

Joining the UK Access Management Federation

Technical Support Pre-requisite Guide

V 0.9

Contents

| | | |
|-------|--|----|
| 1 | Introduction..... | 4 |
| 2 | Server..... | 5 |
| 3 | Directory Development | 6 |
| 3.1 | Why attributes are needed | 6 |
| 3.2 | What attributes do I need? | 6 |
| 3.2.1 | eduPersonScopedAffiliation | 7 |
| 3.2.2 | eduPersonEntitlement..... | 7 |
| 3.2.3 | eduPersonPrincipalName | 7 |
| 3.2.4 | eduPersonTargetedID..... | 8 |
| 3.2.5 | Additional Attributes | 8 |
| 3.3 | Where do I set these values? | 8 |
| 3.4 | How do I set these attributes? | 10 |
| 4 | Authentication Development..... | 11 |
| 5 | Firewall Access..... | 12 |
| 6 | Acquiring a Certificate | 13 |
| 7 | Join UK Access Management Federation | 15 |
| 7.1 | Management Staff..... | 15 |
| 7.2 | Technical Staff | 15 |
| 8 | Updating Links | 16 |
| 9 | Appendix A..... | 18 |
| 10 | Appendix B..... | 21 |
| 11 | Appendix C..... | 22 |
| 12 | Appendix D | 23 |

1 Introduction

Before a Shibboleth Identity Provider (IdP) can be installed at your institution, you must have carried out the pre-requisites necessary for a successful implementation.

This document is designed to ensure that all the pre-requisites have been met. Whilst the sections in this document are sequential, they can be carried out in any order, for example, you do not need to have your attribute store provisioned before you join the UK Access Management Federation (UKAMF).

In order for our Technical Support Team to commence deployment, the following requirements must have been completed. Use the list below as a check sheet ✓ once each step has been met.

As this process also requires close liaison with your Library (LRC), IT and Senior Management teams, it is recommended the "Agenda" items in Appendix C are followed and agreed upon at an early stage.

| | Requirement | Section | Completed |
|---|--|------------|-----------|
| A | Permit technical support admin access to a Shibboleth server meeting the recommended specifications | Section 2 | |
| B | Permit technical support access to an attribute store meeting the specified requirement | Section 3 | |
| C | Permit technical support access to your chosen authentication system | Section 4 | |
| D | Completed Firewall configuration | Section 5 | |
| E | Acquired SSL certificate for Shibboleth IdP server | Section 6 | |
| F | Joined the UK Access Management Federation | Section 7 | |
| G | Returned server/authentication/attribute store details to: feiams@kidderminster.ac.uk | Appendix B | |

Technical Support

Support is available either via our dedicated **helpdesk** during week days between the hours of 9:00 to 17:00, or alternatively our **e-mail** address.

Helpdesk: 01562 512099

E-mail: feiams@kidderminster.ac.uk

Further Contact Information

General Enquiries: 01562 744348

Fax: 01562 512006

Main Switchboard: 01562 820811

2 Server

As a general rule of thumb, the Shibboleth server needs to have plenty of RAM, whilst the specification of the CPU and hard disk can be relatively moderate. Below are the recommended minimum systems requirements:

CPU: Low - Mid range Dual Core XEON

RAM: 2GB

Hard Disk: 2x73GB (15,000rpm if possible, Raid 1)

Note:

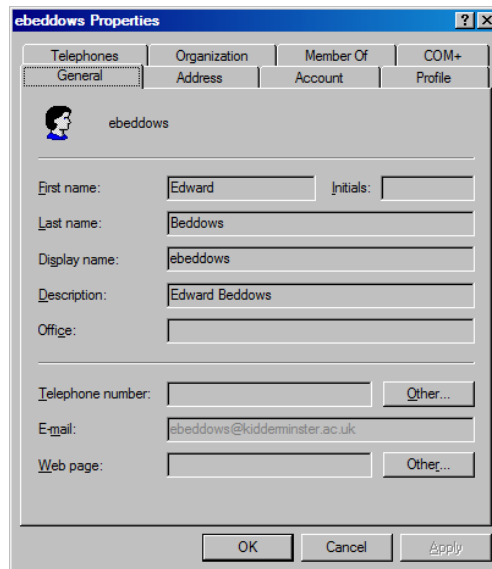
1. The clock speed is more important than the number of CPUs.
2. The operating system must have a valid license, where appropriate

3 Directory Development

3.1 Why attributes are needed

Web applications often require authorisation to allow a user to access their resources. This becomes essential when site subscriptions and individual user features are involved. It is for this reason that we need to pass relevant information to the resource about the user. The Shibboleth framework is based on keeping the user's anonymity where possible. Therefore, no web applications should see values about the user which are not necessary.

