

# UNISA

## University of Nottingham Implementation of Shibboleth for Athens

### JISC Final Report

Dr Ian Vincent

Systems and Security Team  
Information Services  
Kings Meadow Campus  
Lenton Lane  
Nottingham NG7 2NR

[jisc-fam@nottingham.ac.uk](mailto:jisc-fam@nottingham.ac.uk)

2<sup>nd</sup> Draft, 6<sup>th</sup> April, 2006

## Table of Contents

Acknowledgements.....	2
1 Executive Summary.....	3
2 Background.....	4
3 Aims and Objectives.....	4
4 Methodology.....	4
5 Implementation.....	5
6 Outputs and Results.....	7
7 Outcomes.....	7
8 Conclusions.....	7
9 Implications.....	7
10 Recommendations.....	8
11 References.....	8

## Acknowledgements

UNISA, the University of Nottingham Implementation of Shibboleth for Athens, was a pilot project funded by JISC under the Shibboleth Early Adopters section of their Core Middleware Programme. The project team, Information Services and the University of Nottingham are grateful for both their financial and organisational support, through the programme manager Nicole Harris, without which the project would not have been attempted. We are also grateful for the invaluable technical support provided by the JISC funded Middleware Assisted Take-up Unit, MATU, and by Eduserv who run Athens.

The author, who managed the project, wishes to place on record the outstanding contributions made by Andrew Barker, who performed the technical implementation, and Carol Collins, who liaised with colleagues in library services. He is also grateful for the support given and patience shown by those colleagues and the contributions made by other members of the project team: Ann Charlton, who succeeded Carol as our Athens contact, Jenny Coombs (nee Drury), who represented the subject librarians and Sandi Golbey and David Rhead from IT Service Quality, who represented the interests of our users.

## 1 Executive Summary

The aim of the project was to pilot the Shibboleth/Athens gateway in service as a means of authenticating and authorising access to Athens resources. It was successful in this, although the scope of the pilot had to be limited to a subset of our September, 2005, first-year undergraduate intake due to lack of support by some publishers and username housekeeping issues.

The project started in April, 2005 and initially concentrated on technical implementation. The results of this were reviewed at the end of June and a decision was taken to proceed with the pilot, but with its scope limited as described above. The summer was then spent putting the development code into production, updating documentation and providing training prior to the start of session in September.

The start of session deadline was achieved and live service commenced, after which the main activity was in monitoring it. As would have been expected from first year undergraduates, usage was relatively low, but it became evident that we should have done more to communicate with teaching staff, a significant number of whom were, despite our updated documentation, continuing to tell students to register for a Classic Athens username. We had some concerns that the interface provided to students was relatively obscure, particularly first time through, but those that persevered seem to have generally been successful, with few requests for support.

The possibility of providing single sign-on to Athens/Shibboleth resources from our portal was investigated, but it was decided the appropriate point to do this was in the Metalib e-library gateway. A new version of the (commercially supplied) code for this is imminent, which appears to support Shibboleth, so this was not taken further.

Having dealt with username housekeeping issues, we opened up access to the pilot for postgraduate students, though we have not publicised this yet. We have also considered extending it to staff, but there is an issue here in that people registered with staff usernames range from full-time academic staff on the University payroll through to people doing occasional supervision of medical students or visiting academics. It is unclear both as a matter of policy what their respective entitlements to access Athens resources should be and technically how to differentiate between them. The approach we are planning to take is to store an Athens permission set for each user in our LDAP directory, initialised to null when the username is created. When the user first attempts to access the Athens/Shibboleth gateway, an attempt will be made to determine his or her status by means of a database lookup and store an appropriate permission set in the directory for subsequent use, giving access only to publicly available resources in the case of any doubt. A web based interface will be provided for library staff to amend this on application by the user.

Two distinct activities have been agreed in the exit strategy for this project. The first is an primarily an operational one: to cease bulk creating new Classic Athens usernames for students (though leaving them the option of creating one while there are still Athens resources not accessible via Shibboleth), update our documentation to show the Athens/Shibboleth gateway as the primary means of access and implement the handling of permission sets for staff as described above. The second is a developmental one: to develop single sign-on both for Athens managed and local resources and more generally to prepare for joining the recently announced UK Access Management Federation.

