



ShibboLEAP Project

Final Report:

Joint Main Report

Simon McLeish & John Paschoud

May 2006

<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/jointmain.pdf>

1 Project Summary (partners, aims, etc)

This ShibboLEAP project is one of the projects funded under the JISC Call 11/04 for Early Adopters of Core Middleware for Access Management, and was set up in response to a request from JISC to combine six separate similar proposals into a single proposed project.

The London School of Economics acts as co-ordinator and supports the Shibboleth implementations at each site. The six supporting partner institutions are:

- Birkbeck College (Birkbeck)
- Imperial College (Imperial)
- King's College London (KCL)
- Royal Holloway College (RHUL)
- School of Oriental & African Studies (SOAS)
- University College London (UCL)

Each of the seven partners in this proposal maintains an institutional self-archive¹ of academic publications, based on the Eprints.org² software, as part of the SHERPA-LEAP³ consortium. Access to documents in these archives is public and unrestricted, but access management is required to authenticate the identities of academic staff depositing documents, and of library staff who must check or amend descriptive metadata, and approve documents to appear within the public collection. Currently authentication and authorisation is handled within the Eprints.org server, requiring the registration and use of (yet another) password by users, and administration of these registrations by staff supporting the archive.

The project aims were to create a Shibboleth Identity Provider service for all academic and support staff at each of the seven partner institutions in the SHERPA-LEAP consortium, and to implement modifications to their respective Eprints servers to enable them all as Shibboleth Service Providers. The Identity Providers were intended to use existing institutional directory services wherever possible, which means that these Identity Providers would make it possible for staff and students at partner institutions to access other Shibboleth-enabled resources, including those protected by the Eduserv Shibboleth-Athens Gateway. The project also expected to look into membership of both the Eduserv and SDSS (Edina) federations for these Identity Providers, and into setting up a SHERPA-LEAP Federation.

The projects team at the Library of the London School of Economics & Political Science were used to provide project management, technical support for the Shibboleth Identity-Provider and Resource-Provider implementations, and strategic advice and support to other partners on integration with existing institutional services and the organisational issues of supporting such devolved access management. LSE is also a member of the SHERPA-LEAP consortium, and is already capable of operating as a Shibboleth Identity-Provider as a result of prior work (largely supported by JISC) in the SECURE⁴ and PERSEUS⁵ projects. Resources available from the Core Middleware Assisted Take-Up Service to be provided on behalf of JISC from March 2005 were also

¹ The LSE Eprints server is publicly accessible at: <http://eprints.lse.ac.uk/>
Eprints servers of other partners are at similar locations, and all are physically hosted by UCL.

² Eprints.org homepage: <http://www.eprints.org/>

³ SHERPA-LEAP homepage: <http://www.sherpa-leap.ac.uk>

⁴ SECURE Project: www.angel.ac.uk/SECURE

⁵ PERSEUS Project: www.angel.ac.uk/PERSEUS

be used to help to grow local expertise in Shibboleth and related technologies, amongst appropriate support staff at each partner.

Amongst them, the seven partners began the project using a variety of existing methods for user identity and resource access management. These include Athens ('traditional'), AthensDA, various implementations of LDAP, and various data sources used to hold and maintain identity and role attribute information about users (staff and students) registered with them. All had strategic goals to work towards 'single sign-on', and all had the technical capabilities to support the platforms and integration infrastructure needed to operate as Shibboleth Identity-Providers, at least on the pilot scale required to achieve the minimum objectives of this project.

As an alternative to the installation of the eduPerson object class in institutional directories which are crucial to the day-to-day running of the technical infrastructure, several partners chose to use the Identity Provider software to modify the information already available from the directory; it is possible to change the names and values of attributes received from the directory.

This project started on 1 April 2005, and was completed by 30 April 2006 with a final meeting on 5 May 2006 followed by the completion of the final reports.

2 Final Report Structure

Part of the purpose of the project is for the various partners to produce documents which can be used by other institutions to help them to implement a Shibboleth Identity Provider: by choosing the partner most like themselves, an institution should find an account which details how a similar institution installed one, and information about what proved difficult about the implementation.

Thus it makes sense for the ShibboLEAP project to submit a total of eight final reports, which are listed below.

Joint co-ordinating report [this document]

Eprints work report

[<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/eprints.pdf>]

Institutional reports (including details of obstacles; future plans)

- Birkbeck [<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/birkbeck.pdf>]
- Imperial [<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/imperial.pdf>]
- KCL [<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/kcl.pdf>]
- RHUL [<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/rhul.pdf>]
- SOAS [<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/soas.pdf>]
- UCL [<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/ucl.pdf>]

Each of the institutional reports details the installation procedure for their Identity Provider, including the following information:

- Description of the type of institution involved
- Technical description of directories, authentication regimes etc. in use in institution
- Description of installation procedure, including difficulties encountered
- Description of testing by accessing LSE test script and test eprints server
- Future plans for Shibboleth usage

Since part of the purpose of the reports is to act as a source for information on Shibboleth at a specific institution, many of them also include a brief overview of the Shibboleth architecture.

