

# JISC DEVELOPMENT PROGRAMMES

## Project Document Cover Sheet

### FINAL REPORT

#### Project

<b>Project Acronym</b>	EMSS	<b>Project ID</b>	
<b>Project Title</b>	East Midlands Shibboleth Service		
<b>Start Date</b>	January 2005	<b>End Date</b>	30 April 2006
<b>Lead Institution</b>	Nottingham Trent University		
<b>Project Director</b>	Ian Griffiths		
<b>Project Manager &amp; contact details</b>	Francis Lowry Data Warehouse Manager Barnes Wallis Building Burton Street		
<b>Partner Institutions</b>	None but see acknowledgements		
<b>Project Web URL</b>			
<b>Programme Name (and number)</b>	<i>Core Middleware : Early Adopters (11/04)</i>		
<b>Programme Manager</b>			

#### Document

<b>Document Title</b>	<i>Final Report – Draft</i>		
<b>Author(s) &amp; project role</b>	Francis Lowry – Project Manager Matthew Holmes – Lead Developer		
<b>Date</b>		<b>Filename</b>	
<b>URL</b>	<i>if document is posted on project web site</i>		
<b>Access</b>	<input type="checkbox"/> Project and JISC internal	<input type="checkbox"/> General dissemination	

#### Document History

Version	Date	Comments



## **JISC Final Report Template**

### **East Midlands Shibboleth Service (EMSS)**

Francis Lowry  
April 2006



## Table of Contents

<b>JISC DEVELOPMENT PROGRAMMES.....</b>	<b>1</b>
<b>PROJECT DOCUMENT COVER SHEET .....</b>	<b>1</b>
<b>FINAL REPORT– DRAFT .....</b>	<b>1</b>
TABLE OF CONTENTS .....	4
ACKNOWLEDGEMENTS.....	5
EXECUTIVE SUMMARY .....	6
<i>Installation and configuration of Shibboleth idP and SP using Windows technologies.....</i>	<i>6</i>
<i>Account Integration using MS IIFP.....</i>	<i>6</i>
<i>Proposed EMSS Model.....</i>	<i>7</i>
BACKGROUND .....	8
AIMS AND OBJECTIVES.....	9
<i>Aims.....</i>	<i>9</i>
<i>Objectives and how they changed during the course of the project. ....</i>	<i>9</i>
METHODOLOGY .....	10
<i>Approach .....</i>	<i>10</i>
IMPLEMENTATION .....	11
<i>IdP against AD.....</i>	<i>11</i>
<i>Active Directory Account Population.....</i>	<i>13</i>
<i>Service Provider Installation and Setup.....</i>	<i>14</i>
<i>EMSS – Multiple SP’s on a single server.....</i>	<i>15</i>
<i>RIPPLL – PDP using Shibboleth.....</i>	<i>15</i>
OUTPUTS AND RESULTS .....	16
<i>Technical Work.....</i>	<i>16</i>
<i>Problems and potential solutions .....</i>	<i>16</i>
<i>Additional areas for exploration .....</i>	<i>17</i>
<i>Dissemination.....</i>	<i>18</i>
OUTCOMES.....	19
<i>Project achievements against the aims and objectives set.....</i>	<i>19</i>
CONCLUSIONS .....	20
IMPLICATIONS .....	20
RECOMMENDATIONS (OPTIONAL).....	21
APPENDICES .....	21
<i>Glossary of acronyms.....</i>	<i>21</i>

## **Acknowledgements**

This project was conducted under the JISC Circular (11/04): Core Middleware: Early Adopters.

Technical work was led by Francis Lowry at Nottingham Trent University with Matthew Holmes leading the Shibboleth work and Craig Gibson leading the Active Directory work. We would also like to thank Liz Butterworth and the technical team at West Notts College, and Carl Ebrey and his colleagues at Nottingham University for their co-operation and advice. The MATU Support Service for their assistance and guidance, and more importantly sanity checks, and James Higham from the RSC at Loughborough for his invaluable input into how Shibboleth can best support FE. A final thank you to all the contributors on the shibboleth mailing lists at Internet2, whose efforts have helped us considerably with this project.

## Executive Summary

### Installation and configuration of Shibboleth IdP and SP using Windows technologies

In order to provide a solution which 'best fits' the majority of FE Colleges in the East Midlands region, the project attempted to utilise existing Microsoft technologies as far as possible in this investigation. This led to one of the core tensions with the project; Shibboleth has been designed from an open-source perspective using Linux and Tomcat, all the documentation available assumes quite a high technical knowledge of these technologies. In addition, the terminology and configuration changes from version to version, led to quite a steep learning curve. We are fully of the opinion that the choice of MS as the technology platform where possible has contributed to many of the problems experienced with the project. However, it can also be viewed that use of Microsoft technologies is pervasive throughout the education sector, particularly FE, and work in this area is vital for the future.

The Shibboleth IdP has been successfully installed and configured on Windows server 2003 using Active Directory as the identity store with CAS providing the single-sign-on framework. The Shibboleth SP has been successfully installed and configured on Windows server 2003. This configuration was successfully used to model the Shibboleth protected PDP data exchanges for the Nottingham University RIPPL project ([www.nottingham.ac.uk/rippl](http://www.nottingham.ac.uk/rippl)).

Comprehensive installation and configuration documentation for both the IdP and the SP has been created and will be published as part of this project.

