

Federated access management:
case studies supporting the
business case toolkit

Federated access management:

case studies supporting the business case toolkit

CC297D002-1.0

10 July 2007

Cover + 42 pages

Dr Claire Davies
Matt Shreeve

Curtis+Cartwright Consulting Limited

Main Office: Surrey Technology Centre,
Surrey Research Park, Guildford
Surrey GU2 7YG

tel: +44 (0)1483 295020

fax: +44 (0)1483 295021

email: postmaster@curtiscartwright.co.uk

web: <http://www.curtiscartwright.co.uk>

Registered in England: number 3707458

Registered address:
Baker Tilly, The Clock House,
140 London Road, Guildford,
Surrey GU1 1UW

List of contents

List of abbreviations	3
1 Introduction	5
1.1 General	5
1.2 Background	5
1.3 Case studies	5
2 Cardiff University	7
2.1 Overview	7
2.2 Background	7
2.3 Aims	9
2.4 Scope	9
2.5 Plans	10
2.6 Implementation	12
2.7 Issues encountered and lessons identified	14
2.8 Future plans	15
2.9 Useful resources	15
3 Kidderminster College	17
3.1 Overview	17
3.2 Background	17
3.3 Aims	19
3.4 Scope	19
3.5 Plans	19
3.6 Implementation	21
3.7 Issues encountered and lessons identified	23
3.8 Future plans	23
3.9 Useful resources	24
4 University of Surrey	25
4.1 Overview	25
4.2 Background	25
4.3 Aims	27
4.4 Scope	27
4.5 Plans	27
4.6 Implementation	29
4.7 Issues encountered and lessons identified	32
4.8 Future plans	33
5 University of Warwick	35
5.1 Overview	35
5.2 Background	35
5.3 Aims	36
5.4 Scope	36
5.5 Plans	36
5.6 Implementation	38
5.7 Issues encountered and lessons identified	40
5.8 Future plans	41

This page is intentionally blank

List of abbreviations

ASMIMA	Adoption of Shibboleth for Multiple Identity Management Applications
AY	Academic Year
CAS	Central Authentication Service
CM	Core Middleware
FE	Further Education
FTE	Full Time Equivalent
HE	Higher Education
ICT	Information and Communications Technology
IdP	Identity Provider
IDM	IDentity Management
I2	Internet2
INSRV	INformation SeRVices
IT	Information Technology
JISC	Joint Information Systems Committee
KC-ROLO	Kidderminster College - Repository Of Learning Objects
MATU	Middleware Assisted Take-Up
MCE	Member Categorisation and Entitlement
MIS	Management Information System
MWE	Modern IT Working Environment
RSC	Regional Support Centre
SAML	Security Assertion Markup Language
SP	Service Provider
TCO	Total Cost of Ownership
VLE	Virtual Learning Environment
VRE	Virtual Research Environment
WAYF	Where Are You From
WG	Working Group
WM	West Midlands

This page is intentionally blank

1 Introduction

1.1 General

- 1.1.1 This supplement accompanies the JISC business case toolkit to support institutions making decisions about federated access management.¹ This document supports the toolkit by providing "real world" insight through four detailed case studies.

1.2 Background

- 1.2.1 The access management landscape for education and research is undergoing significant change within the UK and the rest of the world. New technologies and services are available to protect electronic resources and services. Universities and colleges need to determine how they will address these changes and opportunities.
- 1.2.2 The development of a new and federated access management infrastructure in the UK has been embodied by the launch of the UK Access Management Federation for Education and Research ("the Federation") by the Joint Information System Committee (JISC) in November 2006.
- 1.2.3 The existing Athens system will be available via a subscription service within the Federation from August 2008. The JISC will not be funding Athens from this date and all institutions using an outsourced identity provider, like Athens, will need to subscribe.
- 1.2.4 The JISC ran two development programmes between April 2004 and March 2006 to plan and prepare for the new infrastructure. These Core Middleware programmes (CM programmes) established the early elements of the infrastructure and generated lessons for institutions in the future. The CM programmes covered internal, third party, inter-institutional and *ad hoc* collaboration uses of federated access management.

1.3 Case studies

- 1.3.1 The case studies presented in this document cover four institutions that have undergone projects to improve their identity and access management systems and processes. These institutions have experience of making strategic and operational access management decisions, completing projects and realising benefits. They are introduced overleaf, and set out in full in the remainder of this document.

¹ *CC297D001-1.0 federated access management: institutional business case toolkit*, 10 July 2007.

Cardiff University

Cardiff University is a large institution comprising approximately 5,000 staff and 18,000 students spread across 28 academic schools and 5 administrative directorates. It has close links with NHS Wales.

The main aim of the project was to implement Shibboleth technology as a replacement for the extant Classic Athens access management system in conjunction with funding received from the JISC as an Early Adopter of Shibboleth technology.

The project was carried out by Cardiff's Directorate of Information Services (INSRV), which aims to deliver superior computer, library and media services that make a distinctive contribution to CU's research, learning, teaching, community activities and administrative functions.

Kidderminster College

Kidderminster College is a small college in the West Midlands, supporting approximately 5,100 students, of which 1,000 are full-time. Kidderminster offers a wide selection of full-time and part-time courses lasting up to 2 years.

The main aim of the project was to implement federated access management using Shibboleth technology within Kidderminster College to link together web-based resources.

The project was carried out by the Development team within ICT Services. Kidderminster, unlike many FE colleges, has a dedicated IT development team that does not have a support remit. The ICT Services Development team is well resourced, well trained, proactive and confident with open source software.

University of Surrey

The University of Surrey is a moderately large campus university, supporting approximately 18,500 users. It has an institution-wide policy to implement mature commercial systems and has a very lean staffing structure.

The main aim of the project was to replace the Classic Athens access management system at Surrey and to implement a devolved authentication system in order to reduce the administrative burden on IT staff.

The project was carried out by the Library and IT Departments which are separate but under the joint remit of the Director of Information Services. IT Services to provide a high quality, user focused IT service that meets both the academic and business needs of the University.

University of Warwick

The University of Warwick is a large institution comprising of approximately 5,000 staff and 16,000 students. It has five main schools, including Warwick Business School.

The main aim of the project was to upgrade the extant access management system (for access to web services) at Warwick to improve its security.

The project was carried out by Warwick's E-lab, the development division of its IT Services. It has teams covering web services, e-learning, projects development and business systems. Its purpose is to provide a focal point for development, especially work relating to the web.

Figure 1-1: institutional case studies

2 Cardiff University

2.1 Overview

2.1.1 Cardiff University embarked on a project to implement Shibboleth technology as a replacement for the extant Classic Athens access management system in conjunction with funding received from the JISC as an Early Adopter of Shibboleth. The Shibboleth project was enabled by a project to upgrade and rationalise its IDentity Management (IDM) procedures, and in turn the Shibboleth project was a major driver for the IDM project to establish and assign user entitlements.

2.1.2 The project was enabled by excellent communication between library and IT staff which was facilitated by Cardiff having a converged library and IT department, INformation SeRVices (INSRV). The project was split into two parts: developing the infrastructure and implementation and rollout; responsibility for the former laid with the IT staff and the latter with library staff. Shibboleth technology was rolled out to new users in July 2006, and will be rolled out to all users in summer 2007. Classic Athens will be switched off in time for July 2008 when OpenAthens becomes a subscription service.

JISC Collections banding	B
Number of users	18,000 FTE students, 5,000 staff
Project start date	April 2005
Project end date	Ongoing (Shibboleth rolled out to new users July 2006)
Key project aims	To implement Shibboleth technology as a replacement for the extant Classic Athens access management system
Decision making stakeholders	Project Director (Assistant Director of Information Services) Project Manager (Principal Consultant for Strategy, Projects and Liaison) Project steering group to approve decisions
Funding	From internal INSRV budget and JISC Early Adopter funding
Key milestone	Rolling out Shibboleth technology to new users
Current access management system	Shibboleth (I2 reference implementation)
Previous access management system	Classic Athens (and Cardiff's unified sign-on system)
Federation members	Yes

2.2 Background

Cardiff University

2.2.1 Cardiff University is a moderately decentralised University which recently merged with the University of Wales College of Medicine, resulting in an institution now comprised of approximately 5,000 staff and 18,000 students spread across 28 schools and 5 administrative Directorates.

