SWISh

South West Implementation of Shibboleth

1st June 2005 – 31st May 2006

Final Report

UNIVERSITY OF
EXETER

JISC

Nick Johnson
Project Officer

Ian Tilsed
Project Manager

Contact:
Ian Tilsed (i.j.tilsed@exeter.ac.uk)

Table of Contents

Acknowledgements

Executive Summary

The SWISh Project was funded as part of the JISC Core Middleware Programme, ran from June 2005 until May 2006, and had the following key aims:

- Implement a Shibboleth pilot service at the University of Exeter, involving registered members of the University based in Exeter, and investigate further implementation within the Peninsula Medical School (PMS) and the Peninsula Allied Health Collaboration (PAHC), and at the Combined Universities in Cornwall (CUC) campus in Cornwall.
- Investigate possible integration with the University portal, being developed by our XPort project, and its potential to interact with other campus services, including our VLE service and the Library Management System (produced by Innovative Interfaces).
- Explore and disseminate the issues arising from these developments and will run through a number of phases, widening the implementation of Shibboleth across partner institutions and collaborations in the south west.

Project SWISh chose an incremental development implementation whereby each topic was thoroughly understood, tested and documented before starting on the next. This necessarily involved the installation of a Shibboleth Identity Provider (IdP), together with the Service Provider (SP) and Where Are you From (WAYF) modules, in order to appreciate the full workflow of a successful Shibboleth transaction.

The first pilot, utilising a small group of Library staff, was successful, although it identified a robust identity management infrastructure as a key pre-requisite of any wider implementation of Shibboleth. It became clear that the institutions to which the second pilot would be extended did not have the required identity management infrastructure, nor was it in place at the project host institution. As a result the second pilot was replaced with a full investigation of the requirements for a wider Shibboleth implementation.

Following the successful implementation of a local Shibboleth solution, attention was directed to its wider integration with other campus services, most particularly the portal, library management system and virtual learning environment. It became clear that a single sign on (SSO) solution would be required and, after a review, CAS was chosen. The integration with Shibboleth, fully documented, was a success and the prototype modelling of Shibboleth within an SSO environment became an important output for the project.

Considerable work was carried out to scope the necessary work for Shibboleth implementation for the Peninsula Medical School (PMS), the students and staff of which are members of both the Universities of Exeter and Plymouth, as well as the NHS. Using a WAYF developed by SWITCHaai, an active web page was developed, offering an informative gateway to PMS members. This prototype listed the electronic resources available at each institution and permitted the user, having selected a resource, to select that institution, authenticate against the associated AuthN service and gain access. This prototype has shown what is possible for a complex environment such as the PMS and will lay the foundations for challenging but exciting work in the future.

In conclusion, the project has been very successful, with deliverables exceeding that originally anticipated. The University of Exeter is now committed to the continuing development of the Shibboleth service and plans are in place to move to a production service within the next twelve months, following the further employment of the project officer. The project will continue to disseminate the various findings both locally within the south west and further afield and contribute to implementing an effective solution not just for the University of Exeter, but also partner institutions within the south west peninsula.

Background

During 2004 the University of Exeter implemented several initiatives regarding middleware and authentication/authorisation systems for access to electronic resources. Building on the LDAP directory service that was first installed in 2002, IT Services developed a new schema involving the adoption of the eduPerson, together with a new Exeter schema to reflect local requirements. This revised infrastructure then enabled the installation of Athens DA – moving from a self-registration scheme to a system that utilised existing login credentials, thus simplifying access to electronic resources.

The middleware infrastructure, together with the experience of successfully implementing Athens DA, provided a solid foundation upon which to investigate true 'single sign on' and the implementation of a solution based on Shibboleth is a natural extension of this work. A successful Shibboleth implementation would offer a means by which campus identity and access management infrastructures could be utilised to authenticate individuals and then pass the information about them to resource sites, both within and without the institution, thus enabling those sites to authorise access as appropriate.

With Shibboleth having been chosen by the JISC as the successor to Athens, the exploration and implementation of Shibboleth became a priority. The funding of SWISh has enabled the University of Exeter to continue developing middleware at a time when its importance to the wider aim of enabling seamless access to electronic resources has never been greater.

Aims and Objectives

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

Aim

The aim of the project is to implement a Shibboleth pilot service at the University of Exeter, involving registered members of the University based in Exeter, within the Peninsula Medical School (PMS) and the Peninsula Allied Health Collaboration (PAHC), and at the Combined Universities in Cornwall (CUC) campus in Cornwall. It will also investigate possible integration with the University portal, being developed by our XPort project, and its potential to interact with other campus services, including our VLE service and the Library Management System (produced by Innovative Interfaces). The SWISh Project will explore and disseminate the issues arising from these developments and will run through a number of phases, widening the implementation of Shibboleth across partner institutions and collaborations in the south west.

Objectives

i.   We will establish a Shibboleth server and develop the means by which the service may be offered to users. It will also establish the necessary data flows between relevant University departments.

ii. We will implement a pilot service to a small constituency of Exeter-based users (both student and staff) and subsequently explore and refine the resulting service.

iii. We will further refine the Shibboleth service, expand the first pilot to a greater constituency, and extend the pilot to valid constituencies in the PMS, PAHC and CUC initiatives.

iv. We will investigate the possible use of Shibboleth in relation to the University portal, being developed by our XPort project, and its potential to interact with other campus services, including the VLE and the Library Management System.

v.   We will disseminate the findings of the project as widely as possible and engage in relevant consultations and discussions to support the wider implementation of Shibboleth in UK higher education.

Change

One objective was subsequently altered slightly as a result of findings from the first Shibboleth pilot.