### Account Integration using MS IIFP

One of the key components in setting up the central repository was the maintenance of the user accounts from the prospective member colleges. Using the IIFP enables account provisioning from remote Active Directories as long as the appropriate permissions are configured. Unfortunately, this provisioning only functions where an account already exists in the destination repository, it does not create new accounts by default. An extension had to be written to create any accounts which did not exist. As the free toolkit only allows AD to AD provisioning, to cater for any potential non-MS directories, a manual mechanism to create accounts based on CSV files was developed.

One major drawback with this approach is that duplicate accounts from different institutions **cannot** be created; one of the institutions will need to change the login. In some cases, this change of account name may have considerable impact on the source institutions, and cannot rely on a seamless integration of this Shibboleth service to local systems. To a degree this goes against one of the principles of Shibboleth in that the local authentication system can be used to authorise the user.

A second major drawback with using IIFP is that the password synchronisation is triggered only on a change of the password in the originating Active Directory. So unless each institution is willing (and able) to force a password change for all their accounts when registering with the EMSS, not all accounts will be able to log in.

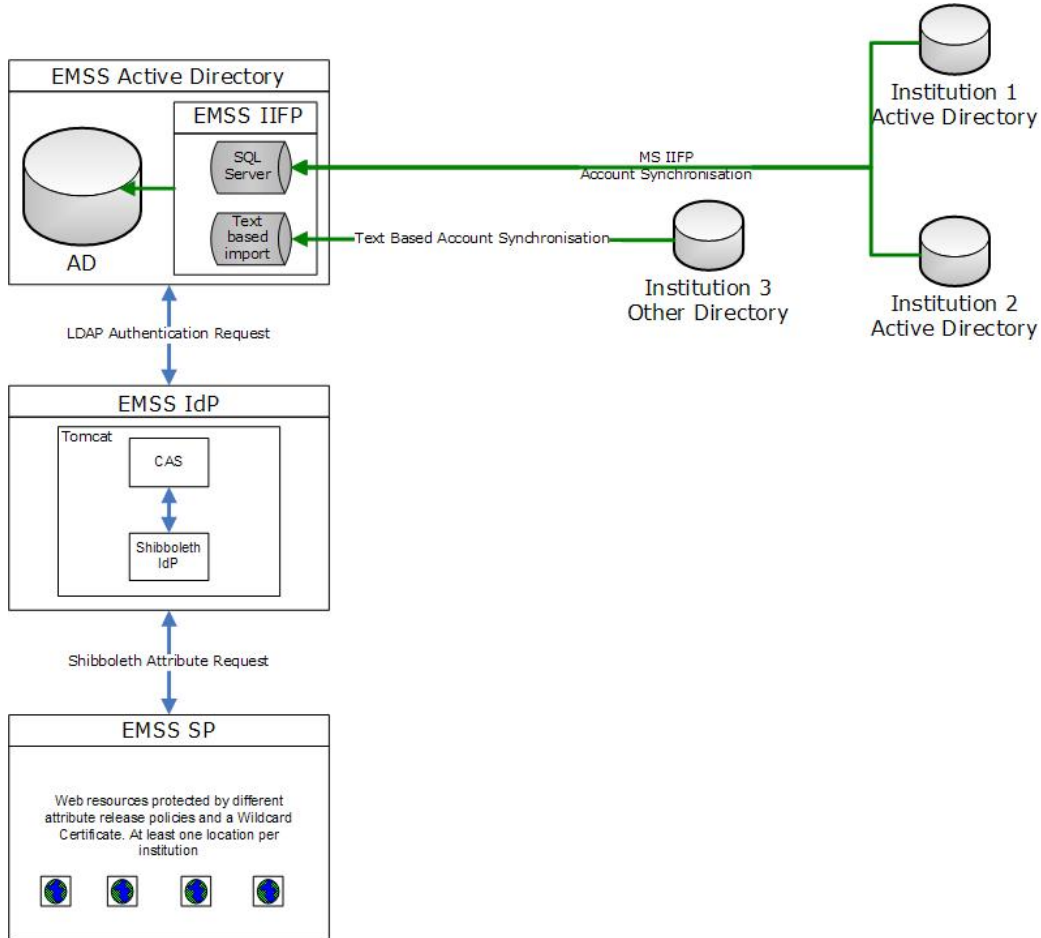
Given these issues with IIFP, the consensus is that a hosted Shibboleth service is not functionally viable given we were attempting to have a cost-effective service with minimal impact on the FE colleges.

Future work in this area should concentrate on providing support for institutions to do their own installations and applications of Shibboleth within their own environment.

**Proposed EMSS Model**

In order to achieve the proposed economies of scale and to maintain architectural simplicity, a three component model was proposed:

- Active Directory (with IIFP and text-based mechanism to maintain accounts)
- Shibboleth IdP
- Shibboleth SP



Each institution would be created as a separate branch off the Users tree in AD, with the Shibboleth IdP starting its account search at the top of the Users node. A wildcard certificate would be installed in IIS to create an SSL-enabled Service Provider for each of the constituent institutions.

Unfortunately, there is no guarantee an account such as 'S000010' would not exist independently at multiple institutions, and result in the creation of duplicate accounts when updates are pushed to the EMSS Active Directory by IIFP.

