

Shibboleth® in Further Education



10th May 2006

Final

Eduserv

Authored by: Tim Hall
ICT Services Development
Team
Kidderminster College

Date: 10th May 2006

Revised by: Richard Dunning
Karin Maslen
Edwood Beddows

Revised date: 19th April 2006

Table of Contents

Executive Summary.....	3
Shibboleth in Further Education	4
Supported Institutions	5
Supported Projects	6
Suitability.....	7
Potential Take-Up.....	7
Barriers to Take-Up	8
Colleges.....	9
Schools	10
Take-Up Costs.....	11
Skills Availability	13
Maintenance and Administration	14
Common Problems.....	14
Applications	15
The Way Forward	16
Conclusion	18
Appendices	19
Appendix 1	19
Appendix 2	20
Appendix 3	22
Appendix 4	23
Appendix 5	24
Appendix 6	25

Executive Summary

As part of the JISC funded Early Adopters programme, Kidderminster College worked on the Shibboleth component of two projects, WM-SHARE and ePistle. These projects involved the design and implementation of a Shibboleth framework to help deliver the required resources to the end-users; our experience in these projects is documented in the report.

Using Shibboleth authentication with these projects has demonstrated the potential applications that Shibboleth can be applied to. By consolidating the number of accounts that a user has, the likelihood of discrepancies found when creating multiple accounts can be reduced. When set up correctly, it also streamlines the log in process, automatically utilising single sign-on (SSO) principles. A single user can access an institution's resources potentially anywhere in the world as long as their institution and the institution providing the resource are in the same group or federation. Shibboleth as an architecture is suitable for most institutions and it is possible to successfully implement Shibboleth IdPs in disparate network environments. It is also flexible enough to function in different network models and authenticate users from many different types of attribute stores. However, the complexity of the environment affects the way Shibboleth is employed as Shibboleth installs tend to differ from site-to-site.

We encountered many barriers during implementation, from the actual software functionality that required creative thinking and expertise to integrate it in some environments. The quality of attributes (edupersonprinciple etc.) contained in the attribute stores differed on an institutional basis; this inconsistency in quality may later affect the effectiveness of Shibboleth itself with certain resources, for example the lack of a required attribute. Throughout our project we found knowledge of Shibboleth was quite low, which was to be expected as it is a new and emerging technology and the framework it is built on is still developing and not found in production use in many Further Education (FE) environments. 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.

Take-up costs are relatively low, the bulk of which being training in Shibboleth and its associated technologies. Shibboleth will run on a relatively low spec of hardware as it is not resource intensive. Take-up costs may however be an issue if the institution does not have the pre-requisites in place, for example an unpopulated or nonexistent attribute store; implementing this from scratch would require a lot of time and money.

Throughout this document, references to "we", "I", "us" and "our" refer to the Kidderminster College project team.

Shibboleth in Further Education

This report is based upon our experiences in a FE environment supporting and implementing Shibboleth technologies for three Joint Information Systems Committee (JISC) funded early adopter projects. Throughout the lifetime of this project, we discovered many barriers and constraints but also demonstrated the practicality and usefulness of Shibboleth in an FE environment.

Shibboleth allows an institution's user to access protected resources or services of another institution by using their attributes stored in their home user data store. Ultimately, this means that an institutional user can access repositories, sites, virtual learning environments (VLEs) etc. from a single user account. We have integrated Shibboleth authentication in three services: the Moodle VLE at RSC West Midlands and Kidderminster, repositories at Kidderminster and the ePistle e-portfolio service hosted by Wolverhampton University. Access to these services is controlled through a federation, the gateway to these being the Where Are You From (WAYF) service hosted by Kidderminster.

Services such as repositories, VLEs etc. are protected by the service provider (SP) instance of Shibboleth hosting, while the authentication is dealt with by the identity provider (IdP) service.

Appendix 1 shows an overview of the KC-Rolo federation that we maintain and support. We have a number of institutional IdPs in disparate educational environments from higher to secondary education.

Supported Institutions

We offer and/or support service provider provision, which features Shibboleth authenticated access, for the following partner institutions:

Higher Education Sector (HE)

- Kidderminster College
Repository of learning objects powered by an engine supplied by Coventry College.
Moodle VLE, five instances broken down into departmental and staff implementations.
- RSC West Midlands
Moodle VLE, a training instance of this VLE for delegates of West Midlands institutions.
- Worcester University
Repository of learning objects powered by an engine supplied by Coventry College.
- Wolverhampton University
ePistle, e-portfolio service based on pebblePad run in partnership with secondary and FE institutions.