Every user in your user database has their own attributes. Examples of common attributes in an LDAP store (such as Active Directory or e-Directory) are *cn*, *givenName*, *sn*. You may be more familiar with seeing these attributes through a graphical front end, e.g., "User and Computers" in Active Directory.



In this example, the *cn* attribute has the value of "ebeddows", *givenName* is "Edward".

Different web applications will require different attributes to function, for example, a Virtual Learning Environment (VLE) may require a username, first name, surname and e-mail address to function correctly, whereas a research site may only need to know the institution the user is from to ensure they are part of an existing subscription.

3.2 What attributes do I need?

The UK Access Management Federation has defined the following core attributes which should be available for exposure to protected resources.

3.2.1 eduPersonScopedAffiliation

This attribute indicates the user's relationship (e.g., staff, student, etc.) with the organisation. For many applications, examination of this attribute is sufficient to determine whether the user has sufficient privileges to access the resource. This attribute is multi-valued, so a user can have "member" and "staff" values at the same time (the role may change depending on the resource). Several values of *eduPersonScopedAffiliation* are regarded as being "contained" within other values, for example, the student value is contained within member. All values are scoped within Shibboleth, which means "@security-domain" is appended to the value, e.g., member@mydomain.ac.uk (the value is stored without the scope).

Users typically have "member" set in addition to the "student" and "staff" values.

| Defined Value | Authorised User | Notes |
|---------------|-----------------|---|
| Student | yes | Undergraduate or postgraduate |
| Staff | yes | UK term for all staff |
| Faculty | yes | US term to distinguish teaching staff |
| Employee | yes | Other than staff/faculty (e.g., contractor) |
| Member | yes | Comprises all the categories named above |
| Affiliate | no | Relationship short of full member |
| Alum | no | Alumnus (graduate) |

3.2.2 eduPersonEntitlement

This attribute enables an organisation to assert that a user satisfies an additional set of specific conditions that apply for access to a particular resource. This attribute is multi-valued, as a user may possess different values of the *eduPersonEntitlement* attribute relevant to different resources.

Values of *eduPersonEntitlement* take the form of a URI, most frequently using the "http" or "urn" schemes. For example:

http://publisher.example.com/contract/GL123

urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted

http://ukfederation.org.uk/entitlements/example

The meaning of a given value of *eduPersonEntitlement* is normally defined by a service provider. In the case of a value using the "http" scheme, it is recommended that the value resolve to a document giving the definition of the value.

3.2.3 eduPersonPrincipalName

This attribute is used where a persistent user identifier consistent across different services is required. It often corresponds to the user's Single Sign-On (SSO) name, and may be useful for securing both internal institutional services and external services where access control lists are used.

The attribute is single-valued and structured as a scoped attribute, with the form `local-name@security-domain`, e.g., `ebeddows@kiddermminster.ac.uk` (stored without the scope in your directory).

3.2.4 `eduPersonTargetedID`

This attribute provides a persistent opaque user pseudonym, distinct for each service provider. This can be generated on the fly and is not necessary to store in your attribute store. However, it must at least be configured in Shibboleth to be generated dynamically.

The attribute enables an organisation to provide a persistent, opaque, user identifier to a service provider. For each user, the identity provider presents a different value of `eduPersonTargetedID` to each service provider to which the attribute is released. The attribute is defined as multi-valued (with one value for each service provider to which `eduPersonTargetedID` is released), though only a single value is ever released at a time. It is structured as a scoped attribute, with the form `pseudonym@security-domain`. The pseudonym is guaranteed to be unique within the context of the security domain. An example value of this attribute is: `s3VjcGuNrzKaeu69/QRfh73hNjU=@mydomian.ac.uk`

This attribute can often be used instead of `eduPersonPrincipalName` to maintain privacy whilst still providing the user with personalisation features.

3.2.5 Additional Attributes

Certain service providers may require more attributes, for example, a VLE may require a user's name and course enrolment data. If this is required, then this data must also be accessible in your attribute store.