The partners were also asked to choose some main points from their reports to highlight, and these are given here.

<i>Partner</i>	<i>Main points of report</i>
Birkbeck	<ul style="list-style-type: none">● Installation process is too complex; the particular skills required are not those of standard system administrators, as tomcat etc. is more web design● There is lots of documentation available from various sources – but it is not all consistent● There is a granularity problem: how many Identity Providers does an institution need in the long term?● Virtual communities are starting to become important, and Shibboleth will be needed to support many of these

Imperial	<ul style="list-style-type: none"> ● Too much documentation available on the web, but of poor quality and lacking in clarity. No high quality definitive site
Kings	<ul style="list-style-type: none"> ● Documentation is a problem – finding the “right one” is hard ● Skill set of main project staff was not directly applicable; this was a resource issue as the UNIX team was already overstretched ● Lots of help was required from the Service Provider to get it working
Royal Holloway	<ul style="list-style-type: none"> ● Quite a big challenge for an institution with a small IT resource ● Installation is too complex ● Requires good understanding of SSO and directory structures ● Inter-institutional courses may provoke move to Shibboleth but for the time being Athens DA is more useful
SOAS	<ul style="list-style-type: none"> ● Not too many technical problems ● Resource issues for support after the end of the project ● Particular problems may occur with adding a new service provider / federation to the configuration as this is an infrequent task so skills atrophy
UCL	<ul style="list-style-type: none"> ● Installation useful in prompting clean-up of directories; there is a question of whether the directory should change to react to new applications, or whether applications should react to directory structure ● Installation was hampered by lack of local expertise in certain components, notably Tomcat ● Documentation is opaque

3 Summary of findings

Several points on which the partners are all, or mostly, agreed stand out from the institutional reports.

- The installation process is still too complex, and requires skills not generally found together in the university IT support environment (Unix system administration combined with tomcat knowledge).
- The documentation of the installation process continues to be problematic (although, as LSE staff pointed out, it is massively improved on earlier versions). There is a multiplicity of official and unofficial documentation available now, not all of it consistent, and it is very hard for the novice installer to work out which documentation is most relevant to their situation.
- The interaction of Shibboleth with the institutional directory may be problematic, with difficulties installing the eduPerson object class on a crucial service. Existing directories may not be ideal for the purpose, with *ad hoc* changes being made over the years that have led to inconsistencies in the data they contain; and some directory products are unfriendly to changes that are made to the directory schemas. Where the data required is already available in the directory, it is simpler and more robust to use the Shibboleth software to transform attribute names and values to those required by eduPerson.
- There are concerns about running a Shibboleth Identity Provider in the long term that need to be addressed. These include maintaining the Identity Provider in an already stretched IT environment, and the current relative lack of resources to which Shibboleth provides access (along with the difficulty of configuration for those that it does). Almost all of the project partners, however, wish to continue using Shibboleth, and those who expect to remain with existing authentication/authorisation regimes feel that participation in the project was a useful experience.

4 ShibboLEAP and MATU

MATU⁶ (the Middleware Assisted Take-up Service) is a service set up to support the efforts of the participants in the Shibboleth Early Adopters projects, including ShibboLEAP. It offers documentation, training and support (including site visits) to installers of Shibboleth software.

The six partners in the ShibboLEAP project generally made little use of MATU, except for RHUL. Three members of the MATU team made a day long site visit and worked through the installation, testing, and configuration of their Identity Provider with RHUL staff, a service which was considered to be excellent and very helpful. Staff from UCL had attended a MATU training event. Other project partners felt that they would have made more use of MATU if their services had been available earlier and better disseminated to partners; when the ShibboLEAP project started, the MATU service was still in a very early stage of development and it was not at that point clear what they could offer to the partners given the involvement in the project of the LSE as experienced users of Shibboleth.

⁶ MATU homepage: <http://www.matu.ac.uk>

5 Project Deliverables

In the following table, deliverables are listed with due dates in the revised schedule (one month later than in the project proposal).