Users at an institution where there is an IdP access these SPs using their authentication credentials at their home institution. These institutions are typically partners of the projects that use Shibboleth for authentication. These projects all utilise the KC-ROLO federation.

Further Education Sector (FE)

- Bourneville College
- Josiah Mason College
- Kidderminster College
- Rodbaston Agricultural College
- RSC West Midlands
- Shireland Language College
- Telford College of Arts and Technology
- Wolverhampton University
- Worcester College of Technology

Secondary Education Sector

- Shirelands Language College
- Leasowes Community College

Supported Projects

There are three supported Shibboleth projects:

- Kidderminster College - <http://kidderminster.ac.uk/kc-rolo>

A two year project investigating and implementing shibbolised access to content. This includes working with the latest versions of Shibboleth, protecting both Kidderminster's Moodle, VLE and repository.

- Worcester University - <http://www2.worc.ac.uk/wm-share>

A project to establish a protected repository of learning resources that are only accessible by partner institutions.

- Wolverhampton University - ePistle (<http://www.pebblelearning.co.uk/>)

Based on pebblePad, ePistle is a flash-based e-portfolio that not only allows protected authentication but also utilises Shibboleth's "attribute release policy" (ARP) to get user-specific data, such as date of birth, thus saving the user the need to submit some personal attributes when they use this system.

These projects all have partner institutions which authenticate against their own user data store, active directory (AD), to access content on each of these projects' SPs. These are from a broad range in Secondary, FE and HE institutions.

Unfortunately, due to reasons beyond our control some of these IdPs were not implemented or are no longer operating. The main inhibitor being the lack of time that these smaller institutions have to provide the information we require, and to make changes to their infrastructure.

Shibboleth is a new technology and subsequently is under continuous development, with the background framework constantly being honed and improved. All of our pilot/production implementations to date use Shibboleth as the security assertion markup language (SAML) authentication component and our services are run on Red Hat Fedora. Our implementations of Shibboleth service and identity providers use Shibboleth version 1.2 upwards and Fedora cores 3 and 4. These servers are supported primarily by the Kidderminster team for the duration of the project and are updated on a regular basis.

The Goal is to upgrade from Shibboleth version 1.2. to 1.3c on servers in use. This upgrade will offer performance and stability improvements and SAML v1.1 compliance as well as the ability to join multiple federations; thus, a single identity provider can be a member of more than one federation or group sharing resources. Fortunately, as the versions are compatible, a gradual upgrade can be conducted without disruption to the service.

Suitability

Shibboleth as a single sign-on technology offers access to services facilitating inter-institutional access to resources. This, in most cases, is the end-user simply using their institutional username and password once. This effectively means that in any institution operating individual user accounts it is feasible to implement a Shibboleth IdP box.

With FE institutional budgets strained, the majority of teaching resources are outsourced. By using a single account to access these subscribed e-resources rather than multiple ones, it is useful in terms of management and user experience, being less time consuming and saving on unnecessary duplication of data.

Resources protected by a Shibboleth service provider such as the Athens gateway can then also be accessed using the same institutional credentials. This is further expanded with e-portfolio and repository services that are being trialled with access allowed to all resources and switching between them while only having to sign on once.

There are instances where Shibboleth protected access to resources are now offered; currently the majority of these within the bounds of their respective projects or trials.

Regardless of educational sector, Shibboleth is useful where protected resources are accessed from external sources. Suitability is dependent on the external resources available, for example, if most resources are geared towards the HE rather than the FE sector, then institutions may feel it is not suitable. However, I do not see this as an issue as many appropriately prepared service providers are starting to appear.

Potential Take-Up

There is a potential for every FE institution in the UK to utilise Shibboleth; this becomes even more relevant with the introduction of the Athens to Shibboleth gateway. The news of a planned UK national federation will appeal to institutions that may have no intention of sharing their own resources.

It is most likely that many FE institutions will choose to implement IdPs because they have insufficient resources to create and share their own content. However, many FE institutions collaborate with each other; for example, Kidderminster shares their VLE with the University of Worcester media students.

Where the Athens service is subscribed to, an institution can benefit from accessing services through the shibbolised Athens gateway. In order to utilise this form of access, Shibboleth

IdP or AthensIM, (a customised version of Shibboleth 1.2) must be implemented; doing so will provide the institution with access to Athens protected resources plus the benefits of Shibboleth, namely low administrative overhead and single sign-on capabilities.