To address this issue, separate AD servers could be hosted centrally for each institution, however, this would impose an additional level of complexity upon the SSO and IdP components, which in turn would need to determine which AD holds the identity attributes for a user. Although a solution may be to host an IdP for each institution and have a single WAYF for the EMSS, this would not be an efficient set up, and in some ways attempts to mirror the decentralised model of Shibboleth within a less practical centralised environment.

Our emphasis is now on providing detailed documentation to assist institutions to perform their own Shibboleth installation, and exploring the integration of appropriate applications which are applicable to the FE community.

## Background

This project was designed to run in parallel to the development work on PDP lead by Nottingham University (RIPPLL) by using Shibboleth as a framework to allow for the identification of a learner and then dynamically access the learner's PDP related data from other sources. The primary aim of this project was to investigate, develop, deliver, support and maintain a hosted Shibboleth capability for use by any East Midlands FE / HE Institution.

It was recognised that FE institutions had a varying degree of technical skills and the migration to Shibboleth on their own could be problematic. In order to facilitate the rollout of Shibboleth to these institutions an additional aim of the project was to produce comprehensive documentation on the installation and configuration of Shibboleth. As far as possible our aim was to utilise Microsoft technologies in the infrastructure and supporting products. This was to ensure that the technology stack was as familiar to the potential users as possible. In addition to this, our own knowledge and experience of Shibboleth itself was limited and our existing background working with the existing MS technologies would place us in a similar technical position to the local FE colleges.

We acknowledged that MS Identity Information Feature Pack, one of the core technologies that we proposed to use, was not something that everyone would be familiar with and that one of the hurdles we would need to overcome was establishing an appropriate level of trust with users to allow NTU to have direct connections to their own Active Directories and pass the basic user details required, including the user passwords, to the EMSS Shibboleth Active Directory.

## Aims and Objectives

The original aims and objectives of the project were as follows:

### Aims

- To investigate, develop, deliver, support and maintain a hosted Shibboleth capability for use by any East Midlands FE / HE Institution.
- To work with the RSC and FE Colleges to ensure that the service would meet local needs.
- To increase the knowledge and understanding of Shibboleth in the East Midlands area.

### Objectives and how they changed during the course of the project.

1. To create the East Midlands Shibboleth Service to allow any FE / HE institution in the East Midlands using Microsoft Active Directory to access Shibboleth based resources.

#### Changes:

The original Project Manager took early retirement and the project was handed over to Francis Lowry in June 2005. We are slightly behind with the testing of the Active Directory account creation; however the feedback from working with both the RSC and local FE Colleges is that if supplied with appropriate installation and configuration documentation which is pitched at the correct level, then FE Colleges would probably want to manage their own Shibboleth infrastructure. This view was reinforced due to the nature of how the IIFP works when integrating remote directories i.e. it is not possible to have multiple login names down different branches of the Active Directory tree. Although it is possible to develop a mechanism to create a unique login name if one already existed by creating an extension for IIFP, creating a new ID would not fit with the user institutions account creation policy.

The result of this was to continue with the overall research and development around creating the EMSS, retaining the emphasis on MS technologies where possible, however we focussed more strongly on the creation of the installation mechanism and documentation for the installations of both the SP and IdP at a level which was comfortable for both the FE colleges and the RSC.

2. To implement both the IdP, as far as possible, using Windows Technologies. As the majority of FE institutions would be using Windows Servers and Active Directory as a core part of their IT solution, we wanted to ensure that any work we did would be transferable to the FE sector.

#### Changes:

We extended the project to include hosting the SP as well as the IdP. Also, based on the work done at K.U.Leuven (<http://shib.kuleuven.be>), we also included CAS between the IdP and Active Directory to manage the single sign-on aspects required by Shibboleth. Although an additional technology to implement, this was a simpler solution than having to develop a simple single sign-on framework.

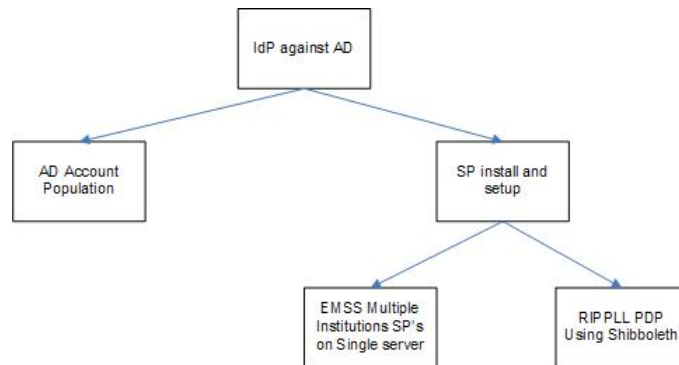
3. To document all development work and source code. Including:
  - Shibboleth IdP installation instructions on Windows - with all pre-requisites documented.
  - Shibboleth IdP installation batch file – based on the one provided by K.U.Leuven.
  - Shibboleth SP installation instructions on Windows - with all pre-requisites documented.
  - MS Active Directory configuration (Including eduPerson schema additions)
  - MS IIFP configuration instructions and source code for extensions.

## Methodology

### Approach

The first phase of the project was purely research through trial and error. With no previous experience of Shibboleth, we found the available documentation to be very sporadic in terms of content and certainly confusing when the terminology changed from one version of Shibboleth to another. The main problem however, was the implied assumptions that the people who would be using the available documentation were knowledgeable in the open source technologies referenced and could plug the numerous gaps themselves. One of our key aims was to install and configure both the IdP and the SP on Windows, however a large part of our time was spent in translating the existing Linux based documentation to apply to a Windows environment and filling in the gaps.