2.2.2 INSRV is a division of Cardiff University which combines the IT and library departments. INSRV manage many different systems and has a wide range of expertise spread across many platforms, vendors and systems, including Unix/Linux systems and tools and Novell products.

Cardiff University has 18 departmental libraries that are independent but work closely together under the common branding of INSRV; with each library also having specific subject librarians.

- 2.2.3 Cardiff University is a major user of Athens protected services, with more than 1 million Cardiff logins to the Athens service each year. The Classic Athens service was a centralised repository of user accounts and credentials managed at a local level. Thousands of Athens accounts were created at the start of each new academic session, with users obtaining their Athens usernames and passwords from library staff.

Early Adopters

- 2.2.4 In April 2005, the Directorate of Information Services at Cardiff University was funded under the JISC Core Middleware Programme for the Adoption of Shibboleth for Multiple Identity Management Applications (ASMIMA) project. The core aim of the project was to implement Shibboleth technology at Cardiff University in order to:

- replace the use of Classic Athens;
- help improve joint Cardiff University/NHS staff's computing experience;
- investigate Shibboleth technology as a method of access management to an e-Science application.

Service providers

- 2.2.5 In addition to Athens protected e-journals, Cardiff has a number of internal web services available to users. Many of these services authenticate users against Active Directory and are part of a unified sign-on system. The web services available to users at Cardiff University that are part of the unified sign-on system include:

- Blackboard Virtual Learning Environment (VLE);
- Voyager library management system;
- email.

Identity management

- 2.2.6 Cardiff has a project to upgrade its identity information (*eg* that held in databases and directory services) to enable access and use to be based upon a person's single identity and administered through a single interface.

- 2.2.7 Cardiff started considering IDM and central repositories in 1998 when it was realised that the institution needed to manage identities rather than usernames. The IDM project started in 2002, three years before the Shibboleth project. The benefits of IDM have already been realised, for example the automated provisioning of user accounts is expected to save 2-3 weeks of effort and time, per school, each year.

2.2.8 The IDM project was considered an enabler for the Shibboleth project. However, the Shibboleth project was also a major driver for the IDM project to assign entitlements to users. To be able to become Shibboleth-enabled, a user must have a Cardiff account and must be a member of Cardiff University. Towards the end of 2005 a Member Categorisation and Entitlement (MCE) Working Group (WG) was set up to establish:

- who is a member of Cardiff University;
- what entitlement to services each user has;
- how groups of users should be categorised.

2.2.9 This has been a very labour intensive task,² particularly in the first 3 months, and has taken 18 months to date. It will result in entitlement policy (and governing processes) being established at a University level through approval by the University Board. Assigning user entitlements has been particularly complicated at Cardiff due to the university being attached to a medical school, which adds a large number of exceptional groups, for example NHS consultants that are training Cardiff students and require some access to elements of the VLE to help with teaching.

2.3 Aims

2.3.1 This case study focuses on the first aim of the ASMIMA project, to implement a Shibboleth Identity Provider (IdP) at Cardiff University as a replacement for the extant Classic Athens access management system.

2.4 Scope

2.4.1 The scope of the project was to Shibboleth-enable Athens protected resources. The Blackboard VLE, email and services from the Modern IT Working Environment (MWE)³ are not in scope. The VLE and email are currently not high priority to Shibbolise as they are already part of Cardiff's unified sign-on system.

² Taking up approximately 3 months at 0.75 FTE of the User Enablement Manager's time, as well as other members' attendance at a WG.

³ Modern IT Working Environment (MWE) is a programme to help staff and students manage many aspects of their University life online, including reading lists, timetables to social events and networking groups and information sharing using collaborative workspaces.

2.5 Plans

Strategic drivers

2.5.1 The major strategic drivers of the project were:

- Classic Athens involved a significant administrative and support burden for library staff;⁴
- the administrative process of account creation at the start of each new academic year was time-consuming and pressured;
- having multiple passwords to remember did not provide a good user experience, and was seen as a barrier to use of e-Resources;
- be aligned with the JISC's initiatives and adopt an internationally recognised standard.

Options appraisal

2.5.2 In 2005 Cardiff was actively looking for a replacement for their Classic Athens system. The Assistant Director of INSRV monitors technological advancements and trends, and was aware of federated access management and a number of technical solutions that were available including Internet2's Shibboleth technology, AthensDA and Liberty Alliance ID-FF solutions.

2.5.3 INSRV's Assistant Director was about to propose a project to implement AthensDA when the JISC announced its plans for Early Adopters of Shibboleth under the CM programmes. INSRV stakeholders met and decided that they should adopt Shibboleth technology in preference to AthensDA.

2.5.4 The major risks of adopting Shibboleth were seen to be:

- Shibboleth was an unproven technology;
- Athens Service Providers may not be compliant with the Shibboleth-Athens gateway in time for deploying Shibboleth technology at Cardiff.

2.5.5 The major benefits of adopting Shibboleth were seen to be:

- minimal duplication of effort. The UK's education and research sector appeared to be converging on Shibboleth technology, so it was likely that they would be required to implement Shibboleth technology in the future;
- Cardiff could apply for funding as an Early Adopter. The Early Adopter project was approached with the intention of going into service, but did not require absolute commitment.⁵

⁴ This was a particular problem as library staff had to issue two usernames and passwords to each user (Athens and local), and there were substantial helpdesk overheads with the majority of queries relating to forgotten passwords.

2.5.6 Although Shibboleth was an unproven technology, it had been internationally adopted and was widely accepted as the way forward for access management. In the event that Shibboleth technology did not meet Cardiff's requirements, AthensDA would still be available as a fall-back option if Shibboleth technology was not successful.

Affordability

2.5.7 Prior to the Shibboleth project, Cardiff had invested in excess of £1M in the IDM project.

2.5.8 Cardiff received £50,000 from the JISC for the ASMIMA project. No additional funding has been formally accounted but any additional funding for the project came out of the INSRV budget. The Shibboleth project was never costed to a point where it was considered unaffordable.

2.5.9 The estimated split of core effort (in hindsight) for the Shibboleth project, including the MCE WG, was:

- **Technical implementation and researching technologies:** 2 months of a dedicated IT officer's time.
- **Chasing publishers for compliancy:** 1-2 months of a librarian's time.
- **User entitlements:** 2 months of a User Enablement Manager's time plus 1 month of stakeholder meetings.
- **Communications:** 1 person-month for communicating and publicising the change.
- **Project management:** 0.5 months of project manager time.
- **Training:** 1 person-month.

2.5.10 A technical expert was brought in for making certain changes to the identity management system.

2.5.11 Hardware purchase costs equalled £6k, although a load-balancer was internally available and not purchased separately. The technical cost of running the full Shibboleth IdP was estimated as £3k for one server with a lifetime of three years: for the 2 servers this is equivalent to £2k/year.

2.5.12 The breakdown above equates to a cost of approximately £30k. However, Cardiff estimates that in reality the total project budget was £75-100k.

⁵ It was, however, stated that after Cardiff was aware that Shibboleth technology was what the UK educational sector was converging around; Cardiff would have chosen to implement Shibboleth technology even if it had not received funding from the JISC.

Achievability

- 2.5.13 It was assessed that the project could be achieved within INSRV's capability and capacity, and that they had adequate in-house skills to carry out the project. However, the JISC Early Adopter money enabled a dedicated IT officer to be employed who has now built up a significant expertise in Shibboleth technology, IDM and directory services.
- 2.5.14 Cardiff University set up a project team for the ASMIMA project and followed the University's project management framework.⁶ A project steering group, comprised of INSRV assistant directors and user representatives, was also set up to act as an authoritative body to approve decisions made by the project team and for exception handling (in the case of major changes in scope or financial issues). The project team met regularly, and there were also meetings at lower levels, for example at one point relevant library staff were meeting every two weeks.