In conclusion, the announcement of this, together with that of the cessation of funding for Athens in July 2008, has to some extent coloured our perception of the value of this project. On the positive side, we have gained valuable experience of Shibboleth and are close to being able to reap the benefits, both for our users and ourselves, of avoiding the need for separate Classic Athens usernames. The downside is that this will be just a step on the way to full Shibboleth implementation, which will require more extensive work on attribute mapping and another change of interface for our users, rather than providing the basis for a continuing service. Sites that have not already followed us down this route may well decide that it is something of a cul-de-sac and concentrate instead on directly accessing resources via Shibboleth, rather than use the Athens/Shibboleth gateway.

## 2 Background

Before this project, Information Services maintained separate ATHENS usernames and passwords for all students by automatically generating bulk upload requests from our user registration database. We had been looking to use the ATHENS devolved authentication mechanism to enable staff and students to use their local (eDirectory) usernames, but the goal of this project was to use the Athens/Shibboleth gateway for this instead.

This would make life easier for our staff and students, as they would not need to keep track of separate usernames and passwords, and decrease the risk of misuse of ATHENS resources. For Information Services, it would remove the need to maintain the hand-crafted code required for bulk uploading at the, hopefully lesser, cost of deploying the Eduserv implementation of Shibboleth Origin, with assistance as required from the Middleware Assisted Takeup Service. It would also give us experience of using Shibboleth, which is seen as an emerging standard for authentication and authorisation.

## 3 Aims and Objectives

In outline, the plan was to deploy the AthensIM implementation of Shibboleth Origin, with assistance as required from the Middleware Assisted Takeup Service, to provide authentication and authorisation attributes from our eDirectory, with a view to rolling this out for first year students and new staff in September, 2005. If successful, we would look at the issues involved in getting staff and students with existing ATHENS usernames to change to using their local ones, and at providing single sign-on to ATHENS resources from our portal. We would document and disseminate our experience in a case study and present it to at least the EMUIT forum.

These objectives remained largely unchanged, except that the rollout in September 2005 was confined to first year undergraduate students. New postgraduates, staff and law and nursing undergraduates were excluded because of concerns about the number of resource providers who did not support the Athens/Shibboleth gateway; issues concerning housekeeping of usernames for postgraduates and staff, and derivation of appropriate permission sets for the latter.

This report is intended to provide the case study and the work was presented to a meeting of the EMUIT directors on 23<sup>rd</sup> February.

## 4 Methodology

After an initial meeting with library staff, to introduce them to the proposed change and seek their cooperation in making it, the initial work was mainly technical: installing and configuring and testing the AthensIM implementation of version 1.2 of the Shibboleth Origin to inter-work with the Eduserv Athens Shibboleth Test Federation on a development server. (Version 1.3 of Shibboleth was announced during the implementation, but the AthensIM software does not support it). The software was run under Tomcat 4.1.31 and Java 1.5, connected via a ModJK 2 connector to an Apache 2.0.52 web server as the front end, all running under version 4 of Whitebox linux.

Library staff were then invited to try the implementation and give feedback about its usability. A decision was then made, in mid-July, that it was feasible to proceed to production for the September intake of undergraduates.

Given that it was thought to be so, the implementation was moved to production hardware and the live Athens UK Federation; some cosmetic changes made and documentation prepared for the new intake. There was then a support phase, as the implementation was used in live service, followed by an evaluation of its success. In the light of that, we planned to look at the issues involved in getting staff and students with existing ATHENS usernames to change to using their local ones, and at providing single sign-on to ATHENS resources from our portal. Finally, we documented our experience in this report and presented it to a meeting of East Midlands University IT Directors.

It was not expected that use of traditional ATHENS usernames would be eliminated entirely within the timescale of the project and use of Shibboleth for access to other resources was outside its scope.

The timescale of the project was expected to be rather tight, especially the early phases, at a time of significant change within Information Services, and this indeed proved to be the case. However, the essential deadline of the start of session was met. Involvement of the library staff was a key factor in its success.

## 5 Implementation

The project was undertaken by a small team (see Acknowledgements above) which met occasionally, but whose members worked largely independently to achieve the agreed goals, communicating in person or by e-mail with each other and other colleagues as required. Monthly Information Services Connected Campus project reports were submitted internally and a mid-term report was submitted to JISC. Members attended four meetings of the Subject Librarians to inform, consult and get feedback from them and the work was reported to the IS Library Systems Project Board.

