

Overview

The JISC Core Middleware initiative aims to improve the way in which users access resources throughout the UK educational sector. Specifically, the goal is to allow users to access internal and external resources seamlessly using a single, institutionally controlled identity. This will reduce substantially (if not eliminate altogether) current problems in which users are required to maintain multiple passwords for multiple resources in multiple domains.

For the last two years JISC has devoted a significant part of its development funding to access management issues. Many different solutions and scenarios have been investigated and tested, alongside research into supporting factors such as cultural change. The outcome is to base the strategy on Shibboleth technology, a new standards-based approach in this area. This paper explains what Shibboleth is and its consequences for universities and colleges.

Athens

Anyone using resources such as databases or e-journals made available over JANET by data centres or publishers will typically use an Athens username and password to gain access. For a number of years the JISC-funded Athens service has put the UK ahead of the rest of the world in providing a consistent and uniform access mechanism to a wide range of different off-campus resources. The Athens interface prompts users for a username and password, and then uses that information to establish access to Athens-protected services.

Shibboleth

While the UK has been using Athens, other countries have been developing their own solutions to the problem of accessing multiple resources with a single identity. Shibboleth, which is a product of the US's Internet2 initiative, has emerged as the front-runner for the most widely adopted standards-based approach. Australia and a number of European countries, including Switzerland, Finland and the Netherlands have already adopted it or are in the process of doing so. A number of commercial service providers are planning to create interfaces to their services using Shibboleth technology or already provide them.

Shibboleth does not carry out authentication itself. Instead, Shibboleth defines a set of protocols for the secure passing of identity information between institutions and service providers.

It relies on the institution to establish identity, and on the service provider to confirm access rights, given information about institutional affiliation. It is written in SAML (Security Assertion Markup Language), an international standard developed by the OASIS Security Services Technical Committee.

How authentication is carried out by the institution, and how rights management is carried out by the service provider is left up to the respective parties. In so doing, Shibboleth depends on a certain level of trust. Service providers need to be confident that the institution or organisation that the user belongs to has a robust and up-to-date authentication system in place.

This need for trust leads to the concept of federations. Federations are groups of similar organisations such as universities, who have agreed to a common set of policies. They are typically being established at a national level. For example US higher education has established a federation known as InCommon. The equivalent in Switzerland is known as SWITCHaa and in Finland as HAKA. The UK access management federation will be run by UKERNA, building on the experiences of a successful pilot federation at EDINA – a JISC data centre. The pilot federation is available to join now, and members will be seamlessly migrated to the new UK access management federation on its launch in July 2006.

Shibboleth

The word comes from the Old Testament (Judges 12:1-6). The Ephraimites who lived to the west of the river Jordan invaded Gilead on the other side of the river and were defeated. Retreating, their way was blocked by the Gileadites who controlled the fords. They had different accents and the Ephraimites pronounced the 'sh' sound as 'si'. To separate friend from foe, those crossing the river were asked to pronounce the word 'shibboleth' (it means an ear of corn). According to the bible, the 42,000 who pronounced it 'sibboleth' were killed.

Another feature of Shibboleth is the emphasis it places on user privacy. The system devolves all responsibility for user authentication to the user's institution. The information passed to the service provider by the institution is of the form 'this user is a member of our institution', or perhaps 'this user is a member of the psychology department of this institution'. In other words, the information passed back to the service provider is about status rather than personal identity.

Why change?

With Athens established as a successful solution, it is reasonable to ask why the UK should change. There are several reasons. Currently, in order to make their products available to the UK community, service providers have to implement Athens on their systems. The classic Athens system uses a separate identifier and password for remote resources. These may be difficult to remember alongside other, locally-used, usernames and passwords. The result is that these are either forgotten, reducing take-up of expensively acquired services, or are written down, compromising security. Shibboleth relies on locally-used identity credentials, which are also likely to provide access to personal information such as library holdings or email. These are much more likely to be remembered and kept confidential.

Finally, there are increasing demands for more sophisticated systems for enabling access to materials and resources driven by initiatives such as e-learning, regional collaborations, and multi-institutional projects. Shibboleth's flexible design provides a good basis for meeting these demands.

What JISC is doing

As part of the move to a Shibboleth-based solution, JISC is supporting and funding a range of activities including:

- The JISC pilot and full production federations
- Adding Shibboleth compliance to the JISC-funded services provided by the national data centres
- Support for a number of 'early adopter' institutions to help them explore internal and external use of Shibboleth-based services
- The use of Shibboleth in some of the JISC distributed e-learning pilots
- The creation of a support service to provide advice, guidance, training and software to the early-adopter institutions

- The development (by Eduserv, who developed the Athens software) of an Athens/Shibboleth gateway, so that institutions who adopt Shibboleth solutions will remain able to access Athens-protected services, and similarly institutions who opt to stay with Athens will be able to access Shibboleth-protected services.

What does this mean for institutions?

Institutions are now being asked to recognise this change within their IT strategies for the next two years. Early adopters are able to start work immediately by using the pilot federation, from which they will be seamlessly migrated to the full production federation from September 2006. Support for all institutions is available through the existing MATU support service at Eduserv, and through the experiences and reports from the JISC-funded early adopter pilots. Announcements about developments in this area will be made on a JISCMail list established for the purpose (JISC-SHIBBOLETH-ANNOUNCE). An open discussion list has also been set up (JISC-SHIBBOLETH).

The current Athens contract with JISC will be renewed until July 2008, and will run in parallel to the UK access management federation and the Athens/Shibboleth gateway for the next two years allowing institutions the time to make a considered choice about when to migrate. From July 2008, JISC will support access management through the UK access management federation within the UK.

Published February 2006

Alternative formats of the briefing paper can be found at:
www.jisc.ac.uk/publications

Further information and resources

JISC Core Middleware web pages:

Information about the JISC Federation:
www.jisc.ac.uk/federation.html

General information on the JISC Core Middleware programme with useful links:
www.jisc.ac.uk/programme_middleware.html

Athens information on Shibboleth

www.athensams.net/shibboleth

Support Service

www.matu.ac.uk

OASIS Security Services Technical Committee

www.oasis-open.org

Internet2 pages on Shibboleth

The Shibboleth project
<http://shibboleth.internet2.edu>

FAQ's on Shibboleth
<http://shibboleth.internet2.edu/shib-faq.html>

Shibboleth-enabled service providers
<http://shibboleth.internet2.edu/seas.html>

JISCMail lists

Discussion list
JISC-SHIBBOLETH@jiscmail.ac.uk

Announcement list
JISC-SHIBBOLETH-ANNOUNCE@jiscmail.ac.uk