Barriers to Take-Up

Where an institution has a secure and managed user attribute store of all its users in a Lightweight Directory Access Protocol (LDAP) or LDAP compatible form, such as an active directory, coupled with a means of opening ports, most Shibboleth implementations should be successful. However, a number of constraints as listed below have been encountered:

General

Confidentiality can potentially become an issue, where an SP requests student names for example, but an institution refuses to release them. This can result in the institution being unable to use that SP as a result of institutional policy prohibiting the release of such attributes for reasons of security or data protection compliance for example.

User Attribute Store

The Shibboleth IdP can interrogate the user attribute store and release details about that user to the service provider. Those details that are released are defined at configuration and can therefore be stored differently on every institution's attribute store. This would mean a customised release policy would be required for each IdP.

In addition, the quantity and quality of the data in this attribute store (e.g. active directory) varies greatly - where one institution may populate their store with copious amounts of data, and others with nothing more than a username. This meant the ePistle and Moodle services needed to cope with atypical data. Both ePistle and Moodle are designed as such to cope with missing fields and will prompt for the required attributes.

Software Design

While a Shibboleth SP can be built, a federation created and a number of IdPs to access it implemented, legal concerns such as property rights, copyright etc. can cause problems when attempting to actually share access to resources. As a result, discussions on how to deal with this can frustrate any ambitions to implement a service that can justify Shibboleth use.

Where an institution wishes to access an SP's resource, they may be bound by the access rules and policies of that SP. Some of these rules may require certain attributes to be present. If this is currently not the case, changes to the internal authorisation system may need to be made, which could require extensive time and resources to achieve.

Colleges

Expertise and time are the major constraints to implementation in a college environment. Shibboleth requires a fairly specialised understanding and very few FE institutions possess the knowledge or experience to implement instances of Shibboleth without training or research.

Where we installed IdPs for partner institutions of Wolverhampton's ePistle project, some technical staff viewed the server with suspicion. Network staff quite rightly expressed doubt over a server within their network that they knew nothing about. In response, we developed a basic Shibboleth institution guide explaining in basic terms how Shibboleth works and why certain changes needed to be made (see Appendix 2).

In most cases, technical staff have complete control over their network and internet access. This facilitates rather than hinders implementation with a typically small number of people in a geographically small area to deal with. Larger organisations or those that outsource, experience greater levels of bureaucracy, which can often hinder and slow down the implementation process.

That said we experienced challenges deploying an IdP in most of the FE institutions. Each institution required a different approach to overcome these challenges in getting the boxes in and running.

The most difficult problem we faced was the amount of time that technical staff were able to offer. As a member of a small team, they were required to deal with a wide range of projects and problems limiting the amount of time they could give to us, understandably not wishing to introduce a new service which would take up extra time, and one which they had not been trained in.

Challenges

Staff turnaround set one institution back whilst a new network manager became familiar with his surroundings and the hardware (firewall, servers etc.).

A college with very knowledgeable IT staff, who were unaware of their shiny new IdP, wanted (needed!) to know about this box which after all was going to sit in their demilitarized zone (DMZ) and have lookup access to the data stored in the active directory. As their data store contained a significant amount of each user's personal details, they had some security concerns that needed to be addressed before the service could go live. As they were busy, it took time to conduct a risk assessment.

Another institution's network was not the typical model that we chose to implement in (see Appendix 3). Where they used a software firewall (ISA Server), we had to install the IdP inside the network (note: this is a greater risk due to the increased exposure should the server be compromised). Some bespoke settings needed to be plugged in and unfortunately the network manager did not have the skills to open up the required amount of access to the IdP. Although it took some time, we eventually cracked it with help from Max Caines at Wolverhampton.

Failed Implementations

We failed to implement planned IdPs in some FE institutions.

One institution provided us with a machine that we had built the IdP service on. Unfortunately, this server is still in our possession awaiting a response as establishing a contact has taken some time.

A common problem was found at all of these institutions namely, time was at a premium. Constraints on funding within the sector have increased the pressure within departments to perform an ever increasing number of tasks with a shortage of skilled staff. Therefore, getting anything done has taken much longer than expected. We feel this was due to the fact that some technical staff regarded this Shibboleth install as a non-critical service making it a low priority; this can be understood as it is essentially a development project and not a fully tested production implementation.