<i>Deliverable</i>	<i>Due date</i>	<i>Delivered date</i>	<i>Notes</i>
Project Plan	April-05	April-05	Available at http://hdl.handle.net/1988/2753 .
Audit reports on technical environments for Identity Providers.	May-05	July-05	Available at https://projectplace.com/pp/pp.cgi/0/60307721 . Reason for delay: decision to integrate with architecture plans.
Eprints Shib-Target specification.	Jul-05	Jul-05	Available at https://gabriel.lse.ac.uk/twiki/bin/view/Projects/EprintsIntro .
Shib-Origin architecture plans.	Jul-05	Jul-05	Contained in the audit reports.
Alpha release of Eprints ShibTarget.	Sep-05	---	Not released. See eprints strand final report.
Interim progress report.	Oct-05	Jan-06	Delivered to JISC
Test reports.	Nov-05	Nov-05 – Apr-06	Contained in institutional final reports. Delays detailed in reports.
Production release of Eprints ShibTarget.	Dec-05	Feb-06	Available at https://gabriel.lse.ac.uk/twiki/bin/view/Projects/ShibbolethIntegration . See eprints strand final report.
Workshop event.	Feb-06	---	Not delivered. Postponed to become part of wider JISC workshop in Jul-06. Budget redirected to supporting other invited dissemination opportunities.
Evaluation Case Study.	Mar-06	---	Not delivered. Eprints release and institutional Identity Providers available too late for widespread testing; see institutional and eprints final reports for details.
Project Completion Report.	Apr-06	May-06	This document.
Published case study article(s).	Apr-06	May-06	The institutional reports.

6 Dissemination Activities

Date	Author	Activity
24 Apr 06	Paschoud, J., McLeish, S.	'ShibboLEAP: a production model for institutional Shibboleth adoption' – presentation at Internet2 Spring Meeting [http://hdl.handle.net/1988/2807]
17 Nov 05	Paschoud, J., Garibyan, M.	'Shibboleth: in the World, Britain and the LSE' - Shibboleth briefing for LSE Library and IT Services staff, LSE Library [http://hdl.handle.net/1988/2789]
7-9 Nov 05	Paschoud, J.	'ShibboLEAP: How to get lots of Shibboleth users, cheap!' - Presentation at EuroCAMP, Portugal [http://hdl.handle.net/1988/2787]
15 Sept 05	Paschoud, J.	'Shibboleth: Access Management (but not Anarchy) in the UK' - ICAU (SMUG) 16th International Consortium of Aleph Users and International SFX/MetaLib User Group Conference, British Library, London [http://hdl.handle.net/1988/2773]
15 Sept 05	Paschoud, J.	'ShibboLEAP: achieving Shibboleth early adoption goals wholesale', 'LSE Library Access Management projects'- 2 presentations for CAUDIT (Council of Australian University Directors of IT) study tour to the UK, LSE [http://hdl.handle.net/1988/2774]
7 July 05	Paschoud, J.	'ShibboLEAP: Seven Libraries, a Repository, and a leap of faith' - JISC Joint Programme Meeting, Cambridge [http://hdl.handle.net/1988/2758]
29 Jun 05	Paschoud, J.	'Shibboleth 101' - Presentation at MIMAS Open Forum, Manchester [http://hdl.handle.net/1988/2754]
April 05	Paschoud, J., Morrow, T.	'Everything you always wanted to know about Shibboleth' - Presentation at UKSG 2005 Conference, Edinburgh [http://hdl.handle.net/1988/85]

Partners also carried out internal dissemination activities within their institutions, explaining Shibboleth and the ShibboLEAP project to the local IT support team and library staff.

A number of dissemination opportunities have already been identified and arranged, beyond the end of the project, including presentations to the London University Libraries Committee, the London e-Services Librarians liaison group, and the UNINETT2006 Conference (Ålesund, Norway). It is hoped that all partner institutions will be able to allow time for staff who have been involved in the project to share their experiences directly in this way, as interest grows amongst the UK HE community.

7 Project Exit Strategy

The reports from individual partners have covered their own independent institutional plans for future development and use of the services and local experience put in place during the project.

The other outcome of potential value from the project has been the partnership itself, and the working contacts established between institutional partners and (in some cases at least) between staff, within the same institution but previously divided by organisational structures. There is potential for developing and exploiting these contacts further, possibly in collaborative work in the following areas:

- Auditing current institutional identity management policies, practices and systems;
- Identifying further examples of cross-institutional identity and access management, either between the partners or involving third parties;
- Evaluating appropriate levels-of-assurance for user authentication and access to different types of secure online resources;
- Development of model architectures for enterprise directory services, and implementing them in practise;
- Development or testing of technologies to meet other requirements 'peripheral' to the implementation of devolved access management, such as attribute release policy management, fine-grain directory management of roles and permissions.

The institutional diversity (in all but geography) of the ShibboLEAP partnership, the experience gained by a large number of participating staff, and the successful outcomes of this project all reflect an investment which should not be wasted.