2.6 Implementation

Outcomes

- 2.6.1 The project was split into two sub-projects with separate allocation of responsibilities:
- development of the IT infrastructure (IT staff);
 - implementation and roll-out (library staff).
- 2.6.2 The technical aspect of the project was seen as the more straightforward aspect of the project, and the Internet2 Shibboleth reference implementation was adequate for Cardiff's requirements. Resilience and load testing was built into the project at an early stage, for example by having a load testing plan and by implementing two servers behind a load-balancing switch to increase resilience. A third virtual server is being implemented to meet the policy of ensuring two live servers for maintenance and upgrades. INSRV decided to migrate users slowly to Shibboleth technology to ensure that the servers could handle the load.
- 2.6.3 It was decided that the library staff were best suited to oversee the implementation and roll-out as they are closer to the users, and better ambassadors who could promote the new technology to the users. The library also meets every new user who comes into the university. The library also took ownership of the new access management system.
- 2.6.4 A large part of the project was pressurising service providers, together with the JISC community, to ensure that the majority of service providers were compliant with the Shibboleth-Athens gateway in time for roll-out of Shibboleth technology at Cardiff.
- 2.6.5 Cardiff rolled out the new service to all users in September 2006. Initially, only new intake (staff and students, approximately 4,500 users) were informed about the new service, so that migration was gradual and the resilience of the system could be monitored. The library also stopped issuing Athens accounts to users requesting access to electronic resources; instead they were given Cardiff Shibboleth-enabled accounts.

⁶ This framework is ordinarily only used for projects >£1M, but was used in this instance to meet the JISC's reporting requirements for the ASMIMA project.

- 2.6.6 Currently, 52% of all traffic goes through the Shibboleth-Athens gateway. There are 10,000 unique users accessing resources via Shibboleth, which means that additional users have migrated independently ahead of schedule (there are only 2,500 first year students). This additional uptake by existing users has been achieved without publicity.
- 2.6.7 The implementation and roll-out required good coordination between all libraries to train staff. Staff training was achieved by:
- emails to subject librarians;
 - presentations to library staff in May and June 2006 explaining what Shibboleth technology is and why Cardiff are implementing it;
 - dissemination of information gathered by library staff at presentations to other library staff.
- 2.6.8 User awareness was achieved by contacting individual schools and advertising as much as possible using a wide variety of media to ensure coverage. This included:
- instructions on web pages on how to use the new service;
 - paper forms in library;
 - presentations available on a shared drive.
- 2.6.9 All libraries can now refresh a user's Shibboleth-enabled local password from any library terminal, and passwords can be reset via one central email address.

Benefits realised

- 2.6.10 This project has brought many benefits to Cardiff University:
- The administration burden associated with Classic Athens has been removed, and the administrative process is now much slicker. Helpdesk enquiries have been cut by half, and the support burden is no longer on the library team;
 - The user experience has been enhanced: all feedback from staff and students has been positive, and many existing users migrated ahead of schedule without publicity to achieve the benefits of unified sign-on;
 - Users are able to access web resources externally;
 - Implementing Shibboleth has saved Cardiff money. The total cost of ownership is assessed to be less than OpenAthens subscription charges;
 - Cardiff has better licence management, and is more prepared for any licensing audits as they now know exactly who their members are and their specific entitlements.
 - Cardiff has been able to have a long migration period that has enabled them to carry out in-depth load and resilience testing. Additionally a large number of users have migrated themselves which has reduced the training burden.

- The Shibboleth project gave an extra spur to the IDM project, and Cardiff found questions that had not even been considered, such as the entitlements of anomalous categories of users, for example visiting academics and NHS staff;
- Cardiff's federated access management infrastructure will facilitate collaborations with other organisations with federated access management in the future, and allow research groups to be spread across multiple institutions.

2.7 Issues encountered and lessons identified

2.7.1 The project is considered to be a great success. Very few issues were encountered throughout the project. The technology worked smoothly and there were very few teething problems. The following issues were encountered:

- Not all service providers are ready for, or are looking to adopt federated access management. In this instance, a significant library overhead was required in summer 2006 to get service providers aware of the issue of compliance with the Shibboleth-Athens gateway to provide their services to Cardiff. There is now only one major service provider that is not compliant; alternative access mechanisms have been implemented in the meantime, which although less than satisfactory is adequate. This exception was not considered to be a sufficient reason to prevent Cardiff going live with federated access management, although the project could have been stopped up until August 2006.
- Logging into Athens using Shibboleth creates a new Athens account, and some personalisation features can be lost in some instances, for example the searches and alerts are not transferred across.
- It was necessary to assign the entitlement to services each user category has to allow fine-grained control over user access.

2.7.2 Cardiff identified the following lessons:

- It is essential for the IT department and the library to work closely together.
- A dedicated IT officer has been beneficial to expedite the implementation process.
- Deploying Shibboleth forces an institution to do several things it probably should have already in place, but likely does not (*eg* a comprehensive identity management system, proper directory services and good intra-institution political goodwill), and reinforced the need for clear policies and guidelines on the many different categories of staff and students and their entitlements. The tightening up of these policies may encounter some user resistance (*eg* implications for retired staff members).
- IDM is greatly complicated by having a medical school attached to the University, and produced many more anomalous categories of users to assign entitlements. It is important to resource assignment of entitlements properly, even though it may be difficult, or impossible, to assess the scale of the task from the outset.
- Clear documentation and user guides will be necessary if users are to make sense of the very complex access management landscape in the UK over the next few years

(*eg* Shibboleth, Shibboleth-Athens gateway, the Athens-Shibboleth gateway, Classic Athens, and IP authentication all existing at the same time).

- INSRV completed an essentially bottom-up project, which revealed problems and opportunities with processes as they went along, which they were fortunately able to solve and exploit. A “big picture” view of all the processes would have helped to identify potential issues early on, but would have been much harder to achieve at the outset.
- Implementing a Shibboleth IdP is technically fairly straightforward, if you have all the necessary back-end requirements in place. Shibboleth technology does not take much to maintain once it is up and running.

2.8 Future plans

2.8.1 Cardiff identified the following plans for the future:

- Cardiff are intending to roll-out Shibboleth technology to all users by summer 2007, and switch off Classic Athens in time for the introduction of the new charging regime in July 2008.
- Consideration is being given to improving the user experience even further, for example by bypassing the WAYF as this is what causes the most user problems.
- Cardiff intend to use Shibboleth Service Providers (SPs) to manage access to its services, for example to enable collaborative research.
- Consideration is being given to marketing their expertise to become an outsourced identity providers for smaller institutions.
- Collaborative working with the NHS to enable medical students to have only one Athens account (at present they have two – one with the NHS and one with Cardiff).
- Cardiff are looking to Shibbolise further applications, for example MetaLib (a consolidated searching environment), and considering using a Shibbolised version of their Blackboard VLE.

2.9 Useful resources

2.9.1 The following resources provide further information on Cardiff’s activities:

- final report from the ASMIMA project;
- exemplar user categories from the MCE WG;
- paper on the resilience of their Shibboleth IdP architecture;
- test plan from their deployment.

2.9.2 These resources are available at:

- http://www.jisc.ac.uk/whatwedo/themes/access_management/federation/federation_re_s_casestudy.aspx.

3 Kidderminster College

3.1 Overview

- 3.1.1 Kidderminster College has deployed federated access management using Shibboleth technology to link together web-based resources. The main aim was to increase the usage of their Moodle VLE by allowing seamless access to the network and the VLE. The project ran smoothly, and the production service went live in April 2006. Kidderminster now operates a single sign-on system that has improved the user experience and allows external access to web resources.

Institution	Kidderminster College
JISC Collections banding	I
Number of users	5,100 students (of which 1,000 are full-time)
Project start date	April 2004
Project end date	April 2006
Key project aims	To increase the usage of Kidderminster's Moodle VLE by making it more user friendly by providing single sign-on between the VLE and network access. It was also intended to share specific courses between institutions using the VLE.
Decision-making stakeholders	Vice Principal Head of ICT Services
Funding	JISC Early Adopter funding and ICT budget
Key milestone	Shibboleth production service going live (April 2006)
Current access management system	Shibboleth v1.3
Previous access management system	Username and password for most services, and Classic Athens
Federation members	Yes

3.2 Background

Kidderminster College

- 3.2.1 Kidderminster College is a small college in the West Midlands, supporting approximately 5,100 students, of which 1,000 are full-time. Kidderminster offers a wide selection of full-time and part-time courses lasting up to 2 years, and is particularly reputable for its performing arts department. Kidderminster also has students from the University of Worcester doing courses at Kidderminster College.
- 3.2.2 Kidderminster has an ICT Services team that, unlike many FE colleges, has a Development team that is dedicated to IT development without a support remit. The ICT Services Development team is well resourced, well trained, proactive and confident with open-source software. This capability was generated from the deployment and subsequent development of the open-source (Moodle) VLE in 2003.