Technical staff at your institution should read the technical recommendations document referred to in section 7.2, which provides more detailed information about attribute usage, including scoping and data privacy issues.

3.3 Where do I set these values?

You may be unfamiliar with the required core attribute names as they are not present in LDAP directories by default. In order for these attributes to be present, the `eduPerson` class must be added to your LDAP directory schema (<http://www.educause.edu/eduperson>).

Schema updates on certain directories can be troublesome and therefore, the decision to implement the `eduPerson` class should not be taken lightly. If you have sufficient experience of adding new schema extensions into your directory, then this is the recommend way to provide the required attributes.

If you are unfamiliar with adding new schemas or do not wish to disrupt your existing directory schema, you can use the name mapping solution as this is a lot easier to implement, though it is not as elegant as using the custom schema. Name mapping allows you to map the value of an existing attribute to anything

you wish, for example, we can expose *eduPersonPrincipalName* from Shibboleth by using the value from *cn*. As all name mapping is done in Shibboleth, the only requirement necessary is to choose a suitable existing attribute for each of the attributes you will need.

The core attributes required are stated above. However, as *eduPersonPrincipalName* is already in place as it is essentially the *cn* of the user and *eduPersonTargetedID* is created within Shibboleth dynamically, no further intervention is necessary. Therefore, the only two core attributes we need to map are values representing *eduPersonScopedAffiliation* and *eduPersonEntitlement*. Both these attributes can have multiple values, so our only requirements for choosing an existing attribute to use are that it is multi-valued and not already in use. Below is a list of attributes that are multi-valued in Active Directory.

- otherFacsimileTelephoneNumber
- otherHomePhone
- otherIpPhone
- otherLoginWorkstations
- otherMailbox
- otherMobile
- otherPager
- otherTelephone
- postalAddress
- postOfficeBox
- url

Table 1 shows an example of attribute mapping in Shibboleth with Active Directory. Note how Shibboleth scopes the values and generates *eduPersonPrincipalName* and *eduPersonTargetedID* from the existing *cn* attribute value.

Table 1

| Local attribute name | Sample attribute value | | Mapped attribute name | Value (with scope if appropriate) |
|----------------------|---|---------------------------|----------------------------|---|
| url | member, student | Passed through Shibboleth | eduPersonScopedAffiliation | student@mydomain.ac.uk |
| otherHomePhone | kid#basic1 http://www.mydomain.ac.uk/staff/view_students | | eduPersonEntitlement | kid#basic1 http://www.mydomain.ac.uk/staff/view_students |
| Cn | Jsmith | | eduPersonPrincipalName | jsmith@mydomain.ac.uk |
| cn* | | | eduPersonTargetedID | s3VjcGuNrzKaeu69/QRfh73hNjU=@mydomain.ac.uk |

* The chosen attribute for *eduPersonTargetedID* must be unique and not reassigned to a user for 24 months after the account has been removed (as stipulated in the UK Federation policies). A better attribute may exist, for example, one which contains the user's unique id code, such as one stored in your

institution's management information system (MIS) or the user's GUID from the directory. Once you have chosen the attributes that will store these two values, you should view the following web page and check which other attributes are required or optional for your subscribed resources.

<http://www.ukfederation.org.uk/content/Documents/AttributeUsage>

3.4 How do I set these attributes?

If you have existing processes in place to create users, these will need to be updated to include the new attribute values, for example, add "member" and "student" to the URL attribute on all new student accounts, and "member" and "staff" for staff accounts.

Existing accounts will also need to be updated with the new attribute values. Where existing user update processes are in place, these also need to be updated. Many institutions do not have processes to update users once they are on the system. However, several options are available to implement these changes, ranging from full Identity Management solutions to custom scripts or free programs. Active Directory users may find the free tool ADModify very useful, which can be found here:

<http://www.codeplex.com/admodify>

It is very important that user attributes are regularly updated to ensure they are accurate, for example, once a night. Failure to keep values up-to-date could result in users being unable to get access to valid resources, or worse still, allow users access to resources they are not entitled to use.

4 Authentication Development

Choosing the method for authenticating users is also an important decision to make. Shibboleth does not provide any authentication mechanisms itself, it simply hooks into pre-existing methods, for example, you may choose to login against your Active Directory or e-Directory using LDAP queries. This is an easy method from an implementation point of view as the system is already in place. However, this lacks the Single Sign-On benefits of implementations such as PubCookie, CAS, iChain or ISA across non-Shibbolised web applications. The disadvantage of these methods is the extra development time involved in setting up the SSO software and the fact you will only see the benefit if your existing applications are integrated with the SSO software.