Objective 3 in the original Project Plan was defined as follows:

> *"We will further refine the Shibboleth service, expand the first pilot to a greater constituency, and extend the pilot to valid constituencies in the PMS, PAHC and CUC initiatives."*

The first pilot of Shibboleth (workpackage 4) identified a pre-requisite for greater use of Shibboleth – namely the existence of an identity management infrastructure with a level of granularity that enabled precise control of attributes and authorisations. It became apparent that this requirement was not currently in place both at the University of Exeter and also at some of the institutions involved in the Peninsula Medical School. It became clear therefore that an extension of the pilot to phase 2, involving a wider constituency beyond the University of Exeter, was not viable.

As a consequence the third objective was re-scoped so that it became a study or exploration of the practicalities and issues involved in the implementation of Shibboleth in the PMS, rather than an implementation per se. This work formed workpackage 7 and provides material that will be used to drive forward the development of a Shibboleth solution.

Methodology

In the classic semantics of methodology science, Project SWISh is a prototyped project of "Functional" and "User Interface" type (rather than a "Performance" type) and it was developed within the "Expendable" and "Evolutionary" scenarios (rather than the "External Design" and "Performance"). This means that technological and efficiency concerns were not as important as proving the data transformation work reliably.

The SWISh Shibboleth installation would have to be integrated into an environment of similar projects developing the university portal, WebCT and Innovative Interfaces Millennium. No evaluation of how this could be achieved has been attempted, so devising a formal development methodology ceased after high level workpackage declarations.

The project prototyping scenario, therefore, lies in the expendable and evolutionary domain. It was anticipated that the integration of Shibboleth with other projects would expose deeper identity management issues. This would trigger a reworking of the not only the Shibboleth installation, but the ways in which the portal, library and learning applications performed their authentication and authorization.

Notwithstanding the prototyping nature of the SWISh, formal SSADM methodology rules were followed in establishing service requirements, evaluating design alternatives and elaborating external specifications for each of the work packages.

Implementation

Project SWISh chose an incremental development implementation whereby each topic was thoroughly understood, tested and documented before starting on the next. The University of Exeter has an LDAP service but no SSO solution. The SWISh project team had to ensure that Shibboleth fundamentals were completely understood before offering to provide recommendations to associated institutions on how they could integrate Shibboleth into their existing ID Management systems.

The initial plan was to install the IdP, join the Athens Touchstone Federation and run a trial for selected Exeter users. While the Shibboleth IdP service was being configured and integrated with the LDAP service, a user survey was conducted to learn what improvements could most benefit users when Shibboleth was introduced. An assessment of the weaknesses of the current AthensDA implementation would provide recommendations for additional features to be included in a Shibbolized service.

This implementation was adjusted as the project evolved and is best illustrated in Figure 1.
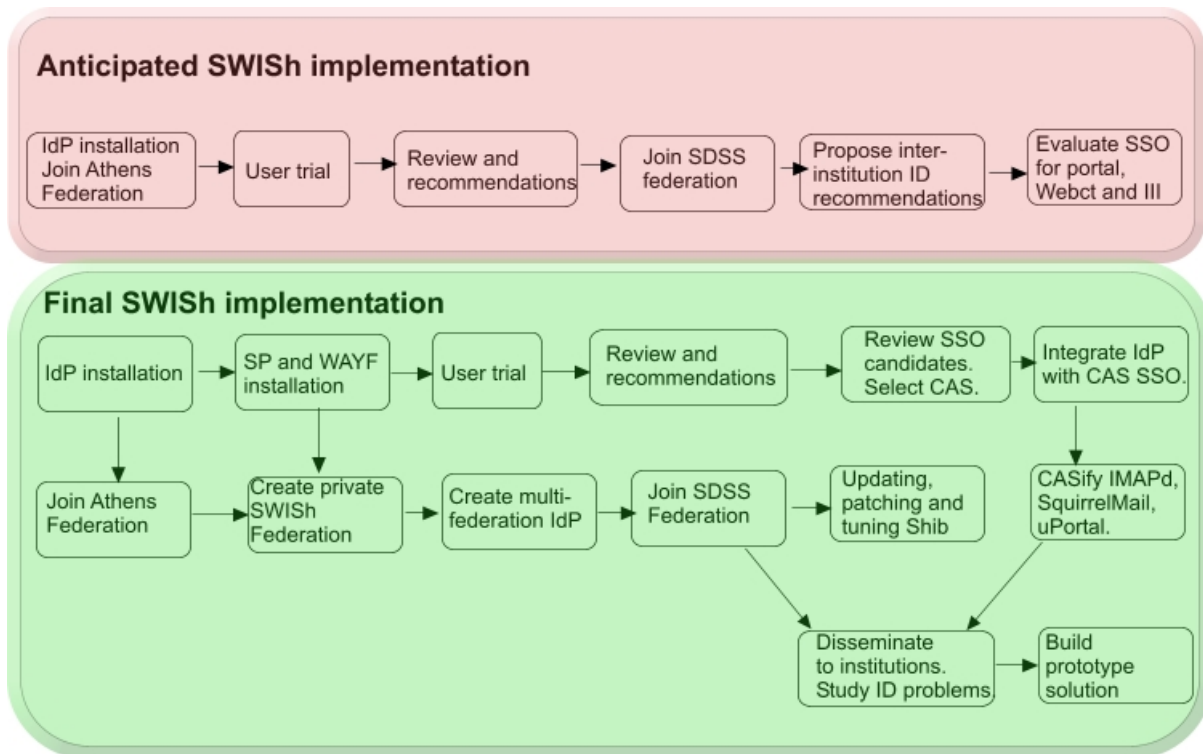
Figure 1. Evolution of Project SWISh implementation

Although the University technically needed to install just a Shib IdP application to gain access to the Shibboleth to Athens Gateway, Project SWISh went on to install the SP and WAYF packages and then configure a private federation. Without gaining this additional expertise, the joining of more federations would have been tedious. A local federation and SP meant that the IdP could be rigorously tested without having to bother AthensDA system administrators for lengthy error message interpretation.