JISC CM projects

- 3.2.3 As part of the JISC funded Regional Pilots within the Distributed e-Learning Programme, Kidderminster College worked on the Shibboleth component of two projects, WM-share⁷ and ePistle,⁸ which involved the implementation and deployment of federated access management to help deliver the required resources to the end-users.
- 3.2.4 Additionally, Kidderminster College (together with partners University of Worcester and RSC West Midlands) was funded for the 2 year Kidderminster College - Repository Of Learning Objects (KC-ROLO) project under the JISC's CM Technology Development Programme. The main aim of the project was to implement federated access management between Kidderminster College and the Regional Support Centre (RSC) West Midlands⁹ to provide a secure way to share repositories and VLEs.
- 3.2.5 The initial approach to the KC-ROLO project was to implement the Shibboleth IdP and SP at Kidderminster College, the element of the JISC funded projects that this case study will focus on. Future work on the KC-ROLO project involved the introduction of multiple IdPs, and setting up a WAYF at Kidderminster for a regional federation.

Service providers

- 3.2.6 The majority of the services offered at Kidderminster are internal services. All users have access to:
- the VLE;
 - file and print services;
 - email (staff only currently; email for students anticipated from July 2007);
 - a limited number of Athens protected resources (although there is very little user-demand for these);¹⁰
 - a web-based information repository (which only staff can add content to).

Identity management

- 3.2.7 When a student enrolls at Kidderminster, they are given a unique identity number that they use to create their own user account (username and password). This account automatically expires after one year unless IT Services are informed otherwise. Expired accounts are archived.

⁷ The West Midlands (WM)-share project to establish a protected repository of learning resources that are only accessible by partner institutions.

⁸ A flash-based e-Portfolio that allows protected authentication and utilises the use of attributes to get user-specific data such as date of birth.

⁹ Before implementing a similar setup at the University of Worcester.

¹⁰ The exceptions are students on the film-making course and hairdressers who use a hairdresser training package.

- 3.2.8 User information is stored in the Management Information System (MIS). Kidderminster's Active Directory links user accounts to attributes ("staff" or "student") for authentication of users, and is kept up-to-date by synchronisation with the MIS every ten minutes. The least amount of information possible is stored in the Active Directory to minimise the impact of security breaches.

3.3 Aims

- 3.3.1 The aim of the internal project¹¹ was to implement federated access management using Shibboleth technology within Kidderminster College to link together web-based resources.
- 3.3.2 ICT Services has the goal that "all resources and services should be accessible using single sign-on and within three clicks".

3.4 Scope

- 3.4.1 The scope of the services within the internal project included the Kidderminster portal, Athens protected resources, the departmental Moodle VLEs and staff extranet Moodle VLE and an information repository.
- 3.4.2 Services that were out of scope included some specific library and careers resources which retained their own access controls.
- 3.4.3 The scope of the JISC-funded projects that Kidderminster were part of was much wider than that of the internal project, and involved setting up multiple IdPs, and a regional federation¹² to facilitate information sharing and collaboration.

3.5 Plans

Strategic drivers

- 3.5.1 The major strategic drivers of the project were:
- the desire to exploit the VLE by making it more accessible and user friendly; the requirement to allow Kidderminster users to access the VLE externally is part of this;
 - the need to retain ICT services staff by providing a challenging and stimulating environment with innovative projects;
 - pressure to reduce reliance on expensive software licenses;

¹¹ The elements of the JISC funded projects relating only to Kidderminster's internal deployment of a federated access management infrastructure.

¹² The KC-ROLO federation.

- the need to develop collaborations with regional institutions and allow users from other colleges and institutions to access the VLE in order to expand provision and exploit teaching capabilities and resources;
- reduce the burden of administration and support overheads.¹³

Options appraisal

- 3.5.2 Shibboleth technology was the only option considered by Kidderminster College. This was largely because at an early stage of researching options, they came across the JISC-funded projects to implement Shibboleth that they subsequently applied and received funding for.
- 3.5.3 Shibboleth was seen as a low risk option because the IT Services Development team were well staffed and skilled with open-source software, and Shibboleth was seen as a vehicle to push the VLE forward.

Affordability

- 3.5.4 An open-source research and investigation project was started prior to the JISC projects to enable Kidderminster to build its capacity, knowledge and in-house expertise. This has subsequently supported Kidderminster's development and roll-out of its Moodle VLE as well as Shibboleth technology. It was estimated that this project cost Kidderminster approximately £39.5k, and included:
- **Research and investigation:** it was estimated that this work was equivalent to 1 year FTE of a developer's time which equates to approximately £25k;
 - **Staff development:** approximately £4k was spent on staff development training courses (*eg* Linux, SAML);
 - **Equipment:** approximately £3.5k was spent on specific equipment (*eg* server) to support the project;
 - **Estates and infrastructure:** approximately £5k was spent on other college resources including staff and hardware and approximately £2k on workspace including premises, heating and lighting.
- 3.5.5 In the wider scope of the JISC projects, Kidderminster received:
- £40,000 for the Shibboleth aspects of the Early Adopter projects;
 - £92,000 of funding for the KC-ROLO project (see paragraph 3.2.4);
 - £24,000 of JISC money from Worcester University.
- 3.5.6 In addition to the JISC money, it was estimated (in hindsight) that Kidderminster contributed approximately £19.5k towards the KC-ROLO project. It is likely that Kidderminster would have implemented Shibboleth without the JISC money, but this would not have been started as early or been implemented in the timescale achieved.

¹³ This was particularly an issue for Worcester University students undertaking courses at Kidderminster, as this required manual provision of accounts.

3.5.7 Due to the wider scope of the JISC projects, Kidderminster is unable to provide specific costing for implementation of federated access management. However, from experience Kidderminster has gained from providing a service to implement and support Shibboleth IdPs and SPs to other institutions, Kidderminster has approximated the general deployment activities and effort for federated access management to be:

- **Internal review:** audit of set-up, file store, security *etc*;
- **Active directory implementation:** training of in-house staff (5 days); audit (3 days with some assistance); implementation (internally 20-30 days over 6 months, or use external specialists);
- **Firewall configuration:** 1 day;
- **Setting up attribute store:** 2 days with some assistance.

Achievability

3.5.8 The project was achieved using the IT Services Development team's capability and capacity. The staff already had a good skills base, including experience with Linux, but had to research other technologies, for example Apache and digital certificates.

3.5.9 The bulk of the work was carried out by one developer. However, Kidderminster also took this opportunity to add strength-in-depth by providing further training for staff (in new and existing skills areas) and employing additional development staff.

3.6 Implementation

Outcomes

3.6.1 Decision-making was carried out by the Head of ICT Services in conjunction with the Vice Principal (Operations Director for ICT), who met every week to discuss the project.

3.6.2 A Shibboleth test service was implemented at the start of the project. The IT Services department also has responsibility for the Kidderminster VLE. There was close communication between these two work streams. The library was not involved until later in the project, as single sign-on to Athens-protected resources was not the primary focus of the project.

3.6.3 The Shibboleth production service was rolled-out to staff and students (the Shibboleth-protected portal, departmental Moodle VLEs and staff extranet Moodle and a Shibbolised repository) in April 2006.

3.6.4 Students and staff now have the ability to access internal web resources without multiple sign-ons, and can access external Athens-protected resources via federated access management.