Schools

Although not FE, some institutions may encounter problems we only found in this environment. In particular, the complexity of the network model used in some schools and the support structure in place made both implementing and resolving issues take longer than that of a typical FE institution. Some FE institutions may have a complex setup similar to this environment, and some may wish to implement a Shibboleth IdP to allow a partner school to implement their shibbolised resources.

Internal Knowledge

Schools have a tight budget and subsequently the staff involved with IT support varies a great deal. As a result, there is an increased likelihood that the support staff will not possess the skill set required to implement Shibboleth. Some schools may not even have a full-time technician. It would therefore require an engineer to visit and implement an IdP solution in this environment.

Take-Up Costs

Shibboleth Service

The cost is dependent on how an institution wishes to use Shibboleth as both an identity provider as well as offer their own shibbolised services or applications.

With the skill set and new knowledge that needs to be acquired, it will take some time for schools to fully understand the implications of implementing both an IdP and SP to access and provide these services. Time and training will be necessary as it is important for schools to understand the security implications for example, where ports and user sensitive data is opened up, in order to prevent inadvertent misuse of the system.

Hardware

Identity Providers (IdPs)

A Shibboleth IdP has relatively low resource overheads when compared to some other Web services; because of this it can be demonstrated as a viable solution on a low end server, this of course is ultimately dependant on the number of concurrent users. If Shibboleth is determined to be an institution resource in a production environment then redundancy is advised, either on a legacy server or a second mirrored desktop.

Service Providers (SPs)

Where an institution chooses to introduce a service provider, the service itself is not resource intensive and like the IdP will run efficiently on a basic machine. Shibbolising will use a minimal amount of existing resources. With the introduction of a complete system, such as a new VLE or repository, consideration needs to be given to the requirements of whatever service is being shibbolised.

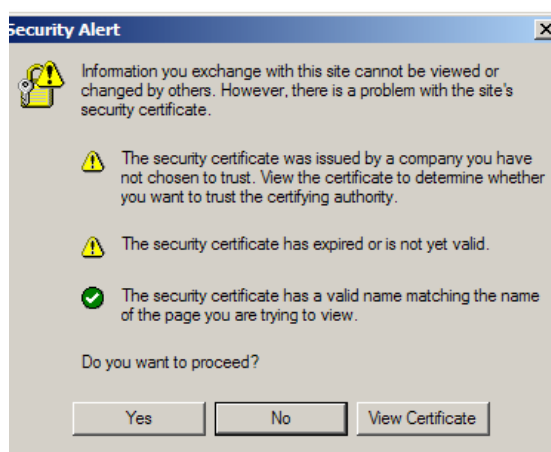
Software

Shibboleth technology is open source and requires no licensing. As it is “free” to obtain and use at personal and enterprise level there are no licensing costs associated with it. This is also true of the components and plug-ins that it uses such as Apache for example. The associated costs are those with maintenance and or training to support the service, which is a critical component, and would need to be considered as part of the initial and ongoing costs. In the instance of an institution not having any directory services implemented there are alternatives, linking directly with an institutions ‘Management Information System’ (MIS) is possible, for example, if MySQL or Oracle is used to store user information then this may be used as both the attribute store and the authentication handler. In the unlikely event that an institution did not have any data store, or if it was not compatible with the methods built into Shibboleth, then extra time and money would probably be required.

Shibboleth itself could be extended so the resolver and 'Handle Service' could link in with bespoke software. This could take considerable time and money if the skill set to do so is not present; perhaps a cheaper alternative would be to implement a free database such as MySQL to take over the role of the MIS system. The latter option however could have far reaching consequences with other software in the organisation. Costs will also be incurred in terms of the time needed by a developer to shibbolise an existing resource such as a VLE or repository. This task may need to be outsourced as existing staff may not possess the necessary skill set and/or time to implement the service.

Certificates

One of the mechanisms for determining trust in the Shibboleth architecture is the use of certificates. During initial development of Shibboleth services, we used certificates that were "self signed". As our self signed certificates do not come from a recognised certificate issuing body (Globalsign, Thwate, Verisign) a dialogue box appears during the process asking the user if they trust the certificate:



While this is acceptable for development use and an experienced user, it is not suitable for production use. More mouse/keyboard entries are required, which will slow the process down and also act to confuse and alienate a significant number of users.