When SWISh joined the SDSS federation, the IdP was already configured as a member of Athens Touchstone, InQueue and the local private federation. So the integration tests with SDSS only need to isolate SDSS SP configuration errors.

Owing to maternity leave in an associated portal project, the final stage of the project was brought forward. This had an added urgency when it was discovered how the associated portal, e-learning and library projects were attempting to perform their versions of SSO. It was agreed to prototype a SSO solution and add the SSO interface modules to as many open source applications as possible to demonstrate the security, clarity and worth of SSO using the LDAP service.

When this was completed, and associated institutions approached to learn how Shib and SSO could improve use experience at the Peninsula Medical School, the SWISh team had a full working knowledge of integrating SSO and Shib into campus applications.

Outputs and Results

1. Shibboleth
The lessons learned about Shibboleth adoption varied from the user perspective of trying to comprehend more new terminology to the administrative backend of how the Attribute Authority (AA) data can be kept up to date. Users are led to believe that Shibboleth is something like AthensDA with additional checking on their rights to see protected web resources. Unfortunately this impression is also being picked up by managers who perceive the change as trivial; after all, the only difference seems to be a "Select Shibboleth Login" button on a web browser. This undersells the architectural impact that the IT Services department has in providing the additional capability.

JISC's announcement of a September launch of the UK Access Management Federation (UK-AMF) is key to conveying the scale of the development work. Project SWISh discovered that one institution is postponing the recruitment of staff to the summer of 2007 as they perceive the integration of Shibboleth as something that can be completed in one year.

The project discovered that installing an IdP alone was not the most effective way of learning Shibboleth, and that it was beneficial to install an SP and a WAYF too This permits a better understanding of the whole Shibboleth process. It is likely that several institutions will not have staff with the full skill set expected by the Shibboleth designers, so a test server is essential. This becomes a workbench on which the Shibboleth administrator can develop specialized Shibboleth knowledge and become familiar with the terminology. Appendix A shows a broad definition of a Shib Administrator skill set.

SWISh created a local private federation, so that the Shibboleth administrator could debug the IdP without having to constantly interrupt an SP, Athens or SDSS asking for copies of their SP error logs. SWISh configured its IdP to be a member of four federations: SDSS, Athens, InQueue and its local private SWISh one.

From the Athens user perspective, the SWISh trial indicated that the change to Shibboleth would help fix "AthensDA problems". These problems were technically nothing to do with the AthensDA architecture, however, but more about its interfaces to LDAP and online resources. For instance, if a student were to enter their student ID number or email address instead of their Exeter userID, the system should recognize the type of invalid input and recommend the user ID. Or, if a connection to an online resource failed because the resource was unavailable they were told that their login had failed implying they had done something incorrectly. Athens administrators use a network monitoring tool to check provider availability. Could this not be integrated into Athens to report how long a provider had been not responding to requests? Library staff at Exeter said that on any day between 10 and 20 online resources could be having problems and 10 to 30% of their week was spent responding to users phone calls and queries about failed access.

2. Attribute Authority

The SWISh trials showed that a single new LDAP attribute, **eduPersonPrincipalName**, (populated generally with their email address) is needed to migrate the user base from using AthensDA to Shibboleth. But SDSS additional attribute requirements[1] displays the potential complexity of administering the attributes for 15,000 students. The special needs for Landmap or EMOL Restricted show that the "single new LDAP Attribute" rule is not valid. If SPs are allowed to flex the full gamut of potential attributes, then the scale of the three dimensional model of (15,000 users x 250 service providers x number of configurable attributes) will be one of UK-AMF's greatest challenges.

From the start of the project, two backend services were installed to capture the knowledge base that SWISh was generating. A Mambo/Joomla content management system[2] (CMS) was configured as a repository for all requirements, designs, installation notes, configuration settings, testing, reports, meeting minutes and presentations. A CVS code repository captured the history of every file alteration on the development server. After Google bots indexed the CMS, the most popular pages on the SWISH website were those describing SSO evaluation. SWISh staff have had requests for help from many UK and European universities after they followed the SWISh SSO installation procedures.

3. Single Sign On

When it was understood that the Shibbed applications for accessing SDSS and Athens were to be pages (tabs) within a portal, the need for SSO was abundantly obvious. To demonstrate the integration elegance of Shibboleth, SSO and a portal, SWISh reviewed the leading SSO products: Yale's CAS, Pubcookie, Cosign and WebAuth. CAS was chosen because of its least possible transmission of a user password, use of SSL, ease of integration with applications and quality of support. Shibboleth was CASified without effort and uPortal installed and CASified.

Demonstrating SSO to Athens and SDSS from within the portal convinced managers to look at how additional applications could be SSO/CAS-ed. As the MyExeter portal was using SquirrelMail and the

---

[1] SDSS Attributes: http://sdss.ac.uk/wiki/wiki.pl?AttributeUsage
[2] Mambo/Joomla CMS: http://gilead.ex.ac.uk/swish

Cyrus IMAPD applications, both these were CAS-ified. Further development work added Moodle to the portal and the completed uPortal demonstration became a central part of selling the need for Identity Management to budget holders.

4. Identity Management
At this point it might seem that SWISh had drifted from its original goal of Shibbolizing a campus. However, it was felt that this was exactly what the Early Adopter programme was attempting to discover. Shibbolizing a campus is not simply installing an IdP. It forces a complete evaluation of a campus ID management. In Exeter's instance this was a topic that had long been considered necessary but a business case had not been made. The SSO-enabled portal focussed attention on the benefits and a IdM plan was written. Its charge is to implement SSO and Shibboleth across the campus, to centralize all user account management and to provide a cross system identifier registry for all campus systems. Tools such as Grouper, Signet and SharpE are being evaluated for use with this service.