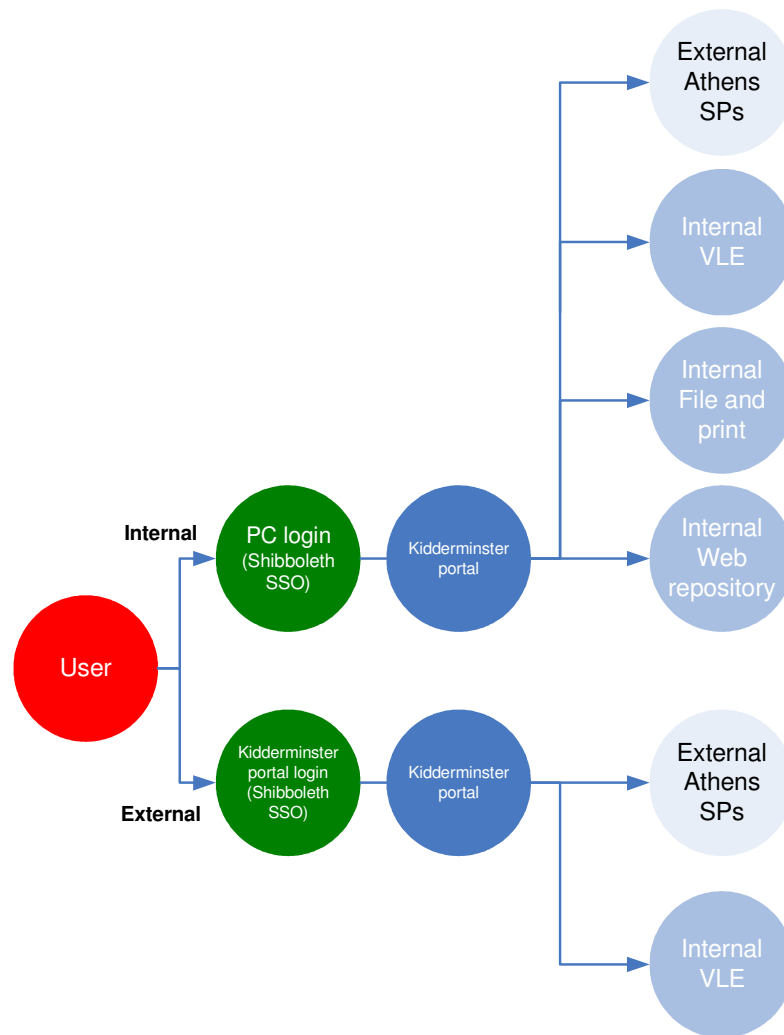


Figure 3-1: current access management set-up at Kidderminster

Benefits realised

3.6.5 This project has brought many benefits to Kidderminster College:

- A single sign-on system has been implemented for access to the network and web resources, improving the user experience;
- External users can now access Kidderminster web resources (including the VLE), for example this is much more convenient for distance learners who are based externally to Kidderminster for the majority of the time;
- The IT Services team believe that usage of the VLE has increased;

- Resources can now be securely shared between institutions, opening up possibilities for inter-institutional access to resources, and allowing staff and students to use learning resources in a collaborative way. Sharing is flexible, *eg* school users who undertake courses at Kidderminster can be given access to the VLE;
- Administration overheads have been reduced, particularly for students taking courses at Kidderminster from Worcester University;
- Kidderminster are now utilising the expertise that they have gained by offering a service to other institutions to implement and support Shibboleth IdPs and SPs. Institutions are trained in the technology with the Kidderminster team providing expert support and cover;
- Working with open-source software has proved stimulating to the development team, has helped with staff retention and has allowed expansion of the department.

3.7 Issues encountered and lessons identified

3.7.1 The Shibboleth implementation at Kidderminster ran very smoothly, and no major issues were encountered.

3.7.2 Kidderminster identified the following lessons from their project:

- The implementation of Shibboleth requires a steep initial learning curve, however once skills are learnt, it is a relatively easy technology to administer and support;
- Start-up costs may be higher if an institution does not have the prerequisites in place, for example an attribute store;
- The bureaucratic process of introducing an IdP in some institutions is such that significant advance planning is imperative to keep roll-out on schedule;
- Library inductions are the main opportunity to get “resource use” messages across to users. Changes must be implemented and trainers trained in time for the inductions;
- Good communication is required between the implementation team and the library;
- Collaboration requires more than common technology: commitment from all parties to share content is essential;
- The project sponsor should be enthusiastic and committed.

3.8 Future plans

3.8.1 Kidderminster identified the following plans for the future:

- increase resilience of services by implementing a second IdP;
- shibbolising more resources (*eg* e-Portfolios);

- improvements to the user friendliness of the Kidderminster WAYF for the KC-ROLO federation.

3.9 Useful resources

3.9.1 The following documentation has been written by Kidderminster:

- Shibboleth in Further Education, 10 May 2006, Tim Hall, ICT Services Development Team, Kidderminster College <http://www.matu.ac.uk/uploaded-pdf/Shib_FE_Final_KM.pdf>
- KC-ROLO Final Report, 14 March 2006, Graham Mason and Ed Beddows <http://www.jisc.ac.uk/media/documents/themes/access_management/kc-rolotfinalreport.doc>
- Shibboleth user guide <<http://Kidderminster.ac.uk/kc-rolot>>

4 University of Surrey

4.1 Overview

- 4.1.1 A project at the University of Surrey to replace the Classic Athens access management system was initiated in April 2005. The main aims of the project were to implement a devolved authentication system in order to reduce the administrative burden on IT staff and reduce the number of usernames and passwords that users need to remember. Surrey decided to implement AthensDA as it was a mature system that was already rolled out in a number of institutions and technical support would be provided by Eduserv. Additionally, Surrey has a lean staffing structure and does not have the necessary extensive in-house technical expertise with open-source technology such as Shibboleth.
- 4.1.2 Surrey went live with AthensDA and a new IDM system in June 2006. All new users in the 2006/2007 academic year were issued with only a local username and password. By November 2006, Surrey removed the ability for extant users to access resources via their Classic Athens username and password.

Institution	University of Surrey
JISC Collections banding	D
Number of users	18,500 (16,000 students and 2,500 staff)
Project start date	February 2005
Project end date	November 2006
Key project aims	To reduce the administration burden of the Classic Athens system and to improve the user experience by including Athens protected resources in the Surrey unified sign-on system
Decision making stakeholders	Deputy IT Director E-strategy and Resource Manager (Library) Academic Services Group Manager (IT Services) (Project manager)
Funding	Library budget (project sponsor: Head of Library Services)
Key milestone	Going live with Athens DA (July 2006) Switching off Classic Athens (November 2006)
Current access management system	Athens DA and Surrey unified sign-on system
Previous access management system	Classic Athens and Surrey unified sign-on system

4.2 Background

University of Surrey

- 4.2.1 Surrey is a moderately large university, supporting approximately 26,000 users. IT Services at the University of Surrey is primarily operations and business, not research and development, focused. Consequently, it tends to avoid technology perceived as risky. It has an institution-wide policy to implement mature commercial systems with paid for support in preference to open-source software. This is largely because Surrey has a very lean staffing structure and does not have extensive in-house technical expertise, particularly with open-source software.

- 4.2.2 The Library was responsible for subscriptions to Service Providers and maintaining the Athens permission sets which controls which resources can be accessed. IT Services was responsible for creating and maintaining Classic Athens accounts for each user. IT Services also ran the student and staff support helpdesk and were responsible for password administration. At this time, a local Surrey username and a separate Athens username and password were issued to each new user.
- 4.2.3 IT provision is relatively distributed at Surrey. IT Services do not have full control over all systems on the Surrey campus, for example departments run their own computers. The student computers that are within IT Service's remit are regularly rebuilt (once a week).

Service providers

4.2.4 The web services available to users at Surrey include:

- e-Journals, e-Databases and e-Books;
- Blackboard VLE;
- email;
- library catalogue.

Identity management

- 4.2.5 IDM at Surrey was upgraded during summer 2006. A key objective of the AthensDA system was to authenticate a users' identity from the computing accounts created by the IDM system. The new automated computing account registration system went live in June 2006.
- 4.2.6 The new system creates computing accounts for all students and staff by pulling information from the:
- registry system (student database);
 - HR system (staff database);
 - manual account registration system (used to register temporary users, *eg* visiting academics).
- 4.2.7 To enable devolved authentication and attribute-based authorisation, an attribute store is maintained as an Oracle table comprising all of the user accounts from the registration system, with an added unique Athens identifier and the appropriate permissions set for each user. To keep the table current, it is synchronised with the registration databases nightly. There are only two user permission sets for Surrey users, staff and students, which the library is responsible for assigning. User logins are authenticated against Active Directory.

4.3 Aims

- 4.3.1 The main aims of the project to replace the Classic Athens access management system were to implement a devolved authentication system in order to reduce the administrative burden on IT staff and to improve the user experience by having a single username and password.

4.4 Scope

- 4.4.1 Surrey already operated a unified sign-on system to allow users to gain access to local resources using the same local username and password, and they wanted to extend the scope of this to include access to Athens protected resources. The services in scope of the unified sign-on system included, but were not limited to, the following internal resources (accessible on- and off-campus):

- network login;
- VLE;
- email.