We took a modular approach to the overall research and development with the two key components IdP and SP being the main linchpin activities. Once the IdP was working on the Windows server and authenticating to our AD, we were able to parallelise activity with the AD account population and the SP install. Similarly, once a basic SP was in place utilising the IdP we started on both the Shibboleth work for Nottingham University's RIPPLL project, and explored setting up the multiple institutions SP's on a single server.



The overarching theme with the project was to come up with a cost-efficient model which would allow FE colleges etc in the East Midlands area to gain access to a hosted Shibboleth service. We did not want to get to the position of having to host individual servers etc for each institution. We wanted to see

1. Could we consolidate the account details from multiple AD's to a single AD hosted at NTU?
2. Could we provide a basic Shibboleth Service Provider for each institution using wildcard certificates?

## Implementation

### IdP against AD

Our starting position was to get a working version of the Shibboleth IdP functional under Windows. This was the most complex part of the project, mainly because we had little pre-knowledge of Shibboleth and the technologies used to develop it, and we wanted to get it working on Windows. Getting an answer to the question 'Where do we start?' caused enough confusion on its own, as several responses pointed to configuring the Service Provider first as it was the simplest to set up, however, although this is technically possible, it was not possible to test it without the Identity Provider in place to provide the login. An 'Example State University' IdP has since been made available by OSU in the InQueue test federation for use with SPs.

We opted for the following approach:

1. Get a working test Active Directory with appropriate test login accounts.
2. Install the IdP on a Windows 2003 server
3. Test the IdP.

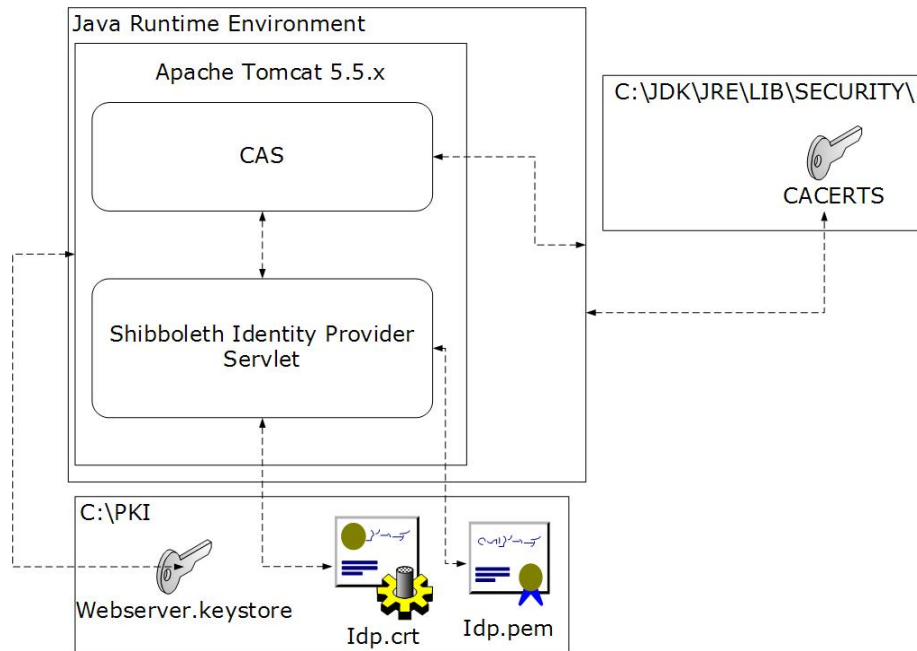
This approach allowed us to get a functioning IdP authenticating to Active Directory and to start to unpick some of the more detailed issues with Shibboleth.

Shibboleth is described on the internet2 web site as '*providing Web Single Sign-on (SSO) across or within organizational boundaries*', however, in order for Shibboleth to work, it requires an existing local SSO framework to broker the authentication request and manage the session cookies set by the IdP. At NTU we do not have a single sign-on framework in place; the closest we have is to get an application to authenticate directly to Active Directory. As we started to unpick this area in November 2005 we came across the documentation on CAS and Windows by K.U.Leuven (<http://shib.kuleuven.be>). Putting CAS between the IdP and Active directory allowed us to very quickly implement a suitable single sign-on framework which would allow Shibboleth to work. The only minor drawback with this approach was the additional complexity of the additional location for the SSL certificates required for the IdP to function.

With CAS now in the equation, we have ended up with 3 separate elements to store SSL information for the IDP, 4 if you need to update the cacerts file for non-commercial certificates:

<b>File</b>	<b>Location</b>	<b>Description</b>
idp.crt	C:\PKI	Public certificate for the Shibboleth IdP installation.
idp.pem	C:\PKI	Private key for the Shibboleth IdP installation.
webserver.keystore	C:\PKI	'webserver' keystore used by Tomcat. This keystore is required to enable an SSL port on Apache Tomcat 5.5.x. An Apache webserver would also require a keystore if used in the place of Tomcat. If mod_jk is installed to broker requests for IIS with Tomcat then IIS will also require its own keystore, in addition to Tomcat's, to run on an SSL port.
cacerts	C:\jdk\jre\lib\security	Trusted certificate authority store used by CAS and held within the JDK. (only edited when using a non-commercial certificate i.e. BOSSIE)

SSL File locations and their relationships to the different components:



The main difficulty with the IdP install was the sheer amount of individual components that needed to be in place and configured while filling in the gaps in the documentation and converting them to a Windows environment.

