

JISC Completion Report

The Liverpool Shibboleth Implementation Programme (LSIP)

Project Overview

1. Background

The University of Liverpool Computing Services Department has made significant progress in making almost all of its user service systems use a single directory for user authentication. With the recent introduction of Athens DA our main computing services now authenticate using our Novell Netware e-directory (using LDAP). The contents of the e-directory itself is controlled by locally developed software that manages the user community, using the University's Personnel and Student systems as the source for the required user information.

Our e-directory also contains identity information for a number of users who have rights to use some (or all) of our systems but who for a variety of reasons have no entry in either the Personnel or Student systems. The number of these entries is increasing as the University diversifies and broadens its activities. We now provide services to individuals, who whilst being registered as students, are following distance learning programmes offered jointly with and managed by external partners. We also provide services to a considerable number of individuals on short programmes and particularly to programmes that support practicing health care professionals. The University is working in partnership with The University of Lancaster for the provision of some medical education and training and we need to provide access to our systems to some medical students from Lancaster. The management of these devolved authentication realms is of some concern.

Shibboleth was identified as the leading candidate for the next generation of user access control systems and will clearly be of importance to the University in the medium term. As Shibboleth provides an architecture for supporting federated access control with the potential for trusted independent organisations controlling the access of their "members", Shibboleth potentially offers a more effective way in which we could manage the devolved user control that is becoming a more pressing problem.

Our present use of Novell's e-directory (other than for Netware Services) is to provide only user authentication; we presently rely on information held in each individual system to hold the rights of the authenticated user on that system. This leads to duplication of information between our systems and requires systems management effort on each of these systems to maintain it. We are interested in making use of additional common attributes in our e-directory that can be used by many of our systems. We believed that Shibboleth could provide support for this mode of working provided that there is agreement between the systems on a common set of user attributes.

The project fulfilled all the needs we originally envisaged and we are now in a very good position to plan the phased introduction of a Shibboleth based user access control system to the services we offer.

2. Aims and Objectives

The University's objective for this project was to have a working Shibboleth environment including origin and target systems that would be used to provide at least parts of its production computing service. A local federation would be established to provide devolved management of users from constituencies outwith the "normal" members of the University (e.g. Health Service workers on short courses, students on distance learning programmes jointly managed with external partners, staff and students on programmes run jointly with other HE/FE bodies).

We feel we have achieved most of these aims and objectives. We have a working Shibboleth environment that could be used to provide parts of our production computing service and we could introduce a local federation for the purposes we intended. We have, however, chosen not to implement this environment at this time but to await the release of the Shibboleth 2.0 system (expected in the Summer of 2006) which differs significantly in its functionality from the 1.2 and 1.3 systems we have successfully worked with. In particular, the Shibboleth 2.0 system should be able to support delegation which, if true and practical, could remove our dependency on the Yale CAS system for some parts of our service.

Whilst our objectives did not change during the project, the software we evaluated and implemented did indeed change from what we had initially envisaged. In particular, we did not envisage upgrades to the Shibboleth code (1.2 to 1.3 in our case) involving changes in the configuration and terminology used by the system and we did not envisage having to work with both PubCookie and Yale CAS authentication systems. Having said that we found the experience very useful and we feel we have a much clearer picture of how we should implement a Shibboleth environment over the coming years.

3. Overall Approach

The impact of testing Shibboleth 1.3 on the overall project schedule (as reported in our Progress Report in September 2005) was to delay the testing with the Athens-Shibboleth Gateway and the local MLE, U-Portal, IMP Web Mail and Oracle Portal systems.

The knock-on effect of the delay was to set back the testing with the uPortal system until February 2006. This part of the project is now expected to complete satisfactorily within a week of the team member responsible for the final uPortal configuration returning from holiday.

If we could start again we do not think we would have proceeded differently. It is our opinion that the delays encountered could not have been foreseen in detail and, indeed, it is only one small part of the project which will not be completed within the timeframe set by the project.

4. Project Outputs

The deliverables to be produced at each phase of the programme were essentially reports documenting the experiences the team had in carrying out the work; they have not duplicated the installation manuals or instructions but sought to clarify these and provide the information that is required but is not in the regular documentation.

All reports from each phase of the project are available on our Project Web site <http://www.liv.ac.uk/LSIP/>.