Internally, the number of logons a user makes can be reduced across web applications by using Kerberos or IIS integrated authentication and a browser with SPNEGO support. These mechanisms provide seamless logins once you have authenticated against the Kerberos server. This method gives the user the experience of Single Sign-On, even though in reality two separate logins are taking place, as can be seen when the user accesses the same two resources externally. This time they would have to authenticate against each separately because the credentials are not embedded in the user's session like they are when on campus; some people call this Simplified Sign-On.

The only true way of getting Single Sign-On is to combine a SSO system which supports SPNEGO (such as CAS) with all of your existing web applications converted to use the SSO client. This clearly requires a lot of planning and implementation time

5 Firewall Access

Firewall rules will need to be put in place to allow connections to be made to the authentication mechanisms and attribute stores. In most common configurations this will mean opening TCP/UDP ports 389 or 636 from the Shibboleth server to the relevant LDAP servers, access to port 443 (https) from all external hosts to the Shibboleth server, and port 22 for SSH (or 3389 RDP for Microsoft servers) from Kidderminster College on IP 194.83.68.131/136 will also be necessary for remote installation and support calls.

6 Acquiring a Certificate

Shibboleth requires SSL certificates to be installed to help maintain security. JANET organisations can now obtain GlobalSign certificates for free. You will have to sign up and follow the instructions at:

<http://www.ja.net/services/server-certificate-applications/server-certificate-service-process.html> for this service. Alternatively, any commercial vendor can be used.

If you intend to join the SCS, we recommend you do this straight away as it can take several days for the application process to be completed. Although we cannot get these certificates signed on your behalf, we are able to create the signing request for you.

In order to join the UK Federation, you will need to obtain one of the X.509 digital certificate products recognised by the Federation. At present these are:

- GlobalSign OrganizationSSL certificates
- JANET Server Certificate Service (JANET SCS) certificates
- TERENA Server Certificate Service (TERENA SCS) certificates
- Thawte SSL web server certificates
- UK e-Science CA host certificates
- VeriSign Secure Site certificates

Choosing the CA

The following issues should be considered when deciding which certificate product to use:

- Wildcard certificates, from any source, are not recommended for use within the UK Federation.
- JANET-connected organisations will normally choose to use free JANET SCS certificates rather than purchase from a commercial supplier, unless the same certificate is to be used to secure financial transactions.
- If an e-Science certificate is seen by a user's browser, a dialogue stating that the certificate is not trusted will appear unless that user has manually installed into their browser the corresponding CA root certificate and any intermediate CA certificates. The other certificate types avoid this user education issue because they are already trusted by common desktop browsers.
- There is a modest cash charge for commercial certificates.

Using other CAs

It is possible to use SSL server certificates from a CA other than one of those listed above (for example, a campus CA already trusted by end-user browsers). Certificates from a CA recognised by the UK Federation are only required for the following machine-to-machine Shibboleth purposes:

- SSO service assertion signing certificate and attribute authority SSL server certificate (for an Identity Provider)
- Attribute requester client certificate (for a Service Provider)

These certificates can be differentiated from your other SSL server certificates, which are seen by end-users, at the price of some additional configuration complexity. However, to keep things simple, the rest of the documentation here assumes that a single certificate from a recognised CA is used for all purposes.

7 Join UK Access Management Federation

This is a brief overview of the process for joining the UK Access Management Federation. For full details, visit this web page:

<http://www.ukfederation.org.uk/content/Documents/JoinFederation>

You may also wish to participate in the JISC-SHIBBOLETH and JISC-SHIBBOLETH-LIBRARIES mailing lists located at: www.jiscmail.ac.uk

7.1 Management Staff

Management staff should read these documents and follow the points listed:

1. "Rules of Membership" and agree to them
<http://www.ukfederation.org.uk/library/uploads/Documents/rules-of-membership.pdf>
2. "Recommendations for use of personal data"
<http://www.ukfederation.org.uk/library/uploads/Documents/recommendations-for-use-of-personal-data.pdf>
3. "Federation operator procedures"
<http://www.ukfederation.org.uk/library/uploads/Documents/federation-operator-procedures.pdf>
4. Send a letter of application to join the UK Federation (see Appendix A).