- Supporting Tools
  - Ant
  - JDK
  - OpenSSL
- Main products
  - Tomcat
  - CAS
  - Shibboleth IdP

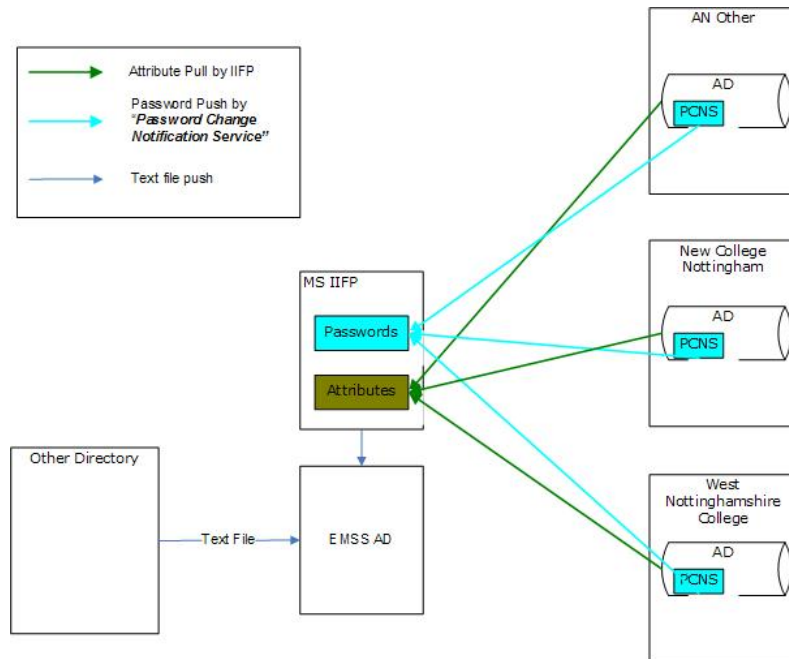
Although for anyone working with Open Source projects on Apache, Tomcat or Linux would be familiar with this setup, FE colleges are not. For us to ensure that we could pass on reasonable documentation, a good amount of our time was spent working through the configuration and set up for all the required components. Although there are two options for the install of the IdP i.e Tomcat standalone, or Tomcat brokered with another webserver (such as Apache or IIS), we concentrated on the Tomcat standalone option, in order to minimise the amount of new toolsets.

To simplify the management of these products, in the main, we did not do a default installation but forced the install homes to be just off the root of C: similar to the K.U.Leuven installs.

- C:\ant\
- C:\pki\
- C:\jdk\
- C:\tomcat\
- C:\shib-idp\
- C:\tmp\ - installation folder, deleted after configuration was completed

## Active Directory Account Population.

The initial proposal was to provide a centrally managed AD using Microsoft's IIFP to allow the synchronisation of account details from remote ADs. In this way, FE colleges would not have to fund and support their own IdP.



The idea behind this model was that the remote Active Directories only needed to create a local account for the central EMSS IIFP to access their data and provide the account synchronisation. However, in order for the password synchronisation to function, the Password Change Notification Service (PCNS) needs to be installed and running on each of the Active Directories in the Forest of each of the source Directories.

The Active Directory was prepared with the EduPerson schema which we used to store some of the common Shibboleth Attributes, however to allow us to differentiate the source of the account details we created an additional attribute `emssOrgDomain`. Here we stored 'westnotts.ac.uk', or 'ncn.ac.uk', using the domains owned by FE colleges as unique identifiers signifying a user's membership to a group.

For the initial testing purposes, we left the accounts at the Users Level and used the `EduPerson OrgUnitDomain` as the attribute describing the remote directory the user account came from.

e.g.

```
ou=users,cn=emss,dc=ntu,dc=ac,dc=uk
dn: cn=USER1,ou=users,dc=emss,dc=ntu,sc=ac,dc=uk
dn: cn=USER2,ou=users,dc=emss,dc=ntu,sc=ac,dc=uk
dn: cn=USER3,ou=users,dc=emss,dc=ntu,sc=ac,dc=uk
dn: cn=USER4,ou=users,dc=emss,dc=ntu,sc=ac,dc=uk
```

However, as we progressed with this route we identified several limitations which made this approach considerably less attractive and practical.

1. Duplicate `SAMAccountNames` in separate remote domains. As this is supposed to be unique for the Active Directory, unless we modified the `SAMAccountName` to make it unique, as more remote domains were included the chance of getting duplicate records increased. However, if the login was modified to be different from that used locally at the remote institution we would be defeating one of the principal purposes of Shibboleth.

2. IIFP will not by default create a new account in the EMSS AD from the remote AD. We had to write an extension to the product to allow for this.
3. IIFP will only pass on password changes, i.e. it will not transfer passwords on the initial account creation, or initial synchronisation and in order for this to work the PCNS needs to be installed and this requires some changes to the AD Schema.
4. For this model to work, each AD in each of the source forests need to be running in 2003 server mode. If one of the AD servers is Windows 2000, then the password provisioning will not work.