Most university IT Service divisions have groups dedicated to PC support, web and email server management, business systems support and the usual networking, telecomm and finance sections. They should be urged to look afresh at delivery of campus IT services. Consider splitting resources into new realms that more accurately reflect today's needs: for example, a dedicated security and internal audit group, middleware provision, upperware (database and business applications), ID Management, local application development (custom integration software development), PC support and so on. This change is illustrated in Figure 2.
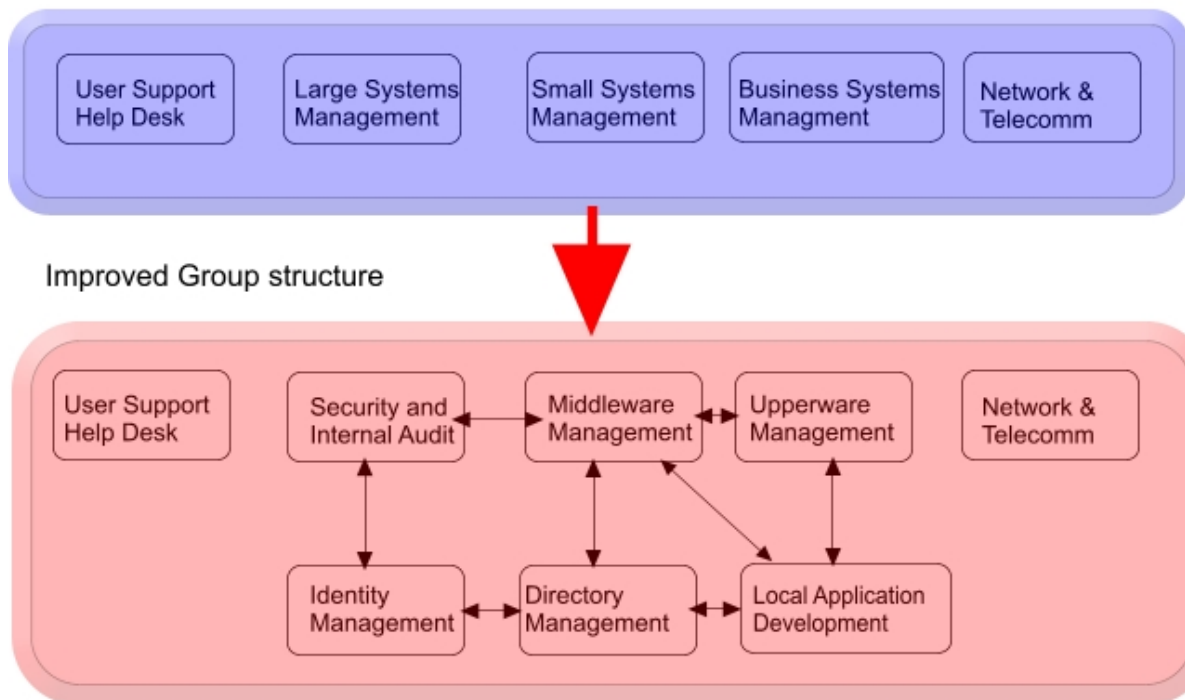

Figure 2. Possible IT Services Reorganization

Shibboleth provision and its associated creation of an AA are absorbed into this kind of structure without effort. It is better that the department reorganize itself before starting on the Shibboleth work and adapt the proposed diagram to better suit their local needs.

5. Peninsula Medical School
The PMS is a joint development by the University of Exeter and University of Plymouth. Staff and students have access to the different Athens resources available to each of these institutions as well as the NHS (if the user is in their third year of study or above) and the PMS' own resources. So users need to understand the reasons for six separate userIDs and passwords: one each for each institution and two more for the classic Athens access using PMS and the NHS. When this administrative

nightmare is added to the requirements of two more local institutions, the Peninsula Area Health Collaboration (PAHC) and the Peninsula Postgraduate Health Institute (PPHI), Figure 3 begins to illustrate the resulting rule set.
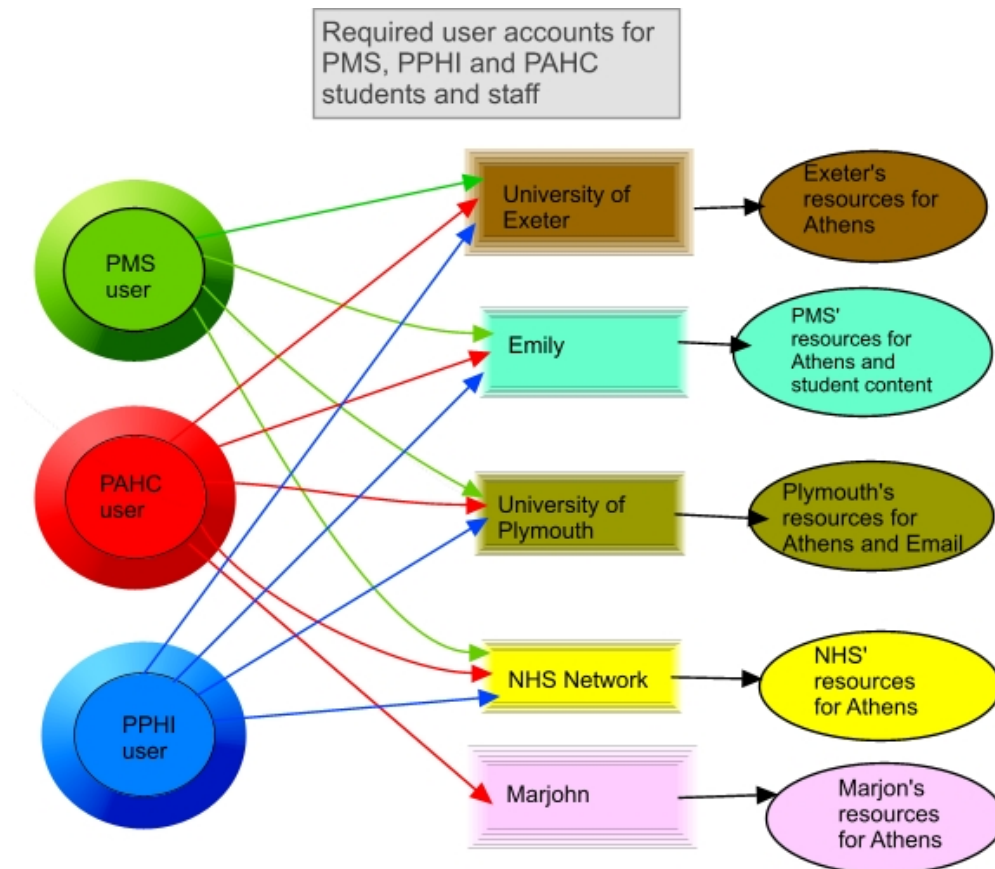