Authentic certificates from a trusted source therefore needed to be obtained. We have selected Globalsign certificates for our servers and Wolverhampton University have provided us with the funds to purchase a wildcard certificate. The wildcard certificate allows us to secure multiple servers using the same domain, for example, idp.kidderminster.ac.uk or any other prefix to the Kidderminster.ac.uk domain could be used; for the end-user it works in the same way as a standard certificate.

These certificates incur ongoing cost as they need to be renewed in annual increments and this will further strain tight budgets. Certificate costs are detailed in Appendix 4.

Skills Availability

Once involved, the concept and the flow of Shibboleth are easy to follow and understand. It does however, require background knowledge, training and research, and most importantly 'time' to implement this technology. Currently, Linux is the preferred platform to implement on and therefore, some experience with Linux and its utilities and applications would be beneficial.

To implement Shibboleth, the administrator requires knowledge of the following technologies (assuming the platform is Linux):

- The chosen Linux distribution
- Firewalls (both hard and software)
- NTP
- Web server (Apache)
- XML
- Internal attribute stores (e.g. active directory, OpenLDAP, MySQL database, Oracle)
- Apache plugins (e.g. auth_ldap), Xerces, Tomcat, Jk2 Connectors
- Certificates
- General networking and concepts.

In our experience most institutions in FE have IT staff who only possess knowledge in Microsoft technologies. This is evident by the fact that all our IdPs access data stores are based on active directory.

Most of the above are explained in installation guides that enable an administrator to successfully install Shibboleth and configure their network without necessarily requiring an in-depth knowledge of the majority of the above. However, it is important that an administrator has a good understanding of their network for security and quality of service (QoS) reasons.

Appendix 5 shows the information we require of an institution in order to implement a Shibboleth IdP.

Support in some cases may come from service providers, particularly with the introduction of more commercial applications, and these providers have a vested interest in an institution using their service so may offer additional help to end-users to get them on the system successfully. This support could help with both the initial IdP setup and the specific settings required to make the Web application work with individual institutions. Limited support may also be offered by federation administrators, which could involve help in configuring IdPs and SPs configurations to successfully take part in the federation.

Maintenance and Administration

A fully configured IdP server practically requires zero maintenance once it is configured and running. Similarly, attention needs to be given to this server as any other, such as updating the systems core programs, backing up files, regular viewing of log files and other operations which ensure the security and stability of the server.

Administration of the user attribute store is vital for Shibboleth to work correctly. It is imperative that the integrity of the user attributes store is accurate. Failure will result in users being unable to access certain SPs.

Updates and backups of data need to be carried out systematically and in accordance with need and policy. As Shibboleth becomes a more established service, redundancies and contingencies require to be put in place.

For the ePistle project, we have IdP contingencies in place. There is a copy of a vanilla implementation of Linux and the Shibboleth IdP on CD and a redundant server. In addition, the institute specific data (attribute release policy, certificate data and so on) is also backed up. In the event of a problem, we can restore the institution specific settings and/or restore the whole operating system with the Linux components installed.

The redundant server we have at base ensures that in the event of catastrophic hardware failure, we can swap servers within an hour. This is important as the service provider can be accessed if the IdP is down. This was tested when disk failure occurred at Wolverhampton College; the entire swap out procedure taking no more than ten minutes on-site.

Where work needs to be carried out on the server, we have remote console access to each IdP which means that most issues can and have been resolved remotely, thus reducing the amount of time a service is down.

Support should be offered to institutions that chose to implement Shibboleth to help tackle the problems during implementation and most important to ensure maximum server uptime when it is relied on to access or share resources.

Common Problems

Shibboleth requires that the time on its servers are the same, big deficiencies will cause an error. As actively managing the clocks on our servers persistently and consistently would be prohibitive, a network time protocol (NTP) time server is used. Most institutions will provide one which goes on to sync with further servers up the tree. Those that do not can always use ntp.ja.net, the Janet ntp service. If the NTP details we are provided with are incorrect,

or a firewall or similar blocks access to the ntp server, the time will not sync and will gradually lose time until an error occurs. Another more immediate example is the transference from GMT to BST and vice versa. We have encountered problems based on the above scenarios at three of the above institutions. A manual clock change is a quick fix, after which investigation is conducted to resolve the problem for good.

A common problem experienced with a number of these institutions is difficulty with the technical staff. Apathy and disorganisation have led to many of these institutions dragging a now relatively simple and streamlined procedure on for weeks and months with no end product as yet in some cases. Technical shortcomings are now overcome quite quickly through the experience of our team in developing solutions based on disparate network models and hardware.