An alternative approach to counter problem 4, is to get each partner institution to install and configure IIFP locally, and push all the changes, both attributes and passwords to the central EMSS AD. However, although this does allow more local management of the accounts, perhaps reducing the occurrence of duplicate accounts, it still does not work around the issue of only changed passwords being transferred, and furthermore requires the partner institution to set up a 2003 server with SQL Server and IIFP along with the PCNS.

In addition to using IIFP, we developed a very basic text file transfer to allow us to create and maintain accounts in the Active Directory.

### **Service Provider Installation and Setup**

In comparison to the research and installation for the IdP, the SP was considerably less complex to install, as the C++ release is provided as a Windows Installer package and is managed as a normal Windows Service.

The installation consists of:

- Setting up the Windows server
- Installing IIS
- Obtaining an SSL certificate
- Install the SSL certificate to IIS
- Installing SP
- Configure IIS with the ISAPI filter
- Configuring the SP

Once the SSL certificate is configured within the SP and IIS, a basic Shibboleth protected resource location can be created. There were quite a lot of problems going past this point.

Although there are more components with the IdP compared to the SP, one of the benefits of this is that there are multiple points which can be configured to log errors. With the SP however, once you get past the basic configuration, when trying to set up multiple applications or websites, any mis-configuration will prevent the SP service from starting, and subsequently will fail to log any errors with the configuration. This has left the debugging of configuration problems with the SP to be a very complex and pedantic job. At times we frequently had to stop and start the service following minor edits, to ensure the Shibboleth configuration files contained well-formed XML and legitimate values.

For FE colleges, having specific applications of Shibboleth are more important than the hosting of the service. Based on feedback from the RSC and other FE Colleges we have identified Moodle as one of the key applications which would demonstrate the functionality of Shibboleth. Since Moodle is one of the applications which already support Shibboleth, we will be looking to set up a practical demonstration of Shibboleth working with Moodle, as part of a future workshop for FE colleges

### **EMSS – Multiple SPs on a single server**

In order to minimise costs, our idea was to configure a single web server with a wildcard certificate hosting multiple websites e.g.

ntu.emss.ac.uk  
westnotts.emss.ac.uk  
ncn.emss.ac.uk

The reason for this was to give each of the client institutions using the service a URL which most closely matched their internal web site and to have appropriate re-directs on logon. We were able to model this scenario with two physical servers running the SP, however what we wanted to do ideally, was to set up a single IIS6 server with multiple websites.

Due to IIS6 marginally supporting multiple SSL sites on the same server, albeit through manually editing site headers and IIS metadata, we have not yet been able to configure a wildcard SP. Coupled with the current view that the EMSS is not technically viable from the integration of the Active Directories, we have focused our attention on protecting multiple virtual directories within a single website.

Our view, from the majority of the responses on the mailing list, is that Apache is a more flexible web server than IIS6 for Shibboleth SPs where fine-grained access control needs to be applied at a resource. One of the things we will be looking at further is a comparison with the configuration and setup of the SP utilising ACLs on Apache compared to IIS.

### **RIPPLL – PDP using Shibboleth**

Once Shibboleth (both the SP and IdP) were functional, work began on a parallel project to use Shibboleth to protect a web service which provided PDP data collated from remote web services and displayed a combined presentational layer.

This work is documented at the Nottingham University RIPPLL website ([www.nottingham.ac.uk/rippll](http://www.nottingham.ac.uk/rippll)). Technical documentation and source code of the web services we developed (nicknamed 'SquirrelWS') will be available from <http://www.ntu.ac.uk/jisc>

## Outputs and Results

### Technical Work

Most of the technical work involved the installation, configuration and setup of Shibboleth IdP and SP on Windows 2003 servers. There was some additional work around developing an extension for MS IIFP to allow it to create accounts which did not exist at the destination AD.

The detailed technical documentation on the installation and configuration of all components in the project will be made available soon on the project website.

In addition to this we will continue to work closely with the RSC at Loughborough on implementations of Shibboleth at FE colleges and we hope to be able to work directly with both New College Nottingham and West Nottinghamshire College in getting a Shibboleth installation completed at their sites.

### Problems and potential solutions

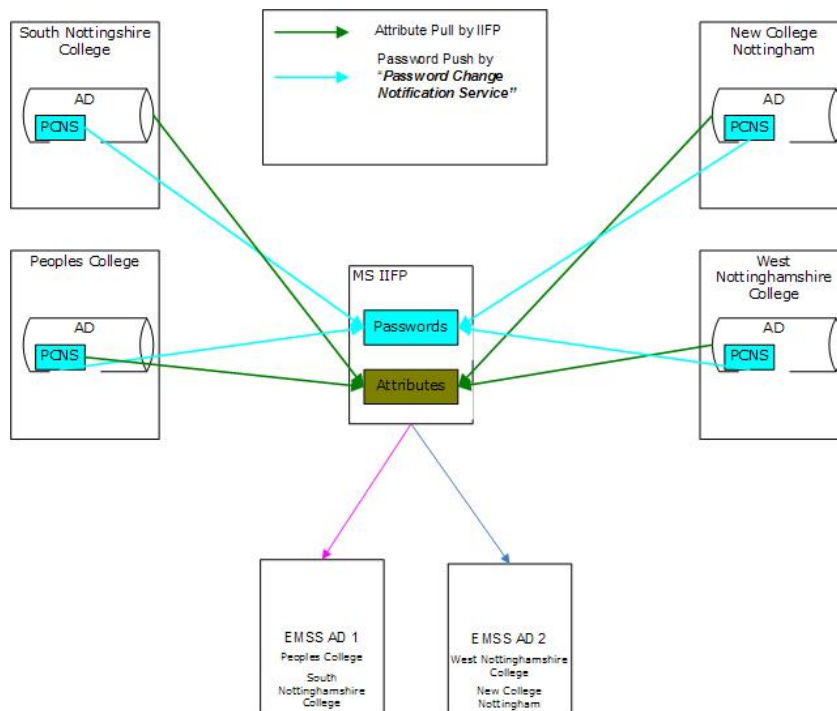
The two core problems with the proposed service are summarised as follows:

1. Login id conflict - Potential for different institutions to have the same login id's.
2. Password provisioning - IIFP will only provision password changes.

There are several options for reducing or resolving these.

#### Login id conflict

A minor change to the proposed model is to add more EMSS Active Directories and analyse the login id format before assigning specific institutions to EMSS Active Directories.



For example if, after analysis we find that:

- South Nottinghamshire College have the same Login ID format as New College.
- Peoples College have the same login id format as West Nottinghamshire College.

We can set MS IIFP to transfer passwords and attributes to two different destination Active Directories and get Shibboleth IdP to look in the two ADs.

The main drawback with this approach is that even using an option such as 'FailOverDependency' within the IdP, we would only be able to have a maximum of two ADs. The Fail-Over option is also only useful when an account can't be located in the first AD. If there is a duplicate account in both ADs there is no way to determine which account should be authenticated. To avoid this problem we would need to start adding additional IdPs to the system for each institution and AD.

Without including any resiliency options we are starting to increase the number of servers required and the complexity and maintenance of the system.

### **Password Provisioning.**

The simplest solution to this is to get each institution to agree when they apply to the service that an essential part of the implementation is for them to reset all user passwords once the EMSS service is in place.

Based on some informal feedback, this approach would not really be palatable to a lot of FE Colleges and would prohibit them from taking up the service.

### **Additional areas for exploration**

#### **Exemplar FE Services using Shibboleth**

One of the key questions that kept coming back from conversations with FE Colleges and initially the RSC was 'What is Shibboleth, and what can we do with it?' James Higham at the RSC summed it up nicely by highlighting that Shibboleth on its own will not sell itself, it needs to be partnered with one or more FE specific examples. Moodle was suggested as a good practical example. As the integration work has already been done, we are going to attempt to demonstrate this to the RSC and some local FE Colleges.

The main point here is that the application of Shibboleth for FE colleges is a more constructive method to encouraging uptake. Perhaps an additional small project to analyse potential applications in the FE and other non-HE sectors would be of benefit to the whole community.

#### **East Midlands Shibboleth Federation**

The initial proposal of a centrally hosted service has been found to be impractical. Rather than host IdPs and SPs for other institutions, we believe a better approach to encourage adoption of Shibboleth is to provide FE colleges with detailed documentation so they are able to perform their own installations of Shibboleth, and subsequently increase their understanding of both the technology and a decentralised access model.

From discussions with the RSC, we believe demonstrations of secure access to shared resources and deployments of Shibboleth-enabled FE applications would present a strong selling point to the FE community, and increase adoption of Shibboleth within the region.

We propose the formation of an East Midlands Federation to provide support and a common operational framework for FE colleges who are looking to install and operate their own Identity or Service Providers. A central EMSF website would function as a central repository for federation metadata and provide a service catalogue of inter-institutional resources and collaborative works for colleges installing Shibboleth.

Without a coordinated push, we believe the potential of a decentralised access model will not be realised by the FE community, leaving locally installed Shibboleth implementations to be abandoned as rudimentary SSO systems. Our approach therefore would be to take a step back from the technology and work with pilot FE colleges to determine the level of collaboration, and type of resources, they desire, where possible. This feedback will then allow investigation of how Shibboleth may be fit for the purpose, and in doing so will sell its own benefits to the FE community. This approach will be more receptive than trying to push a technology to a college without providing a context or reason for them to change.

Furthermore, a regional federation could also serve as a gradual transition to a national Shibboleth federation for FE institutions.

### **Dissemination**

We will be planning a workshop with the RSC for FE Colleges in the East Midlands to discuss the work done through this project and to help identify uses of Shibboleth which are of specific use to the FE sector.

## Outcomes

### Project achievements against the aims and objectives set

Aim	Evaluation
To investigate, develop, deliver, support and maintain a hosted Shibboleth capability for use by any East Midlands FE / HE Institution	After this investigation, we are unable to recommend the implementation of a hosted service for the following reason. <ul style="list-style-type: none"> <li>• Implementing work-arounds for the technical limitations of the MS IIFP is unworkable.</li> <li>• The changes required to the business processes of FE colleges to reset all passwords and to manually maintain account names for Shibboleth is prohibitive.</li> </ul>
To work with the RSC and FE Colleges to ensure that the service would meet local needs.	Direct feedback from both the RSC and local colleges have indicated that although the installation is complex, having the installation locally with good detailed documentation and contacts with colleagues who have implemented Shibboleth on the Windows framework is more valuable than the potentially hosted service.
To increase the knowledge and understanding of Shibboleth in the East Midlands area.	There is more work to do here, hopefully by demonstrating the uses of Shibboleth, perhaps by using Moodle we hope to encourage some more FE Colleges to work with us and the RSC on Shibboleth implementations.

