management system for controlling secure access to web based services

Athens-Shibboleth Gateway – A service that allows Athens users to connect to Shibboleth Service Providers using Athens as an Identity Provider

E_Directory - Novell E_Directory (formerly called Novell Directory Services) is an X.500 compatible directory service software product released in 1993 by Novell for centrally managing access to resources on multiple servers and computers within a given network

EduServ - A not-for-profit IT services group, providing support and solutions for business critical hosting, for e-learning, e-government and e-commerce, and for network identity management. Currently hold the JISC contract to run Athens.

Internet2 - Internet2 is a consortium being led by 207 US universities working in partnership with industry and government to develop and deploy advanced network applications and technologies, accelerating the creation of tomorrow's Internet. Internet2 is recreating the partnership among academia, industry and government that fostered today's Internet in its infancy.

IdP - Shibboleth Identity Provider

JISC - Joint Information Systems Committee

LDAP - A protocol used to access a directory listing

Nabataea – Final report – 1.0 – 30 April 2007

LIS – Learning and Information Services

LRS – Learning and Research Support

MATU - Middleware Assisted Take-up Service. A pilot service to assist Shibboleth Early Adopters, funded by JISC. <http://www.matu.ac.uk/>

Mod_jk - An interface between Apache and Tomcat

MySQL - A multithreaded, multi-user SQL database management system (DBMS)

Nabataea – The name of the project under which TVU implemented Shibboleth technology

SDSS (Shibboleth Development Support Service) - A development Shibboleth federation for managing access to UK academic online resources

Shibboleth - A technology developed by Internet2

Shibboleth-Athens Gateway - A service that allows users with an institutional IdP to connect to existing Athens Service Providers, based on Athens becoming a Shibboleth Service Provider in its own right

SP - Shibboleth Service Provider

SSL - Secure Sockets Layer (a communications protocol)

SSO - Single Sign On

Tomcat - A Java Servlet container and web server

UK Access Management Federation – Federation supported by JISC and Becta, and operated by UKERNA. The federation provides a single solution to access online resources and services for education and research. It is a significant development for the next generation access management systems based on Shibboleth technology.