Figure 3: Athens resources for PMS and associated users

PMS students access their Blackboard portal (Emily) and choose a Library tab. They are given a comprehensive but initially confusing gateway to all the library resources to which they are entitled. Appendix B shows how this can be quite daunting for new users, especially as it is not immediately obvious what resources each link can offer.

Using the WAYF developed by SWITCHaai[3], an active webpage was developed by SWISh. Figure 4 shows how the list of resources for each institution is displayed as the mouse is hovered over the name of the institution. When the user sees the journal they are looking for, they select that institution's name and it asks them to authenticate against the associated AuthN service (Figure 5) Figure 6 shows the resulting access for a PMS user using Exeter's Athens resources.

---

[3] SWITCHaai WAYF: http://www.switch.ch/aai/wayf/

Figure 4 SWISh prototype of a PMS Library gateway
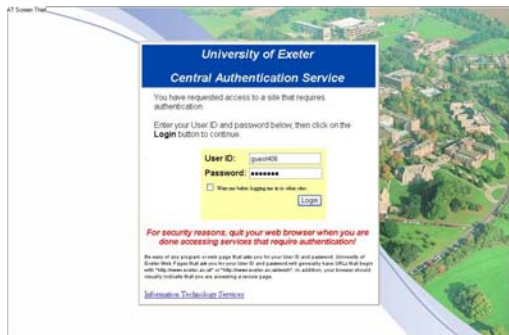
Figure 5 SWISh SSO login page   **Figure 6 Journal page showing correct identification**

The challenge for SWISh was to specify what had to be done to make it work. The Exeter Shibboleth SSO handler was successfully integrated with this test script, but to expand it to the companion institutions requires them all to migrate to Shibboleth. This will be done by PMS and Plymouth by the summer of 2008, but the NHS plans are still difficult to determine. So far there is only a plan for the NHS to introduce SSO using SAML2 standards. Interestingly, Microsoft Vista's InfoCard application does not use the SAML protocol although it can handle SAML1.1 tokens.[4] Design and architecture committees are still debating internally the pros and cons of Shibboleth, principally because of the scale of the implementation. More detail of the NHS infrastructure developments is in Appendix C.

---

[4] MS InfoCard: http://msdn.microsoft.com/msdnmag/issues/06/05/SecurityBriefs/default.aspx

To streamline user logins at PMS, and provide a template solution for similar organizations will require:

- Installation of Shibboleth IdP and associated AA by the University of Plymouth (due 2008) and PMS. As UoP Information Learning Services (ILS) provides PMS' IT server facilities, these are directly connected.
- Installation of SAML2 compliant IdP and associated AA by NHS, within their Contact program.
- Conversion of the demonstration page to use a list of resources using an AJAX script to select, format and sort the set of resources for each institution.

The Athens Linked Accounts project[5] has started trials during the completion of the SWISh project. Its current design limits its use to solving authentication for users with multiple Athens accounts to a just only one AthensDA account but multiple classic Athens accounts. Soon Athens will drop this restriction and SWISh has asked to participate in trials of the Athens Linked Accounts later in 2006.

Outcomes

The project has been able to meet the aims and objectives identified at the outset of the project. The approach was also flexible enough to adapt to developments as they arose during the work, as has been illustrated by the slight re-scoping of objective three relating to the Peninsula Medical School.

In relation to the aim of the project, all three components have been successfully addressed. A prototype Shibboleth IdP has been implemented and a pilot run within the University of Exeter. Furthermore, whilst the second pilot to institutions beyond the University was not implemented, considerable work has scoped the requirements and challenges of such a wider Shibboleth roll-out between institutions within the south west. The aim of investigating wider Shibboleth integration with other campus services has also been successfully addressed. Indeed the work in this area has vastly exceeded expectations and has brought a fuller understanding of SSO and Shibboleth integration, and the requirement for a robust ID management approach. The third aim addressed the need for dissemination within the south west and beyond. In the latter stages of the project, as the wider implementation of Shibboleth was explored, this aim was addressed with vigour and, as a result, has laid firm and promising foundations for future collaborative work within the south west.

The project successfully met the slightly revised five objectives as detailed earlier in this report. A Shibboleth IdP service was successfully implemented with a web front-end, which was subsequently trialled by a small group of Library staff. The flow of data between departments was identified, as were the additional attributes needed in the LDAP Directory. The lack of a robust identity management infrastructure at the University of Exeter (and associated institutions) resulted in the re-scoping of objective three, however. This moved from being a second, extended pilot to a scoping study, which was successfully completed during the later stages of the project. Further work on the integration of a single sign on (SSO) solution with Shibboleth led to a thorough review of wider application with other campus IT services. This work, together with the establishing of a working Shibboleth IdP, was disseminated widely to associated institutions in the south west. The online depository of material arising from the project has also received considerable attention from the wider middleware community, both in the UK and abroad.