### Satisfaction of objectives

To create the East Midlands Shibboleth Service to allow any FE / HE institution in the East Midlands using Microsoft Active Directory to access Shibboleth based resources.	As we ran into the technical limitations of IIFP this objective changed to providing detailed installation and configuration instructions for the Shibboleth IdP and SP. We are pulling this documentation together now for publication on our website XXXX. Although we have not satisfied the original objective, we believe we will satisfy the overall one of encouraging the uptake of Shibboleth in the FE sector here in the East Midlands.
To implement both the IdP and the SP, as far as possible, using Windows Technologies	Although we are now of the opinion that Apache may be a better suited Web Server for the Service provider than IIS. It is possible to set up a fully functional SP using IIS, we only hit the limitations as we attempted to host multiple web domains on the same server using a wildcard certificate. Open source Technologies are required, but the complexity of these can be contained by comprehensive installation and configuration documentation and examples.
To document all development work and source code	This is in progress and the bulk of the documentation Should be on the web site by the end of May. This will be enhanced with working examples from future partner colleges as they come on board.

Who will benefit from the work, how, and why

NTU, the RSC at Loughborough and the other RSCs, East Midlands FE Colleges and the Shibboleth community will benefit from this work. As we get more practical examples of how Shibboleth can benefit the FE community, these benefits can be passed onto others.

Lessons learned

One of the main lessons is not to rely wholly on provider's documentation either from Software Suppliers (Microsoft) or Open Source. With IIFP all the documentation implied that it would run out of the box with AD, that password synchronisation would work. With the Shibboleth documentation, we had many headaches trying to find a definitive set of documentation which was applicable to our environment. We were ambitious to offer up the hosted service without having a deeper practical knowledge of both Shibboleth and IIFP, it is easy to say with hindsight we would have proposed a different model if we had this deeper knowledge. At least some areas of IIFP are now uncovered, and we have a better understanding of how Shibboleth can benefit us.

**Conclusions**

The core part of this project was to research and implement a cost effective centrally hosted Shibboleth Service for the East Midlands area. The initial project was based on supporting a single Active Directory using IIFP to provision the accounts. We demonstrated that this was possible, however the problems of multiple logon ID's and IIFP only provisioning password changes makes this solution impractical to implement as the impact on the source colleges' internal business processes is too great.

The process of physically attempting this setup has increased our own knowledge of Shibboleth, and has allowed us to share with some local colleges and the RSC what Shibboleth is. With the additional work done with the RIPPL project at Nottingham, referencing PDP data using shibboleth protected web services, we have raised the profile of Shibboleth more by providing an example of how Shibboleth can work.

We realised by December 2005 that the IIFP limitations would make the offering of a hosted service impractical, however, by using Windows as the base technology and going through the complete configuration of Shibboleth, both IdP and SP, we will be able to return back to the community some more detailed information of how to install and configure Shibboleth assuming no prior knowledge.

As mentioned in several occasions within this document, the main effort we had was in filling in the gaps and converting the existing Shibboleth documentation to apply to a Windows environment. All the current document appears to assume a good prior knowledge of the underlying technologies below Shibboleth. FE Colleges in the main will not have this deeper technical knowledge. We have realised this and will be gearing all our documentation to assume no prior knowledge except that of administration level over the local authentication mechanism primarily Active Directory, and Windows server administration.

**Implications**

The main implication of this work is that we will be unable to provide a hosted Shibboleth service. However, by providing good clear installation and configuration instructions, along with some demonstration uses of Shibboleth (Moodle) we hope to give the local FE community sufficient technical resource and support for them to set up for themselves.

## Recommendations (optional)

- Funded investigation into appropriate support mechanisms specifically aimed at helping FE colleges and Schools adopt Shibboleth.
- Funded investigation into example applications of Shibboleth, in particular focusing on sector specific examples of peer to peer resource sharing.
- Funded exploration of the possibility of creating an East Midlands FE Shibboleth Federation with the emphasis on getting the basic shibboleth IdP installed and access to some basic shared resources, similar to the [KC Rollo](#) Shibboleth work.

## Appendices

### Glossary of acronyms

ACL	Access Control List – definable set of user access rules applied to a resource
AD	Active Directory
CAS	Open Source Single sign-on from Yale University
CSV	Comma-separated values
EMSF	East Midlands Shibboleth Federation
EMSS	East Midlands Shibboleth Service
FE	Further Education
HE	Higher Education
IdP	Shibboleth Identity Provider
IIFP	Identity Integration feature pack
IIS	Internet Information Server (Microsoft)
MATU	Middleware Assisted Take-Up service
MSAD	Microsoft Active Directory
NCN	New College Nottingham
NTU	Nottingham Trent University
OSU	Ohio State University
PCNS	MS IIFP Password Change Notification Service
PDP	Personal Development Planning
PKI	Public Key Infrastructure
RIPPLL	Regional Interoperability Project on Progression for Lifelong Learning
RSC	Regional Support Centre (JISC)
SP	Shibboleth Service Provider
SSL	Secure Socket Layers – an encryption protocol for data sent by a browser
SSO	Single Sign-On
WAYF	Where Are You From – allows users to identify their institution from a list