5. Project Outcomes

We have:

- Successfully implemented Shibboleth SP and IdP on UNIX platforms (Solaris and Linux).
- Successfully used Novell E-Directory for authentication and attribute repository.
- Successfully set up a local federation.
- Successfully implemented access to Athens protected resources via the Athens-Shibboleth gateway.
- Successfully implemented access to Blackboard (our VLE).
- Successfully investigated integration of IMP Webmail.
- Successfully assessed the potential use with Oracle Portal and SunGard Banner
- Successfully implemented the Oxford SPIE glue code for uPortal.
- Successfully implemented and integrated both Pubcookie and Yale CAS SSO systems.
- Produced reports on our experiences with all the above on the Project Web Site.

The project outcomes have been:

- Single sign on
- Attribute (or role) based authorisation

The main lessons we have learned from the project that we feel could be applied elsewhere are:

- Software installation / integration projects must be aware that there is always development work going on and that new releases of software invariably require changes to the software/operating system environments in which they operate.
- Projects must be prepared to change the versions of any or all of the systems used to support what you are trying to implement. This has been particularly true with Shibboleth.

There have been unexpected outcomes:

- We did not expect to have to implement two Single Sign On systems but we feel the experience gained was well worthwhile.
- We did not expect Shibboleth 1.3 implementation to be quite as different to that of 1.2 as it was. However, we feel that solving the configuration issues involved has put us in a much better position to deal with Shibboleth 2.0 implementation which we know will be just as, if not more, challenging.

6. Stakeholders

Our own user population will be the main beneficiaries. They will benefit not only from the single sign on to all local systems but also from the ability to gain access to local facilities whilst being members of the HE Federation (see section 20 below).

Other projects embarking on their own implementations of Shibboleth will, we believe, benefit from the documentation we have produced and will be able to call on our expertise. This has already been demonstrated by the assistance we have already given to the Cheshire 3 and Learning Matrix projects.

10. Intellectual Property Rights

None to clear.

Project Resources

11. Project Partners

None.

We gave advice to the Cheshire 3 project and the Learning Matrix Project.

12. Project Management

Early involvement of all members of the project team with the aims of the project and the timescales envisaged for their individual contributions. We found that this helped focus the plans of those involved in the later stages of the project.

Of course, one has to be prepared for the unexpected especially in the latter stages of the project as relatively small delays actually amount to large delays in absolute terms.

There were no changes in the project staff or their roles throughout the project. We feel that those involved with the project have acquired new, relevant, skills and experience which will benefit them in their career development.

The staff involved with the project (and their FTE equivalent contributions) at the end of the project were:

- Iain Stinson, Director of Computing Services, Project Management (0.05 FTE)
- Chris Wooff, Deputy Director of Computing Services, Project Management (0.1 FTE)
- Pete Mallinson, LSIP Team Leader (0.2 FTE)
- John Gilbertson, Corporate Web Team (0.3 FTE)
- Jake Gannon, Groupware Team Leader (0.1 FTE)
- Duncan Appelbe, Groupware Team (0.2 FTE)
- Simon Hatton, E-Mail Team (0.1 FTE)
- Mike Sandells, E-Directory Team (0.1 FTE)
- Unix Systems Support (0.3 FTE)
- Banner and Oracle Support Staff (0.15 FTE)

13. Programme Support

We felt that we received the support we needed from programme and programme manager and from those with whom we made contact throughout the project.

As early adopters we realised that we were venturing into the only partially known and that the documentation we required would probably not be available when we required it. Having said that we found email contacts made on the Internet2 / Shibboleth mailing lists to be really helpful and we wish to mention the very positive effect these had on the project.

The Katholieke Universiteit Leuven are to be particularly thanked for all their assistance.

The SPIE project team at Oxford were extremely helpful in the uPortal integration phase of our project.

We found the web site maintained by the IAMSECT project at Newcastle to be very useful as a source of relevant information.

14. Budget

Overall, the project expenditure was in line with our original proposal. However, the lack of appropriate Shibboleth training within the community at the time it was required meant that the Project Team spent extra time acquiring appropriate Shibboleth skills. This is reflected in the final budget as a zero spend on "Shibboleth Training and staff development" but an increase in the time spent working on the project principally by the Core Team Leader and the Unix Support Staff. In addition, the cost of the 2 ALC Grade 2 Core team staff has been shared equally between the JISC and the University.