A significant outcome that was not initially scoped at the start of the project relates to identity management. Early work during the project identified a robust identity management infrastructure as an essential pre-requisite to the successful production implementation of a Shibboleth and SSO solution. It soon became clear that this infrastructure was not sufficient to permit a wider inter-institutional implementation, nor was it sufficient to move to a production Shibboleth service within the University of Exeter. The identity management issue has, as a direct result of the SWISh project, become a key, strategic deliverable for the newly merged Information Services within the next year. The service requires full time dedicated staff to explain and guide its adoption as well as software developers to configure, integrate and verify the main features of an Enterprise Directory, group management, privilege management and adapting core campus applications to use SSO.

---

[5] Athens Linked Accounts: http://www.athensams.net/news/update_250406.html

Conclusions

Project SWISh has steered away from a deep technical evaluation of Shibboleth as this work is best left to the experts who are still developing and improving it. The Internet2 Shibboleth mailing lists occasionally illustrate the technical complexity that has to be understood before valid contributions can be made to the topic. Instead, SWISh chose to focus on the effects of introducing Shibboleth to a relatively unprepared campus IT infrastructure. After local skills ad been built, the same introduction was made to associated institutions.

University administrators are seeing the migration to Shibboleth as being a similar exercise to migrating their library from classic Athens to AthensDA. This task was delegated down to the owners of LDAP and Active Directory servers and they implemented the task from design, configuration, testing, documentation and migration in at most two FTE months.

The Core Middleware Early adopter programme message will hopefully introduce middleware to campuses where no such ownership authority currently exists. JISC has rightly made a point of referring to the topic throughout its programmes, but it is not certain that the message has been received and understood by all campus IT departments. The belief that Shibboleth is as relatively trivial as AthensDA, and only relates to electronic resources, seemingly persists.

Looking at the cross-institutional needs of Identity Management, focussing especially on PMS student's need to rapidly learn where and how to access resources they are entitled to, SWISh showed that no real progress is possible until Shibboleth Identity Provider services integrated with SSO and AA are added to the University of Plymouth and NHS networks. The work of Malcolm Teague's NHS/HE Forum[6] should be closely watched as this will announce the news of NHS SSO and SAML2 plans as soon as they are publicly available.

In conclusion, the project has been very successful, with deliverables exceeding that originally anticipated. The University of Exeter is now committed to the continuing development of the Shibboleth service and plans are in place to move to a production service within the next twelve months. The project will continue to disseminate the various findings both locally within the south west and further afield and contribute to implementing an effective solution not just for the University of Exeter, but also partner institutions within the south west peninsula.

Implications

In May 2006, only three online resources remained to be converted for use with the Shibboleth to Athens Gateway: Westlaw UK, Dialog Datastar and CrossFire Service. The initial temptation is to recommend the change over to the Shibboleth to Athens Gateway as soon as these resource providers have migrated their services to Shibboleth. Westlaw and Dialog Datastor are the main two providers on which the University of Exeter is dependent and they have yet to convert. The Exeter IT Services department can populate the new eduPersonPrincipalName attribute to the LDAP directory during their next routine service upgrade. With the addition of spare hardware to protect the IdP against catastrophic failure, the SWISh pilot could be transformed into a SWISh production service.

However, with the announcement that UKERNA will introduce the UK Access Management Federation in September 2006, this exercise could be largely academic. If the new federation has the complexity of attributes that SDSS are now using, then the Attribute Authority design and management at Exeter becomes significantly more complex than the addition of a single attribute. As stability of user service is of paramount importance and changes for users need to be kept to an absolute minimum it is preferred to wait until the UK federation is ready and integration is thoroughly tested before migrating the campus user base.

Recommendations

The project identified some specific areas where outcomes led to recommendations that may be of use to the wider middleware community:

---

[6] NHS-HE Forum: http://www.nhs-he.org.uk/

1. The evaluation of usability of the Shibboleth/Athens gateway was delayed by a month because SWISH populated the **eduPersonScopedAffiliation** LDAP attribute as the Athens website documentation explained, but **eduPersonTargetedID** was really required.

> Recommendation: regular review of the content of the federation service provider documentation for accuracy and completeness.

2. The Shibboleth/Athens Gateway trial successfully verified the stable operation of Shibboleth IdP. The major points to emerge are:
- The obfuscated TargettedID appears in the user's browser as a confusing message that reports that, for example, "**_4esmrmxvu6lmcbvcjxv** logged in from **University of Exeter (Local Authentication)".** Although this is technically perfectly correct, a naïve user would be worried that they had not been correctly identified.
- Enabling detailed debugging to Tomcat, Apache and the Shibboleth IdP can add a significant delay in being redirected to the Athens list of Shibbolized resources. This degrades response time from 3 to 30 seconds.
- Some key resources have yet to announce a completion date for Shibbolizing their resources. Of particular interest to Exeter are JSTOR and Westlaw.

> Recommendation: New UK Shib administrators should be pointed to the JISC's UK Shibboleth mailing list. Many topics do not warrant discussion on the Internet2 list where new users are very hesitant to ask basic questions for fear of invoking terse remarks that they should not have started Shibboleth work until they thoroughly understood the fundamentals. MATU is ideally placed to anchor the JISC list.

3. Setting up the SDSS EMOL Restricted service required alterations to configurations at SDSS and SWISh. One exceptional configuration directive had not been fully described: the "scope" of the special **eduPersonEntitlement** attribute apparently should **not** be set to "ex.ac.uk" like every other attribute. SDSS has now posted additional detail on their excellent website, but the odd value remains.