Active directory functions as a LDAP directory and as most of our partner institutions' user attribute stores are built around active directory, it is important that Shibboleth can resolve data from the active directory data store. The predetermined structure of AD is determined at its inception and is a logical tree typically containing a number of folders, organisational units (OUs). Depending on how these OUs are structured, we found that we could only search one OU from the root of the structure. Therefore, when we found instances where multiple user stores were at the root (e.g. students and staff OUs), we were unable to search in more than one OU at the root. We struggled to resolve this and eventually used a workaround with global cataloguing. Whilst not ideal, it offered some functionality. We eventually discovered and resolved essentially a DNS issue (see Appendix 6 for details).

Applications

Due to the nature of FE funding, an FE institution typically does not have the resources to produce sufficient learning materials. With this in mind, the learning resources are "outsourced" in the form of books, videos and e-learning materials. We found that using passwords and user accounts to access these subscribed e-learning resources was far from ideal. Requiring a user to remember multiple user accounts and passwords can be inhibitive and more intensive logistically in administering and storing multiple data stores containing similar data.

As the Shibboleth service binds to many types of attribute store, more details than a user's account name can be released. The ePistle service benefited from this, saving a user the monotony of entering their date of birth for example. There are problems with this however, with regard to the attribute structure and its content. The attribute release policy that is configured can be customised to give disparate attributes in a standard form so that disparate fields in the local data stores are represented in a common format at the service

provider end. The problem with the user attribute stores (active directories) was with the differing level of data populating these stores.

The user's name for example, was stored in the display name field at some institutions, whilst being stored in the first and second name fields in others. This is not a problem however, as the attribute resolver can release these as "UserPrincipalName" to the service provider depending on how the attribute release policy is configured. We found when a greater amount of detail is required about a user, the likelihood of some user attribute stores containing blank fields increased. In a large number of cases, the user account contained usernames and given names and nothing more, whereas some were populated with a large amount of information.

The service that the SP protects, in this example the ePistle service, needed to cope with missing or incomplete fields where they were not released or not present in the user attribute store.

An institution can choose to implement an IdP where it can allow federated access to services or resources that are shared. These institutions can also choose to provide these services or resources to partner colleges.

Moodle VLE for example, now has a production quality component that simplifies the process of shibbolising the resource.

The Way Forward

Inter-institutional single sign-on technologies such as Shibboleth can only be a success if there are gains to be made from implementing it. Using common user attributes to authenticate against a number of internal and external resources as well as streamlining the process of connecting to external resources, Shibboleth justifies its use by making these gains both from the end-user's point of view and administrators who control access.

Shibboleth is ultimately built upon SAML, which is an XML derivative that is used for authenticating users between institutional domains using an identity provider and a service provider.

The goal of SAML is to offer single sign-on authentication for users of multiple resources in intranet and extranet applications. Ratified as a standard by the Organization for the Advancement of Structured Information Systems (OASIS), SAML is available in various implementations such as OpenSAML. Shibboleth itself is a SAML implementation but is not exclusively used. Other SAML implementations that fall under the JISC umbrella include Guanxi and AthensIM.

Shibboleth now at version 1.3c is the most popular SAML implementation in academia and early adopter schemes. It uses a cookie based system that does not send a user's credentials over the internet but rather encrypts user attributes depending on what the service provider requires.

When Shibboleth forms the authentication to enable access to resources inside and outside of an institution, it becomes a core service component. With this in mind, the service would need to be covered in the policies and procedures (e.g. security policy; business impact plan; disaster recovery) developed to deal with a failure of service. A support and implementation service for institutions that wish to utilise Shibboleth to access national shibbolised gateways and services such as Athens, and local ones such as WM-Share needs to be accessible and maintained.

Currently, we use a Linux box for our Shibboleth services, however, in a typical Windows environment the user has to enter their details twice; once to login to the Windows machine and then to re-enter their details once they open a browser instance to authenticate against their IdP in order to be able to reach an SP. Requiring a user to enter their details twice could be considered a barrier or a hindrance, meaning resources are not as accessible as we would like. To resolve the issue of having to re-submit a user's details on their first attempt to connect to an SP, we have implemented an IdP in Windows Server 2003 and linked the handle service to integrated Windows authentication. This automatically logs the user in if they are logged onto the domain. Whilst this is still at a development stage, where active directory is used, we can further streamline access to external resources.