Detailed Project Planning

16. Evaluation Plan

The project web site contains the project outputs (which are all documentation) and also links to demonstrations of the results described in the documentation. The majority of the links are for internal use only because they demonstrate the authentication and authorisation processes and hence require a valid University of Liverpool username in order to function.

17. Quality Assurance Plan

The links from the project web site to the system implemented demonstrate that we have successfully implemented the systems described in the documentation.

18. Dissemination Plan

All reports are published, without restriction, on the Project Web Site: <http://www.liv.ac.uk/LSIP/>.

19. Exit Plan

No specific arrangements have been made to *archive/preserve project outputs in a JISC data centre or managed repository* but the University will commit to keeping the project documentation available on the University's web site for as long as is required.

All core project documents have been submitted to and accepted by the JISC.

The University will commit to hosting the project web site for at least 3 years after the project ends and will assist the JISC in archiving it subsequently. Links to the demonstration systems will, however, not be maintained after the final project report has been accepted (although they may still continue to work).

20. Sustainability Plan

We will be introducing Shibboleth into user service for the 2007/2008 academic year. A full business plan will be produced as soon as it is clear what the impact of Shibboleth 2 will be.

There are several issues which have emerged from the project which merit, indeed demand, further investigation by ourselves.

We have identified a series of investigations which we need to pursue in order to achieve our objectives. We are aware of the work on Shibboleth 2 and the UK HE Federation and need to track this closely. We will also need to investigate how those applications currently available via our Portal should be integrated into our production Shibboleth environment. We need to investigate how Shibboleth may be integrated in Microsoft Exchange and SharePoint environments. Following the introduction of large scale Grid Computing systems within our Computing Service we need to investigate how developments in the GridShib project may best be utilised.

Appendixes

Appendix A. Summary of Project Achievements

The University's objective for this project was to have a working Shibboleth environment which provided access to a subset of the Web based facilities available from the Computing Services Department to authenticated individuals to whom authorisation to access the facilities had been granted.

It is also the University's objective that once an individual has been authenticated (has proved who they are to the satisfaction of the University) they should not be **required** to re-authenticate (i.e. the system used to authenticate should be a "Single Sign On" [or SSO] system).

Once authenticated, an individual will be allowed or denied access to facilities depending on whether or not they are authorised to do so.

Within the scope of this project, authentication was to be against the University's Novell e-Directory (via its LDAP interface) and only those attributes held in the e-Directory would be used in the authorisation process.

The project proceeded in four separate phases. Each phase was designed to ensure that the installation and configuration processes involved in that phase would build on any verified processes from previous phases.

In phase 1 two separate test Shibboleth environments were set up, one based on Shibboleth 1.2 and one on Shibboleth 1.3. Each test environment consisted of "Service Providers", or "SPs", (a set of web URLs) configured to be accessible to only some individuals based on the values of the attributes associated with their authenticated persona and an "Identity Provider", or "IdP", which provided those attributes in a secure manner. The IdP software was configured to use the PubCookie SSO as its method of authentication (which in turn was configured to use the e-Directory LDAP) and our e-Directory as the source of the attributes used in the authorisation process.

In phase 2 the two test environments were "federated" (i.e. configured so that each SP trusted both IdP's to perform the authentication process) and a "Where Are You From" (WAYF) service installed and configured in such a way that SPs from both environments allowed the end user to choose which environment they wished to perform the authentication. The two environments were configured to release different attributes to the same SP hence enabling verification of the whole process.

In phase 3 access to Athens protected resources (SPs) via the Athens-Shibboleth Gateway was set up. This process involved joining the Athens Touchstone Federation in order for our IdP to be trusted to perform authentication of individuals and to release those attributes required by those SPs.

In phase 4 we setup environments that enabled our VLE (Blackboard), Portal (uPortal) and Web Mail (IMP WebMail) systems as Shibboleth SPs utilising our test Shibboleth environments for authentication. Two of these systems (uPortal, and IMP WebMail) act as "front ends" to other systems which issue authentication requests. In order to allow the "front ends" to perform this delegated authentication in our Shibboleth environments we installed Yale CAS (Central Authentication System) and configured Shibboleth to use this as its authentication system for those SPs.

This project has demonstrated that the Shibboleth environment is able to support the University's objectives with regard to authentication and authorisation and has committed to introducing Shibboleth into user service for the 2007/2008 academic year.