7.2 Technical Staff

Technical staff are required to have read and understood the following documents:

- <http://www.ukfederation.org.uk/library/uploads/Documents/technical-recommendations-for-participants.pdf>
- <http://www.ukfederation.org.uk/library/uploads/Documents/federation-technical-specifications.pdf>

8 Updating Links

Links to most resources can remain the same, however, users will be asked where they are from using a WAYF (Where Are You From) discovery service. The user is required to choose the institution they are from using a drop-down list which is growing all the time and may eventually cause some usability issues. Whilst mechanisms such as cookies can be set to reduce the number of times this selection is made, this may still cause confusion with some end users.

Screenshot of the UK Federation WAYF.

There are ways to bypass the WAYF when accessing Shibboleth protected resources. This is accomplished by using specially constructed URLs. In some cases, WAYF bypassing can be achieved by the Service Provider, more commonly however it is done by sending the user directly to your Shibboleth IdP server and embedding the required resource details in the URL.

URLs to resources can be constructed in the following format:

- **<SSO endpoint of your Shibboleth IdP server>**
- **?target=<URL of resource you want to access>**
- **&shire=<Assertion Consumer Service of SP>**
- **&providerId=<Provider ID of SP>**

<SSO endpoint of your Shibboleth IdP server>: This is the SSO endpoint your IdP uses to authenticate users, which can be found in idp.xml and the metadata file, e.g. , <https://idp.yourdomain.ac.uk/shibboleth-idp/SSO>

<URL of resource you want to access>: This may either be a deep link into the site or just the home page of the resource. This can also be set to "cookie" by the SP. This method embeds the redirect URL in a cookie in the users browser, e.g., <http://www.resource.com/application/topsecret>

<Assertion Consumer Service of SP>: The ACS of the Service Provider. This can be found in the metadata file, e.g., <http://www.resource.com/Shibboleth.sso/SAML/POST>

<Provider ID of SP>: The Provider ID of the Shibboleth Service Provider. This can be found in the metadata file, e.g., <http://www.resource.com/shibboleth>

The link below shows an example following this convention. Note that this example has the links URL encoded.

```
https://idp.yourdomain.ac.uk/shibboleth/SSO?target=https://weather.atomwide.com/&shire=https%3A%2F%2Fweather.atomwide.com%2FShibboleth.sso%2FSAML%2FPOST&providerId=https%3A%2F%2Fweather.atomwide.com%2Fshibboleth
```

An easy way to create these links is to access the resource. Go through the normal WAYF selection, then once you are redirected to your IdP, stop the browser processing and copy the URL in the address bar. It is recommended you strip out the "&time=" variable as this is the current time stamp and will not be relevant when used in the future.

This method is dependent on the Service Provider and in some cases it will not work due to the way the application has been written. In situations where WAYF bypassing cannot be done using this method, it is recommended that you contact the Service Provider to see if other possible solutions exist.

9 Appendix A

Example letter of application to join the UK Federation

A request to join the UK Federation must be signed by a senior officer of the organisation, the Executive Liaison, who is authorised to bind the organisation to the UK Federation's Rules of Membership. For schools, the Executive Liaison is a senior officer of the responsible Local Authority or Regional Broadband Consortium.

An example letter of application is provided, but please read all of the pages you are currently looking at before sending in your letter of application.

The application must be in writing, on the organisation's letterhead, and sent to the federation operator:

UK Federation Operator
JANET (UK)
Lumen House
Library Avenue
Harwell Science and Innovation Campus
Didcot
Oxfordshire OX11 0SG

The application must contain the following information:

- The name and job title of the Executive Liaison, who is the signatory of the letter.
- The full name and postal address of the organisation.
- A statement that the organisation agrees to be bound by the federation's Rules of Membership, as published on the federation website:
(<http://ukfederation.org.uk/content/Documents/FedDocs>).
- The name and contact details of one or more Management Liaisons authorised to make registration requests. In most cases, each Management Liaison will be an officer of the organisation itself, responsible to the Executive Liaison. This also applies where the organisation employs an outsourced provider.

If subsequent to joining the federation, an organisation requires further Management Liaisons to be authorised, a further letter giving names and contact details, signed by the Executive Liaison, should be sent to the above address.