A single implementation of an IdP, stored at a central server farm which supports multiple user attribute stores, can reduce the need for multiple IdPs for each satellite institution served by the same server farm. This type of future development is ideal in the case of the local authority server farm scenario that is employed at Shireland (see Appendix 3, Fig 1).

A shibbolised NLN gateway with VLE compatible metadata would remove the need for identical de-centralised repositories. This would be similar to that of an Athens shibbolised central repository of NLN content, rather than the current implementation which causes the duplication of NLN materials at every institutional repository. This ensures that the quality of NLN objects are up-to-date and consistent but on the other hand, may be too resource intensive.

Conclusion

Shibboleth is a technology that will have a useful application in academia. Where an institution frequently links and uses resources external to their own internal authentication, it can save on administration and ultimately the end-user's time. However, difficulties will be encountered that need to be overcome.

Shibboleth does not require a large investment in equipment as either existing legacy hardware or the acquisition of an inexpensive server can be used. This will be of particular importance with regard to school link schemes in order to utilise the school-based user attribute stores to access an FE service provider. There are a number of things to consider when implementing Shibboleth regarding costs, the greatest of these we believe to be the training of technical staff in implementing and maintaining their Shibboleth servers. An implementation and support service would help smaller colleges where resources and expertise is unavailable.

An important pre-requisite often overlooked is an accurate attribute store, in many institutions we have seen this not to be the case, and in these circumstances considerable time and resources may be needed to attain full functionality.

The bureaucratic process of introducing an IdP in some institutions is such that significant advanced planning is imperative to keep rollout on schedule. Issues that can hinder or slow down an implementation of a Shibboleth server such as network complexity or lack of expertise can result in an institution not being ready for a new academic year for example.

An institution's technical staff need to be on board from the start of discussions to introduce Shibboleth. This is important as there are security and data protection issues that need to be considered. In addition to this, Shibboleth is a service that cannot easily be dropped into an existing environment without extensive planning and preparation, due to its dependence on other services already existing on the network.

A basic guide explaining the impact of implementation, configuration information needed and risks associated to aid smaller institutions and non technical staff, such as a start up manual could speed up the implementation of Shibboleth in many institutions.

Appendix 2

Shibboleth Guide for Partner Institutions

The security and authentication for the ePistle/eportfolio service provided by Wolverhampton University is built upon Shibboleth technology. This document aims to provide a basic understanding of the Shibboleth architecture, how it is network linked and documents institution specific data.

Shibboleth Overview

Shibboleth technology operates within a single sign-on (SSO) environment that authenticates users of external services against their home site authorisation systems.

The benefits of this include:

- Enabling partner institutions to share objects and resources.
- Improving the access management of accounts; only one account is used to access resources.
- Securing the user's data does not pass beyond the institution's network.

Shibboleth is built on SAML, an XML standard that allows a user to securely log on to affiliated but separate Web sites. This technology comprises two primary components:

- o Identity Provider (IdP), the user's home organisation; in this case partner institution.
- o Service Provider (SP), the resource owner; in this case servers based at Wolverhampton.

In addition, a secondary service component, WAYF (Where Are You From?), is used to determine which institution to authenticate a user account against. This service is hosted at Kidderminster.

Users access the ePistle server (SP) employing their assigned attributes (username, password etc.) contained within their institution's (IdP) active directory. None of this data is passed across in clear text and the username and passwords are not passed beyond the institution's IdP. This is executed by a handle or identifier authorising access to the ePistle server.

In order to facilitate access, modifications need to be made to your firewall. Ports 80, 8443 and 443 need to be opened to allow http and SSL access for Shibboleth to function. To allow remote access using SSH, port 22 also needs to be opened. SSH is a secure encrypted channel whereby a user can access and configure a server

remotely. To facilitate lookups, an account inside your active directory structure is created.

Below is the institution specific data for your Shibboleth IdP server.

Shibboleth IdP Server Data

Shibboleth IdP Configuration		Server Configuration		Active Directory Lookup Information	
Admin account name	XXXXXX	DNS name	XXXXXX	LDAP/AD IP address	XXXXXX
Password	XXXXXX	NTP service IP address	XXXXXX	AD account name	XXXXXX
		Subnet mask	XXXXXX	Lookup account full path	XXXXXX
		Gateway	XXXXXX	Lookup account password	XXXXXX
		DNS server used	XXXXXX		

Appendix 3

Network Model

As a local authority would serve a number of institutions, the network model that is used will differ and therefore be more complex. Below are typical examples of an institution's route to the Internet