4.5 Plans

Strategic drivers

- 4.5.1 The key strategic drivers for this project were:
- the overhead for creating of two usernames and passwords for each new user was a significant administrative burden and considered unsatisfactory;
 - the automated creation of Athens accounts at the start of each academic year was pressured and was prone to failure at peak loading, requiring manual intervention to rectify;
 - users having multiple passwords to remember did not provide a good user experience, and was seen as a barrier to use of e-Resources.

Options appraisal

- 4.5.2 Surrey had the following requirements for any new access management system:
- a reliable and mature technology that had already been rolled out institution-wide in a production environment;
 - a preference for commercial technologies with paid for support;
 - a desire to avoid running two services concurrently.

4.5.3 Surrey considered three options to replace the Classic Athens system:

- AthensDA;
- Shibboleth technology;
- AthensIM.

4.5.4 The options, and the benefits and considerations for each, were researched by the project manager, who subsequently set out the options in a resourcing decision-making document in April 2005. Additionally, the decision-making stakeholders met with the Middleware Assisted Take-Up (MATU) team¹⁴ to further discuss these options in November 2005.

4.5.5 The following benefits and risks for Surrey were assigned to each option:

- **AthensDA:**
 - **Benefits:** allows devolved authentication; mature and already rolled out in a number of institutions; technical support provided by Eduserv;
 - **Risks:** AthensDA will be a short-term solution and will be overtaken by Shibboleth implementations due to JISC and international acceptance; the cost benefits will be less justifiable;
 - **Costs:** implementation time (few resource requirements), OpenAthens subscription costs (not known at the time);
- **Shibboleth technology:**
 - **Benefits:** could be used to provide single sign-on across the University; alignment with the JISC's plans for the UK education and research community;
 - **Risks:** no external technical support provided; relying on the community; implementations largely confined to pilot environments;
 - **Costs:** free software, large amount of in-house technical resources required to implement;
- **AthensIM:**
 - **Benefits:** could be used to provide single sign-on across the University; alignment with the JISC's plans for the UK education and research community; Eduserv would provide support;
 - **Risks:** AthensIM was only released in February 2005 and had only been rolled out in small pilot environments;
 - **Costs:** free software; perceived large amount of in-house technical resources required to implement.

4.5.6 The two most favourable options were to implement AthensDA or AthensIM, primarily because Surrey preferred not to rely on community support for Shibboleth technology. Although it was noted that the option to "leap frog" AthensDA to Shibboleth would be a better long-term solution, AthensDA was unanimously chosen as the way forward as it was

¹⁴ The MATU service was part of the JISC's CM programmes. It advised and supported Early Adopters of federated access management among FE and HE institutions.

imperative that the service was robust, and Surrey did not want to be on the leading edge with a production service.

Affordability

- 4.5.7 The project was funded from within the IT Services budget, with the Head of Library Services sponsoring the project. The capital expenditure for the project was low, although the manpower requirement was more substantial. The effort required by each team member was initially estimated in a Project Initiation Document. The actual total amount of effort required was:
- IT Services: 15 weeks;
 - technical development: 2.5 weeks;
 - library testing time: 3 weeks.¹⁵
- 4.5.8 All library resources, including e-resources, are financed from the library resources budget (£1.8M/year). It is currently unclear which department will fund the OpenAthens subscription cost in 2008.

Achievability

- 4.5.9 It was assessed that the project could be achieved within the Library and IT Services current capability. External technical support was provided by Eduserv when required.
- 4.5.10 The decision-making stakeholders comprised three people: the project manager and IT and Library Services representatives.
- 4.5.11 The project team comprised of:
- project manager (from the IT Services Academic Services Group);
 - technical lead (from IT Services);
 - developer for infrastructure development (from the IT Services Corporate Infrastructure team);
 - library staff for testing and communication (E-Strategy and Resource Manager).

4.6 Implementation

Outcomes

- 4.6.1 Surrey went live with AthensDA in July 2006. All new users in the 2006/2007 academic year were issued with only a local username and password. In November 2006 Surrey removed the

¹⁵ Spread over the duration of the project from January 2006 through September 2006.

ability for extant users too access resources via their Classic Athens username and password. This approach, a relatively swift transition, worked well.

4.6.2 The timeline for implementation of AthensDA was:

- April 2005: options appraisal document prepared by project manager;
- November 2005: meeting with MATU to further discuss Surrey's options;
- December 2005: decision made to implement AthensDA;
- January-March 2006: AthensDA system built;
- March-May 2006: AthensDA system tested (including testing the compliance of resources);
- June 2006: decision to go live was made (the new IDM system also went live);
- July 2006: AthensDA production service was deployed;
- August 2006: embedding of service;
- November 2006: all extant Classic Athens accounts were expired.

4.6.3 Alongside the technical development and testing of the new infrastructure, AthensDA and its implications was heavily publicised to users, in advance of AthensDA going live. This included sending a series of emails to users, advertising with posters and on the library website and communicating changes to course boards. Resilience was built into the system by running two servers and using load-balancing software which has worked well in practice.

4.6.4 The current access management situation at Surrey comprises the following:

- **Unified sign-on:** network, VLE, AthensDA resources, email, staff intranet;
- **Library system:** Barcode and PIN (Library Account only);
- **Specific Sign-On:** specific username and passwords for specific services, *eg* SAP;
- **Off campus access:** a gateway enables off campus users to access information resources that are only available via IP authentication and a user's personal/shared central file storage.

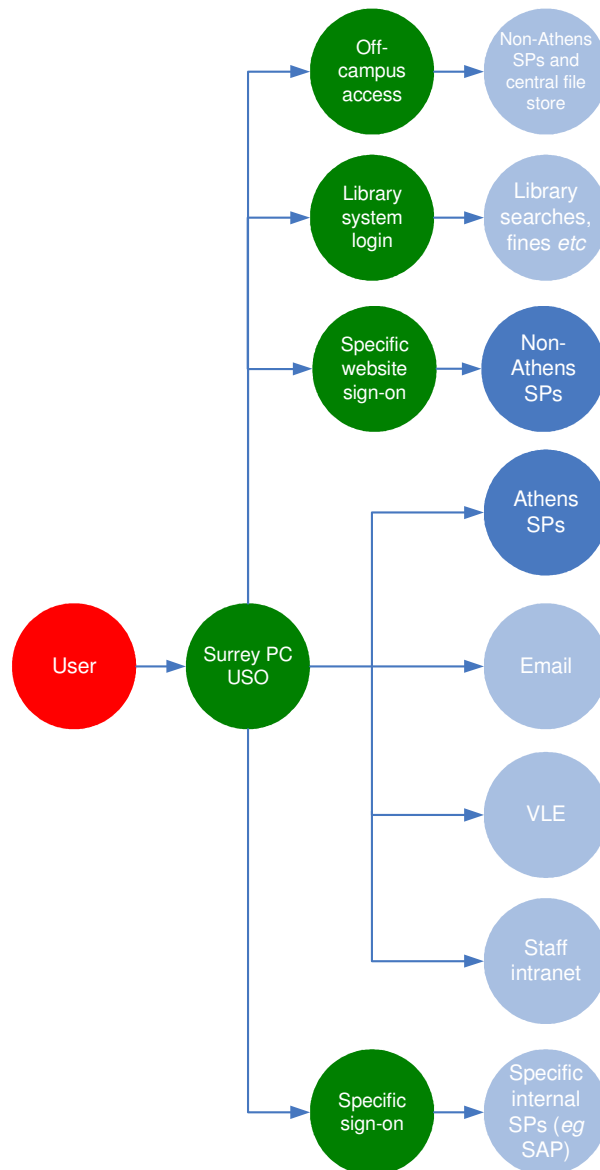


Figure 4-1: current access management set-up at Surrey

Benefits realised

4.6.5 This project has brought many benefits to Surrey:

- Athens protected resources are now part of the unified sign-on system and are accessed with the local username and password. The library has received good feedback from users on the new system, and is considered to have improved the user experience.
- Library overheads for helpdesk enquiries have been reduced, and are now generally limited to one common problem (see issues identified) for which there is a standard response.