The following issues were anticipated in the project plan:

a) Any software implementation issues.

These were resolved with assistance from MATU and Eduserv and documented for them. Overall, the implementation took somewhat longer and required more effort than had been anticipated, due to unfamiliarity with the protocols and difficulty of getting diagnostics due to the distributed nature of the interactions, but we managed to get a demonstration environment working by the end of June. This was only possible because of the high quality of the AthensIM Shibboleth Origin implementation, the documentation provided with it, local technical expertise and the support we received.

Apart from learning, testing and debugging, the main work involved was to write about 300 lines of Java code to tailor the AthensIM implementation to for local use, in particular to generate a permission set from the departmental code which forms the prefix of our usernames.

b) The mapping of attributes required by ATHENS Shibboleth targets to those available in our directory.

In contrast, the mapping of attributes for students proved to be less problematic than expected as we seem to be able to get away with a minimalist approach of just passing a pseudo-anonymous identifier (though we had problems with this due to a typo in our configuration file) and an Athens permission set, which we derive from the departmental code owning the username via a lookup table.

For staff, however, we have the issue that people registered with staff usernames range from full-time academic staff on the University payroll through to people doing occasional supervision of medical students or visiting academics. It is unclear both, as a matter of policy, what their respective entitlements to access Athens resources should be and, technically, how to derive them. The approach we are planning to take is to store an Athens permission set as an attribute of each user in our LDAP directory, but leave it null when the username is created. When the user first attempts to access the Athens/Shibboleth gateway, an attempt will be made to determine his or her status by means of a database lookup, generate the name of an appropriate permission set, based on their status and department, and store it in the directory for subsequent use, giving access only to publicly available resources in the case of any doubt. A web based interface written in Java will be provided for library staff to amend this on application by the user.

c) Ease of use, in particular explaining the concepts to our customer base and helpdesk staff.

The main issue here is that the Athens user interface is still primarily designed for use with Classic Athens usernames. Users of local usernames via Shibboleth or AthensDA are required to opt for 'Alternative Login', identify their site, select an option from a locally provided web page and finally supply their username and password. The path is a bit shorter on subsequent attempts, if a cookie has been set in the browser indicating which site the person is from, but may be off-putting to

newcomers. We were unable to pre-set the cookie in browsers on public workstations because both access methods were in use during the pilot.

d) Performance and reliability.

Although not instantaneous, performance has been acceptable, with the only noticeable delay being after supplying the username and password, but covered by a 'you are being logged in message'.

Reliability has generally been good, except that we have experienced occasional failures of communication between Apache and Tomcat on our Shibboleth server (which uses a ModJK 2 connector). These have occurred about once a month and have been circumvented by restarting the processes. We intend to do so weekly on a scheduled basis to avoid unscheduled failures. There was also a single instance of a problem caused by clocks getting out of step due to a failure to set up time synchronisation.

We have considered load sharing across two servers to reduce risk of service loss due to server failure, but concluded that this would only be possible with an active-passive configuration, due to the risk of various requests in the authorisation process being directed to different servers.

e) Interfaces for support staff to resolve problems.

Support staff have no access to the Shibboleth server, so any problems have to be investigated by technical staff. In practice, this has not been too much of an issue as few problems have been experienced.

f) Logging and analysis of access to enable legitimate usage of resources to be metered and any misuse to be detected.

No analysis of log files has been performed, other than to count the number of login attempts and number of distinct usernames given.

g) Maintenance of state, e.g. saved searches, for individual users and transfer of such state from traditional ATHENS usernames.

It appears that sites which enable state to be saved generally require an additional, non-Athens, site-specific username created on the site itself and the state is saved under that, rather than the Athens username itself. Given that, moving from a Classic Athens to a Shibboleth enabled username for the initial site access should not be an issue.

h) Management of and publicity for transition from traditional ATHENS usernames for existing users.

This fell outside the scope of the pilot.

i) Integration with our portal.

The possibility of providing single sign-on to Athens/Shibboleth resources from our portal was investigated, but it was decided the appropriate point to do this was in the Metalib e-library gateway. A new version of the (commercially supplied) code for this, which appears to support Shibboleth, is imminent so this was not taken further.