Executive Liaison

An application from an organisation to join the UK Federation must be signed by a senior officer of the organisation, known as the Executive Liaison, who would normally sign important contracts for the organisation. (For example, in a university or college of further education, the Executive Liaison might be Director of Information Services, or Principal or Vice-Principal of the organisation.)

The Executive Liaison is authorised to legally bind the organisation to the federation's Rules of Membership, which are described in the federation website:

(<http://ukfederation.org.uk/content/Documents/FedDocs>).

For schools, the Executive Liaison is a senior officer of the responsible Local Authority or Regional Broadband Consortium.

Management Liaison

A Management Liaison is a person authorised by an organisation to make requests to the federation operator to register identity providers or service providers on its behalf. A Management Liaison would also register an organisation's use of an outsourced provider.

Each member organisation must have at least one Management Liaison, nominated by the Executive Liaison when applying to join the federation. Larger organisations might find it administratively convenient to have more than one Management Liaison, who may be nominated by the Executive Liaison in the letter of application, or subsequently.

If an organisation has more than one Management Liaison, the Executive Liaison may choose to allocate responsibilities between them, for example in a manner reflecting the organisation's internal structure. However the federation operator does not record and is not aware of such allocations.

In most cases, a Management Liaison will be an officer of the organisation itself, perhaps a senior manager responsible for technical development. Each Management Liaison will be responsible to the Executive Liaison.

Sample letter of application to join the UK federation

The following text is for guidance only. If you plan to **outsource** the operation of your federation systems, then both you and the organisation to whom you outsource the work must apply for membership.

Note the requirement to write your actual letter of application on your organisation's letterhead.

At least one Management Liaison must be authorised. Larger organisations might wish to authorise more than one Management Liaison; this can be specified in the initial letter of application, or subsequently.

<name of Organisation>
<postal address of Organisation>

<date>

UK Federation Operator,
JANET (UK),
Lumen House,
Library Avenue,
Harwell Science and Innovation Campus,
Didcot,
Oxfordshire OX11 0SG

Dear Sir/Madam,

On behalf of <name of Organisation> I write to apply for membership of the UK Access Management Federation for Education and Research. I confirm that <name of Organisation> agrees to be bound by the UK federation's Rules of Membership in effect at the date of this letter, as published on their website.

The following person has [persons have] been designated by <name of Organisation> as Management Liaison with the UK federation, and as such is [are] authorised to make requests to register Identity Providers and/or Service Providers [delete where appropriate] with the UK federation on behalf of <name of Organisation>:

<name of Management Liaison>
<job title of Management Liaison>
<contact details for Management Liaison:
- postal address
- telephone number
- email address >

[Further Management Liaisons may be authorised in the letter, with details specified for each as above.]

Yours faithfully,

<signature of Executive Liaison>

<name of Executive Liaison>
<job title of Executive Liaison>
<name of Organisation>

10 Appendix B

Shibboleth Server/Authentication/Attribute Information

Please complete and return the following information to: feiams@kidderminster.ac.uk

| Item | Value |
|--|-------|
| Institution Name | |
| Shibboleth server placement (e.g., DMZ, Internal network) | |
| Shibboleth server DNS name (e.g., Active Directory, e-Directory) | |
| LDAP Server names/ips | |
| Type (e.g. Active Directory, edirectory) | |
| SSL required? (if SSL, ensure CA is available on arrival e.g., yes/no) | |
| BaseDN (e.g., "DC=mydomain,DC=local") | |
| OU to search (e.g., "OU=College_Users,DC=mydomain,DC=local" where staff/students, leave blank to search from root) | |
| DN of user to perform search (e.g., "CN=ldapauth,CN=Users,OU=College_Users,DC=mydomain,DC=local", ignore if anonymous) | |
| Attribute for eduPersonScopedAffiliation (chosen multi-valued attribute) | |
| Attribute for eduPersonEntitlement (chosen multi-valued attribute) | |
| Attribute for eduPersonPrincipalName (Generally, username attribute, e.g., <i>cn</i>) | |
| Attribute for unique user id not to be re-used within 24 months of account termination (Maybe the username unless re-used, otherwise use unique value, e.g., student/staff MIS ID or directory GUID) | |

11 Appendix C

AGENDA

- Arrange Strategy Meeting with SMT/LRC/IT Services
- Assess Server Requirements
- Organise Directory Development
- Verify Attribute Requirements
 - check UK Federation website
 - update schemas
 - update attributes regularly
- Review Authentication Development
- Set Up Firewall Access
- Obtain a Certificate
- Join the UK Access Management Federation
- Establish an IdP Implementation Timeline.