- It is believed that there is less account sharing between users, as users are less inclined to share their local accounts than they were to share the Classic Athens accounts.
- The requirement for manual intervention by IT Services for account creation at peak times has been reduced.
- The AthensDA project has forced Surrey to upgrade their identity management processes, and responsibility for authentication is held by the institution. This is considered to be one step closer to being ready to adopt federated access management.

4.7 Issues encountered and lessons identified

Issues

4.7.1 The implementation of AthensDA was very successful, and ran very smoothly. The project benefited from having a very good project manager. The main issues encountered were:

- **Cookie management:** AthensDA requires the user to have a persistent cookie which identifies which organisation should authenticate. The cookie has to be present on the PC the user is actually using for it to be detected by the Athens Access Management system. But, Surrey users do not have roaming profiles and students will use multiple PCs. In addition, campus student PCs are rebuilt each week thus deleting all cookies. IT Services implemented a workaround for users accessing AthensDA resources on campus from PCs supported by IT Services, so that the cookie is automatically and transparently created for the user as they login to a PC. However, off campus users are advised to create the cookie on their own PCs and this can be problematic for some users.
- **Accessibility of Athens resources:** NHS firewalls are restrictive, and Surrey encountered some problems surrounding access of NHS students to AthensDA resources.
- **Account transitioning:** AthensDA required users to register their details again with some service providers, *eg* ScienceDirect. The functionality/attributes of these individual accounts were not transferred over from the Classic Athens to the AthensDA account (*eg* saved searches, registration for statistical data). This was another issue for users, but has not been a major problem as those people who used such features recreated their personalised registrations.

Lessons

4.7.2 The following lessons were identified:

- There is a requirement to understand the implication of cookies with shared PC facilities such as open access student desktops. It is important to investigate desktop management policies to understand how the AthensDA organisational cookie will be affected by those policies.
- It is helpful to talk to other institutions who have implemented the same access management systems to help identify potential issues in advance.

- It was helpful to have a test environment, as it enables the institution to be more confident when rolling out the live production service.
- Widespread publicising of a new system to users is imperative: although however much publicising is done, there will always be queries with new systems.

4.8 Future plans

4.8.1 Surrey has identified the following plans for the future:

- It is anticipated that Surrey will continue with AthensDA after July 2008 when AthensDA becomes part of the OpenAthens subscription service. It is likely that Surrey will wait for Shibboleth technology to mature and be rolled out as a production service elsewhere before considering implementing it at Surrey.
- Granularity of access is starting to become an issue, as Surrey are partnering with lots of different groups of users who are not entitled to use Surrey resources. For example, "Study Group" courses where users are not registered at Surrey, but are learning English at Surrey. If Surrey had more granularity, they could give users access to specific resources and could negotiate with vendors to increase licensing agreements. Surrey are currently undergoing a change in IT Director and restructuring of the IT department, which makes it very difficult to plan for the future. However, the benefits of Shibboleth technology are being considered. Additionally, IT Services are investigating single sign-on solutions, including Kerberos and other vendor solutions.

This page is intentionally blank

5 University of Warwick

5.1 Overview

- 5.1.1 A project was started in January 2005 to upgrade the extant single sign-on access management system to improve its security. Warwick developed a Shibboleth-profile based system. Athens resources are accessed via the Shibboleth-Athens gateway. Warwick University are ready for federation membership and federated access management when required.

JISC Collections banding	C
Number of users	~5,000 staff, ~20,000 users
Project start date	January 2005
Project end date	Reached key milestone in September 2006, although ongoing
Key project aim	To upgrade the extant access management system (SSOv2) to provide more a more secure and robust single sign-on system for users at Warwick to access web services
Decision-making stakeholders	IT Services
Funding	No specific project funding, the budget came from within the web team budget
Key milestone	Deployment of SSOv3 Shibboleth-Athens gateway going live
Current access management system	SSOv3 with customised implementation of AthensIM (using Shibboleth-Athens gateway). AthensDA to access non-Shibboleth compliant Athens resources.
Previous access management system	SSOv2 (Java and cookies) and Classic Athens
Federation members	Not currently

5.2 Background

University of Warwick

- 5.2.1 The University of Warwick is a moderately decentralised university supporting approximately 5,000 staff and 20,000 students. Warwick has a well-funded and resourced IT Services, with a capable and mature in-house development team. The E-lab is a division within IT Services that is responsible for coordinating the delivery of Warwick's e-Strategy programme and researching and developing new technologies, especially in the areas of web services and e-Learning. The E-lab is proud of its achievements in providing a range of high-availability and innovative web services. It is currently moving to ITIL service management.
- 5.2.2 Warwick has had a single sign-on system in place since 2002 to facilitate access to web services and web applications. This was initially a simple cookie approach combined with Classic Athens (SSOv1), which was then upgraded to a Java-based system using cookies and with Classic Athens (SSOv2).

Service providers

- 5.2.3 Warwick University has approximately 40 services that are part of their single sign-on system. All of these services are internal and have been developed by Warwick themselves, and include contact management, a blogging platform, forum system, permission based search engines and a web-group system (*eg* timetables, module registration). The only external service providers are Athens-protected resources.
- 5.2.4 Initial log on to campus computers and web email are not part of the single sign-on system. Some Warwick users require access to external non-Athens services, for example some databases.

Identity management

- 5.2.5 Student records and registration information pushes into a centralised membership database, which itself pushes into approximately five satellite servers. There are other separate databases that hold the identity information of other groups of members, for example the business school (which is very independent from the rest of the university), alumni and the National Academy for Gifted and Talented Youth database (which has 40,000-50,000 users).
- 5.2.6 There is an ongoing IT Services project, initiated in early 2006, to rationalise the identity database.

5.3 Aims

- 5.3.1 The main aim of the project was to upgrade the extant access management system (for access to web services) at Warwick to improve its security.

5.4 Scope

- 5.4.1 The scope of the project was the current single sign-on system and single sign-on system-enabled services (paragraph 5.2.3).

5.5 Plans

Strategic drivers

- 5.5.1 In recent years, Warwick has developed a large number of web services, many of which allow students to publish their own material. This facility brings with it the potential opportunity for compromise of a user's identity, for example by posting information using another person's identity, or accessing material meant for other users.
- 5.5.2 The main strategic driver for upgrading the extant single sign-on system was the requirement for increased robustness and security of the single sign-on system against cross-site attack.

Options appraisal

- 5.5.3 Desk-based research was carried out in January 2005 by the E-lab to assess the technical options available. Warwick considered the specifications of a number of off-the-shelf solutions, including:
- Microsoft solutions;
 - Sun Access Manager;
 - Yale University’s Central Authentication Service (CAS);
 - Liberty Alliance ID-FF solutions;
 - Internet2’s Shibboleth technology.
- 5.5.4 As Warwick already had a single sign-on system in place, they had a good idea of their requirements for the new system. The solution had to fit their current architecture and methodology (*eg* Java-based), meet all of their current functionality and meet the additional requirements for increased security and robustness. During the research, it was discovered that the JISC were moving towards Shibboleth technology for UK FE and HE.
- 5.5.5 Many of the options did not meet their requirements. For example, whilst CAS allowed single sign-on, it did not do single log-out. The only option that met their requirements was Shibboleth technology. However, in early 2005, there were not many implementations of the Shibboleth profile available at the time, thin on the ground and did not fit their architecture and methodology. The option chosen was to develop its own implementation of the AthensIM reference implementation of the Shibboleth profile, and build it into the wider single sign-on system.

Affordability

- 5.5.6 There were no specific budget requirements for this project as it was not funded as a specific project. Funding for the project came directly out of the IT Services web team budget.
- 5.5.7 The main body of the work was carried out by a single Developer, and took approximately 1 year of solid effort, with some work still being carried out today. The majority of the work was spent researching the customised implementation of the Athens IM reference implementation.

Achievability

- 5.5.8 It was assessed that the project could be achieved within the E-lab’s current capability and capacity, and that they had adequate in-house skills to carry out the project.

5.6 Implementation

Outcomes

5.6.1 All decision-making was carried out by the E-lab, encompassing:

- Head of e-Learning;
- Developer;
- Web team leader.

5.6.2 SSOv3 went live in September 2005 for access to Warwick-developed web services. However, due to a number of critical Athens databases not being available via the Shibboleth-Athens gateway in September 2005, Shibboleth authentication to Athens resources was withheld until September 2006. In September 2006, the majority of Athens resources could be accessed via AthensDA and the Shibboleth-Athens gateway, however two major databases were still not compliant so can be accessed via Classic Athens and not as part of the single sign-on system.