The main issue that was not anticipated was that of the inaccessibility of some publishers' sites due to them not running a sufficiently recent version of the Athens software. The number of resources affected was initially quite large, in excess of a hundred, but fell dramatically as the project progressed. It is now down to a hard core of less than 20 publishers: the list is at <http://www.athensams.net/nongatewayresources.php>.

The AthensIM Shibboleth Origin software was written to version 1.2 of the Shibboleth standard, though 1.3 was announced fairly early in the life of the project. However, the Athens gateway appears to support both versions, though we see no reason to upgrade at present.

## 6 Outputs and Results

During the period of the pilot, covering the first two terms of the academic year, about 16,800 authorisation requests were processed for some 2,500 different usernames, about half the potential user group. About 2690 classic Athens usernames were requested by this group, which suggests that the other half fell back to the traditional route, either because they were advised to do so by out of date lecture notes, found that the publisher sites they needed to access did not support the Athens/Shibboleth gateway or had difficulty using it (though some users may have used both routes and others neither).

The work was presented and discussed at a meeting of East Midlands Universities IT (EMUIT) directors and we received a visit from staff at Wakefield College who wished to learn what we had done.

## 7 Outcomes

The main objective, that of piloting the Athens/Shibboleth gateway in live service, has been met and our experience with it has been sufficiently encouraging for us to plan to expand its usage. Students who have successfully navigated the path to it seem to have used it with very few reported problems and have avoided the inconvenience of needing a separate Athens username and password. The main organisational benefit will come when use of Classic Athens usernames can be dispensed with entirely.

Other sites thinking of progressing down this route may benefit from our experience, but the incentive to do so will have been considerably reduced by the announcement of the move to a pure Shibboleth solution by July 2008: their efforts may be better spent in developing that.

The methodology of having a small, cross-disciplinary, project group generally worked well, and the communication with and the support we received from library staff was good. However, although involving just one person in the technical implementation was highly productive, it has left us vulnerable should he not be available.

## 8 Conclusions

The Athens/Shibboleth gateway is a viable means of authenticating and authorising access to Athens resources, requiring only the name of an Athens permission set to be held or derived for each user. The AthensIM implementation of the Shibboleth Origin software generally worked well. However, using the gateway is clearly dependent on the continuing existence of the Athens infrastructure and thus has a maximum lifetime of two years, unless support for Athens is extended.

## 9 Implications

Our experience has been that a high degree of technical expertise is needed to understand the Shibboleth protocol and support the software that implements it: the complexity of it may be daunting to sites without such resources.

Undoubtedly, having Athens as an intermediary between ourselves and the publishers sites has made it considerably easier to manage access than we suspect will be the case when we need to interact directly with them via Shibboleth. In particular, the concept of the Athens permission set is a convenient way of specifying access rights; mapping attributes from our own schema of user attributes to those of the proposed federation could be a lot more difficult. Having a single point of contact for support issues is also likely to be missed.

## 10 Recommendations

The two-year timescale for the switch from Athens to a pure Shibboleth access mechanism seems tight, even given the advantage we have had of exposure to Shibboleth technology through this project. We suggest that the timing of the cessation of support for Athens should be reviewed in the light of the experience of the early adopters of its proposed replacement; we are not convinced that using the Athens/Shibboleth gateway in the way that we have piloted is sufficiently close to the direct use of Shibboleth to give us confidence that we are aware of and have resolved all the issues involved in that. Note that if Athens were to be turned off at the end of July 2008, masters students whose courses run until September would either have to experience a change of access method mid-way through their course, or we would have to be running pure Shibboleth access for them by September, 2007, which is less than 18 months away.

As more sites start to use local authentication rather than Classic Athens it would help their users if the login dialogue could give more prominence to this.

## 11 References

The web site for the project materials, including the presentation to EMUIT directors, is at

<http://www.nottingham.ac.uk/is/about/projects/unisa>

Athens documentation about Shibboleth interoperability, including a link to download the AthensIM Shibboleth Origin implementation, is at:

[http://www.athensams.net/local\\_auth/shibboleth/](http://www.athensams.net/local_auth/shibboleth/)