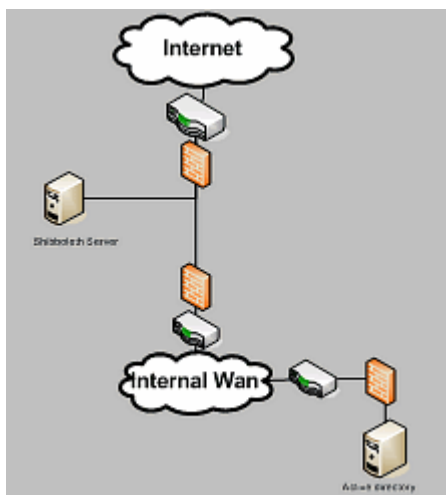


Figure 1 shows how an IdP can be placed within a local authority network.

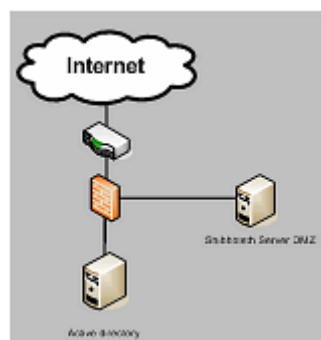


Figure 2 shows an institution with a direct connection to the Internet.

The local authority model above (Figure 1) shows multiple devices which are more than one person's area of responsibility. As well as an increased number of points of failure, fault finding is also more difficult. This model is based on a real world scenario where the IdP is operating from a local authority's server farm. In the case of this model, several schools connect to this server farm via the local authority's internal WAN. If a number of these schools chose to use Shibboleth in association with their local college for example, there would be a number of IdP servers based at that server farm.

Appendix 4

Certificate Pricing - Globalsign

ServerSign SSL Certificate prices		
<u>1 year</u>	<u>2 years</u>	<u>3 years</u>
175 Euro (excl. VAT)	322 Euro (excl. VAT)	430 Euro (excl. VAT)

ServerSign Wildcard SSL Certificate prices			
No. Licences	1 year	2 years	3 years
2-50	577 Euro	866 Euro	1299 Euro
51-100	871 Euro	1306 Euro	1959 Euro
101+	1267 Euro	1900 Euro	2850 Euro

Appendix 5

Information Required for a Shibboleth IdP Install

1. Address of an NTP server used to synchronize times on your servers, if available.
2. Fully-qualified DNS domain name you would like the server to use (e.g. shib-origin.wlv.ac.uk).
3. IP address and netmask for the server (where a private address is used, both a private and a public address is needed).
4. IP address of the default gateway for the server.
5. IP addresses of one or more DNS servers it can use.
6. Type of authentication used on your network (Microsoft Active Directory, NT4, Novell).
7. If it is active directory:
 - i. are the domain controllers Windows 2000 or Windows 2003?
 - ii. what is the Windows domain DNS name (e.g. "unv.wlv.ac.uk")
 - iii. if the DCs are 2003, your server will need its own username and password in order to use active directory for authentication. Please create such an account and supply the username and password. The account needs no privileges, nor does it need "log on locally" rights on any of your servers.

We also need your LDAP IP address as well as search and bind DNS. As our attempts to bind anonymously with Windows 2003 do not appear to work, we need a bind and test account.

Appendix 6

Multiple Organisational Unit (OUs) Lookups from Active Directory Root

Taken From: <https://mail.internet2.edu/wws/arc/Shibboleth-users/2005-12/msg00032.html>

ebeddows@kidderminster.ac.uk wrote:

Thanks for the replies, it was a DNS issue in the end, as the server is querying against our external DNS server there are some dns entries missing for the referral part of the search (other partitions in AD), to find these out I did an ldap search, the output of which displays the search referral dns names being used. In our case:

```
# search reference
```

```
ref: ldap://ForestDnsZones.kiddercoll.local/DC=ForestDnsZones,DC=kiddercoll,DC=local
```

```
# search reference
```

```
ref: ldap://DomainDnsZones.kiddercoll.local/DC=DomainDnsZones,DC=kiddercoll,DC=local
```

```
# search reference
```

```
ref: ldap://kiddercoll.local/CN=Configuration,DC=kiddercoll,DC=local
```

To fix the issue I simply put kiddercoll.local, DomainDnsZones.kiddercoll.local and ForestDnsZones.kiddercoll.local in the servers hosts file. So even if you are querying your DC using an IP, the referrals in the background will use names.

Thanks again for the info.Ed