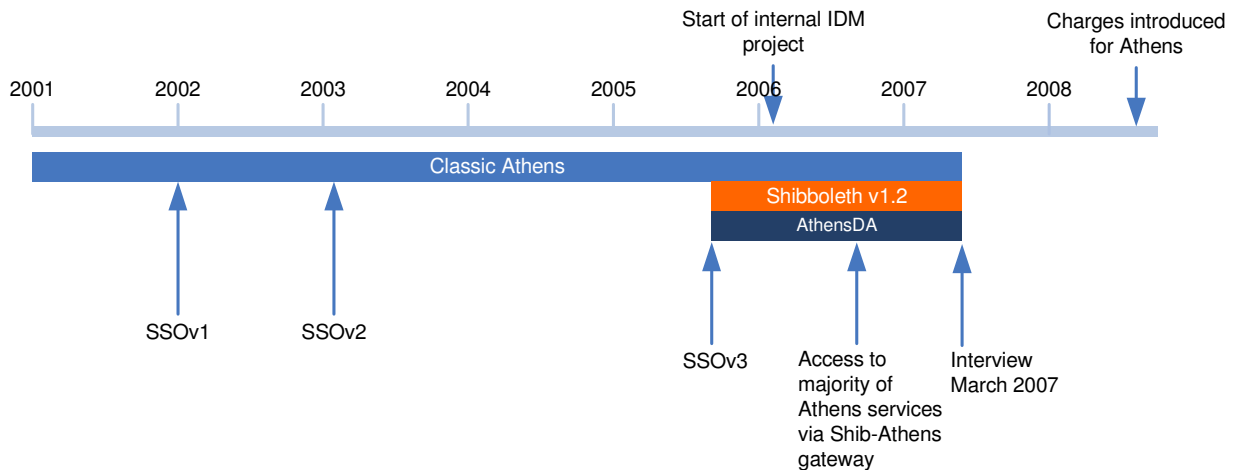


Figure 5-1: Access management timeline

5.6.3 The current access management situation at Warwick comprises the following:

- Single sign-on (local username and password) to:
 - internal (Shibbolised) web services (*eg* blogs);
 - majority of Athens resources;
- Unified sign-on (local username and password) to:
 - Campus PCs;
 - internal non-Shibboleth services (*eg* email);

- Other (specific username and password):
 - non-Shibboleth compliant Athens resources via Classic Athens username and password (users who wish to use these resources must register for Athens);
 - non-Athens services via library user number and PIN;¹⁶
 - specific internal services (*eg* financial systems) via specific username and passwords.

5.6.4 An increasing number of departments wish to shibbolise their own applications, and the IT Services is willing to provide support where possible. These applications are not part of the single sign-on system, but have the same local username and password.

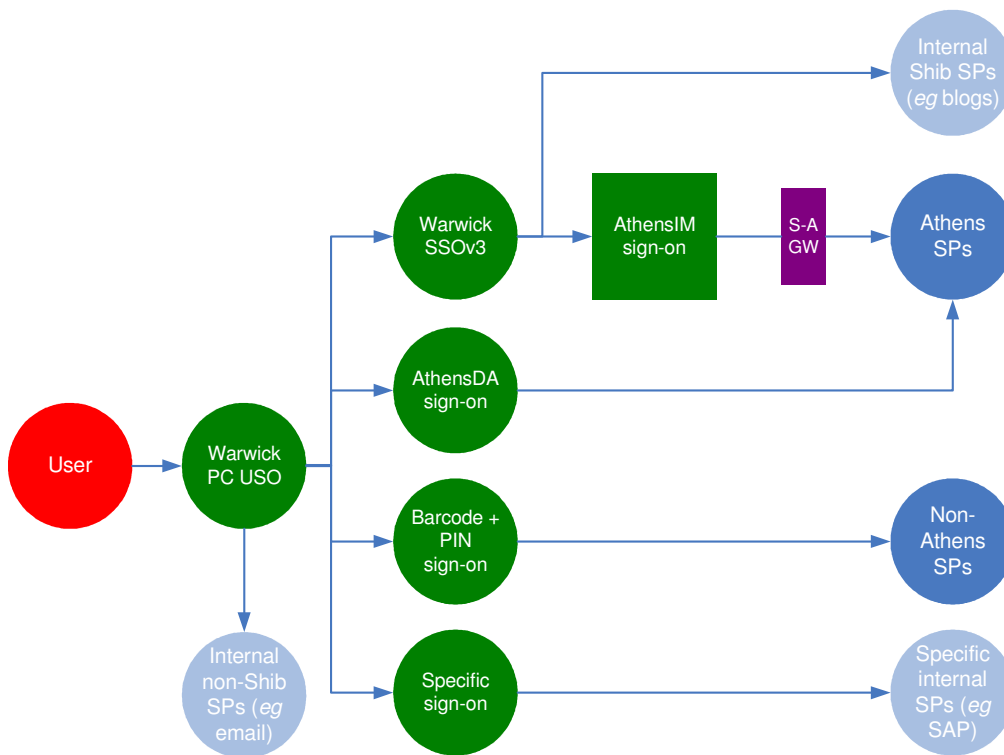


Figure 5-2: current access management set-up at Warwick

Benefits realised

5.6.5 This project has brought many benefits to Warwick University:

- The user experience has been improved as there is now largely one local username and password for each user for single sign-on system-enabled services;
- Users are able to access web resources externally;

¹⁶ Authentication is via a proxy server. This is not considered to be an ideal solution, especially for some distance learners.

- IT Services believe that the number of helpdesk enquiries regarding passwords has been reduced. Additionally, the nature of the queries has changed and now more generally allow a generic response;¹⁷
- Shibboleth technology brings increased security benefits (*eg* session cookies as opposed to persistent cookies, and encrypted traffic to reduce packet sniffing). There have been no known security breaches to date. Furthermore, users have more inhibitions about sharing their local Warwick password than their Athens password;
- Warwick is ready join the Federation and configure to use full federated access management when required.

5.7 Issues encountered and lessons identified

5.7.1 The major issue that was encountered during the project was the compliancy of Athens services with the Shibboleth-Athens gateway, and encountered configuration management problems. This meant that they had to hold back with Shibboleth-based authentication for Athens services until September 2006. Two major Athens services are still not compliant with the Shibboleth-Athens gateway and an Athens username and password are required to access these services.

5.7.2 Warwick identified the following lessons from their project:

- The project turned out to be harder and more complicated than initially assumed. This is because implementing a single sign-on system that works across many applications, is convenient for the user and is secure is a very hard problem and the code was more complicated to write than anticipated;
- Each database must be configured by Athens and the database suppliers. Testing compliance of these resources is paramount, particularly if you want to ensure that there is minimal down-time when the service goes live;
- Access management must have a comprehensive identity management system in place;
- Availability of IT infrastructure is critical for users and must be designed and managed correspondingly;
- Institutions may not realise all of the flexibility benefits of single sign-on with off-the-shelf implementations of the Shibboleth profile. Customised implementations allow for easier modification of infrastructure to support future markets;
- It is very difficult to provide adequate technical security if a University does not have full control of the content published on their website;
- Change management processes are needed for web applications that the IT Services do not own;

¹⁷ As the university is running two systems concurrently they have not yet seen a reduction in queries.

- It is important to work closely with the library to achieve all of the benefits of this project, for example, the senior librarian had to agree the project direction.
- Time must be taken to train staff so that they can train users (*eg* librarians over the summer).

5.8 Future plans

5.8.1 Warwick identified the following plans for the future:

- The infrastructure is in place for Warwick to become a full IdP within the Federation, which will be between September and December 2007. There are currently no plans, or anticipated need, to release Warwick services (*eg* blogs and forums) as federated services though this is a possibility.
- Warwick remain open and flexible to alternative technical solutions. As standards mature and more features are introduced Warwick may consider switching to a Shibboleth reference implementation. This may reduce in-house support costs.
- Resolve the issues with non-compliant Athens resources through technical upgrades by the database providers and Athens.
- Expand the scope of the single sign-on system by supporting departments wishing to utilise the infrastructure.

This page is intentionally blank