> Recommendation: that service providers should standardize on their "scope". The UK Access Management Federation can couple this with reducing the diversity of eduPerson attribute settings required by every SP in the new federation. This will streamline Attribute Authority maintenance at IdPs.

4. There is no requirement that Shibboleth use a single-sign-on service, but campuses need educating in the larger concept of Identity Management. Having SSO in place reduces later design effort when Shibboleth is implemented on additional campuses services.

> Recommendation: that JISC continue to convince campuses to pay as much attention to enabling ID Management on campuses as they are doing for Shibboleth. SWISH convinced IT managment that ID Management should be a separate line item in budgets requiring its own staffing and financing.

5. MATU was not able to offer the assistance at the start of Project SWISh (June 2005) as they were still recruiting staff. However, after a meeting in Exeter three months later, MATU proved invaluable in getting SWISh' AA SSL layer to work. Like many other early adopters, SWISh developed scripts to assist in debugging and displaying Shib transactions.

> Recommendation: Set up a CVS repository at MATU where locally developed scripts (See Appendix D) can be lodged, version tracked and documented. SWISh has heard informally that this is being set up in the summer of 2006.

References
References have been included as footnotes where required.

Appendix A. Recommended capabilities for a new UNIX Shibboleth Administrator

Shibboleth has been packaged so that an experienced administrator can install and customize a set of files. It is rare that all System Administrators have the full set of core skills before starting a Shibboleth installation, especially as they have to integrate it with a campus' existing infrastructure. Internet 2's Steve Cantor's instructions and replies to email assume a very high standard of knowledge of specific topics. He does not have time to personally tutor every sysadmin who wants to install Shibboleth, so it is important that a sysadmin know what they are expected to be able to problem-solve before they start the work. A straightforward shrink-wrapped Shibboleth installation is a luxury. Making it work within a federation requires many other skills so Table C1 describes the level a *NIX administrator should have.

Skill area	Minimum requirements
Operating System	Security policy management for controlling port use Where to install applications, configuration files. Syslogd operation, writing startup services, obtaining and inspecting packet dumps, writing scripts to monitor and control multiple log files in many windows and using filtering, sorting and pattern matching to reformat output.
Webserver (Apache, IIS)	Knowledge of the configuration files for the webserver and being able to correctly specify values for all directives. Virtual host configuration with SSL. Adding modules, building modules Configuring a content management system to host documentation about procedures and configuration file changes.
SSL	PKI Use of the openssl command and every option Trust stores and certificate stores Obtaining certificates, installing them, converting to/from different encoded methods. Building certificate chains.
HTTP and HTML	Writing simple web pages Meaning of every HTTP code CSS authoring
Tomcat	Configuration files: server.xml, workers2.properties, tomcat-users.xml Application WAR deployment Use of conf, webapps, WEB-INF and classes directories. Mod_jk use and Tomcat modification to use it "ant command" and editing build.properties and build.xml files. Build WAR and dist files.
Java	Log4j and log4cpp configuration options Analyzing stack traces and locating configuration errors.
XML	Format and content of XML files Namespace (xmlns) definition and use XML Schema definitions
SAML	Profiles, bindings and extensions
CVS	Setting up a CVS Repository. Populating (importing) new data Check out/in.

Appendix B: The PMS Emily Library Gateway web page

Library

Accessing Electronic Journals

Access Electronic Journals, up to date lists and collections through both the University of Exeter and University of Plymouth Library Sites. Please see below....

Most Frequently Asked Question

Q. Why is there not a comprehensive list of all the Journals we have access to?

A. The University of Exeter has a Journal Catalogue and the University of Plymouth has an A to Z List of Journals. Both these resources are updated automatically giving you the most recent information and up to date access to Journals. Our previous A to Z listing was often out of date and failed to enable any direct access to the titles located, the new system is regularly updated and provides a direct link to titles located. The advantage of the new system, although having to search two lists means you have access to the most recent and up to date resources.

University Libraries

▶ **Live link to University of Exeter Library site**
To access this site and its links below you need to use an Exeter IT Services Login.

📁 Find a Journal through the Exeter Catalogue
📁 Find a Journal through the Exeter EBSCO EJS Link

What is the difference? Please read this before accessing the above links

❓ More information or help with the UoE Library? ▶ **Live link to University of Plymouth Library site**
To access this site and its links below you need to use your Email login and password.
❓ More information or help with the UoP Library?

Library FAQ's page for frequently asked questions about the libraries
Click here to access the Library Forum
Need help with Emily? Use the **Emily Help Form**

Marjon Library

▶ Click here to access the Marjon **Library site**.

▶ Click here to view Marjon **Library Catalogue**

▶ Take a **Virtual and Audio tour** around Marjon Library

Alternatively, should you need to apply for a Marjon Athens account, please click here for further information and fill out an Athens application form.