12 Appendix D

Sample Site Visit Document

Site Visit: Ashton 6th Form College

Date: Thursday 31st January 2008

Present:

Ashton 6th Form College

Sandra Taylor (e-Learning Manager)
David Bridge (Network Manager)
Lee Morris (Asst. Network Engineer)
Derrick Lack (Assistant Principal (OS))
Anton McGrath Assistant Principal (Curr.)

Kidderminster College

Karin Maslen (Project Manager)
Graham Mason (Head of ICT)
Rhys Smith (Consultant Engineer)
Edward Beddows (Senior Engineer)

Objective(s):

- To provide advice and guidance on completing stages 1 & 2 of the JISC roadmap
- To build a picture of current subscribed resources that are Shibboleth enabled
- To agree a time frame for the implementation of stages 3 & 4 of the JISC roadmap.

Background:

Ashton 6th Form College, commissioned Kidderminster College to install Shibboleth on their exiting VLE (Moodle) in October 2007 and have since then a continued support service relationship (Service Level Agreement). Inline with their intention to join the UK Access Management Federation (UKAMF) and adopt Shibboleth technology for institutional access, the college was encouraged by the RSC Northwest to apply for support via the JISC Institutional Access Management Support Project (JIAMSP). As the assigned third party service provider, Kidderminster College via its JISC affiliated Further Education Institutional Access Management Support (FEIAMS) project has been tasked with carrying out the Shibboleth Identity Provider (IdP) deployment at Ashton.

Current Technology:

The college uses Active Directory for Directory Management, with student and staff profiles that allow access via permissions set by the Network Manager.

Current Resources:

Of the 9 resources currently subscribed to, seven are through JISC Collections. Classic Athens is used to access these resources with only two: *Film and Sound Online* and *Education Image Gallery* not being native Shibboleth enabled.

Points Discussed:

1. Open Athens: following July 2008, the college would need to subscribe to Open Athens in order to continue accessing the seven non-shibbolised resources via the gateways, until a point in time where the Service Providers (SP) have migrated to the UK Access

Management Federation. This will entail the college paying the annual subscription fee as outlined in EduserV's current price list for at least one year.

2. *Pre-requisites*: the following requirements need to be carried out before Shibboleth (IdP) implementation can be completed:
 - Letter of application to join the UK Access Management Federation.
 - Nomination of Senior and Technical Management Executives as liaison officers.
 - Server registration with UKAMF
 - Populate Active Directory with attributes to connect to the Service Provider. Values needed are Eduperson scoped affiliation (4 core attributes listed on UKAMF website). Differentiate between staff and students with separate fields i.e., <member> <student>, <member> <staff>. Advisable to give staff unique ID and use one multi-valued attribute to populate Athens.
 - Update links on Internet to indicate WYAF.
3. *Training*: the Kidderminster service team would provide basic technical Shibboleth training for strategic staff members to enable them to manage the installed software self-sufficiently. Support documentation and guidance worksheets will also be available from the project website: feiams.Kidderminster.ac.uk
4. *August 2008*: following the end of the project period, further technical support will be provided by JANET as well as technical training, which will also be available through NetSkills.

Action Points:

| Action | Institution | Person | Deadline |
|--|---------------|---------------|---------------------------------|
| Provide details of joining UKAMF & guidance in completing paperwork. | Kidderminster | Ed Beddows | Wk starting 4 th Feb |
| Provide technical advice connecting MIS (Unit-E) with LDAP and AD | | | Wk ending 8 th Feb |
| Complete, update and populate AD attribute store | Ashton | David Bridge | Wk ending 8 th Feb |
| Apply to join the UKAMF | Ashton | Sandra Taylor | ASAP |
| Remote deployment of Shibboleth software | Kidderminster | Ed Beddows | Wk ending 15 th Feb. |

Conclusion:

All parties agreed that the proposed deadline for completing the installation requirements for steps 3 & 4 should be mid February, preferably no later than week ending 15th Feb. 2008. Following implementation, Ashton College has agreed to provide a brief feedback report to the JISC and to discuss suitable copy for a case study/newsletter article with the FEIAMS Project Manager.