❓ If you need further help with the Marjon Library you can use the online enquiry form or email libraryenquiries@marjon.ac.uk

---

PMS Journals update

Please note, we are in the process of subscribing to the following Journals:-

Medical Education, Medical Teacher, Teaching and Learning in Medicine, Journal of Clinical Endocrinology & Metabolism, Journal of Pediatric Endocrinology & Metabolism, Annals of Internal Medicine, Evaluation, Genetic Epidemiology, Health Education and Behaviour, Archives of Internal Medicine, British Journal of General Practice, Medicine & Science in Sports and Exercise, Neuron, Cell, British Journal of Pharmacology, Nature Medicine, Nature Genetics, Nature Cell Biology

If you have any comments of queries about this please contact emily@pms.ac.uk

PMS Journals

Academic Medicine
Journal Information

click here if you are on a UoP computer

click here if you are on a UoE computer or off campus, you will be prompted for your PMS athens username and password

Advances in Health Sciences Education

Journal and Access Information
The BMJ collection
Journal and Access Information

The New England Journal of Medicine (NEJM)

Journal and Access Information

<>

PMS Athens?
The Journals above are subscribed to by PMS. To access them off-campus you will need to use your PMS athens username and password. Athens is an authentication system which is used to ensure that only PMS students and staff are able to access PMS subscribed resources. Your athens username and password will be as follows: place pms in front of your username, for example pmspm04pj (for students) or pmsjbloggs (for staff) and athens1 as the password. If your athens username and password does not work or you have any questions please email emily@pms.ac.uk

Your Comments

Welcome to your new look Library Page. We would welcome any comments or suggestions, please email us
emily@pms.ac.uk

NHS Libraries

▶ **Live link to the Exeter Health Library**

❓ Need help? Email medlib@ex.ac.uk

▶ **Live link to the South Devon and Plymouth NHS Medical Library**

❓ Need help? Email library@phnt.swest.nhs.uk

▶ **Truro NHS Medical Library**

❓ Need help? Email: health.library@cornwall.nhs.uk

The National Electronic Library for Health Programme (NeLH)
Information

Quick link to full text Journals provided on the the NeLH
Information

Other Resources

BioMed Central
Information

Medical Links
Information

View UoP's Online Newspapers and Magazines
To access this you need to use your email login and password.

View UoE's Online Newspapers and Magazines
To access this you need to use an Exeter IT Services Login

Appendix C: NHS Information Technology Infrastructure for England

The Department of Health's "Connecting for Health" agency created in April 2005 is now responsible for the national programme of IT for the NHS. They admit that nothing on this scale has ever been attempted before. It is a system for the NHS in England only and although it "recognizes the importance of compatibility between the systems in use in Scotland and Wales"[7], there is no further elaboration on how these systems are to be compatible. In England, there are 28 Strategic Health Authorities and groups of five, six or seven of them have been brought together into regional clusters to enable local IT solutions to be provided.[8] Each region has selected its own Local Service Provider (LSP) Four IT services consortiums are now developing proprietary solutions for the regional clusters as shown in Table 1.

Cluster	Local Service Provider
Eastern	Accenture
London	BT Capital Care Alliance
NorthEast	Accenture
Northwest and West Midlands	CSC Alliance comprised of CSC, iSoft, Hedra and SCC
Southern	Fujitsu Services providing Cerner Millennium

Table 1. NHS Connecting for Health Local Service Providers

On the face of it this is potentially bad news for unified identity management in the NHS. Each LSP has its own internal identity solution such as Cerner Millennium's Enterprise Master Person Index[9]. However, a set of National Application Service Providers have been appointed to develop major strands of service that affect all services in England. Table 2 shows the organizations that will be developing these services. For SWISh, the most important one is Contact[10]. As well as providing NHSMail, it is the reference name service for SSO and ultimately a SAML 2 service. Currently user databases are maintained regionally on LDAP servers.

Strand	Provider
NHS Care Records Service	BT
Choose & Book	Atos Origin
Electronic Transfer of Prescriptions	
National Broadband network (N3)	BT
Picture Archiving and Communications System	
IT for GPs such as a Quality Management and Analysis System	
Contact – central email and directory service for the NHS	Cable and Wireless

Table 2. NHS Connecting for Health National Application Service Providers

The NHS Central Design Authority and Technology Office develops and controls standards for the NHS IT systems by devising the business and technical architectures within the service. Reduction of diversity of systems and ensuring common use of platforms are naturally important and Enterprise Wide Arrangements with major IT suppliers (Cisco, Documentum, EMC, HP, Novell, Oracle, Sun and others) have been signed.

The National Library for Health (previously known as the National electronic Library for Health) has an Enterprise Architecture Design Authority Group. Malcolm Teague at UKERNA reprsents HE on this board and should be contacted for the latest news in NHS/HE topics.

---

[7] NHS IT compatibility: http://www.connectingforhealth.nhs.uk/faq#faqs
[8] NHS Regional clusters: http://www.connectingforhealth.nhs.uk/regions/
[9] Cerner Millennium EMPI: http://www.cerner.com/public/Cerner_3.asp?id=774
[10] Contact: http://www.connectingforhealth.nhs.uk/delivery/programmes/contactmail

Appendix D: Locally developed scripts for SWISh operation and development

Script name	Purpose	Run frequency
Parse-shib-logs.pl	Display three columns showing parsed and stripped log entries for IdP, WAYF and SP for a specified minute	As required to analyze a recent session
Parse-idp-logs	Detailed colour-coded IdP parsed and stripped log interpretation for a specified minute	As required to analyze a recent session
Startlogwindows.sh	Open 10 xterm windows, each tailing a specified log file	When debugging sessions
Restart-web-sh	Shut down and restart tomcat, httpd and shibd	After configuration change
Del-old-logs.sh	During debugging many directories fill with unwanted log files, so this script prunes older log files	Once a week it clears 14 day old logs.
Overnight-safety.sh	Additional safety script that tar's /opt, /var/www/html/ and /var/lib/mysql and rotates the previous 4 tar files. The resulting tar is copied off the server each night	Every night
Check_shib_logs.sh	Look through all Shib logs for WARN or ERROR and email the results to the Shib administrator	Before start of work each day
Shib-cvs-audit-sh	Check all CVS-ed directories for files that have been modified or created, that are not fully synced in the CVS repository	Whenever a new feature has been added or debugged
Shib-cvs-check.pl	Interactively verifies every file in all CVS-ed directories with "cvs status" and shows a "cvs diff" and offers a "cvs commit" for any non-synced files.	Whenever a new feature has been added or debugged